แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์

พ.ต.ต.กิจชัยยะ สุรารักษ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต
สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2562

PREVENTIVE APPROACH AGAINST CRIME USING CRYPTOCURRENCY IN THAILAND: A CASE STUDY OF BITCOIN

Pol.Maj. Kijchaiya Surarak

A Dissertation Submitted in Partial Fulfillment of the Requirements
for the Degree of Doctor of Philosophy in Criminology and Criminal Justice
Department of Sociology and Anthropology
FACULTY OF POLITICAL SCIENCE
Chulalongkorn University
Academic Year 2019

หัวข้อวิทยานิพนธ์	แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์
โดย	พ.ต.ต.กิจชัยยะ สุรารักษ์
สาขาวิชา	อาชญาวิทยาและงานยุติธรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.จุฑารัตน์ เอื้ออำนวย

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต

..... คณบดีคณะรัฐศาสตร์
(รองศาสตราจารย์ ดร.เอก ตั้งทรัพย์วัฒนา)

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(พ.ต.ต.ดร.ชวนัสถ์ เจนการ)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.จุฑารัตน์ เอื้ออำนวย)

..... กรรมการ
(รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง)

..... กรรมการ
(อาจารย์ ดร.ปิติ เอี่ยมจำรูญลาภ)

..... กรรมการภายนอกมหาวิทยาลัย
(พ.ต.อ.ดร.สัญญา เนียมประดิษฐ์)

กิจชัยยะ สุรารักษ์ : แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์. (PREVENTIVE APPROACH AGAINST CRIME USING CRYPTOCURRENCY IN THAILAND: A CASE STUDY OF BITCOIN) อ.ที่ปรึกษาหลัก : รศ. ดร.จุฑารัตน์ เอื้ออำนวย

การศึกษาวิจัยครั้งนี้มีวัตถุประสงค์เพื่อศึกษาลักษณะ รูปแบบ สภาพปัญหาและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ ตลอดจนศึกษาแนวนโยบาย กฎหมายและมาตรการต่างๆที่เกี่ยวข้องกับสกุลเงินเข้ารหัสทั้งในประเทศไทยและต่างประเทศ เพื่อเสนอแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทยได้อย่างเหมาะสม การศึกษาวิจัยครั้งนี้เป็นการวิจัยเชิงคุณภาพด้วยการศึกษาจากเอกสารและการวิจัยภาคสนามโดยการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญ

ผลการศึกษาพบว่าปัจจุบันมีการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรงด้วยการนำไปใช้เป็นสื่อกลางในการกระทำความผิดในรูปแบบต่างๆ ได้แก่ การซื้อขายแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย การฟอกเงินและการสนับสนุนเงินทุนให้กลุ่มผู้ก่อการร้าย และการนำไปใช้เป็นเครื่องมือในทางอ้อมด้วยการนำเอาชื่อของบิทคอยน์ไปหลอกลวงฉ้อโกงในลักษณะคล้ายกันกับแชร์ลูกโซ่ โดยมีสภาพปัญหาและสาเหตุจากลักษณะพิเศษต่างๆของบิทคอยน์ที่เอื้อต่อการนำไปใช้ในการก่ออาชญากรรม โดยเฉพาะคุณสมบัติที่ไม่มีการเปิดเผยตัวตนผู้ใช้งาน สภาพปัญหาและสาเหตุจากกฎหมาย ได้แก่ สถานภาพทางกฎหมายที่ไม่ชัดเจนของบิทคอยน์ กฎหมายที่เกี่ยวข้องยังไม่สามารถใช้ป้องกันการนำบิทคอยน์ไปใช้ในการกระทำผิดได้ ปัญหาในด้านการตีความกฎหมายที่ขัดแย้งกันเกี่ยวกับการเก็บพยานหลักฐานทางอิเล็กทรอนิกส์ และการขาดกฎหมายที่บัญญัติหลักเกณฑ์และวิธีการในการยึดและอายัดบิทคอยน์ รวมทั้งสภาพปัญหาและสาเหตุจากการบังคับใช้กฎหมายที่เจ้าหน้าที่ที่เกี่ยวข้องยังขาดองค์ความรู้ วิธีการ และเครื่องมือหรือกลไกต่างๆ ทั้งยังขาดการบูรณาการร่วมกันทั้งจากหน่วยงานของรัฐ ภาคเอกชนและความร่วมมือระหว่างประเทศ และจากการศึกษาแนวนโยบาย กฎหมายและมาตรการต่างๆที่เกี่ยวข้องพบว่าแต่ละประเทศมีทิศทางการกำหนดนโยบายที่แตกต่างกันทั้งรูปแบบของการยอมรับ กึ่งยอมรับกึ่งควบคุม และปฏิเสธบิทคอยน์และสกุลเงินเข้ารหัสต่างๆขึ้นอยู่กับแนวคิดทางการเมือง สภาพเศรษฐกิจและวัฒนธรรมของประเทศนั้นๆ

ทั้งนี้ ประเทศไทยควรมีการกำหนดมาตรการในการยืนยันตัวตนผู้ใช้งาน กำหนดหลักปฏิบัติในการเก็บรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์ที่ชัดเจน บัญญัติหลักกฎหมายเกี่ยวกับการยึดและอายัดสกุลเงินเข้ารหัส ส่งเสริมให้มีการศึกษาวิจัยและพัฒนาองค์ความรู้ เครื่องมือ และกลไกต่างๆ การสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชนและหน่วยงานระหว่างประเทศ รวมทั้งการผลักดันให้มีการพัฒนาสกุลเงินดิจิทัลแห่งชาติ และการสร้างความรับรู้ให้แก่ประชาชนในประเด็นที่เกี่ยวข้องกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

สาขาวิชา อาชญาวิทยาและงานยุติธรรม ลายมือชื่อนิสิต .....

ปีการศึกษา 2562 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6081352924 : MAJOR CRIMINOLOGY AND CRIMINAL JUSTICE
KEYWORD: Bitcoin, Cryptocurrency, Crime Prevention, Cybercrime

Kijchaiya Surarak : PREVENTIVE APPROACH AGAINST CRIME USING CRYPTOCURRENCY IN THAILAND: A CASE STUDY OF BITCOIN . Advisor: Assoc. Prof. JUTHARAT UA-AMNOEY, Ph.D.

The objectives of this research project are to study on the nature, pattern, issues and causes of crimes whereby bitcoin, a cryptocurrency, is used as the tool, and to study on cryptocurrency-related policies, laws and measures in Thailand and some other countries in order to suggest the proper direction for preventing cryptocurrency-related crimes in Thailand. This study is a qualitative research work that relies on the schemes of documentary research and field research to collect information from key informants, with a structured interview script used as the data collection tool.

The findings from the research reveal that currently, bitcoin is used as a direct tool for committing crimes, as the medium for offensive activities, such as for exchanging with illegal merchandises and services, money laundering and terrorist financing; and as an indirect tool such as to be mentioned in fraudulent activities like Ponzi scheme. The major cause is the special features of bitcoin that facilitate the use in crime-related activities. The related issues include construction and absence of legal coverage, as well as law enforcers' lack of proficiency in preventing such crimes. From the study on related policies, laws and measures, it is discovered that each country has the direction for setting related policies that is different from that of one another, depending on political concept, economic condition and culture of each country. Therefore, as for Thailand, there should be a proper measure that enforces the identification of each user. In addition, laws should be amended in order to have better clarity and coverage. Furthermore, law enforcers should be improved to have more proper bodies of knowledge, tools and mechanisms.

Field of Study: Criminology and Criminal Justice Student's Signature .....
Academic Year: 2019 Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์เล่มนี้สำเร็จลุล่วงได้เป็นอย่างดี ด้วยความเมตตากรุณาอย่างสูงยิ่งจากท่าน รองศาสตราจารย์ ดร.จุฑารัตน์ เอื้ออำนวย อาจารย์ที่ปรึกษาหลักวิทยานิพนธ์ ที่ได้กรุณาถ่ายทอดองค์ความรู้ ชี้แนะแนวทางในการศึกษาค้นคว้า ตลอดจนให้ข้อเสนอแนะอันเป็นประโยชน์ต่อการศึกษาวิจัยอย่างเต็มที่ ด้วยความเสียสละและมุ่งมั่นด้วยแรงกล้าที่จะทำให้ผู้วิจัยได้รับประโยชน์สูงสุดจากการศึกษาวิจัยครั้งนี้ ทั้งยังใส่ใจ ให้กำลังใจ และติดตามความก้าวหน้า เพื่อให้วิทยานิพนธ์เล่มนี้สมบูรณ์สูงสุด ผู้วิจัยสำนึกในบุณคุณและขอกราบขอบพระคุณท่านอาจารย์เป็นอย่างสูงมา ณ โอกาสนี้

ขอกราบขอบพระคุณอาจารย์ พันตำรวจตรี ดร.ชวนัสถ์ เจนการ ประธานกรรมการสอบวิทยานิพนธ์ รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง กรรมการ อาจารย์ ดร.ปิติ เอี่ยมจำรูญลาภ กรรมการ และ พันตำรวจเอก ดร.สัญญา เนียมประดิษฐ์ กรรมการภายนอกมหาวิทยาลัย ที่กรุณาให้คำแนะนำจนทำให้วิทยานิพนธ์เล่มนี้ถูกต้องและเป็นไปตามหลักวิชาการอย่างสมบูรณ์มากยิ่งขึ้น

ขอกราบขอบพระคุณผู้ให้ข้อมูลสำคัญทุกท่าน ที่ได้ให้ความอนุเคราะห์เข้าร่วมการวิจัยในครั้งนี้ โดยเฉพาะอย่างยิ่งผู้วิจัยขอกราบขอบพระคุณ พลตำรวจโทเพิ่มพูน ชิดชอบ ผู้ช่วยผู้บัญชาการตำรวจแห่งชาติ และ พลตำรวจโท ดร.อดุลย์ ณรงค์ศักดิ์ อดีตผู้ทรงคุณวุฒิพิเศษ สำนักงานตำรวจแห่งชาติ ที่เป็นผู้บังคับบัญชาที่กรุณาให้โอกาสและสนับสนุนให้ผู้วิจัยเข้าศึกษา เป็นผู้ให้ข้อมูลสำคัญอันเป็นประโยชน์ต่อการศึกษา และเป็นดั่งญาติผู้ใหญ่ที่คอยแนะนำ สั่งสอนและส่งเสริมจนผู้วิจัยสำเร็จลุล่วง

ขอกราบขอบพระคุณคณาจารย์ทุกท่าน ที่กรุณาถ่ายทอดองค์ความรู้ต่างๆจนผู้วิจัยสามารถสำเร็จการศึกษาครั้งนี้ไปด้วยดี รวมทั้งขอขอบคุณเพื่อนนิสิตทุกท่าน ที่ได้ร่วมเรียน ร่วมศึกษา ด้วยความรักและมิตรภาพอันดีต่อกันเสมอมา

ท้ายนี้ผู้วิจัยขอมอบความสำเร็จครั้งนี้แด่ นายสนิท - นางสงวนศรี สุรารักษ์ และ นางนันทรัตน์ โรจน์ทอง บิดา มารดาและพี่สาวผู้เป็นที่รัก ที่คอยสนับสนุนส่งเสริม ให้ความรักและให้กำลังใจตลอดชีวิตของผู้วิจัยตั้งแต่ให้กำเนิดจนถึงปัจจุบัน และนางสาวกนกพร รักท้วม ภรรยาผู้เป็นที่รักที่ให้การสนับสนุนการศึกษาครั้งนี้ในทุกขั้นตอน ตลอดจนทุ่มเท แรงกาย แรงใจ เสียสละ อดทน เพื่อส่งเสริมและผลักดันจนผู้วิจัยสำเร็จการศึกษาได้ด้วยความภาคภูมิใจสูงสุด

กิจชัยยะ สุรารักษ์

สารบัญ

หน้า

สารบัญตาราง

หน้า

สารบัญภาพ

หน้า

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

นับตั้งแต่การปฏิวัติอุตสาหกรรมเป็นต้นมา มนุษย์ได้พยายามพัฒนาเทคโนโลยีต่าง ๆ เพื่อให้เกิดการเปลี่ยนแปลงอย่างก้าวกระโดดในด้านการคิดค้นนวัตกรรมใหม่ ๆ มุ่งสู่ความสะดวกสบายสูงสุดในการดำรงชีวิตในด้านต่าง ๆ ไม่ว่าจะเป็นด้านการเดินทางและขนส่ง ด้านการสื่อสารโทรคมนาคม ด้านการประกอบธุรกิจหรือการติดต่อค้าขาย ด้านระบบการเงินการธนาคาร ไปจนถึงการซื้อขายแลกเปลี่ยนสินค้าและบริการต่าง ๆ ซึ่งต่างก็ได้ถูกเทคโนโลยีสมัยใหม่เข้ามาช่วยเหลือและแทนที่วิถีการดำรงชีวิตแบบเดิมไปอย่างสิ้นเชิง จนเรียกได้ว่าเทคโนโลยีสมัยใหม่ได้เข้ามาเป็นส่วนสำคัญของการดำรงชีวิตของมนุษย์ในทุกขั้นตอนอย่างสมบูรณ์

ในด้านระบบเงินตราและการซื้อขายแลกเปลี่ยนสินค้าและบริการนั้น จากในอดีตที่เมื่อมนุษย์ต้องการทรัพย์สินต่าง ๆ ที่ตนไม่ได้ครอบครองอยู่ ก็จะใช้วิธีการเจรจาแลกเปลี่ยนทรัพย์สินต่าง ๆ ซึ่งกันและกันโดยตรง จนเกิดปัญหาในความเหมาะสม ความยุติธรรมและความพึงพอใจระหว่างคู่กรณีทั้งสองฝ่ายขึ้น ทำให้มนุษย์ได้คิดค้นระบบเงินตราขึ้นเพื่อเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการให้มีความเป็นสากลมากยิ่งขึ้น โดยระบบเงินตรานี้ได้ถูกนำไปใช้อย่างแพร่หลาย ในรูปแบบที่แตกต่างกันออกไปตามแต่ละวัฒนธรรมของสังคมหรือชนเผ่านั้นๆ โดยระบบเงินตราดังกล่าวนี้ ได้มีวิวัฒนาการมาพร้อมกับความเจริญก้าวหน้าของมนุษย์เริ่มจากการกำหนดให้วัตถุใดวัตถุหนึ่งเป็นสิ่งมีค่าและสามารถใช้แลกเปลี่ยนสินค้าและบริการได้ เช่น กระดูกสัตว์ หินสวยงาม เบี้ยหอย สินแร่และโลหะมีค่าต่าง ๆ มาจนถึงยุคที่มนุษย์มีความรู้จนสามารถที่จะผลิตเหรียญประทับตราจากโลหะ ซึ่งมีความสวยงามและมีความเป็นสากลมากยิ่งขึ้น จนนำไปสู่ยุคที่มนุษย์สามารถที่จะผลิตเหรียญกษาปณ์และธนบัตรรูปแบบต่าง ๆ ซึ่งถือเป็นเงินตราที่ได้รับการยอมรับและถูกนำไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการในโลกสมัยใหม่นี้อย่างแพร่หลาย แต่ถึงอย่างนั้นมนุษย์ก็ยังมีความพยายามในการคิดค้นรูปแบบและวิธีการใหม่ ๆ ในการซื้อขายแลกเปลี่ยนสินค้าและบริการต่าง ๆ เพื่อให้เกิดความสะดวกสบายสูงสุดอยู่เสมอ โดยเฉพาะอย่างยิ่งเมื่อโลกได้ก้าวเข้าสู่ยุคโลกาภิวัฒน์ (Globalization) ที่การติดต่อสื่อสารกันสามารถทำได้อย่างรวดเร็ว เป็นยุคที่ข้อมูลข่าวสารต่าง ๆ สามารถส่งต่อถึงกันทั่วทุกมุมโลกภายในไม่กี่นาที รวมทั้งปัจจัยสำคัญที่ผลักให้โลกเข้าสู่ยุคแห่งการ

ดำเนินวิถีชีวิตใหม่ก็คือ อินเทอร์เน็ต (Internet) ระบบอินเทอร์เน็ตนี้ไม่เพียงเปลี่ยนรูปแบบการใช้ชีวิตและการติดต่อสื่อสารของมนุษย์เท่านั้น แต่ยังส่งผลให้เกิดการพัฒนาของรูปแบบการเงินการธนาคารรูปแบบใหม่ด้วย เช่น การทำธุรกรรมบนอินเทอร์เน็ต (Internet Banking) ซึ่งหมายถึงการที่ผู้ใช้บริการสามารถทำธุรกรรมทางการเงินต่าง ๆ ได้โดยไม่ต้องเดินทางไปที่ธนาคารอีกต่อไป เพียงเข้าระบบของธนาคารผ่านอินเทอรเน็ตก็สามารถทำธุรกรรมต่าง ๆ ได้ในทันทีจากทุกหนแห่งทั่วโลก

ด้วยความสามารถในการพัฒนาที่ไม่มีสิ้นสุดของมนุษย์ ทำให้มีการคิดค้นนวัตกรรมใหม่ ๆ อยู่เสมอจนมีการนำระบบอินเทอร์เน็ตและระบบเทคโนโลยีสารสนเทศสมัยใหม่มาประยุกต์ใช้และคิดค้นจนเกิดเป็นการประดิษฐ์สกุลเงินเข้ารหัส (Cryptocurrency) ขึ้นซึ่งถือเป็นนวัตกรรมใหม่ (Disruptive Innovation) ที่จะเปลี่ยนวิถีชีวิตของมนุษย์ไปอย่างสิ้นเชิง กล่าวคือระบบสกุลเงินเข้ารหัสนี้เป็นระบบการเงินทางเลือกที่จะทำให้มนุษย์มีความสะดวกสบายมากยิ่งขึ้น มนุษย์ไม่จำเป็นจะต้องใช้เงินสดไม่จำเป็นต้องเก็บรักษาหรือใช้บริการของธนาคารหรือสถาบันการเงินต่าง ๆ อีกต่อไป โดยเพียงแค่มีอุปกรณ์สื่อสารสมัยใหม่ อย่างโทรศัพท์สมาร์ทโฟนหรือเครื่องคอมพิวเตอร์พกพาที่สามารถเชื่อมต่อกับระบบอินเทอร์เน็ตได้ ก็สามารถใช้สกุลเงินเข้ารหัสนี้ซื้อขายแลกเปลี่ยนสินค้าและบริการได้ในทันทีทุกที่ทุกเวลา แม้ในปัจจุบันสกุลเงินเข้ารหัสนี้จะยังไม่สามารถมาแทนที่ระบบเงินตราดั้งเดิมได้อย่างสมบูรณ์ เนื่องจากมูลค่าของสกุลเงินเข้ารหัสไม่ได้ยึดโยงอยู่กับสินทรัพย์หรือสถาบันการเงินใดๆ อีกทั้งสังคมโลกส่วนใหญ่ยังไม่ยอมรับให้เป็นวัตถุที่ชำระหนี้กันได้ตามกฎหมายก็ตาม แต่จากผลการสำรวจสถานการณ์การใช้สกุลเงินเข้ารหัสทั่วโลกของสถาบันวิจัยด้านการเงินแห่งมหาวิทยาลัยเคมบริดจ์ (Centre for Alternative Finance, University of Cambridge) ก็ยังพบว่ามีผู้ใช้งานสกุลเงินเข้ารหัสเป็นจำนวนมากถึง 2.9 ล้าน ถึง 5.8 ล้านคนทั่วโลกและมีบัญชีกระเป๋าเงินดิจิทัล (Digital Wallet) ที่มีการเปิดใช้งานอยู่กว่า 5.8 ล้าน ถึง 11.5 ล้านบัญชีทั่วโลก (Garrick Hileman & Michel Rauchs, 2017) อีกทั้งยังมีจำนวนบัญชีกระเป๋าเงินดิจิทัลเพิ่มขึ้นเป็น 40 ล้านบัญชีทั่วโลกในเดือนมิถุนายน ค.ศ.2019 (Statista, 2019) ขณะที่ปัจจุบันมีสกุลเงินเข้ารหัสสกุลต่างๆเกิดขึ้นกว่า 2,300 สกุล โดยสกุลเงินเข้ารหัสที่มีผู้ใช้งานสูงสุดในขณะนี้คือ**“บิทคอยน์ (Bitcoin)”**

บิทคอยน์**เป็นสกุลเงินเข้ารหัสที่ถูกสร้างขึ้นและถูกนำมาใช้งานได้จริงเป็นสกุลแรกของโลก** อีกทั้งยังเป็นสกุลเงินเข้ารหัสสกุลแรกที่นำระบบการเก็บข้อมูลแบบบล็อคเชน (Blockchain) มาใช้ภายใต้แนวคิดในการกระจายข้อมูลที่ไม่มีการเก็บฐานข้อมูลการทำธุรกรรมของผู้ใช้บริการไว้ที่ส่วนกลาง (Server) เหมือนอย่างระบบการเงินการธนาคารดั้งเดิม แต่ใช้วิธีการกระจายข้อมูลบันทึก

ทางธุรกรรมต่างๆ ให้กลุ่มผู้ใช้งานในระบบ (Nodes) แต่ละคนทราบอย่างเปิดเผยด้วยระบบบัญชีสาธารณะ (Public Ledger) เพื่อให้ผู้ใช้งานในระบบร่วมกันทำการตรวจสอบความถูกต้องและบันทึกข้อมูลต่อเนื่องกันไปในลักษณะสายโซ่ของข้อมูลที่ไม่สามารถลักลอบเปลี่ยนแปลงแก้ไขได้ ทำให้ผู้ใช้งานสามารถนำบิทคอยน์ไปใช้ในการซื้อขายแลกเปลี่ยนสินค้าและบริการ และการทำธุรกรรมต่างๆ แทนการใช้เงินสกุลจริงได้ทั่วโลกภายในระยะเวลาอันสั้น โดยที่ผู้ใช้งานไม่จำเป็นต้องระบุตัวตนที่แท้จริงแต่อย่างใด ด้วยลักษณะต่างๆเหล่านี้ จึงทำให้มีผู้ใช้งานบิทคอยน์มากเป็นอันดับหนึ่ง ดังจะเห็นได้จากมูลค่าของสกุลเงินเข้ารหัสในตลาดการซื้อขาย (Cryptocurrencies Market Cap) ดังนี้

Cryptocurrencies ▾ Exchanges ▾ Watchlist

#	Name	Symbol	Market Cap	Price
1	Bitcoin	BTC	$160,043,535,111	$8,765.04
2	Ethereum	ETH	$25,374,280,906	$230.66
3	XRP	XRP	$10,231,208,421	$0.233493
4	Bitcoin Cash	BCH	$5,894,857,303	$321.79
5	Tether	USDT	$4,649,902,082	$1.00

ภาพที่ 1 มูลค่าการซื้อขายในตลาดของสกุลเงินเข้ารหัสสกุลต่างๆ

(Coinmarketcap, 2020)

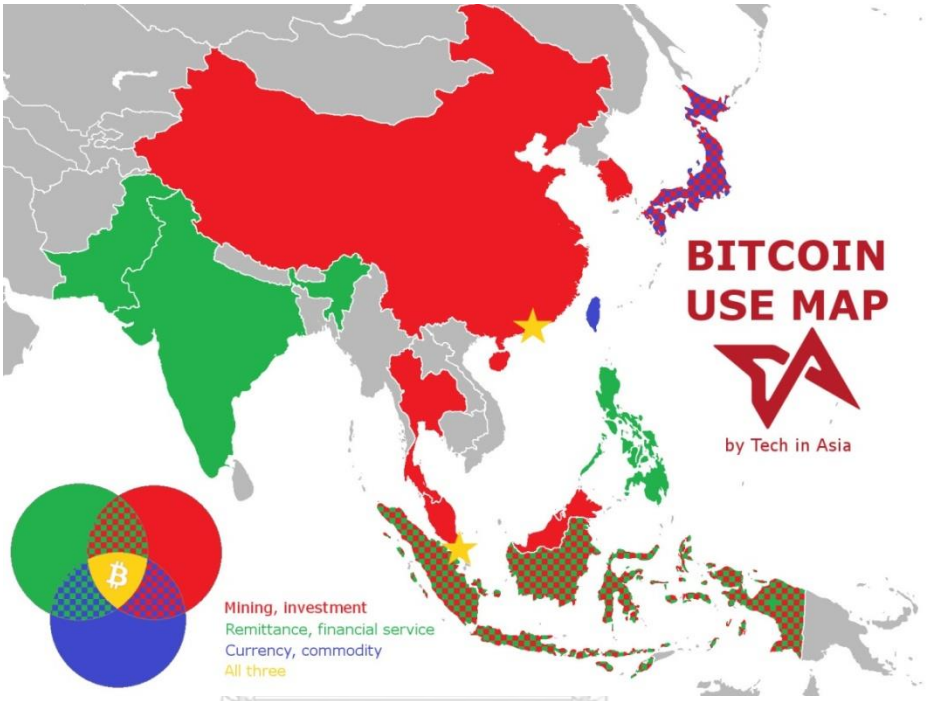
จากข้อมูล ณ เดือนมีนาคม 2563 ของเว็บไซต์คอยน์มาร์เก็ตแค็ป (Coinmarketcap) ซึ่งเป็นเว็บไซต์ที่รวบรวมข้อมูลเกี่ยวกับมูลค่าตลาดการซื้อขายสกุลเงินเข้ารหัสสกุลต่างๆ พบว่า **บิทคอยน์** มีมูลค่าในตลาดการซื้อขายสูงสุดเป็นอันดับหนึ่ง โดยมีมูลค่าอยู่ที่ประมาณ 160,000 ล้านเหรียญสหรัฐ รองลงมาคือ อีเธอเรียม (Ethereum) ที่มีมูลค่าอยู่ที่ประมาณ 25,000 ล้านเหรียญสหรัฐ และเอ็กซ์อาร์พี (XRP) ที่มีมูลค่าประมาณ 10,000 ล้านเหรียญสหรัฐ เป็นอันดับที่สองและสามตามลำดับ

ในขณะที่ผู้ใช้บริการทั่วไปได้รับความสะดวกสบายจากการใช้บิทคอยน์ดังกล่าว อาชญากรก็ได้เล็งเห็นประโยชน์จากคุณลักษณะของบิทคอยน์ที่ถูกออกแบบให้บุคคลทั่วไปหรือแม้กระทั่งเจ้าหน้าที่ของรัฐไม่สามารถระบุตัวตนของเจ้าของบัญชีได้ หรือถึงแม้กระทำได้ก็เป็นไปด้วยความ

ยากลำบากหรือจำเป็นต้องใช้องค์ความรู้และความชำนาญทางด้านระบบคอมพิวเตอร์ชั้นสูงและต้องใช้ทรัพยากรเป็นจำนวนมาก ทำให้อาชญากรเลือกใช้บิทคอยน์เป็นสื่อกลางในการกระทำความผิดในรูปแบบต่าง ๆ เช่น การลักลอบซื้อขายยาเสพติด การซื้อขายอาวุธสงครามหรืออาวุธปืนเถื่อน การซื้อขายสื่อลามกอนาจาร การจ้างวานฆ่าและการเรียกค่าไถ่โดยให้ชำระเป็นบิทคอยน์ การฟอกเงินและการสนับสนุนเงินทุนให้กลุ่มผู้ก่อการร้าย หรือ แม้กระทั่งการนำเอาประโยชน์จากการที่บิทคอยน์มีมูลค่าผันผวนสูง ไปชักชวนให้เหยื่อเข้าร่วมระดมเงินทุน โดยหลอกลวงเหยื่อให้เชื่อว่าจะมีการนำเงินไปลงทุนเก็งกำไรผ่านการซื้อขายบิทคอยน์และจะมีการปันผลตอบแทนให้กับเหยื่อ แต่แท้ที่จริงแล้วกลับเป็นการกระทำผิดในลักษณะคล้ายกันกับแชร์ลูกโซ่ เป็นต้น ซึ่งจากการที่อาชญากรนำบิทคอยน์มาใช้เป็นเครื่องมือในการกระทำความผิดในลักษณะต่าง ๆ ดังที่ได้กล่าวมานี้ ทำให้การป้องกันอาชญากรรมแบบใหม่นี้เป็นไปด้วยความยากลำบาก เช่น ไม่สามารถเฝ้าระวังและป้องกันได้อย่างสมบูรณ์เนื่องจาก แม้จะสามารถตรวจสอบข้อมูลทางธุรกรรมที่มีความผิดปกติได้ แต่ก็ไม่สามารถระบุตัวตนเจ้าของบัญชีที่ทำธุรกรรมดังกล่าวได้ จึงส่งผลต่อเนื่องทำให้การรวบรวมพยานหลักฐานที่เกี่ยวข้องกับการกระทำความผิดที่ใช้บิทคอยน์เป็นเครื่องมือเพื่อจะนำไปสู่การเอาผิดอาชญากรนั้นเป็นไปด้วยความยากลำบาก จนอาจทำให้ผู้กระทำผิดลอยนวลและสามารถก่ออาชญากรรมในลักษณะนี้ซ้ำแล้วซ้ำเล่าได้อย่างไม่มีความเกรงกลัวต่อกฎหมาย หรืออาจกล่าวได้ว่าในปัจจุบันรัฐยังขาดแนวทางและมาตรการต่างๆที่จะป้องกันอาชญากรรมสมัยใหม่นี้ได้อย่างมีประสิทธิภาพ ทำให้สังคมโลกเริ่มหันมาให้ความสนใจในประเด็นที่เกี่ยวกับการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสมากขึ้น

สำหรับสถานการณ์และแนวโน้มในการใช้บิทคอยน์และสกุลเงินเข้ารหัสในประเทศไทยนั้น เมื่อพิจารณาจากยุทธศาสตร์ชาติ 20 ปี พ.ศ.2561 - 2580 ในด้านการสร้างความสามารถในการแข่งขัน ซึ่งได้มีการกำหนดเป้าหมายในการกระตุ้นให้มีการนำเอาวัฒนธรรมและวิถีชีวิตดั้งเดิมมาประยุกต์ผสมผสานกับเทคโนโลยีและนวัตกรรมเพื่อให้สอดรับกับบริบทของเศรษฐกิจและสังคมสมัยใหม่ ประกอบกับการออกพระราชกำหนดการประกอบธุรกิจดิจิทัล พ.ศ.2561 เมื่อวันที่ 13 พฤษภาคม 2561 โดยมีเหตุผลในการประกาศใช้พระราชกำหนดฉบับนี้ คือ เพื่อเป็นการกำกับและควบคุมดูแลการประกอบธุรกิจที่เกี่ยวกับสกุลเงินเข้ารหัส และเพื่อรองรับการนำเทคโนโลยีมาทำให้เกิดการพัฒนาทางเศรษฐกิจและสังคมอย่างยั่งยืน อันจะเป็นการสนับสนุนให้เกิดการพัฒนาศักยภาพในการระดมทุน รวมทั้งเพื่อให้ประชาชนและผู้ที่เกี่ยวข้องมีข้อมูลที่ชัดเจนเพียงพอในการตัดสินใจและป้องกันมิให้มีการนำสินทรัพย์ดิจิทัลที่ไม่มีแหล่งที่มาที่ชัดเจนไปใช้ประโยชน์หรือกระทำการใดใน

ลักษณะที่เป็นการหลอกลวงประชาชนหรือเกี่ยวข้องกับอาชญากรรม เพื่อประโยชน์ในอันที่จะรักษาความมั่นคงในทางเศรษฐกิจของประเทศ นอกจากนี้ข้อมูลจากเว็บไซต์เทคอินเอเชียที่ได้ทำการสำรวจสถานภาพการใช้งานบิทคอยน์จากทุกภูมิภาคทั่วโลก ได้แสดงผลการใช้งานบิทคอยน์ของประเทศต่างๆในภูมิภาคเอเชียปรากฏตามภาพดังต่อไปนี้



ภาพที่ 2 การใช้บิทคอยน์ของประเทศต่าง ๆ ในภูมิภาคเอเชีย
(Paul Bischoff, 2015)

จากภาพดังกล่าวจะเห็นได้ว่าในส่วนของประเทศไทยนั้นมีการใช้บิทคอยน์ไปในลักษณะของการลงทุนเพื่อเก็งกำไรจากการซื้อ-ขายมูลค่าของบิทคอยน์ และการดำเนินการสร้างอุปกรณ์และโปรแกรมคอมพิวเตอร์เพื่อให้ได้มาซึ่งบิทคอยน์หรือที่กลุ่มผู้ใช้บิทคอยน์มักเรียกกันว่าการขุดบิทคอยน์เป็นจำนวนมาก จากกรณีดังกล่าวจึงมีความเป็นไปได้อย่างยิ่งว่าในอนาคตอันใกล้นี้บิทคอยน์และสกุลเงินเข้ารหัสสกุลต่าง ๆ น่าจะเข้ามามีบทบาทในระบบเศรษฐกิจ ระบบการเงินการธนาคารและการซื้อขายแลกเปลี่ยนของประเทศไทยและในขณะเดียวกันการแพร่หลายของบิทคอยน์และสกุลเงินเข้ารหัสก็อาจเป็นช่องทางให้อาชญากรหรือกลุ่มผู้กระทำความผิดนำบิทคอยน์หรือสกุลเงินเข้ารหัสสกุลอื่น ๆ ไปใช้เป็นเครื่องมือในการกระทำความผิดรูปแบบต่าง ๆ โดยอาศัยโอกาสจากการที่มาตรการต่าง ๆ ของรัฐที่เกี่ยวข้องกับสกุลเงินเข้ารหัส ยังไม่ครอบคลุมหรือยังไม่มีประสิทธิภาพเพียงพอที่จะป้องกัน

ปราบปรามอาชญากรรมสมัยใหม่นี้ได้ ดังนั้น ผู้วิจัยในฐานะที่เป็นผู้ที่ศึกษาทางด้านอาชญาวิทยาและกระบวนการยุติธรรม อีกทั้งยังเป็นเจ้าหน้าที่ของรัฐที่มีหน้าที่ในการป้องกันปราบปรามอาชญากรรม จึงตระหนักถึงความสำคัญของปัญหาอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสรูปแบบต่าง ๆ ที่จะเกิดขึ้น จึงเกิดความสนใจที่จะศึกษาว่า อาชญากรรมที่ใช้บิทคอยน์เป็นเครื่องมือนั้นคืออะไร เกิดขึ้นได้อย่างไร เกิดจากปัจจัยใดบ้าง มีลักษณะรูปแบบและวิธีการกระทำผิดอย่างไร และประเทศไทยควรมีแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอย่างไร เพื่อรัฐจะได้มีกลไกการป้องกันปราบปรามและเตรียมพร้อมรับมือกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสที่จะเกิดขึ้นได้อย่างทันท่วงที อันจะเป็นประโยชน์ต่อความมั่นคงและความสงบสุขของประเทศและสังคมต่อไป

1.2 คำถามการวิจัย

อาชญากรรมที่มีการใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ มีลักษณะและรูปแบบอย่างไร มีสภาพปัญหาอย่างไรและอาชญากรรมดังกล่าวเกิดจากสาเหตุใด ในประเทศไทยและต่างประเทศมีแนวนโยบาย กฎหมาย และมาตรการต่าง ๆ ที่เกี่ยวข้องกับสกุลเงินเข้ารหัสอย่างไร และประเทศไทยควรมีแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอย่างไร

1.3 วัตถุประสงค์ของการศึกษา

1. เพื่อศึกษาลักษณะ รูปแบบ สภาพปัญหาและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ

2. เพื่อศึกษาแนวนโยบาย กฎหมาย และมาตรการต่าง ๆ ที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและต่างประเทศ

3. เพื่อเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือในประเทศไทย

1.4 ขอบเขตการวิจัย

1.4.1 ขอบเขตด้านเนื้อหา

การศึกษาครั้งนี้ทำการศึกษาในเนื้อหาเกี่ยวกับ ลักษณะและรูปแบบของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส กล่าวคือการนำเอาสกุลเงินเข้ารหัสไปใช้เป็นสื่อกลางหรือเครื่องมือในการกระทำความผิด เพื่อให้เกิดความสะดวกสบายและเป็นการหลีกเลี่ยงการถูกตรวจสอบโดยเจ้าหน้าที่ของรัฐ **เฉพาะที่มีการนำไปใช้กระทำผิดโดยทางตรง** ได้แก่ การลักลอบซื้อขายยาเสพติด อาวุธเถื่อน

การว่าจ้างให้ผู้อื่นกระทำผิดกฎหมาย การซื้อขายสื่อลามกอนาจาร การเรียกค่าไถ่ การระดมเงินทุนของกลุ่มผู้ก่อการร้ายโดยมีการใช้บิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆในการเป็นสื่อกลางในการกระทำความผิด รวมทั้งการฟอกเงินผ่านบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ **ทั้งนี้ไม่รวมถึง**การกระทำความผิดที่เกี่ยวข้องกับการใช้สกุลเงินเข้ารหัสในทางอ้อม เช่น การนำเอาชื่อ “บิทคอยน์” ไปหลอกลวงชักชวนให้เหยื่อมาลงทุนเก็งกำไรจากการซื้อขายแลกเปลี่ยนบิทคอยน์ หรือ การหลอกลวงให้มาลงทุนในธุรกิจการขุดบิทคอยน์ และเมื่อเหยื่อหลงเชื่อผู้กระทำความผิดก็ยักยอกเงินแล้วหลบหนีไปในลักษณะเดียวกันกับแชร์ลูกโซ่ และการหลอกลวงฉ้อฉลในการซื้อขายแลกเปลี่ยนหรือในภาคการลงทุนหรือภาคธุรกิจ ซึ่งไม่ได้เป็นการใช้บิทคอยน์หรือสกุลเงินเข้ารหัสเป็นสาระในการก่ออาชญากรรม รวมทั้งยังศึกษาถึงสภาพปัญหาและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ แนวนโยบาย กฎหมาย และมาตรการต่าง ๆ ที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ และแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือในประเทศไทย

1.4.2 ขอบเขตด้านประชากร

ผู้วิจัยศึกษาแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: ศึกษากรณีบิทคอยน์ ด้วยการศึกษาวิจัยเอกสารประกอบกับการวิจัยภาคสนามด้วยการเก็บข้อมูลด้วยวิธีการสัมภาษณ์ผู้ให้ข้อมูลสำคัญที่เกี่ยวข้อง โดยแบ่งเป็น 4 กลุ่ม ได้แก่ กลุ่มที่ 1 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในเรื่องสกุลเงินเข้ารหัส และนโยบาย กฎหมายและมาตรการต่าง ๆ ที่เกี่ยวข้อง กลุ่มที่ 2 ผู้เชี่ยวชาญทางด้านกฎหมายที่เกี่ยวกับสกุลเงินเข้ารหัส กลุ่มที่ 3 ผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือ และ กลุ่มที่ 4 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการเสนอแนวทางในการป้องกันอาชญากรรม

1.4.3 ขอบเขตด้านระยะเวลา

การศึกษาแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: ศึกษากรณีบิทคอยน์ จะทำการศึกษาตั้งแต่เริ่มมีการสร้างบิทคอยน์เป็นสกุลเงินเข้ารหัส และเริ่มมีการนำบิทคอยน์ไปใช้ในการประกอบอาชญากรรมมาจนถึงปัจจุบัน

1.5 นิยามศัพท์ที่ใช้ในการวิจัย

1.5.1 **สกุลเงินเข้ารหัส (Cryptocurrency)** หมายถึง สิ่งประดิษฐ์ทางนวัตกรรรมและเทคโนโลยีที่อยู่ในรูปแบบของข้อมูลคอมพิวเตอร์ ที่มุ่งนำมาใช้ในเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการระหว่างกันในลักษณะเดียวกันกับสกุลเงินจริง โดยมูลค่าของสกุลเงินเข้ารหัสไม่ได้ยึดโยงหรืออ้างอิงอยู่กับสินทรัพย์หรือสถาบันการเงินใด ๆ แต่จะเปลี่ยนผันไปตามความต้องการของตลาดการซื้อขาย

1.5.2 **บิทคอยน์ (Bitcoin)** หมายถึงสกุลเงินเข้ารหัสประเภทหนึ่งที่มีผู้นิยมใช้งานเป็นจำนวนมาก มีคุณลักษณะพิเศษ คือ ไม่มีการเก็บฐานข้อมูลการทำธุรกรรมของผู้ใช้บริการไว้ที่ส่วนกลาง (Server) แต่ใช้วิธีการส่งต่อข้อมูลบันทึกทางธุรกรรมต่าง ๆ ที่ถูกเข้ารหัสแล้ว ให้กลุ่มผู้ใช้งานในระบบทำการตรวจสอบความถูกต้องและบันทึกข้อมูลต่อเนื่องกันไปด้วยระบบบล็อคเชน (Blockchain) อีกทั้งจะไม่มีการเปิดเผยตัวตนของเจ้าของบัญชีผู้ใช้งาน เพื่อเป็นการรักษาความมั่นคงปลอดภัยให้แก่ผู้ใช้งาน

1.5.3 **อาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส** หมายถึง การนำเอาสกุลเงินเข้ารหัสไปใช้เป็นสื่อกลางหรือเครื่องมือในการกระทำความผิด เพื่อให้เกิดความสะดวกสบายและเป็นการหลีกเลี่ยงการถูกตรวจสอบโดยเจ้าหน้าที่ของรัฐ เฉพาะที่มีการนำไปใช้กระทำผิดโดยทางตรง ได้แก่ การลักลอบซื้อขายยาเสพติด อาวุธเถื่อน การว่าจ้างให้ผู้อื่นกระทำผิดกฎหมาย การซื้อขายสื่อลามกอนาจาร การเรียกค่าไถ่ การระดมเงินทุนของกลุ่มผู้ก่อการร้ายโดยมีการใช้บิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆในการเป็นสื่อกลางในการกระทำความผิด รวมทั้งการฟอกเงินผ่านบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ **ทั้งนี้ไม่รวมถึง**การกระทำความผิดที่เกี่ยวข้องกับการใช้สกุลเงินเข้ารหัสในทางอ้อม เช่น การนำเอาชื่อ “บิทคอยน์” ไปหลอกลวงชักชวนให้เหยื่อมาลงทุนเก็งกำไรจากการซื้อขายแลกเปลี่ยนบิทคอยน์ หรือการหลอกลวงให้มาลงทุนในธุรกิจการขุดบิทคอยน์ และเมื่อเหยื่อหลงเชื่อผู้กระทำความผิดก็ยักยอกเงินแล้วหลบหนีไปในลักษณะเดียวกันกับแชร์ลูกโซ่ และการหลอกลวงฉ้อฉลในการซื้อขายแลกเปลี่ยนหรือในภาคการลงทุนหรือภาคธุรกิจ ซึ่งไม่ได้เป็นการใช้บิทคอยน์หรือสกุลเงินเข้ารหัสเป็นสาระในการก่ออาชญากรรม

1.5.4 **การป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส** หมายถึง การกำหนดนโยบายกฎหมาย มาตรการหรือแนวทางการปฏิบัติงานของหน่วยงานของรัฐและหน่วยงานที่เกี่ยวข้อง เพื่อมุ่งยับยั้งและป้องกันมิให้มีการนำเอาสกุลเงินเข้ารหัสไปใช้เป็นเครื่องมือในการก่ออาชญากรรม

1.6 ประโยชน์ที่คาดว่าจะได้รับ

การศึกษานี้จะทำให้เกิดองค์ความรู้เกี่ยวกับความเป็นมาและสถานภาพของสกุลเงินเข้ารหัส สภาพปัญหา ลักษณะ รูปแบบและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ รวมทั้งทำให้เกิดความรู้ ความเข้าใจเกี่ยวกับแนวนโยบาย กฎหมาย และมาตรการต่างๆ ที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ เพื่อให้สามารถนำเอาองค์ความรู้ดังกล่าวไปวิเคราะห์จนสามารถเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือในประเทศไทยได้อย่างมีประสิทธิภาพ

1.7 วิธีการดำเนินการวิจัย

การวิจัยเรื่อง "แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์" เป็นงานวิจัยเชิงคุณภาพ (Qualitative Research) โดยมีวิธีการดำเนินการวิจัยดังนี้

1.7.1 การค้นคว้าจากเอกสาร (Documentary Study)

โดยการศึกษาจากหนังสือ วารสาร เอกสาร บทความ สื่ออิเล็กทรอนิกส์และข่าวสารต่างๆที่เกี่ยวข้อง ทั้งภาษาไทยและภาษาต่างประเทศ รวมทั้งศึกษาจากงานวิจัยและวิทยานิพนธ์ต่างๆที่เกี่ยวข้องกับประวัติความเป็นมาของสกุลเงินเข้ารหัส สถานการณ์การใช้สกุลเงินเข้ารหัสทั้งในประเทศไทยและต่างประเทศ รวมทั้งนโยบาย กฎหมายหรือมาตรการต่างๆที่นานาชาติรวมทั้งประเทศไทยใช้ในการควบคุม กำกับดูแลการใช้งานสกุลเงินเข้ารหัส สภาพปัญหา ลักษณะและรูปแบบของอาชญากรรมที่ใช้สกุลเงินเข้ารหัสหรือเสมือนใช้สกุลเงินเข้ารหัสเป็นเครื่องมือในการกระทำความผิด โดยเฉพาะกรณีของบิทคอยน์นั้นเป็นอย่างไร ตลอดจนศึกษาบทวิเคราะห์ในงานวิจัย เอกสารวิชาการ หนังสือพิมพ์ วารสารและสื่ออิเล็กทรอนิกส์ต่างๆ ที่มีการวิเคราะห์ถึงความเป็นไปได้ที่สกุลเงินเข้ารหัสจะถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรมรูปแบบต่างๆในอนาคต

การค้นคว้าจากเอกสาร (Documentary Study) ตามเนื้อหาดังกล่าว เป็นการศึกษารวบรวมข้อมูลเพื่อให้เกิดความรู้ ความเข้าใจในเบื้องต้นว่า สถานการณ์อาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือโดยเฉพาะอย่างยิ่งกรณีของบิทคอยน์นั้น เป็นอย่างไร เพื่อเป็นการสร้างองค์ความรู้พื้นฐานที่ถูกต้องให้กับ

ตัวผู้ศึกษา เพื่อให้สามารถทำการสัมภาษณ์เชิงลึกต่อผู้ทรงคุณวุฒิ ผู้เชี่ยวชาญ หรือ ผู้ที่มีประสบการณ์เกี่ยวข้อง ได้อย่างถูกต้อง ครบถ้วน ตรงประเด็น และเกิดประโยชน์สูงสุดต่อการวิจัยครั้งนี้ต่อไป

1.7.2 การศึกษาภาคสนาม (Field Study)

โดยใช้แบบสัมภาษณ์เป็นเครื่องมือในการเก็บรวบรวมข้อมูลจาก ผู้ให้ข้อมูลสำคัญ (Key Informants) โดยการสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ทรงคุณวุฒิ ผู้มีความรู้และประสบการณ์เกี่ยวกับระบบสกุลเงินเข้ารหัส กฎหมายที่เกี่ยวข้องกับสกุลเงินเข้ารหัส อาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส อาชญากรรมทางเทคโนโลยีและคอมพิวเตอร์ และผู้ที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการกำหนดหรือเสนอแนวนโยบายหรือมาตรการต่างๆที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส เพื่อให้ได้มาซึ่งข้อมูลเชิงลึกที่มีความครบถ้วนและสมบูรณ์ตลอดจนสามารถนำข้อมูลที่ได้ไปวิเคราะห์ สังเคราะห์ ถึงสภาพปัญหาและสาเหตุ อันจะนำไปสู่การเสนอแนวทางการป้องกันอาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือในประเทศไทยได้อย่างมีประสิทธิภาพต่อไป

1.7.3 การเลือกกลุ่มตัวอย่าง ผู้มีส่วนร่วมในการวิจัย/ ผู้ให้ข้อมูลสำคัญ (Key Informants)

การวิจัยครั้งนี้ใช้การเลือกกลุ่มตัวอย่างแบบเฉพาะเจาะจง โดยเลือกผู้ให้ข้อมูลสำคัญที่มีองค์ความรู้ มีความชำนาญ มีอำนาจหน้าที่เกี่ยวข้อง หรือ มีประสบการณ์ในด้านต่างๆที่เกี่ยวข้อง ดังนี้

กลุ่มที่ 1 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในเรื่องสกุลเงินเข้ารหัส ทั้งในส่วนภาครัฐและภาคเอกชน ได้แก่

1) ผู้ทรงคุณวุฒิด้านตลาดการเงิน ธนาคารแห่งประเทศไทย จำนวน 1 ราย (A1)

2) ผู้ทรงคุณวุฒิด้านเทคโนโลยีทางการเงิน สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ จำนวน 2 ราย (A2 และ A3)

3) ผู้ทรงคุณวุฒิจากสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ จำนวน 1 ราย (A4)

4) ผู้บริหารเว็บไซต์และผู้เขียนหนังสือให้ความรู้ทางด้านบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จำนวน 1 ราย (A5)

กลุ่มที่ 2 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในด้านกฎหมายที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ได้แก่

1) ผู้พิพากษาที่เชี่ยวชาญทางด้านกฎหมายการเงิน จำนวน 1 ราย (B1)

2) พนักงานอัยการที่มีความเชี่ยวชาญด้านกฎหมายการเงิน จำนวน 1 ราย (B2)

กลุ่มที่ 3 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญหรือผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส ได้แก่

1) ผู้ทรงคุณวุฒิจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) จำนวน 1 ราย (C1)

2) ผู้เชี่ยวชาญจากกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) จำนวน 1 ราย (C2)

3) ผู้ทรงคุณวุฒิจากกรมสอบสวนคดีพิเศษ จำนวน 1 ราย (C3)

4) ผู้ทรงคุณวุฒิจากสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) จำนวน 1 ราย (C4)

กลุ่มที่ 4 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการเสนอแนวทางในการป้องกันอาชญากรรม ได้แก่

1) ผู้บริหารระดับสูง สำนักงานตำรวจแห่งชาติ จำนวน 1 ราย (D1)

2) อดีตผู้ทรงคุณวุฒิพิเศษ สำนักงานตำรวจแห่งชาติ จำนวน 1 ราย (D2)

1.7.4 เกณฑ์การคัดเลือกผู้มีส่วนร่วมในการวิจัยและเกณฑ์พิจารณาให้ผู้มีส่วนร่วมในการวิจัยออกจากโครงการ และอื่นๆ

1) เกณฑ์การคัดเข้า

การคัดเลือกผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญจะพิจารณาจากผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีความรู้ความสามารถ มีประสบการณ์หรือความความชำนาญในด้านต่างๆที่เกี่ยวข้องโดยแบ่งเป็น 4 กลุ่ม ดังนี้

กลุ่มที่ 1 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในเรื่องสกุลเงินเข้ารหัสทั้งในส่วนภาครัฐและภาคเอกชน จำนวน 5 ราย

กลุ่มที่ 2 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญทางด้านกฎหมายเกี่ยวกับสกุลเงินเข้ารหัส จำนวน 2 ราย

กลุ่มที่ 3 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญหรือผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส จำนวน 4 ราย

กลุ่มที่ 4 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการเสนอแนวทางในการป้องกันอาชญากรรม จำนวน 2 ราย

ทั้งนี้ผู้ที่ได้รับการคัดเข้าร่วมการวิจัยจะต้องเป็นผู้ที่ได้รับข้อมูลที่เกี่ยวกับการวิจัยดังที่ระบุไว้ในเอกสารข้อมูลสำหรับผู้มีส่วนร่วมในการวิจัยและเป็นผู้สมัครใจและยินยอมที่จะเข้าร่วมทำการวิจัย

2) เกณฑ์การคัดออก

หากระหว่างการวิจัยหรือระหว่างขั้นตอนการเก็บข้อมูลในการวิจัยครั้งนี้ ทำให้ผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญ รู้สึกไม่ปลอดภัยหรือไม่ต้องการที่จะให้ข้อมูลหรือให้สัมภาษณ์ต่อไป ผู้วิจัยจะพิจารณาให้ผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญออกจากการวิจัยได้ทุกเมื่อตามความต้องการและความสมัครใจของผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญ และจะได้พิจารณาคัดผู้เข้าร่วมวิจัยตามเกณฑ์การคัดเข้าทดแทนต่อไป

1.7.5 รายละเอียดเกี่ยวกับวิธีการติดต่อและวิธีการเข้าถึงผู้มีส่วนร่วมในการวิจัย/ ผู้ให้ข้อมูลสำคัญ (Key Informants)

การติดต่อเพื่อเข้าถึงผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญ จะใช้การติดต่อผ่านหนังสือขอทำการเก็บข้อมูลอย่างเป็นทางการซึ่งออกโดย คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย หรือออกโดยผู้วิจัยซึ่งได้รับการรับรองจากอาจารย์ที่ปรึกษาแล้วนำส่งไปยังที่สถานที่ทำการ หรือ สถานที่อื่นๆที่สามารถติดต่อผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญได้ เมื่อได้รับความยินยอมและได้รับการติดต่อกลับจาก ผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญแล้ว จึงทำการนัดหมายและเข้าพบผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญเพื่อทำการสัมภาษณ์และเก็บข้อมูล

1.7.6 วิธีการพิทักษ์สิทธิ ป้องกันความเสี่ยง และรักษาความลับของผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญ (Key Informants)

1) การแจ้งข้อมูลเกี่ยวกับงานวิจัย วัตถุประสงค์ของการวิจัย ประโยชน์ที่คาดว่าจะได้รับ วิธีการเก็บข้อมูล เงื่อนไขในการเปิดเผยข้อมูล รายละเอียดเกี่ยวกับผู้วิจัย และรายละเอียดอื่นๆ

ที่เกี่ยวข้องให้ผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญได้รับทราบ ซึ่งเป็นการให้ข้อมูลเบื้องต้นเพื่อประกอบการตัดสินใจในการยินยอมเข้าร่วมในการวิจัย

2) แจ้งให้ผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญทราบว่ามีสิทธิที่จะยินยอมหรือปฏิเสธการเข้าร่วมในการวิจัยได้ด้วยความสมัครใจ หรือหากต้องการถอนตัวก็สามารถทำได้ทันทีตามความประสงค์โดยไม่ต้องแจ้งเหตุผลให้ผู้วิจัยทราบ

3) ผู้วิจัยจะปฏิบัติตามเงื่อนไขที่ได้ระบุไว้ในหนังสือยินยอมเข้าร่วมในการวิจัยอย่างเคร่งครัด กล่าวคือ ข้อมูลที่ได้จากการสัมภาษณ์ ข้อมูลส่วนตัวของผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญ จะถูกเก็บรักษาเป็นความลับ และการนำเสนอผลการวิจัยจะเป็นภาพรวมโดยไม่ระบุข้อมูลใดๆ ที่จะนำไปสู่ตัวผู้มีส่วนร่วมในการวิจัย/ผู้ให้ข้อมูลสำคัญ

1.7.7 เครื่องมือที่ใช้ในการวิจัย

การศึกษาครั้งนี้เป็นการวิจัยเชิงคุณภาพใช้วิธีการเก็บข้อมูลด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) ใช้เทคนิคการสัมภาษณ์แบบมีโครงสร้าง (Structured Interview) โดยใช้แบบสัมภาษณ์ที่มีการกำหนดหัวข้อสัมภาษณ์ (Questionnaire Guide) ที่เกี่ยวข้องกับแนวทางการป้องกันอาชญากรรมใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือในประเทศไทย แบ่งออกเป็น 4 ชุด สำหรับผู้ให้ข้อมูลสำคัญกลุ่มต่างๆ มีรายละเอียดดังนี้

แบบสัมภาษณ์ ชุดที่ 1 สำหรับผู้ให้ข้อมูลสำคัญกลุ่มที่ 1 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในเรื่องสกุลเงินเข้ารหัส ทั้งในส่วนภาครัฐและภาคเอกชน แบ่งเป็น 4 ส่วน คือ

ส่วนที่ 1 ข้อมูลส่วนบุคคล

ส่วนที่ 2 ข้อมูลเกี่ยวกับบิทคอยน์

ส่วนที่ 3 นโยบาย กฎหมายและมาตรการต่างๆที่เกี่ยวข้องกับสกุลเงินเข้ารหัสในปัจจุบัน

ส่วนที่ 4 ข้อเสนอแนะ

แบบสัมภาษณ์ ชุดที่ 2 สำหรับผู้ให้ข้อมูลสำคัญกลุ่มที่ 2 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญทางด้านกฎหมายเกี่ยวกับสกุลเงินเข้ารหัส แบ่งเป็น 4 ส่วน คือ

ส่วนที่ 1 ข้อมูลส่วนบุคคล

ส่วนที่ 2 ประเด็นเกี่ยวกับสถานภาพทางกฎหมายของบิทคอยน์

ส่วนที่ 3 ข้อกฎหมายและกระบวนการทางกฎหมายที่เกี่ยวข้องกับบิทคอยน์

ส่วนที่ 4 ข้อเสนอแนะ

แบบสัมภาษณ์ ชุดที่ 3 สำหรับผู้ให้ข้อมูลสำคัญกลุ่มที่ 3 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญหรือผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส แบ่งเป็น 4 ส่วน คือ

ส่วนที่ 1 ข้อมูลส่วนบุคคล

ส่วนที่ 2 อาชญากรรมที่เกี่ยวกับบิทคอยน์

ส่วนที่ 3 บุคลากรและเครื่องมือที่ใช้ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์

ส่วนที่ 4 นโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับบิทคอยน์

แบบสัมภาษณ์ ชุดที่ 4 สำหรับผู้ให้ข้อมูลสำคัญกลุ่มที่ 4 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการเสนอแนวทางในการป้องกันอาชญากรรม แบ่งเป็น 3 ส่วน คือ

ส่วนที่ 1 ข้อมูลส่วนบุคคล

ส่วนที่ 2 อาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

ส่วนที่ 3 แนวทางการป้องกันอาชญากรรมเกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

1.7.8 การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลเชิงคุณภาพใช้วิธีวิเคราะห์เนื้อหา (Content Analysis) จากการรวบรวมข้อมูลวิจัยเอกสาร และการสัมภาษณ์แบบเจาะลึก โดยสามารถสรุปขั้นตอนการประมวลผลได้ ดังนี้

1) ตรวจสอบและประเมินคุณค่าของข้อมูลเอกสารทุติยภูมิ และข้อมูลที่ได้จากการสัมภาษณ์แบบเจาะลึก

2) จัดระเบียบข้อมูล เพื่อตอบคำถามในแต่ละประเด็นตามวัตถุประสงค์การวิจัย

3) ตรวจสอบความครบถ้วนของคำตอบในแต่ละประเด็น และความถูกต้องของข้อเท็จจริง

1.7.9 จริยธรรมการวิจัยในคน

การศึกษาวิจัยครั้งนี้ได้ผ่านการพิจารณาจากคณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย เป็นโครงการวิจัยที่ 121/62 ตามใบรับรองโครงการวิจัยที่ COA No.112/2562 วันที่รับรอง 25 พฤศจิกายน 2562 วันหมดอายุ 24 พฤศจิกายน 2563

บทที่ 2
แนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้อง

ในบทนี้ผู้วิจัยจะได้นำเสนอถึงแนวคิด ทฤษฎี และงานวิจัยที่เกี่ยวข้องกับอาชญากรรมที่ใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นเครื่องมือ เพื่อใช้เป็นข้อมูลในการกำหนดกรอบแนวคิดการวิจัย และนำไปใช้ศึกษาวิเคราะห์และอภิปรายผลการศึกษาตามคำถามการวิจัยและวัตถุประสงค์ของการวิจัย ดังต่อไปนี้

2.1 แนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ (Computer Crime)

2.2 แนวคิดเกี่ยวกับอาชญากรรมเศรษฐกิจ (Economic Crime)

2.3 แนวคิดเกี่ยวกับอาชญากรรมข้ามชาติ (Transnational Crime)

2.4 ทฤษฎีคิดก่อนกระทำผิด (Rational Choice Theory)

2.5 ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory)

2.6 ทฤษฎีความล้าหลังทางสังคม (Culture Lag Theory)

2.7 ทฤษฎีป้องกันหรือทฤษฎีการข่มขู่ยับยั้ง (Deterrence Theory)

2.8 ทฤษฎีบังคับใช้กฎหมาย (Law Enforcement Theory)

2.9 แนวคิดเกี่ยวกับนโยบายสาธารณะและตัวแบบนโยบายสาธารณะแบบกลุ่ม (Group Model)

2.10 แนวคิดเกี่ยวกับมาตรการทางกฎหมาย

2.11 งานวิจัยที่เกี่ยวข้อง

2.1 แนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ (Computer Crime)

ตามที่ได้กล่าวมาแล้วว่า “บิทคอยน์” รวมทั้งสกุลเงินเข้ารหัสสกุลอื่นๆ อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์และมีการทำงานอยู่บนระบบเครือข่ายคอมพิวเตอร์ ดังนั้น การก่ออาชญากรรมประเภทต่างๆที่เกี่ยวกับบิทคอยน์หรือสกุลเงินเข้ารหัสประเภทต่างๆนั้น จึงจำเป็นจะต้องกระทำผ่านการใช้อุปกรณ์สมัยใหม่อย่างเครื่องคอมพิวเตอร์หรือโทรศัพท์สมาร์ทโฟน (Smart Phone) รวมทั้งในการกระทำความผิดรูปแบบต่างๆก็จะเกิดขึ้นในระบบเครือข่ายคอมพิวเตอร์ จึงมีความจำเป็นที่จะต้องทำความเข้าใจถึงแนวคิดที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์ ทั้งในด้านความหมาย บทบาทหน้าที่

ของเครื่องคอมพิวเตอร์ในการก่ออาชญากรรมคอมพิวเตอร์ ประเภทและลักษณะของอาชญากรรมคอมพิวเตอร์ประเภทต่างๆ ดังนี้

2.1.1 ความหมายของอาชญากรรมคอมพิวเตอร์ (Computer Crime)

ได้มีผู้ให้ความหมายเกี่ยวกับ “อาชญากรรมคอมพิวเตอร์” ไว้ดังนี้

“อาชญากรรมคอมพิวเตอร์” หมายถึง การกระทำผิดทางอาญาในระบบคอมพิวเตอร์ หรือการใช้คอมพิวเตอร์เพื่อกระทำผิดทางอาญา เช่น ทำลาย เปลี่ยนแปลง หรือขโมยข้อมูลต่าง ๆ เป็นต้น ระบบคอมพิวเตอร์ในที่นี้หมายรวมถึงระบบเครือข่ายคอมพิวเตอร์และอุปกรณ์ที่เชื่อมกับระบบดังกล่าวด้วย สำหรับอาชญากรรมในระบบเครือข่ายคอมพิวเตอร์ (เช่น อินเทอร์เน็ต) อาจเรียกได้อีกอย่างหนึ่งคืออาชญากรรมไซเบอร์ (Cybercrime) อาชญากรที่ก่ออาชญากรรมประเภทนี้มักถูกเรียกว่า แครกเกอร์ (กองวิจัย สำนักงานยุทธศาสตร์ตำรวจ สำนักงานตำรวจแห่งชาติ, 2559)

“อาชญากรรมคอมพิวเตอร์” คือ

1) การกระทำการใดๆ เกี่ยวกับการใช้คอมพิวเตอร์อันทำให้เหยื่อได้รับความเสียหายและผู้กระทำได้รับผลประโยชน์ตอบแทน

2) การกระทำผิดกฎหมายใดๆซึ่งใช้เทคโนโลยีคอมพิวเตอร์เป็นเครื่องมือและในการสืบสวนสอบสวนของเจ้าหน้าที่เพื่อนำผู้กระทำผิดมาดำเนินคดีต้องใช้ความรู้ทางเทคโนโลยีเช่นเดียวกัน (ญาณพล ยั่งยืน, 2545 อ้างถึงใน ประพัทธ์โชต งามขำ, 2548)

“อาชญากรรมคอมพิวเตอร์” หมายถึง การกระทำผิดกฎหมายใดๆ ซึ่งความรู้ในเทคโนโลยีทางคอมพิวเตอร์มีความสำคัญต่อผลสำเร็จของการกระทำหรือการดำเนินคดี และเป็นการกระทำผิดทางอาญาซึ่งก่อการคุกคามต่อผู้ใช้คอมพิวเตอร์มากกว่าผู้ที่มิได้ใช้คอมพิวเตอร์ อันประกอบไปด้วยการกระทำ 2 ชนิดด้วยกัน คือ (ฉัทปณัย รัตนพันธ์, 2547)

1) การใช้คอมพิวเตอร์เพื่อที่จะกระทำความผิดฐานฉ้อโกง ลักทรัพย์ และยักยอกโดยมีเจตนาที่จะได้ไปซึ่งประโยชน์อันเกี่ยวกับเงิน การค้า ทรัพย์สิน หรือบริการ และ

2) การกระทำต่อตัวเครื่องคอมพิวเตอร์เอง เช่น การลักโขมยเครื่องคอมพิวเตอร์หรือ ซอฟท์แวร์ การทำลาย แก้ไข เปลี่ยนแปลงเครื่องคอมพิวเตอร์หรือสิ่งที่บรรจุอยู่ภายในเครื่องคอมพิวเตอร์

จากที่มีผู้ให้ความหมายไว้ดังกล่าว สามารถสรุปได้ว่า **อาชญากรรมคอมพิวเตอร์** หมายถึงการกระทำผิดกฎหมายที่มีลักษณะดังต่อไปนี้

1) การนำเครื่องคอมพิวเตอร์ ระบบคอมพิวเตอร์ หรืออุปกรณ์อื่นใดที่เชื่อมต่อกับระบบคอมพิวเตอร์ต่างๆ มาใช้ก่ออาชญากรรมในรูปแบบดั้งเดิมเพื่อให้เกิดความสะดวกสบายขึ้น เช่น การติดต่อซื้อขายยาเสพติดกันผ่านระบบอินเทอร์เน็ต หรือ การเผยแพร่สื่อลามกอนาจารผ่านระบบคอมพิวเตอร์ เป็นต้น

2) การกระทำความผิดต่างๆ ที่กระทำต่อเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ เช่น การลักลอบเจาะระบบคอมพิวเตอร์เพื่อเข้าถึง ทำลาย เปลี่ยนแปลง แก้ไขข้อมูลต่างๆ, การดักรับข้อมูลทางคอมพิวเตอร์, การลักลอบทำซ้ำโปรแกรมและซอฟท์แวร์ต่างๆ และ การโจมตีระบบคอมพิวเตอร์เพื่อให้ระบบหยุดทำงาน เป็นต้น

2.1.2 บทบาทหน้าที่ของเครื่องคอมพิวเตอร์ในการก่ออาชญากรรมคอมพิวเตอร์

สามารถแบ่งได้เป็น 3 ลักษณะดังนี้ (จตุชัย แพงจันทร์, 2547 อ้างถึงใน กองวิจัย สำนักงานยุทธศาสตร์ตำรวจ สำนักงานตำรวจแห่งชาติ, 2559)

1) คอมพิวเตอร์ในฐานะที่มีส่วนเกี่ยวข้องกับการกระทำความผิด (Computers as Incidental to Crime) การกระทำความผิดในลักษณะนี้คอมพิวเตอร์จะไม่มีความสำคัญมากนัก หรือกล่าวได้ว่าคอมพิวเตอร์ไม่ใช่สาระสำคัญในกระทำความผิด แม้ไม่มีคอมพิวเตอร์อาชญากรก็สามารถกระทำผิดสำเร็จได้ เพียงแต่คอมพิวเตอร์เป็นอุปกรณ์เสริม ที่ช่วยอำนวยความสะดวกให้กับการกระทำผิดในรูปแบบดั้งเดิมเท่านั้น เช่น ใช้คอมพิวเตอร์เก็บข้อมูลเกี่ยวกับบัญชีเงินที่เกี่ยวข้องกับยาเสพติด หรือใช้เครื่องคอมพิวเตอร์ในการติดต่อสื่อสารภายในองค์กรอาชญากรรม หรือ ใช้คอมพิวเตอร์เก็บสื่อลามกอนาจาร เป็นต้น

2) คอมพิวเตอร์ในฐานะที่เป็นเครื่องมือที่ใช้ในการกระทำความผิด (Computers as a tool in the commission of a crime) การกระทำความผิดในลักษณะนี้จำเป็นจะต้องอาศัยคอมพิวเตอร์เป็นเครื่องมือหลักในการกระทำผิด หรือหากไม่มีเครื่องคอมพิวเตอร์จะไม่สามารถกระทำความผิดได้สำเร็จ เช่น การเผยแพร่ภาพลามกอนาจาร การพนันออนไลน์ การหลอกลวงสนทนาออนไลน์เพื่อประสงค์ต่อทรัพย์ (Romance Scam) การหมิ่นประมาทผู้อื่นโดยการโฆษณาโดยอาศัยเครือข่ายอินเทอร์เน็ต การละเมิดทรัพย์สินทางปัญญาด้วยการดาวน์โหลดหรือทำซ้ำผลงานอันมี

ลิขสิทธิ์ต่างๆ การลักลอบหรือขโมยใช้บริการสารสนเทศต่างๆโดยไม่ได้รับอนุญาต การหลอกขายสินค้าและบริการต่างๆบนอินเทอร์เน็ต การลักลอบโขมยข้อมูลสำคัญจากฐานข้อมูลของบริษัทคู่แข่งทางธุรกิจ เป็นต้น

3) คอมพิวเตอร์ในฐานะที่เป็นเป้าหมายของการกระทำความผิด (Computers as a target of the crime) การกระทำความผิดในลักษณะนี้ มุ่งเป้าที่คอมพิวเตอร์และระบบคอมพิวเตอร์โดยตรง เช่น การจงใจเจาะเข้าระบบเพื่อทำลายระบบคอมพิวเตอร์ต่างๆให้เกิดความเสียหายหรือไม่สามารถใช้การได้ หรือ การเจาะเข้ามาในระบบคอมพิวเตอร์เพื่อเปลี่ยนแปลงแก้ไขชุดข้อมูลคำสั่งต่างๆจนทำให้เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ทำงานผิดปกติจนเสียหาย การปล่อยไวรัสหรือมัลแวร์เข้าใส่ระบบคอมพิวเตอร์เป้าหมาย การลักลอบติดตั้งโปรแกรมเพื่อหยุดการทำงานของระบบเพื่อแลกกับค่าไถ่ (Ransomware) หรือ การโจมตีระบบด้วยการเข้าใช้งานเพื่อให้ระบบทำงานมากกว่าปกติในเวลาเดียวกันจนไม่สามารถทำงานได้ (Denial-of-Service) เป็นต้น

2.1.3 ประเภทของอาชญากรรมคอมพิวเตอร์

อนุสัญญาของสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 (The Council of Europe ‘s Convention on Cybercrime 2001) หรือ “อนุสัญญากรุงบูดาเปสต์” ซึ่งถือเป็นอนุสัญญาต้นแบบในการวางหลักเกณฑ์ในทางกฎหมายเกี่ยวกับอาชญากรรมคอมพิวเตอร์ทั่วโลก ได้กำหนดให้ชาติสมาชิกที่ร่วมให้สัตยาบัน นำลักษณะการกระทำความผิดรูปแบบต่างๆตามที่ได้กำหนดไว้ในอนุสัญญานี้ ไปเป็นแนวทางในการบัญญัติกฎหมายที่เกี่ยวกับการกระทำความผิดที่เป็นอาชญากรรมคอมพิวเตอร์ที่เป็นกฎหมายภายในของแต่ละประเทศให้มีความสอดคล้องกัน โดยอนุสัญญาดังกล่าวได้มีการแบ่งลักษณะการกระทำความผิดที่เป็นอาชญากรรมคอมพิวเตอร์ออกเป็น 4 ประเภท ดังนี้ (Council of Europe , 2001)

ประเภทที่ 1 การกระทำความผิดอันเป็นการกระทบต่อความลับ ความมั่นคงปลอดภัย และความสมบูรณ์ของข้อมูลและระบบคอมพิวเตอร์ (Offences Against Confidentiality, Integrity and Availability of Computer Data and Systems)

ประเภทที่ 2 การกระทำความผิดที่มีความเกี่ยวข้องกับคอมพิวเตอร์ (Computer – Related Offences)

ประเภทที่ 3 การกระทำความผิดที่เกี่ยวกับเนื้อหาที่มีการเผยแพร่ทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ (Content – Related Offences)

ประเภทที่ 4 การกระทำความผิดที่เกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิ์อื่นๆที่เกี่ยวข้อง (Offences Related to Infringements of copyright and related rights)

โดยในแต่ละประเภทยังแบ่งได้เป็นลักษณะการกระทำความผิดต่างๆ สามารถแยกอธิบายได้ดังนี้

ประเภทที่ **1 การกระทำความผิดอันเป็นการกระทบต่อความลับ ความมั่นคงปลอดภัย และความสมบูรณ์ของข้อมูลและระบบคอมพิวเตอร์ (Offences Against Confidentiality, Integrity and Availability of Computer Data and Systems) มีลักษณะของการกระทำความผิดตามมาตราต่างๆดังนี้**

มาตรา 2 (Article 2) การเข้าถึงข้อมูลโดยมิชอบ (Illegal Access) หมายถึงการกระทำด้วยวิธีใดๆเพื่อเข้าถึงข้อมูลคอมพิวเตอร์ไม่ว่าจะทั้งหมดหรือบางส่วน ผ่านเครื่องคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ โดยผู้ที่กระทำผิดทราบดีอยู่แล้วว่าตนไม่มีสิทธิ์โดยชอบธรรมที่จะเข้าถึงข้อมูลนั้นๆ แต่ยังจงใจและเจตนาที่จะลักลอบเข้าถึงข้อมูลดังกล่าวโดยไม่ได้รับอนุญาต เช่น การลักลอบเจาะเข้าระบบ (Hacking) หรือการขโมยรหัสผ่านเพื่อลักลอบเข้าระบบ เป็นต้น

มาตรา 3 (Article 3) การดักรับข้อมูลโดยมิชอบ (Illegal Interception) หมายถึงการกระทำทางเทคนิคต่างๆ ที่มีลักษณะเป็นการเจตนาลักลอบดักรับและได้มาซึ่งข้อมูลคอมพิวเตอร์ที่มิใช่ข้อมูลสาธารณะ ในระหว่างที่มีการ รับ – ส่ง ข้อมูลกันผ่านระบบคอมพิวเตอร์ ไม่ว่าจะเป็นการส่งระหว่างเครื่องคอมพิวเตอร์ การส่งข้อมูลภายในระบบเครือข่ายคอมพิวเตอร์หนึ่ง หรือการส่งข้อมูลไปยังระบบเครือข่ายคอมพิวเตอร์อื่นๆก็ตาม โดยที่ผู้กระทำไม่มีสิทธิ์หรือไม่ได้รับอนุญาตให้เข้าถึงข้อมูลนั้นๆ

มาตรา 4 (Article 4) การลักลอบแทรกแซงข้อมูล (Data Interference) หมายถึงการลักลอบทำลาย การลบ การทำให้เสื่อมสภาพ การดัดแปลงแก้ไข รวมทั้งการขัดขวางการทำงานของข้อมูลคอมพิวเตอร์โดยเจตนา โดยผู้ที่กระทำผิดไม่มีสิทธิ์หรือไม่ได้รับอนุญาตให้เข้าถึงข้อมูลนั้นๆ เช่น การสร้างโปรแกรมไวรัส (Virus) ในลักษณะต่างๆแล้วนำไปเผยแพร่เข้าสู่ระบบคอมพิวเตอร์เพื่อให้มีการโจมตีจนเกิดความเสียหายต่อข้อมูลคอมพิวเตอร์ เป็นต้น

มาตรา 5 (Article 5) การลักลอบแทรกแซงระบบ (System Interference) หมายถึง การเจตนาลักลอบเข้าไปควบคุมหรือจัดการระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตด้วยวิธีต่างๆ ไม่ว่าจะเป็นการใส่ข้อมูล การส่งข้อมูล การทำให้เสียหาย การลบ การทำให้เสื่อมค่า การแก้ไขดัดแปลงข้อมูลคอมพิวเตอร์ จนทำให้เกิดความเสียหายอย่างรุนแรงต่อระบบคอมพิวเตอร์ เช่น การโจมตีให้ระบบคอมพิวเตอร์อยู่ในสภาวะปฏิเสธการทำงาน (Denial of Service) ด้วยการส่งข้อมูลเป็นจำนวนมากเกินกว่าปกติเข้าไป จนทำให้ระบบไม่สามารถทำงานได้ หรือ กรณีของการแพร่โปรแกรมต่างๆที่เข้าไปขัดขวางการทำงานของระบบคอมพิวเตอร์ตามปกติอย่างโปรแกรมเรียกค่าไถ่ (Ransomware) ที่จะเข้าไปขัดขวางการทำงานของระบบคอมพิวเตอร์จนได้รับความเสียหาย เป็นต้น

มาตรา 6 (Article 6) การใช้อุปกรณ์และข้อมูลในทางที่มิชอบ (Misuse of Device) หมายถึง การผลิต การขาย การเป็นธุระจัดหา การนำเข้า หรือการเผยแพร่แจกจ่าย

(1) โปรแกรมคอมพิวเตอร์ที่ถูกสร้างหรือดัดแปลงขึ้นเพื่อนำมาใช้ในการกระทำผิดที่มีลักษณะตามมาตรา 2 – 5

(2) รหัสผ่านเพื่อเข้าสู่ระบบคอมพิวเตอร์ รวมทั้งข้อมูลอื่นๆที่มีลักษณะเช่นเดียวกัน ไม่ว่าจะเป็นข้อมูลทั้งหมดหรือเพียงบางส่วนอันอาจจะใช้เพื่อเข้าสู่ระบบโดยไม่ชอบได้

โดยการกระทำดังกล่าวต้องเป็นการกระทำโดยเจตนาและผู้กระทำผิดมุ่งที่จะกระทำผิดตามลักษณะที่ได้กล่าวในมาตรา 2 – 5

ประเภทที่ 2 การกระทำความผิดที่มีความเกี่ยวข้องกับคอมพิวเตอร์ (Computer – Related Offences)

มาตรา 7 (Article 7) การปลอมแปลงทางคอมพิวเตอร์ (Computer – Related Forgery) หมายถึง การกระทำโดยเจตนาเพื่อปลอมแปลงข้อมูลคอมพิวเตอร์ต้นฉบับ ด้วยการกรอกข้อมูล การดัดแปลงแก้ไข การลบ หรือการทำลายข้อมูลคอมพิวเตอร์ต้นฉบับโดยไม่ได้รับอนุญาต เพื่อนำข้อมูลคอมพิวเตอร์ที่ถูกลักลอบปลอมแปลง ไปใช้ในทางกฎหมายหรือนำไปแสดงให้ผู้อื่นหลงเชื่อว่าข้อมูลคอมพิวเตอร์ดังกล่าวเป็นข้อมูลที่ถูกต้อง เช่น การลักลอบเข้าไปปลอมแปลงตัวเลขทางบัญชีการเงินของบริษัทที่ถูกจัดเก็บอยู่ในระบบคอมพิวเตอร์จนเกิดความเสียหาย เป็นต้น

มาตรา 8 การฉ้อโกงทางคอมพิวเตอร์ (Computer – Related Fraud) หมายถึง การกระทำใดๆอันเป็นการก่อให้เกิดความเสียหายต่อทรัพย์สินของผู้หนึ่งผู้ใด โดยวิธีการดังต่อไปนี้

(1) โดยการนำเข้าข้อมูล การดัดแปลงแก้ไข การลบหรือการทำลายข้อมูลคอมพิวเตอร์

(2) โดยการแทรกแซงการทำงานของระบบคอมพิวเตอร์

โดยการกระทำดังนี้จะเป็นความผิดก็ต่อเมื่อผู้กระทำผิดไม่ได้รับอนุญาตให้เข้าถึงข้อมูลคอมพิวเตอร์ดังกล่าวและกระทำไปโดยมีเจตนาที่จะฉ้อโกงเพื่อให้ได้รับผลประโยชน์แก่ตนเองหรือผู้อื่น

ประเภทที่ 3 การกระทำความผิดที่เกี่ยวกับเนื้อหาที่มีการเผยแพร่ทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ (Content – Related Offences)

มาตรา 9 (Article 9) การกระทำความผิดเกี่ยวกับสื่อลามกอนาจารเด็ก หมายถึงการกระทำที่มีลักษณะดังต่อไปนี้

(1) การผลิตสื่อลามกอนาจารเด็กโดยมีวัตถุประสงค์เพื่อการเผยแพร่ผ่านระบบคอมพิวเตอร์

(2) การเสนอขายหรือการเป็นธุระจัดหาซึ่งสื่อลามกอนาจารเด็กให้แก่ผู้อื่นผ่านระบบคอมพิวเตอร์

(3) การเผยแพร่หรือการส่งสื่อลามกอนาจารเด็กให้แก่ผู้อื่นผ่านระบบคอมพิวเตอร์

(4) การซื้อสื่อลามกอนาจารเด็กผ่านระบบคอมพิวเตอร์ให้แก่ตนเองหรือผู้อื่น

(5) การมีสื่อลามกอนาจารเด็กไว้ในความครอบครองในระบบคอมพิวเตอร์ หรืออุปกรณ์ในการเก็บข้อมูลทางคอมพิวเตอร์

โดย “สื่อลามกอนาจารเด็ก” ในที่นี้หมายถึง สื่อลามกอนาจารในรูปแบบต่างๆที่สามารถมองเห็นหรือรับรู้ได้ที่แสดงถึงการกระทำกิจกรรมทางเพศของเด็ก หรือการกระทำกิจกรรมทางเพศต่อเด็ก หรือ ภาพเสมือนจริงที่สื่อถึงการกระทำกิจกรรมทางเพศของเด็ก

นอกจากนี้ในมาตรา 9 ยังได้กำหนดเกณฑ์อายุที่จะเข้าข่ายความเป็น “เด็ก” ในมาตรานี้คือบุคคลที่มีอายุไม่ถึง 18 ปี ทั้งนี้ชาติสมาชิกที่ให้สัตยาบันจะกำหนดเกณฑ์อายุเป็นอย่างอื่นก็ได้ แต่ต้องไม่กำหนดให้ต่ำกว่า บุคลลที่มีอายุไม่ถึง 16 ปี

ประเภทที่ 4 การกระทำความผิดที่เกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิ์อื่นๆที่เกี่ยวข้อง (Offences related to infringements of copyright and related rights)

มาตรา 10 (Article 10) การกระทำความผิดที่เกี่ยวกับการละเมิดลิขสิทธิ์และสิทธิ์อื่นๆที่เกี่ยวข้อง หมายถึง การละเมิดลิขสิทธิ์และสิทธิ์อื่นๆที่เกี่ยวข้องตามที่ระบุในอนุสัญญากรุงปารีสซึ่งปรับปรุงแก้ไขโดยอนุสัญญาเบิร์นว่าด้วยการคุ้มครองวรรณกรรมและงานศิลปะ ข้อตกลงว่าด้วยหลักเกณฑ์ที่เกี่ยวข้องกับการค้าในทรัพย์สินทางปัญญา และสนธิสัญญาขององค์การทรัพย์สินทางปัญญาโลกว่าด้วยเรื่องลิขสิทธิ์ ด้วยการใช้ระบบคอมพิวเตอร์และได้กระทำลงด้วยเจตนาเพื่อผลประโยชน์ทางการค้า

2.1.4 อาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือกับความเป็นอาชญากรรมคอมพิวเตอร์

จากการศึกษาแนวคิดเกี่ยวกับอาชญากรรมคอมพิวเตอร์ (Computer Crime) ตามที่ได้กล่าวมาแล้ว ทำให้สามารถอธิบายอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้ว่า **การนำบิทคอยน์และสกุลเงินเข้ารหัสสกุลต่างๆมาใช้ในการก่ออาชญากรรมนั้นมีลักษณะเป็นอาชญากรรมคอมพิวเตอร์** สามารถวิเคราะห์ได้ ดังนี้

1) เมื่อวิเคราะห์จาก**บทบาทหน้าที่ของเครื่องคอมพิวเตอร์ในการก่ออาชญากรรม**คอมพิวเตอร์แล้ว ด้วยลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสสกุลต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่จะต้องอาศัยการทำงานบนระบบเครือข่ายคอมพิวเตอร์ จะพบว่าการใช้บิทคอยน์และสกุลเงินเข้ารหัสสกุลอื่นๆในการกระทำผิดลักษณะต่างๆ ก็ย่อมจะต้องกระทำผ่านระบบเครือข่ายคอมพิวเตอร์ด้วย จึงมีลักษณะเป็น**อาชญากรรมคอมพิวเตอร์ในลักษณะที่คอมพิวเตอร์เป็นเครื่องมือจำเป็นที่ต้องใช้ในการกระทำความผิด**

แต่ในขณะเดียวกันเมื่อวิเคราะห์จากอีกมุมมองหนึ่งจะเห็นว่า แท้จริงแล้วเนื้อแท้ของการก่ออาชญากรรม ยังเป็นรูปแบบของอาชญากรรมปกติหรืออาชญากรรมดั้งเดิม เช่น ฉ้อโกง ฟอกเงิน ยาเสพติด ซื้อขายสินค้าและบริการที่ผิดกฎหมายต่างๆ ความผิดเกี่ยวกับสื่อลามกอนาจาร การเรียกค่าไถ่ ซึ่งมีพฤติกรรมการกระทำผิดไม่แตกต่างจากเดิม เพียงแต่มีการนำบิทคอยน์ซึ่งเป็นข้อมูลอิเล็กทรอนิกส์และทำงานผ่านระบบคอมพิวเตอร์มาใช้เพื่อให้เกิดความสะดวกสบายในการกระทำผิดเท่านั้น แม้ไม่มีบิทคอยน์อาชญากรรมต่างๆนี้ก็ยังคงมีโอกาสที่จะเกิดขึ้นได้ จึงมีลักษณะเป็น**อาชญากรรมคอมพิวเตอร์ในลักษณะที่คอมพิวเตอร์มีส่วนเกี่ยวข้องกับการกระทำความผิด**ได้เช่นกัน

2) เมื่อวิเคราะห์ตามประเภทและลักษณะของอาชญากรรมคอมพิวเตอร์ตามหลักเกณฑ์ของอนุสัญญาแห่งสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 แล้วจะพบว่ามีการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรงบางลักษณะที่จะเป็นอาชญากรรมคอมพิวเตอร์ตามหลักเกณฑ์ดังกล่าวอย่างชัดแจ้ง ได้แก่ การใช้บิทคอยน์เพื่อการซื้อขายสื่อลามกอนาจาร กรณีที่เป็นการซื้อขายสื่อลามกอนาจารที่เกี่ยวกับเด็ก ซึ่งถือเป็นอาชญากรรมคอมพิวเตอร์ตามที่ระบุไว้ในมาตรา 9 (Article 9) ประเภทที่ 3 การกระทำความผิดที่เกี่ยวกับเนื้อหาที่มีการเผยแพร่ทางคอมพิวเตอร์หรือระบบคอมพิวเตอร์ (Content – Related Offences) และกรณีของการเรียกค่าไถ่โดยการใช้โปรแกรมเรียกค่าไถ่ (Ransomware) และมีการเรียกร้องให้มีการจ่ายค่าไถ่เป็นบิทคอยน์หรือสกุลเงินเข้ารหัสสกุลอื่นๆ ซึ่งถือเป็นอาชญากรรมคอมพิวเตอร์ในลักษณะของการลักลอบแทรกแซงระบบ (System Interference) โดยไม่ได้รับอนุญาต จนทำให้เกิดความเสียหายอย่างรุนแรงต่อระบบคอมพิวเตอร์ ตามมาตรา 5 (Article 5) ถือเป็นอาชญากรรมคอมพิวเตอร์ประเภทที่ 1 การกระทำความผิดอันเป็นการกระทบต่อความลับ ความมั่นคงปลอดภัย และความสมบูรณ์ของข้อมูลและระบบคอมพิวเตอร์ (Offences against Confidentiality, Integrity and Availability of Computer Data and Systems) ดังนั้น หากเกิดการกระทำความผิดทั้งสองประเภทนี้ขึ้นในประเทศที่ได้ให้สัตยาบันหรือได้มีการนำอนุสัญญาแห่งสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 ไปใช้เป็นแนวทางในการออกกฎหมายแล้ว นอกจากจะสามารถนำกฎหมายอาญาหรือกฎหมายที่มีโทษทางอาญาอื่นๆที่เกี่ยวข้องมาใช้บังคับได้แล้ว ยังสามารถนำกฎหมายและบทลงโทษที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์มาใช้บังคับได้อีกด้วย

ในขณะที่การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรง ลักษณะอื่นๆ ได้แก่ การลักลอบซื้อขายยาเสพติดโดยการชำระเงินด้วยบิทคอยน์ การซื้อขายอาวุธเถื่อนโดยการชำระเงินด้วยบิทคอยน์ การว่าจ้างผู้อื่นให้กระทำผิดกฎหมายโดยชำระค่าจ้างด้วยบิทคอยน์ การระดมเงินทุนของกลุ่มผู้ก่อการร้ายด้วยบิทคอยน์ และการฟอกเงินผ่านบิทคอยน์นั้น แม้จะต้องอาศัยเครื่องคอมพิวเตอร์หรือโทรศัพท์สมาร์ทโฟน (Smart Phone) ในการกระทำผิดและต้องกระทำผิดผ่านระบบเครือข่ายคอมพิวเตอร์ก็ตาม แต่ก็เป็นไปเพียงเพื่อให้การกระทำความผิดสำเร็จเท่านั้น โดยยังไม่เข้าหลักเกณฑ์จะเป็นอาชญากรรมคอมพิวเตอร์อย่างชัดแจ้งแต่อย่างใด ส่วนกรณีของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมทางอ้อม อย่างการหลอกลวงและชักชวนผู้อื่นว่าจะมีการนำเงินไปลงทุนเก็งกำไรในมูลค่าของบิทคอยน์หรือการขุดบิทคอยน์นั้น เป็นการนำชื่อของ

บิทคอยน์ไปใช้หลอกลวงเหยื่อเท่านั้น ไม่ได้มีใช้ข้อมูลคอมพิวเตอร์หรืออาศัยระบบคอมพิวเตอร์ในการกระทำผิดแต่อย่างใด ดังนั้นจึงไม่ถือเป็นอาชญากรรมคอมพิวเตอร์แต่อย่างใด และเมื่อการกระทำผิดในกลุ่มหลังนี้ไม่ถือเป็นอาชญากรรมคอมพิวเตอร์แล้ว การนำมาตรการทางกฎหมายมาปรับใช้ ก็จะต้องอาศัยหลักกฎหมายทั่วไป กฎหมายอาญาหรือกฎหมายที่มีโทษทางอาญาอื่นๆที่เกี่ยวข้อง มาใช้เท่านั้น ไม่อาจนำกฎหมายที่เกี่ยวกับอาชญากรรมคอมพิวเตอร์มาใช้บังคับได้ โดยจะได้กล่าวถึงแนวนโยบาย กฎหมายและมาตรการต่างๆที่เกี่ยวข้องต่อไป

2.2 แนวคิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (Economic Crime)

ด้วยความที่สกุลเงินเข้ารหัสถูกสร้างขึ้นด้วยเจตนาในการเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการรูปแบบใหม่ จึงมีแนวโน้มในการนำไปใช้ในการกระทำความผิดต่างๆ ซึ่งอาจส่งผลกระทบต่อระบบเศรษฐกิจ ดังนั้นเพื่อเป็นการศึกษาแนวคิดต่างๆอย่างรอบด้าน จึงได้ทำการศึกษาแนวคิดเกี่ยวกับอาชญากรรมเศรษฐกิจ ดังนี้

2.2.1 ความหมายของอาชญากรรมทางเศรษฐกิจ

อาชญากรรมทางเศรษฐกิจถูกกล่าวถึงครั้งแรกโดย เอ็ดวิน เอช ซัทเทอร์แลนด์ (Edwin H. Sutherland) นักอาชญาวิทยาและสังคมวิทยาที่ได้ทำการศึกษาถึงความแตกต่างของอาชญากรรมประเภทนี้ ที่มิได้มีลักษณะการกระทำความผิดเหมือนอาชญากรรมทั่วไป อย่าง การลักทรัพย์หรือการทำร้ายร่างกายธรรมดา แต่พบว่าเป็นการกระทำโดยบุคคลชั้นสูงหรือชนชั้นปกครอง ที่ใช้อำนาจหน้าที่หรือตำแหน่งของตนเพื่อผลประโยชน์ส่วนตนโดยมิชอบ จนส่งผลให้เกิดความเสียหายต่อสาธารณะ ทำให้เกิดแนวคิดของ “อาชญากรรมคอเชิ้ตขาว” ซึ่งหมายถึงลักษณะการกระทำความผิดของชนชั้นสูงขึ้น ต่อมาเฮอร์เบิร์ต อีเดอฮาร์ต (Herbert Edelhertz) ได้นำแนวคิดของอาชญากรรมคอเชิ้ตขาวนี้ ไปพัฒนาและให้ความว่า หมายถึงการกระทำความผิดที่ไม่ได้กระทำให้เห็นได้ชัดทางกายภาพ แต่อาศัยการปิดบังซ่อนเร้นและการหลอกลวงฉ้อฉล เพื่อให้ได้มาซึ่งทรัพย์สินหรือผลประโยชน์ใดๆทางเศรษฐกิจ (วีระพงษ์ บุญโญภาส ,2552) นอกจากนี้ได้มีนักวิชาการและผู้ทรงคุณวุฒิกล่าวถึงความหมายของอาชญากรรมเศรษฐกิจ ไว้โดย วีระพงษ์ บุญโญภาส (2552) ให้ความหมายไว้ว่า “การกระทำความผิดต่อกฎหมาย ซึ่งมีผลกระทบต่อเศรษฐกิจและความมั่นคงของประเทศ โดยมิได้จำกัดเฉพาะความผิดในทางอาญาเท่านั้น ผู้กระทำความผิดดังกล่าว มักจะผู้ที่มีสถานภาพในทางสังคม มีตำแหน่งหน้าที่การงานและความรู้”

สามารถสรุปได้ว่า “อาชญากรรมทางเศรษฐกิจ” หมายถึง การกระทำความผิดที่กระทำโดยผู้ที่มีฐานะทางสังคม โดยอาศัยประโยชน์จากอำนาจ หน้าที่ หรือตำแหน่งของตนในทางใดทางหนึ่ง เพื่อให้ได้มาซึ่งผลประโยชน์ในทางมิชอบซึ่งมักเป็นการกระทำในทางลับ อันจะส่งผลกระทบหรือเกิดความเสียหายเป็นจำนวนมาก

2.2.2 ประเภทของอาชญากรรมทางเศรษฐกิจ

จากการศึกษารวบรวมข้อมูลต่างๆพบว่า มีหน่วยงานและนักวิชาการที่เกี่ยวข้องได้ทำการแบ่งประเภทของอาชญากรรมทางเศรษฐกิจไว้ต่างกันดังนี้

ตำรวจสากล (Interpol) ได้แบ่งประเภทตามแนวคิดเกี่ยวกับขอบเขตของอาชญากรรมทางเศรษฐกิจ ว่ามีขอบเขตตั้งแต่การโจรกรรมหรือการฉ้อโกงที่เกิดจากการกระทำผิดของบุคคลหรือกลุ่มบุคคลไปจนถึงการกระทำความผิดที่มีลักษณะเป็นองค์กรอาชญากรรม ที่มีกระบวนการและการวางแผนก่อนการกระทำความผิด จึงสามารถแบ่งประเภทได้ดังนี้ (Interpol, 2020)

1) การโจรกรรม (Theft)

2) การฉ้อโกง (Fruad)

3) การหลอกลวงด้วยกลอุบายต่างๆ (Deception)

4) การขู่กรรโชก (Blackmail)

5) การทุจริตของเจ้าหน้าที่รัฐ (Corruption)

6) การฟอกเงิน (Money Laundering)

7) การกระทำผิดอื่นๆที่มีลักษณะเป็นการกระทบต่อผลทางเศรษฐกิจ

เมื่อพิจารณาจากแนวคิดการแบ่งประเภทของตำรวจสากล จะพบว่ามีการแบ่งประเภทตามความหมายอย่างกว้าง ซึ่งหมายถึงอาชญากรรมใดๆก็ตามที่สามารถส่งผลต่อระบบเศรษฐกิจและการเงินได้ทางใดทางหนึ่ง ไม่ว่าจะเป็นการกระทำความผิดโดยอาชญากร กลุ่มอาชญากร หรือองค์กรอาชญากรรม หรือเจ้าหน้าที่ของรัฐก็ตาม

ขณะที่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ หรือ บก.ปอศ. ซึ่งเป็นหน่วยงานในสังกัด กองบัญชาการตำรวจสอบสวนกลาง สำนักงานตำรวจแห่งชาติ ที่มีหน้าที่รับผิดชอบเกี่ยวกับการป้องกันปราบปรามอาชญากรรมทางเศรษฐกิจ ได้มี

การแบ่งประเภทของอาชญากรรมทางเศรษฐกิจ ตามอำนาจหน้าที่รับผิดชอบของหน่วยงานในสังกัด เป็น 3 ประเภท คือ (บก.ปอศ. , 2561)

1) การกระทำความผิดเกี่ยวกับภาษี

2) การกระทำความผิดเกี่ยวกับการละเมิดทรัพย์สินทางปัญญา

3) การกระทำความผิดเกี่ยวกับการเงินการธนาคาร

นอกจากหน่วยงานราชการที่มีหน้าที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมทางเศรษฐกิจแล้ว (วีระพงษ์ บุญโญภาส , 2552) ได้แบ่งกลุ่มของอาชญากรรมทางเศรษฐกิจดังนี้

1) อาชญากรรมที่เกี่ยวกับการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์ การฉ้อโกงประชาชนและการกู้ยืมอันเป็นการฉ้อโกงประชาชน ได้แก่

1.1) การกระทำผิดเกี่ยวกับตลาดทุน

1.2) การฉ้อโกงของบริษัทประกันภัย

1.3) การล้มละลายโดยการฉ้อฉล

1.4) การฉ้อโกงค่าธรรมเนียมการโอนเงินข้ามชาติ

1.5) อาชญากรรมคอมพิวเตอร์

1.6) การกระทำผิดที่เกี่ยวกับห้างหุ้นส่วนบริษัท

1.7) แชร์ลูกโซ่

2) อาชญากรรมที่เกี่ยวกับการเงินและเครดิต ได้แก่

2.1) การกระทำความผิดเกี่ยวกับตลาดเงิน

2.2) การกระทำความผิดเกี่ยวกับเงินนอกระบบ

2.3) การกระทำความผิดเกี่ยวกับธุรกิจเงินสดทันใจ

2.4) การกระทำความผิดเกี่ยวกับเงินกู้ จำนอง ขายฝาก

2.5) การกระทำความผิดเกี่ยวกับธุรกิจเช่าซื้อ

2.6) การกระทำความผิดเกี่ยวกับบัตรเครดิต

2.7) การกระทำผิดในลักษณะของธนาคารใต้ดินหรือโพยก๊วน

2.8) การกระทำความผิดในลักษณะของการค่าเงินเถื่อน

3) อาชญากรรมเศรษฐกิจรูปแบบอื่นๆ

3.1) การโจรกรรมรถยนต์

3.2) การลักลอบหลบหนีศุลกากร

3.3) การละเมิดลิขสิทธิ์

3.4) การค้าขายอิเล็กทรอนิกส์บนเครือข่ายอินเทอร์เน็ต

3.5) อาชญากรรมทางเศรษฐกิจกับการทุจริตค่าใช้จ่ายขององค์กรภาครัฐ

2.2.3 อาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือกับความเป็นอาชญากรรมทางเศรษฐกิจ

การนำบิทคอยน์ไปใช้ในการกระทำความผิดอาจมีลักษณะเป็นอาชญากรรมเศรษฐกิจในกรณีต่างๆ เช่น การหลอกลวงฉ้อโกงให้เหยื่อนำเงินมาลงทุนเก็งกำไรในมูลค่าของบิทคอยน์ แต่แท้จริงเป็นการกระทำความผิดในลักษณะของแชร์ลูกโซ่จนทำให้เกิดความเสียหายต่อประชาชนเป็นจำนวนมาก ซึ่งการกระทำความผิดดังกล่าวจะส่งผลทางเศรษฐกิจต่อประเทศและสังคมโดยรวม ดังนี้ (ณรัณ โพธิ์พัฒนชัย, 2561)

1) ด้านเสถียรภาพทางการเงินและเศรษฐกิจ

การนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมที่เกี่ยวกับการเก็งกำไรอาจส่งผลทางใดทางหนึ่งให้มีโอกาสที่จะทำให้เกิดภาวะการพุ่งทะยานหรือการปรับตัวลดลงอย่างกระทันหันของมูลค่าของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่มีความผันผวนสูง ซึ่งเมื่อเกิดภาวะดังกล่าวขึ้นก็จะส่งผลทำให้เกิดการขาดสภาพคล่องในตลาดซื้อขายสกุลเงินเข้ารหัส และจะส่งผลโดยตรงต่อเสถียรภาพทางการเงินของประเทศในภาพรวมอีกด้วย เช่น หากมีการโจมตีในลักษณะของการปั่นราคา การโจมตีหรือเจาะระบบ การขโมยสกุลเงินเข้ารหัสต่างๆในปริมาณมหาศาล การฉ้อโกงกันในการลงทุนหรือซื้อขายแลกเปลี่ยนบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ หรือการกระทำอื่นๆที่มีผลต่อความเชื่อถือในการลงทุนอันส่งผลทำให้มูลค่าของบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆเกิดการปรับตัวลดลงอย่างรวดเร็วทำให้นักลงทุนได้รับความเสียหาย กรณีที่นักลงทุนใช้บริการเงินทุนกู้ยืมจากสถาบันการเงินต่างๆ ก็จะส่งผลให้เกิดเป็นหนี้เสียและทำให้สถาบันการเงินต่างๆได้รับผลกระทบด้วย อีกทั้งหากกรณีที่นักลงทุนประกอบธุรกิจที่เกี่ยวข้องกันหลายกลุ่มธุรกิจหรือหลายภาคส่วนย่อมทำให้ส่งผลกระทบเป็นวงกว้าง

ในขณะที่ภาครัฐไม่สามารถแทรกแซงเข้าไปควบคุมราคาได้อย่างกรณีของสินทรัพย์อื่นๆ ทำให้เกิดผลกระทบต่อเสถียรภาพทางการเงินและเศรษฐกิจในภาพรวมได้

2) ด้านสถานะทางการเงินของประชาชนทั่วไป

ในกรณีของการก่ออาชญากรรมทางเศรษฐกิจในลักษณะของแชร์ลูกโซ่ (Ponzi Scheme) ที่เกี่ยวข้องกับบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ ในลักษณะของการนำชื่อ “บิทคอยน์” มาหลอกลวงให้เหยื่อซึ่งเป็นนักลงทุนมือใหม่หรือผู้ที่ยังขาดประสบการณ์และองค์ความรู้ที่เกี่ยวข้องนำเงินมาร่วมลงทุนโดยอ้างว่าจะมีการลงทุนเก็งกำไรจากมูลค่าของบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ รวมทั้งในกรณีของการหลอกลวงว่าจะมีการลงทุนในการขุดบิทคอยน์ ซึ่งการดำเนินการในลักษณะนี้มักเป็นการประกอบกิจการที่เป็นการหลอกลวงประชาชน ทำให้มีจำนวนผู้ที่หลงเชื่อและได้รับความเสียหายเป็นมูลค่ามหาศาลและเกิดขึ้นในวงกว้าง เช่น กรณีที่ผู้กระทำผิดสามารถหลอกลวงเหยื่อให้นำเงินมาร่วมลงทุนได้เป็นจำนวนมาก และมีการจ่ายเงินปันผลตามที่ได้ตกลงกันไว้ไประยะหนึ่ง จนกระทั่งต่อมาได้มีการปิดกิจการ หยุดจ่ายเงินปันผลแล้วหลบหนีไปอย่างกระทันหัน ทำให้ผู้ที่หลงเชื่อได้สูญเสียเงินทุน จนอาจทำให้เกิดเป็นปัญหาความยากจนในระดับจุลภาค ส่งผลให้เกิดปัญหาทางด้านสังคม ปัญหาครอบครัว และส่งผลให้เกิดปัญหาอาชญากรรมในที่สุด

ทั้งนี้ การกระทำความผิดที่เกี่ยวกับการปั่นราคา การโจมตีหรือเจาะระบบ การขโมยสกุลเงินเข้ารหัสหรือการฉ้อโกงกันในการลงทุนหรือซื้อขายแลกเปลี่ยน และการกระทำความผิดในลักษณะของการนำชื่อเสียงของบิทคอยน์หรือสกุลเงินเข้ารหัสมาใช้ในการกระทำความผิดในทางอ้อม อย่างกรณีของแชร์ลูกโซ่ (Ponzi Scheme) ที่เป็นเพียงการนำชื่อของบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆมาอ้างถึง เพื่อจูงใจให้เหยื่อหลงเชื่อนั้น ไม่อยู่ในขอบเขตของการศึกษาวิจัยในครั้งนี้ เนื่องจากในมุมมองของผู้วิจัยแล้ว การกระทำผิดในลักษณะดังกล่าวนี้ บิทคอยน์และสกุลเงินเข้ารหัสต่างๆไม่ได้ถูกนำมาใช้อย่างแท้จริง หรืออีกนัยหนึ่งแล้วบิทคอยน์และสกุลเงินเข้ารหัสไม่ใช่สาระสำคัญของการกระทำผิดแต่อย่างใด เพียงแต่เป็นการฉ้อโกงในทางธุรกิจที่สามารถเกิดขึ้นได้กับทุกผลิตภัณฑ์การลงทุนที่ได้รับความนิยม หรือมีลักษณะเป็นเพียงการอาศัยชื่อของสินทรัพย์ซึ่งได้รับความนิยมในด้านการลงทุนที่จะแตกต่างกันไปตามช่วงเวลาต่างๆมาใช้ให้เข้ากับกระแสความสนใจของประชาชน ซึ่งในอนาคตรูปแบบของพฤติกรรมการกระทำผิดในลักษณะนี้ก็จะมีลักษณะไม่แตกต่างจากเดิม แต่จะมีการเปลี่ยนเป้าหมายหรือชื่อสินทรัพย์ที่ใช้ในการหลอกลวง เช่น จากในอดีตที่มีการฉ้อโกงและหลอกลวงลงทุนในราคาทองคำ น้ำมัน ธุรกิจขายตรง หรือ เปลี่ยนจากบิทคอยน์เป็นสินทรัพย์รูปแบบ

ใหม่ที่จะเกิดขึ้นในอนาคต เป็นต้น โดยในหัวข้อนี้ผู้วิจัยเพียงต้องการนำเสนอถึงมุมมองและผลกระทบที่อาจเกิดขึ้นจากการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในมิติของอาชญากรรมทางเศรษฐกิจ เพื่อให้เกิดความรู้ความเข้าใจถึงสภาพปัญหาได้อย่างครบถ้วนในทุกมิติ

2.3 แนวคิดเกี่ยวกับอาชญากรรมข้ามชาติ (Transnational Crime)

2.3.1 ความหมายของอาชญากรรมข้ามชาติ

แนวคิดเกี่ยวกับอาชญากรรมข้ามชาติเกิดขึ้นในช่วงปี ค.ศ. 1980 ที่เป็นช่วงของการเกิดขบวนการลักลอบค้ายาเสพติดข้ามชาติขึ้นเป็นจำนวนมาก ส่งผลให้หลายประเทศต้องดำเนินนโยบายในการประกาศสงครามยาเสพติดขึ้น ขณะเดียวกันอาชญากรรมประเภทต่างๆเริ่มมีการพัฒนาเปลี่ยนแปลงรูปแบบไปสู่การกระทำที่มีลักษณะต่อเนื่องกันหลายประเทศ เช่น การลักลอบขนส่งอาวุธเถื่อน การปล้น การก่อการร้าย การโจมตีค่าเงินในรูปแบบต่างๆ จนทำให้นักวิชาการที่ศึกษาเกี่ยวกับอาชญากรรมเริ่มหันมาสนใจและพยายามเสนอแนวคิดและความหมายของ “อาชญากรรมข้ามชาติ” ขึ้นโดยในปี ค.ศ.1990 อังเดร บอซซาด (Andre Bossard) ได้ให้คำนิยามไว้ในหนังสือเรื่อง อาชญากรรมข้ามชาติกับกฎหมายอาญา (Transnational Crime and Criminal Law) ไว้ว่า หมายถึง “การกระทำที่ได้กระทำลงและถูกพิจารณาว่าเป็นอาชญากรรมจากประเทศต่างๆอย่างน้อยสองประเทศ” ซึ่งเป็นผลมาจากการพัฒนาของระบบขนส่ง,โทรคมนาคมและการติดต่อสื่อสาร และ ระบบอินเทอร์เน็ตและคอมพิวเตอร์ ต่อมาองค์การสหประชาชาติ (United Nations) จึงได้ให้คำนิยามของอาชญากรรมข้ามชาติ ไว้ในอนุสัญญาสหประชาชาติว่าด้วยการต่อต้านองค์กรอาชญากรรมข้ามชาติ (UN Convention against Transnational Organized Crime) ว่าเป็นการกระทำผิดที่มีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้ (United Nations, 2000)

1) การกระทำผิดที่ได้กระทำลงมากกว่าหนึ่งรัฐ

2) การกระทำผิดได้กระทำลงในรัฐหนึ่ง แต่ส่วนสำคัญของการกระทำผิด เช่น การเตรียมการ การวางแผน หรือการควบคุมการกระทำผิดนั้นๆอยู่ในอีกรัฐหนึ่ง

3) การกระทำผิดที่ได้กระทำลงในรัฐหนึ่ง แต่มีส่วนเกี่ยวข้องกับองค์กรอาชญากรรมที่มีพฤติกรรมเกี่ยวข้องกับอาชญากรรมต่างๆในพื้นที่มากกว่าหนึ่งรัฐ

4) การกระทำผิดได้ทำลงในรัฐหนึ่ง แต่ผลเสียหายหลักไปเกิดกับอีกรัฐหนึ่งหรือหลายรัฐ

2.3.2 อาชญากรรมข้ามชาติกับความเป็นองค์กรอาชญากรรม

มีนักวิชาการเป็นจำนวนมากมีความเห็นว่า การกระทำความผิดที่มีลักษณะเป็นอาชญากรรมข้ามชาตินั้นมักจะเกิดจากการกระทำขององค์กรอาชญากรรม หรืออาจกล่าวถึงอาชญากรรมประเภทนี้ว่าเป็น “องค์กรอาชญากรรมข้ามชาติ” แทนที่จะกล่าวถึงอาชญากรรมข้ามชาติเพียงอย่างเดียว (Fijnaut, 2000) แต่เมื่อกล่าวถึงความเป็นมาของการศึกษาองค์กรอาชญากรรมในประเทศสหรัฐอเมริกานั้น จะพบว่าในยุคที่สหรัฐอเมริกานั้นต่อสู้กับปัญหายาเสพติด จนเริ่มเกิดแนวคิดเกี่ยวกับปัญหาองค์กรอาชญากรรม ได้เริ่มต้นจากการมองปัญหาเกี่ยวกับกลุ่มชาติพันธุ์ที่อพยพเข้ามาในพื้นที่แล้วพยายามที่จะต่อต้านสังคมเดิมหรือพยายามที่จะเข้าควบคุมจัดการสังคมใหม่นั้นๆ จนเกิดการพัฒนาไปเป็นกลุ่มผู้มีอิทธิพลหรือมาเฟียไปในที่สุด รูปแบบ (Model) ของการเกิดองค์กรอาชญากรรมลักษณะนี้ ถูกนำมาเป็นต้นแบบในการอธิบายการเกิดขึ้นขององค์กรอาชญากรรมมาโดยตลอด มาจนถึงปัจจุบันที่ความหมายของ “องค์กรอาชญากรรม” หมายถึง กลุ่มของอาชญากรที่มีการจัดการระบบการกระทำผิดในลักษณะขององค์กร เช่น มีการจัดลำดับศักดินา หรือ ลำดับการบังคับบัญชา ,มีกฎระเบียบปฏิบัติและข้อห้าม, มีหลักเกณฑ์และวิธีการในการกระทำความผิด และ มีเจตจำนงร่วมกันที่จะใช้ความรุนแรง เป็นต้น ซึ่งถ้าพิจารณาตามความหมายนี้แล้วก็จะพบว่าอาชญากรรมที่เกิดขึ้นในปัจจุบันนั้น มีจำนวนไม่มากนักที่จะมีลักษณะเป็น “องค์กรอาชญากรรม” จริงๆ เมื่อเป็นอย่างนั้น การนำอาชญากรรมข้ามชาติไปรวมกับองค์กรอาชญากรรมจึงอาจไม่ถูกต้องเสมอไปนัก

อาชญากรรมข้ามชาติอาจไม่จำเป็นจะต้องอาศัยลักษณะของความเป็นองค์กรที่เข้มแข็งอย่างองค์กรอาชญากรรมเสมอไป แต่อาชญากรรมข้ามชาติสามารถกระทำได้เพียงอาศัย **เครือข่าย (Networks)** เครื่อข่ายในที่นี้ หมายถึง การเชื่อมต่อกันหรือการติดต่อสื่อสารกันระหว่างผู้กระทำผิดส่วนต่างๆ ไม่ว่าจะเป็นเครือข่ายขนาดใหญ่หรือเล็ก จะเป็นเครือข่ายในท้องถิ่นหรือเครือข่ายทั่วโลก หรือจะเชื่อมต่อโดยตรงจากศูนย์กลางหรือไม่ก็ตาม โดยอาชญากรรมข้ามชาติที่มีความเป็นเครือข่าย เช่น การลักลอบค้ายาอีที่มีการขนส่งส่วนผสมและสารตั้งต้นมาจากประเทศเยอรมันและจีน เพื่อนำไปทำการอัดเม็ดขึ้นรูปที่เนเธอร์แลนด์และเบลเยี่ยม จากนั้นจึงถูกส่งต่อไปขายในออสเตรเลีย และนำผลประโยชน์ที่ได้ไปฟอกเงินที่หมู่เกาะเวอร์จิ้น เป็นต้น จะเห็นว่าการกระทำลักษณะนี้ ก็ถือเป็นอาชญากรรมข้ามชาติ ที่ไม่ได้มีรูปแบบขององค์กรอาชญากรรมแต่อย่างใด

2.3.3 ประเภทของอาชญากรรมข้ามชาติ

ซีริล ฟินอท (Cyrille Fijnaut) นักกฎหมายและนักวิชาการทางด้านอาชญาวิทยา ได้ทำการศึกษาเกี่ยวกับอาชญากรรมข้ามชาติ โดยในบทความเรื่อง “Transnational Crime and the Role of the United Nations in its Containment through International Cooperation: A Challenge for the 21st Century” ได้มีการแบ่งประเภทอาชญากรรมข้ามชาติตามลักษณะของการกระทำไว้ ดังนี้ (Fijnaut, 2000)

1) กลุ่มอาชญากรที่มีการจัดการในรูปแบบขององค์กร (Organized Crime) ได้แก่ การลักลอบนำเข้าส่งออกและค้าขายสิ่งผิดกฎหมายทุกประเภท โดยเฉพาะอย่างยิ่ง พวกกลุ่มยาสูบ เครื่องดื่มแอลกอฮอล์ และเนื้อสัตว์

2) กลุ่มที่มีลักษณะเป็นองค์การถูกกฎหมาย แต่มีการกระทำผิดอยู่เบื้องหลัง (Corporate Crime) เช่น การเลี่ยงภาษีและการฉ้อโกงประกันสังคม, การปั่นและแทรกแซงกลไกการตลาด, การประทุษร้ายและการทุจริตต่อสิทธิครอบครองพื้นที่, การจารกรรมข้อมูลคู่แข่ง, การทิ้งขยะหรือสิ่งปฏิกูลมีพิษ และการนำเข้าหรือส่งออกพันธุ์ไม้หายากใกล้สูญพันธุ์ เป็นต้น

3) อาชญากรรมอาชีพ (Professional Crime) เช่น การปล้น การฉ้อโกง การลักพาตัว โจรสลัด การลักลอบส่งออกวัตถุโบราณ การละเมิดลิขสิทธิ์เครื่องหมายการค้า การฉ้อโกงประกันภัย การปลอมธนบัตร และการปลอมแปลงเอกสาร เป็นต้น

4) อาชญากรรมการเมือง (Political Crime) ซึ่งรวมถึงการก่อการร้าย และการใช้กลอุบายในการใช้มาตรการลงโทษของสหประชาชาติ และการฆ่าล้างเผ่าพันธุ์

2.3.4 อาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือกับความเป็นอาชญากรรมข้ามชาติ

ด้วยคุณลักษณะของบิทคอยน์ที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ซึ่งมีการทำงานอยู่บนระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ ทำให้เป็นการยากที่จะพิสูจน์ว่าการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการกระทำความผิดนั้น คนร้ายกระทำจากที่ใด หรือภายในประเทศใด อย่างไรก็ตามการกระทำผิดในลักษณะดังกล่าวนั้นมีโอกาสที่จะมีลักษณะเป็นอาชญากรรมข้ามชาติได้ เช่นในกรณีของการใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมายอย่างในกรณีของการลักลอบซื้อขายยาเสพติดข้ามชาติโดยใช้บิทคอยน์ชำระแทนเงินสกุลจริง เป็นต้น

2.4 ทฤษฎีคิดก่อนกระทำผิด (Rational Choice Theory)

ทฤษฎีคิดก่อนกระทำผิด (Rational Choice Theory) ได้ถูกนำเสนอสู่วงการอาชญาวิทยาโดยนักเศรษฐศาสตร์ ได้แก่ แกรี เบเกอร์ (Gary Becker) และ โรเบิร์ต ครอท (Robert Crouch) ทฤษฎีดังกล่าวนี้ได้รับอิทธิพลมาจากหลักปรัชญาของสำนักอาชญาวิทยาดั้งเดิมที่มีแนวคิดสำคัญเกี่ยวกับธรรมชาติของมนุษย์ 3 ประการ คือ 1) มนุษย์มีอิสระในการเลือกพฤติกรรมหรือมีเจตจำนงอิสระ (Free Will) 2) มนุษย์มีความสามารถในการใช้เหตุและผลในการตัดสินใจกระทำการใดๆ (Rationality) 3) มนุษย์คำนึงถึงผลประโยชน์ที่จะได้รับสูงสุดจากการกระทำต่างๆ (Utility) โดยนักอาชญาวิทยาแนวทฤษฎีคิดก่อนทำนี้ ได้นำหลักการของสำนักอาชญาวิทยาดั้งเดิมดังกล่าวไปพัฒนาและสร้างเป็นสมมติฐานที่อธิบายถึงพฤติกรรมการกระทำผิดของอาชญากรสองประการ คือ (พรชัย ขันตี, 2558)

1) บุคคลเป็นผู้มีอิสระในการเลือกที่จะกระทำผิดกฎหมาย

2) แนวทางในการเลือกพฤติกรรมการกระทำผิดกฎหมายนี้ ขึ้นอยู่กับความพึงพอใจหรือผลประโยชน์สูงสุดที่จะได้รับจากการกระทำความผิดนั้น โดยผลประโยชน์ดังกล่าว ไม่จำกัดว่าจะต้องเป็นทรัพย์สินเงินทองเท่านั้น แต่หมายความรวมถึงผลประโยชน์หรือความพึงพอใจทางด้านจิตใจด้วย

จากสมมติฐานของทฤษฎีดังกล่าว สามารอธิบายได้ว่า ก่อนที่อาชญากรจะตัดสินใจกระทำความผิดจะมีการใช้เหตุผลเพื่อคิดไตร่ตรองและชั่งน้ำหนัก โดยจะคิดคำนวณถึงผลที่จะตามมาภายหลังจากได้ก่ออาชญากรรมไปแล้ว เช่น ผลประโยชน์ที่จะได้รับ ความเป็นไปได้ที่จะถูกจับกุม อัตราโทษที่จะได้รับหากถูกพิจารณาคดี ตลอดจนจะพิจารณาทางเลือกอื่นๆที่ถูกกฎหมายด้วย (พรชัย ขันตี, 2558) โดยหากอาชญากรได้คำนวณเปรียบเทียบแล้วว่า ผลประโยชน์ที่จะได้รับจากการกระทำความผิดทำให้ตนได้รับความสุขมากกว่าโทษที่จะได้รับหรือผลประโยชน์ดังกล่าวเป็นที่ต้องการต่อตนมากพอจนทำให้เกิดความคุ้มค่าที่จะเสี่ยง หรือ มีโอกาสสูงที่จะกระทำความผิดได้สำเร็จ หรือ มีโอกาสหลบหนีการจับกุมได้สูง อาชญากรก็จะตัดสินใจกระทำความผิด

นอกจากการคิดคำนวณเพื่อชั่งน้ำหนักถึงผลประโยชน์และโทษที่จะได้รับจากการกระทำความผิดแล้ว อาชญากรยังมีการคิดไตร่ตรองอย่างมีเหตุผลเพื่อพิจารณาถึงโอกาสที่จะกระทำความผิดสำเร็จจากปัจจัยสองประการคือ (Larry J. Siegel, 2016)

1) ปัจจัยด้านสถานการณ์ในการกระทำความผิด (Offense Specific) หมายถึง ในการก่ออาชญากรรมแต่ละครั้ง อาชญากรจะพิจารณาถึงสภาพแวดล้อมและสภาวการณ์ต่างๆ เพื่อพิจารณาถึงความเป็นไปได้ที่จะก่อเหตุสำเร็จ ตัวอย่างเช่น หากจะเข้าไปโจรกรรมภายในบ้านพักของเหยื่อนั้น อาชญากรจะพิจารณาประเด็นต่างๆ เช่น

- ประเมินตัวเหยื่อ ว่าจะมีการต่อสู่ขัดขวางหรือไม่
- บ้านที่จะก่อเหตุมีการติดตั้งกล้องวงจรปิดหรือสัญญาณกันโขมยหรือไม่
- มีตำรวจสายตรวจออกตรวจตราอยู่ในละแวกที่จะก่อเหตุหรือไม่
- มีความเป็นไปได้ว่าจะถูกจับกุมมากน้อยเพียงใด
- จะสามารถนำทรัพย์สินที่ได้จากการปล้นไปขายได้หรือไม่ และจะนำไปขายที่ไหน
- จะมีจำนวนผู้พักอาศัยอยู่ในบ้านจำนวนเท่าใด
- จะมีเพื่อนบ้านในละแวกนั้น พบเห็นหรือได้ยินเสียงการกระทำผิดหรือไม่
- มีสุนัขเฝ้าอยู่ในบริเวณบ้านหรือไม่
- ภายหลังก่อเหตุแล้ว สามารถหลบหนีไปด้วยเส้นทางใด
- มีทางเข้าและทางออกจากบ้านเป้าหมายกี่จุด

2) ปัจจัยส่วนตัวของผู้กระทำความผิด (Offender Specific) หมายถึง ในการกระทำผิดครั้งหนึ่ง นอกจากอาชญากรจะพิจารณาถึงปัจจัยด้านสถานการณ์ที่เป็นสภาวะแวดล้อมต่างๆแล้ว อาชญากรจะพิจารณาถึงปัจจัยส่วนตัวต่างๆของตนเองก่อนที่จะตัดสินใจกระทำความผิด เช่น

- ตนเองมีทักษะ ความชำนาญที่จำเป็นในการก่ออาชญากรรมหรือไม่
- มีอุปกรณ์ที่จะใช้ในการก่ออาชญากรรมเพียงพอหรือไม่
- ความกลัวที่จะถูกจับกุมและถูกลงโทษมีมากน้อยเพียงใด
- ความพร้อมทางด้านกายภาพ เช่น สุขภาพร่างกาย ความแข็งแรง
- ความจำเป็นที่ต้องการเงินหรือสิ่งของมีค่า ณ ขณะนั้น เป็นอย่างไร
- มีช่องทางอื่นที่สามารถได้เงินหรือทรัพย์สินที่ต้องการโดยไม่ต้องกระทำความผิดหรือไม่
- มีวิธีการกระทำผิดอื่น ที่ตนสามารถกระทำได้สำเร็จมากกว่าหรือไม่

โดยหลังจากที่ได้มีการคิดคำนวณตามปัจจัยต่างๆที่กล่าวมาแล้ว อาชญากรจึงจะตัดสินใจว่าจะประกอบอาชญากรรมหรือไม่

จากสมมติฐานและแนวคิดของนักทฤษฎีคิดก่อนกระทำผิดตามที่ได้กล่าวมาแล้ว ทำให้สามารถอธิบายได้ว่า **โครงสร้างของอาชญากรรม**ตามแนวคิดทฤษฎีดังกล่าวมีองค์ประกอบ 2 ประการ คือ (Larry J. Siegel, 2016) (สุดสงวน สุธีสร, 2547)

1) การเลือกสถานที่ในการประกอบอาชญากรรม (Choosing the Place of Crime) หมายถึง อาชญากรจะมีการพิจารณาอย่างถี่ถ้วนเพื่อจะเลือกสถานที่ที่จะทำให้การก่ออาชญากรรมสำเร็จ ตัวอย่างเช่น เด็กเดินยาจะเลือกนัดรับส่งยาที่บริเวณกลางซอยแคบที่สามารถมองเห็นได้ตั้งแต่ต้นถึงท้ายซอย เพราะตนจะสามารถเห็นเจ้าหน้าที่ตำรวจและสามารถหลบหนีได้ก่อนที่เจ้าหน้าที่ตำรวจจะมาถึงตัว เป็นต้น

2) การเลือกเป้าหมายในการประกอบอาชญากรรม (Choosing Targets) หมายถึง นอกจากอาชญากรจะมีการเลือกสถานที่เพื่อให้สามารถกระทำผิดได้สำเร็จแล้ว อาชญากรยังมีการพิจารณาเลือกเป้าหมายที่จะทำให้โอกาสในการกระทำผิดสำเร็จมีมากขึ้น เช่น หากอาชญากรจะทำการลักลอบเข้าไปลักทรัพย์ภายในบ้านก็จะพิจารณาเลือกบ้านเป้าหมายที่ไม่มีคนอยู่ ไม่มีสุนัข หรือไม่มีระบบการรักษาความปลอดภัย เป็นต้น

จากแนวคิดของทฤษฎีคิดก่อนกระทำผิด (Rational Choice Theory) สามารถอธิบายการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมได้ว่า เพราะผู้กระทำผิดได้คิดไตร่ตรองและชั่งน้ำหนักอย่างมีเหตุผลแล้วว่า ตนจะได้รับผลประโยชน์และสามารถรอดพ้นจากการตรวจสอบจับกุมโดยเจ้าหน้าที่ของรัฐได้ด้วยคุณลักษณะพิเศษของบิทคอยน์ที่ไม่ระบุตัวตนเจ้าของบัญชีที่แท้จริง เช่น อาชญากรที่ทำการเรียกค่าไถ่ได้ทำการชั่งน้ำหนักแล้วว่า หากเรียกร้องให้มีการชำระค่าไถ่เป็นบิทคอยน์ จะทำให้เจ้าหน้าที่ตำรวจไม่สามารถติดตามเส้นทางทางการเงินได้โดยง่าย และถึงแม้ติดตามได้ก็ไม่สามารถยืนยันตัวตนเจ้าของบัญชีบิทคอยน์ได้ ทำให้อาชญากรได้รับผลประโยชน์และประเมินว่ามีโอกาสรอดพ้นจากการจับกุมสูงจึงตัดสินใจกระทำความผิด เป็นต้น

2.5 ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory)

ทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) เป็นอีกทฤษฎีหนึ่งที่มีรากฐานแนวคิดมาจากสำนักคิดอาชญาวิทยาดั้งเดิม อีกทั้งทฤษฎีนี้ยังเหมือนเป็นทฤษฎีที่ตอบรับกันกับทฤษฎีคิดก่อนกระทำผิด เพราะทั้งสองทฤษฎีกล่าวถึงความสัมพันธ์ของการเกิดอาชญากรรมกับโอกาส กล่าวคือ

ในกรณีของทฤษฎีคิดก่อนกระทำผิดอาชญากรได้คิดพิจารณาชั่งน้ำหนักถึงโอกาสที่จะกระทำผิดสำเร็จและคิดพิจารณาถึงผลประโยชน์สูงสุดที่จะได้รับจากการกระทำผิด ขณะที่แนวคิดของทฤษฎีนี้นั้นมีนักอาชญาวิทยา คือ ลอวเรนซ์ โคเฮน และ มาร์คัส เฟลสัน (Lawrence E. Cohen and Marcus Felson) เสนอแนวคิดของทฤษฎีนี้ว่า อาชญากรรมเป็นผลของการมีวิถีชีวิตหรือพฤติกรรมการใช้ชีวิตของคนในสังคมที่เกิดขึ้นซ้ำๆกันเป็นประจำสม่ำเสมอจนกลายเป็นกิจวัตร (Routine Activity) เช่น พฤติกรรมการเดินทาง เข้า – ออกจากบ้านเพื่อเดินทางไปทำงานหรือเรียนหนังสือในช่วงเวลาเดิมซ้ำๆกันทุกวัน จนทำให้อาชญากรที่เฝ้าสังเกตุและรอโอกาสที่จะก่อเหตุสามารถทราบได้ว่าช่วงเวลาใดที่ในบ้านเป้าหมายจะไม่มีคนอยู่บ้าน หรือ กรณีของการเดินทางด้วยรถประจำทางจากป้ายรถประจำทางเดิมซ้ำๆกันทุกวัน และใช้เวลาการเดินทางเช่นเดิมเหมือนปกติทุกวันจนทำให้อาชญากรที่เฝ้าสังเกตุอยู่ทราบทันทีว่า หากมาดักรอเหยื่อในเวลาและสถานที่ดังกล่าว ก็จะสามารถพบเหยื่อได้อย่างแน่นอน

จากแนวคิดดังกล่าวโคเฮนและเฟลสันจึงวิเคราะห์ว่า อาชญากรจะตัดสินใจก่ออาชญากรรมก็ต่อเมื่อได้ทราบถึงกิจวัตรประจำวันของเหยื่อตามที่ได้กล่าวมาแล้ว ประกอบกับการวิเคราะห์ถึงโอกาสที่จะกระทำผิดสำเร็จจากองค์ประกอบ 3 ประการตามภาพนี้

องค์ประกอบของการเกิดอาชญากรรม	*ความหมาย*	*แนคิดในทางอาชญาวิทยา*
มีผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender)	บุคคลที่มีนิสัยหรือแนวโน้มที่พร้อมจะก่ออาชญากรรมอยู่ก่อนแล้ว และได้แรงรับกระตุ้นจากองค์ประกอบต่างๆ	เมื่ออาชญากรได้รับแรงจูงใจที่จะก่ออาชญากรรมแล้ว ก็จะตัดสินใจลงมือทำโดยที่ไม่จำเป็นจะต้องสนใจหรือพิจารณาองค์ประกอบอื่นๆอย่างเหยื่อที่เหมาะสมหรือการขาดความสามารถในการป้องกัน
เป้าหมายที่เหมาะสม (Suitable Target)	สิ่งของ บุคคล ทรัพย์สินต่างๆ ที่คนร้ายต้องการครอบครอง	อาชญากรรมจะไม่เกิดขึ้นหากไม่มีเหยื่อที่เหมาะสม โดยที่ความเหมาะสมในที่นี้อาจหมายถึง มีลักษณะเอื้อให้กระทำความผิดเช่น สร้างมูลค่าให้ได้อย่างเงิน หรือสามารถเคลื่อนย้ายได้ง่าย เช่น เครื่องคอมพิวเตอร์
การขาดความสามารถในการป้องกันเป้าหมาย (Absence of a Capable Guardian	ผู้ป้องกันอาจเป็นได้ทั้งกลุ่มเพื่อน ครอบครัว เจ้าหน้าที่รักษาความปลอดภัยส่วนบุคคล หรือแม้กระทั่งสุนัข รวมทั้งตนเองสามารถเป็นผู้พิทักษ์ความปลอดภัยของตนเองและทรัพย์สิน	การมีการป้องกันที่ดีจะสามารถป้องกันอาชญากรรมได้ ขณะที่หากขาดการป้องกันแล้วอาชญากรรมจะเกิดขึ้น

ภาพที่ 3 แนวคิดองค์ประกอบของการเกิดอาชญากรรมตามแนวคิดทฤษฎีกิจวัตรประจำวัน (Rountine Activity Theory) ของโคเฮนและเฟลสัน

(ประยุกต์จาก Lawrence E. Cohen and Marcus Felson, 1979 อ้างถึงใน J. Robert Liily, Francis T. Cullen and Richard A. Ball, 2011)

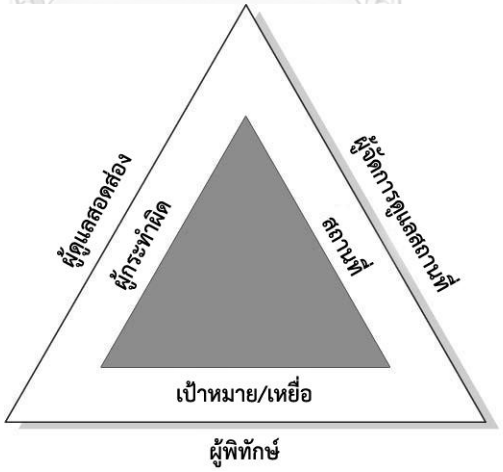
จากภาพดังกล่าวสามารถอธิบายได้ว่าอาชญากรจะก่ออาชญากรรมเมื่อองค์ประกอบทั้งสามประการเกิดขึ้นครบถ้วนได้แก่

1) มีผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender) หมายถึง ผู้กระทำผิดที่มีเหตุผลหรือความต้องการส่วนตัวเป็นแรงผลักดัน ทำให้มีความพร้อมและต้องการที่จะก่ออาชญากรรมอยู่ตลอดเวลา

2) มีเป้าหมายที่เหมาะสม (Suitable Target) หมายถึง บุคคล สถานที่ ทรัพย์สินหรือวัตถุสิ่งของมีค่าต่างๆ ที่มีลักษณะสอดคล้องกับความต้องการของผู้กระทำผิด และมีลักษณะที่เอื้อประโยชน์ต่อความสำเร็จในการกระทำผิด เช่น สามารถนำทรัพย์เป้าหมายไปขายหรือแลกเปลี่ยนเป็นเงินสดได้ง่าย หรือ สามารถนำทรัพย์สินนั้นหลบหนีไปได้ง่าย (เช่น ตามตัวอย่างที่ได้มีการเปรียบเทียบทรัพย์ที่เป็นเป้าหมายระหว่างเครื่องคอมพิวเตอร์ กับ ตู้เย็น ว่าคนร้ายจะสามารถเคลื่อนย้ายเครื่องคอมพิวเตอร์ได้ง่ายกว่าการลักขโมยตู้เย็น เป็นต้น)

3) การขาดความสามารถในการป้องกันเป้าหมาย (Absence of a Capable Guardian) โดยที่การป้องกันเป้าหมายนี้ อาจเป็นการป้องกันโดยกลุ่มเพื่อน ครอบครัว เจ้าหน้าที่รักษาความปลอดภัยส่วนตัว การใช้สุนัข หรือจะเป็นการป้องกันตนเองและทรัพย์สินของตนเองก็ได้ โดยหากการป้องกันต่างๆดังที่กล่าวมานี้มีประสิทธิภาพเพียงพอ ก็จะสามารถป้องกันการเกิดอาชญากรรมได้ ขณะเดียวกันถ้าการป้องกันเหล่านี้ไม่มีประสิทธิภาพ อาชญากรก็จะลงมือกระทำความผิด

ต่อมา จอหน์ เอ็ค (John E. Eck) จึงได้รับเอาแนวคิดเกี่ยวกับทฤษฎีกิจวัตรประจำวันไปพัฒนาจนเกิดเป็นแนวคิดในการอธิบายการเกิดอาชญากรรมและการป้องกันอาชญากรรมด้วย “สามเหลี่ยมอาชญากรรม (Crime Triangle)” ดังภาพต่อไปนี้



ภาพที่ 4 แนวคิดในการอธิบายการเกิดอาชญากรรมและการป้องกันอาชญากรรมด้วย
สามเหลี่ยมอาชญากรรม (Crime Triangle) ของจอหน์ เอ็ค (John E. Eck)
(ประยุกต์จาก J. Robert Liily, Francis T. Cullen and Richard A. Ball, 2011, P.339)

จากภาพสามเหลี่ยมอาชญากรรมดังกล่าว สามารถอธิบายได้ว่าอาชญากรรมจะเกิดขึ้นเมื่อผู้กระทำผิด (Offender) ที่มีแรงจูงใจและพร้อมที่จะกระทำความผิดอยู่แล้ว ตัดสินใจก่ออาชญากรรม เนื่องจากได้เล็งเห็นว่ามีเป้าหมายหรือเหยื่อ (Target/Victim) ซึ่งอาจจะเป็นบุคคลหรือทรัพย์สินที่มีลักษณะเป็นไปตามที่ผู้กระทำผิดต้องการ อยู่ในสถานที่ (Place) ที่เอื้อต่อการกระทำความผิดหรือปราศจากการคุ้มครองที่มีประสิทธิภาพ ตัวอย่างเช่น เมื่อมีคนร้ายซึ่งมีความต้องการในการลักทรัพย์ได้สังเกตุเห็นว่าร้านค้าทองแห่งหนึ่งจะนำทองคำรูปพรรณออกมาขาย ตามเวลาเปิด-ปิดร้านเป็นกิจวัตรประจำวันเหมือนกันทุกวัน ซึ่งทรัพย์ที่เป็นทองรูปพรรณนั้นเหมาะสมแก่การก่อเหตุเนื่องจากสามารถนำติดตัวหลบหนีไปได้ง่าย อีกทั้งยังสามารถนำไปขายเพื่อแลกเปลี่ยนเป็นเงินได้ทั่วไป โดยหากร้านค้าทองเป้าหมายไม่มีระบบการรักษาความปลอดภัย เช่น ไม่มีกล้องวงจรปิด ไม่มีประตูอัตโนมัติ ไม่มีเจ้าหน้าที่ตำรวจหรือเจ้าหน้าที่รักษาความปลอดภัยอยู่ในบริเวณร้าน ก็จะทำให้องค์ประกอบในการก่อเหตุครบถ้วนตามหลักสามเหลี่ยมอาชญากรรม และผู้กระทำผิดก็จะตัดสินใจปล้นทองรูปพรรณไปในที่สุด

ดังนั้นหากต้องการจะป้องกันอาชญากรรมตามแนวคิดนี้ ก็จำเป็นจะต้องทำให้องค์ประกอบใดองค์ประกอบหนึ่งไม่เกิดขึ้น โดยหากตัวผู้กระทำผิดเองได้รับความสุข ความอบอุ่น ความพอใจ ความรักจากคนรอบข้าง เช่น จากคนรัก ครอบครัว เพื่อนบ้าน ชุมชน สังคม หรือมีการดูแลติดตามสอดส่องอย่างใกล้ชิดของผู้ที่เกี่ยวข้อง (Handler) ก็จะทำให้ผู้กระทำผิดขาดแรงจูงใจ หรือไม่เกิดโอกาสหรือช่องว่างที่จะสามารถประกอบอาชญากรรมได้ ในขณะที่หากเป้าหมายหรือเหยื่อมีการป้องกันหรือเฝ้าระวังที่มีประสิทธิภาพ (Guardian) ก็จะทำให้คนร้ายหมดโอกาสที่จะก่ออาชญากรรม ประกอบกับหากสถานที่ที่เป็นเป้าหมาย มีการบริการหรือมีผู้บริการ (Manager) จัดการในเรื่องการรักษาความปลอดภัยที่ดี ก็จะทำให้ผู้กระทำผิดไม่กล้าก่อเหตุ ตัวอย่างเช่นในกรณีการปล้นทองรูปพรรณที่กล่าวมาแล้ว หากปรากฏว่าทองรูปพรรณซึ่งเป็นที่ต้องการของผู้กระทำผิด มีการพิทักษ์รักษาอย่างเข้มงวด มีเจ้าหน้าที่ตำรวจรักษาความปลอดภัยอยู่ภายในร้าน ตลอดจนสถานที่ร้านค้าทองเองก็มีมาตรการครบถ้วนทั้งกล้องวงจรปิด ประตูอัตโนมัติ มีการโครงเหล็กรักษาความปลอดภัยทรัพย์สิน มีสัญญาณกันขโมย ก็จะทำให้ผู้กระทำผิดไม่กล้าตัดสินใจก่อเหตุเนื่องจากแทบไม่มีโอกาสที่จะก่อเหตุสำเร็จได้แต่อย่างใด

จากแนวคิดของทฤษฎี**กิจวัตรประจำวัน (Routine Activity Theory) และแนวคิดเกี่ยวกับสามเหลี่ยมอาชญากรรม (Crime Triangle)** สามารถอธิบายการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมได้ว่า

1) อาชญากรมีแรงจูงใจพิเศษ (Motivated Offender) อันเกิดจากการที่อาชญากรกลุ่มนี้เป็นผู้ที่มีความรู้และความเชี่ยวชาญในเรื่องระบบคอมพิวเตอร์และเทคโนโลยีสมัยใหม่ จึงเล็งเห็นถึงประโยชน์ของการนำบิทคอยน์ซึ่งถือเป็นนวัตกรรมทางเทคโนโลยีสมัยใหม่ และมีคุณลักษณะพิเศษที่ไม่ระบุตัวตนที่แท้จริงของผู้ใช้งาน (Anonymity) มาใช้เป็นเครื่องมือในการก่ออาชญากรรม

2) การนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมในทางอ้อม เช่น การหลอกลวงชักชวนให้มีการลงทุนในมูลค่าของบิทคอยน์ หรือ การหลอกให้มาร่วมลงทุนในการขุดบิทคอยน์ ซึ่งแท้จริงเป็นการฉ้อโกงหรือเป็นการกระทำผิดในลักษณะคล้ายแชร์ลูกโซ่ดังที่ได้กล่าวมาแล้ว เกิดจากการที่อาชญากรได้ทำการประเมินผู้ที่ตกเป็นเหยื่อแล้วพบว่าเป็น**เป้าหมายที่เหมาะสม (Suitable Target/Victim) เนื่องจากผู้ที่ตกเป็นเหยื่อจะสนใจแต่ผลตอบแทนที่จะได้รับเป็นเงินจำนวนมาก แต่ยังขาดความรู้ในเรื่องการลงทุนและไม่ได้สนใจที่จะศึกษาหรือทำความเข้าใจเกี่ยวกับระบบการทำงานพื้นฐาน กลไกการกำหนดมูลค่า ขั้นตอนการทำเหมืองหรือการขุดบิทคอยน์อย่างจริงจัง เพราะมีความซับซ้อน ยากต่อการเข้าใจ เป็นข้อมูลเชิงลึกที่ต้องอาศัยองค์ความรู้เกี่ยวกับโปรแกรมคอมพิวเตอร์ชั้นสูง** จึงทำให้กลุ่มคนเหล่านี้มักจะหลงเชื่อและถูกหลอกหลวงได้ง่าย ทำให้อาชญากรเลือกกระทำผิดต่อเหยื่อดังกล่าว

3) นอกจากตัวเหยื่อแล้วอาชญากรยังเล็งเห็นว่า**เจ้าหน้าที่ของรัฐที่มีหน้าที่ในการป้องกันปราบปรามการกระทำผิดเกี่ยวกับบิทคอยน์ยังขาดความรู้และขาดศักยภาพที่จะสืบสวนติดตามจับกุมการกระทำผิดที่ใช้บิทคอยน์เป็นเครื่องมือได้ (Absence of a Capable Guardian)** โดยจากการรวบรวมข้อมูลของผู้วิจัยทำให้พบว่าการจับกุมผู้กระทำผิดที่ใช้บิทคอยน์เป็นเครื่องมือในการก่ออาชญากรรมที่ผ่านมานั้น เกิดจากการสืบสวนและรวบรวมข่าวสารจากปัจจัยแวดล้อมต่างๆ เช่น พฤติกรรมการใช้อินเทอร์เน็ตไปยุ่งเกี่ยวกับเว็บไซต์ใต้ดินหรือดาร์คเว็บต่างๆ พฤติกรรมการส่งหรือรับพัสดุทางเรือจากต่างประเทศเป็นประจำ หรือ อาศัยประวัติอาชญากรรมที่เกี่ยวข้อง เท่านั้น โดย**ยังไม่ปรากฏหลักฐานที่บ่งชี้ว่าเจ้าหน้าที่สามารถจับกุมผู้กระทำผิดได้จากการตรวจสอบเส้นทางการเงินหรือร่องรอยหลักฐานที่เกิดจากบิทคอยน์โดยตรง** จึงทำให้อาชญากรอาศัยโอกาสจากการขาด

ประสิทธิภาพในการสืบสวนจับกุมของเจ้าหน้าที่ของรัฐดังกล่าวนี้ใช้บิทคอยน์เป็นเครื่องมือในการก่ออาชญากรรม

4) **องค์ประกอบเรื่องสถานที่ (Place)** นั้น การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการกระทำความผิดจะเกิดขึ้นบนระบบเครือข่ายอินเทอร์เน็ต ซึ่งทำให้อาชญากรได้เปรียบเป็นอย่างมากเพราะในโลกอินเทอร์เน็ตไม่มีขอบเขต ไม่ถูกจำกัดด้วยเส้นแบ่งเขตแดนของรัฐ อาชญากรสามารถใช้บิทคอยน์กระทำผิดได้จากทุกที่ทุกเวลาทั่วโลก เช่น ผู้ที่ต้องการซื้อยาเสพติดสามารถสั่งจ่ายเงินเป็นบิทคอยน์ให้กับผู้ค้ายาเสพติดได้จากทุกที่ทั่วโลกผ่านระบบอินเทอร์เน็ต เป็นต้น

2.6 ทฤษฎีความล้าหลังทางสังคม (Culture Lag Theory)

ทฤษฎีความล้าหลังทางสังคม เป็นทฤษฎีที่อธิบายถึงสาเหตุของการเกิดปัญหาสังคมต่างๆโดยมีในแนวคิดรากฐานมาจากแนวคิดในเรื่องการพัฒนาสังคมที่มีหลักการว่าสังคมมนุษย์จะมีการพลวัตไม่หยุดอยู่กับที่แต่จะมีการเปลี่ยนแปลงไปตามแต่ละยุคสมัยอยู่เสมออันเป็นผลมาจากการที่มนุษย์มีปัญญาและมีความพยายามในการพัฒนาคุณภาพชีวิตให้ดีขึ้นอยู่เสมอ โดยทฤษฎีความล้าหลังทางสังคมนี้ถูกกล่าวถึงครั้งแรกในหนังสือเรื่อง “Social Change with Respect to Culture and Original Nature” โดย วิลเลียม เอฟ. อ็อกเบิร์น (William F. Ogburn) นักสังคมวิทยาชาวอเมริกันซึ่งได้อธิบายแนวคิดหลักของทฤษฎีนี้ว่า การเปลี่ยนแปลงทางสังคมจะเกิดจากการที่วัฒนธรรมในสังคมนั้นๆถูกเปลี่ยนแปลงไปนามแนวคิดหรือสิ่งประดิษฐ์ทางเทคโนโลยีสมัยใหม่มากระทบ โดยวัฒนธรรมที่ถูกเปลี่ยนแปลงไปนั้นแบ่งได้เป็น 2 ประเภท คือ (William F. Ogburn, 1922)

1) วัฒนธรรมทางวัตถุ (Material Culture) หมายถึง วัฒนธรรมที่เป็นเรื่องเกี่ยวกับทางด้านวัตถุสิ่งของต่างๆ เช่น วัฒนธรรมการแต่งกายหรือการใส่เสื้อผ้าเครื่องประดับ วัฒนธรรมที่เกี่ยวกับของใช้หรือเครื่องอุปโภคต่างๆ วัฒนธรรมในการใช้ยานพาหนะ เป็นต้น

2) วัฒนธรรมที่ไม่ใช่วัตถุ (Non - Material Culture) หมายถึงวัฒนธรรมในเรื่องที่เกี่ยวกับแบบแผนของพฤติกรรมหรือแบบแผนทางความคิดต่างๆ เช่น ความเชื่อ ค่านิยม อุดมการณ์ ร่วมทั้งบรรทัดฐานทางสังคม รวมทั้งกฎหมายและประเพณีต่างๆ

โดย วิลเลียม เอฟ. อ็อกเบิร์น อธิบายว่าเมื่อมนุษย์ได้มีการคิดค้นหรือทำการสร้างนวัตกรรมทางเทคโนโลยีสมัยใหม่ต่างๆขึ้น จะส่งผลให้เกิดการเปลี่ยนแปลงทางสังคม โดยที่**การเปลี่ยนแปลงทางวัฒนธรรมที่เป็นวัตถุจะเกิดขึ้นรวดเร็วกว่าการเปลี่ยนแปลงทางวัฒนธรรมที่ไม่ใช่วัตถุ**

เนื่องจาก การเปลี่ยนแปลงทางวัตถุนั้นไม่ได้มีผลกระทบต่อจิตใจหรือความเชื่อใดๆ จึงทำให้เกิดการเปลี่ยนแปลงได้ง่าย ในขณะที่การเปลี่ยนแปลงทางวัฒนธรรมที่ไม่ใช่วัตถุนั้นไม่สามารถเปลี่ยนแปลงได้อย่างรวดเร็วหรือกะทันหัน เนื่องจากจำเป็นจะต้องอาศัยระยะเวลาในการบ่มเพาะทางความคิดเพื่อให้เกิดการเปลี่ยนแปลงทางด้านทัศนคติหรือความเชื่อ **จนทำให้การเปลี่ยนแปลงทางวัฒนธรรมทั้งสองประเภทนี้ไม่สมดุลกันและเกิดเป็นช่องว่างที่ทำให้เกิดปัญหาสังคมรูปแบบต่างๆ** ตัวอย่างเช่น ในอดีตเมื่อครั้งที่มนุษย์เริ่มการพัฒนาในเรื่องที่เกี่ยวกับเทคโนโลยียานยนต์ทำให้เกิดการประดิษฐ์รถยนต์ซึ่งถือเป็นยานพาหนะชนิดใหม่ในขณะนั้นออกมาใช้งาน ในขณะที่การเปลี่ยนแปลงทางวัฒนธรรมที่ไม่ใช่วัตถุอย่าง การสร้างวินัยจราจร กฎหมายที่เกี่ยวกับการจราจร รวมทั้งโครงสร้างทางสังคมต่างๆที่มารองรับรถยนต์ เช่น ถนนหรือระบบการขนส่งต่างๆยังไม่สามารถปรับตัวให้ทันกับนวัตกรรมใหม่ดังกล่าวได้ จนทำให้เกิดสภาพความไร้ระเบียบและเกิดปัญหาต่างๆในช่วงแรกเช่น ปัญหาทางด้านอุบัติเหตุจราจร

ทฤษฎีความล้าหลังทางวัฒนธรรม (Culture Lag Theory) สามารถนำไปใช้ในการวิเคราะห์หรือใช้ในการอธิบายสาเหตุของการเกิดอาชญากรรมต่างๆได้ เช่น เมื่อครั้งที่อินเทอร์เน็ต (Internet) ถูกสร้างขึ้นซึ่งส่งผลทำให้เกิดสภาวะโลกาภิวัฒน์ที่ข้อมูลข่าวสารและการติดต่อสื่อสารต่างๆสามารถเกิดขึ้นได้ในทันทีส่งผลทำให้วิถีชีวิตมนุษย์เปลี่ยนแปลงไปอย่างสิ้นเชิง โดยวัฒนธรรมที่เปลี่ยนแปลงไปได้ก่อนคือ วัฒนธรรมทางวัตถุ (Material Culture) ซึ่งในที่นี้หมายถึง มนุษย์ได้เปลี่ยนจากการใช้อุปกรณ์ดั้งเดิมในการติดต่อสื่อสารหรือการใช้ชีวิตประจำวันมาเป็นการพึ่งพาระบบอินเทอร์เน็ตในรูปแบบต่างๆ รวมทั้งอาชญากรหรือผู้กระทำผิดที่มีการนำอินเทอร์เน็ตไปใช้เป็นช่องทางในการก่ออาชญากรรมจนทำให้เกิดอาชญากรรมรูปแบบใหม่คืออาชญากรรมไซเบอร์ (Cyber Crime) ในขณะที่วัฒนธรรมดังกล่าวเปลี่ยนแปลงไปอย่างรวดเร็ว ปรากฏว่าวัฒนธรรมที่ไม่ใช่วัตถุ (Non - Material Culture) ได้แก่ กฎหมายและการป้องกันปราบปรามอาชญากรรมต่างๆ ไม่สามารถปรับตัวให้เท่าทันกับปัญหาอาชญากรรมที่เกิดขึ้นได้ จนทำให้เกิดปัญหาอาชญากรรมไซเบอร์ขึ้นเป็นจำนวนมาก เป็นต้น

2.7 ทฤษฎีป้องกันหรือทฤษฎีการข่มขู่ยับยั้ง (Deterrence Theory)

ทฤษฎีป้องกันหรือทฤษฎีข่มขู่ยับยั้งนี้ มีรากฐานหรือพัฒนามาจากแนวคิดหลักของกลุ่มสำนักคิดอาชญาวิทยาดั้งเดิม ที่มองว่าบุคคลมีอิสระในการกำหนดพฤติกรรมของตนเอง และจะตัดสินใจกระทำความผิดเมื่อได้ชั่งน้ำหนักแล้วว่าตนจะได้รับผลประโยชน์มากกว่าโทษที่จะได้รับ ดังนั้นการ

ป้องกันอาชญากรรมตามแนวคิดดังกล่าว จึงจะมีลักษณะของการกำหนดบทลงโทษที่เหมาะสม มีการลงโทษที่รวดเร็วและมีความโปร่งใส ดังนั้น จึงอาจกล่าวได้ว่ากลุ่มทฤษฎีนี้นั้นได้ศึกษาถึงการยับยั้งอาชญากรรมมากกว่าการค้นหาสาเหตุของการเกิดอาชญากรรม โดยทฤษฎีป้องกันหรือทฤษฎีข่มขู่ยับยั้งนี้ได้นำเอาหลักการดังกล่าวไปพัฒนาและนำเสนอแนวคิดต่อเนื่องจากการกำหนดบทลงโทษที่เหมาะสมว่า ภายหลังที่มีการลงโทษผู้กระทำผิดแล้วจะทำให้เกิดปรากฏการณ์ขึ้นด้วยกัน 2 ลักษณะ คือ (พรชัย ขันตี, 2558)

1) การป้องกันหรือการข่มขู่ยับยั้งทั่วไป (General Deterrence)

หมายถึง การที่รัฐหรือฝ่ายปกครองมีระบบกฎหมายและกระบวนการยุติธรรมที่มีความพร้อม มีความชัดเจนและมีประสิทธิภาพเพียงพอที่จะลงโทษผู้กระทำผิดได้อย่างเหมาะสม เปิดเผย และโปร่งใส จนส่งผลทำให้สาธารณชนรับทราบถึงผลร้ายที่จะเกิดขึ้นกับตนเองหากตนตัดสินใจกระทำความผิด จนทำให้เกิดความกลัวและไม่กล้าที่จะก่ออาชญากรรม ซึ่งในทางกลับกันหากกฎหมายหรือกระบวนการยุติธรรมของรัฐ ไม่มีความชัดเจนหรือขาดประสิทธิภาพในการลงโทษผู้กระทำผิด หรือขาดกระบวนการบังคับใช้กฎหมายหรือกระบวนการยุติธรรมที่โปร่งใสแล้ว บุคคลทั่วไปก็จะไม่เกรงกลัวและจะตัดสินใจเลือกที่จะก่ออาชญากรรมในที่สุด

2) การป้องกันหรือการข่มขู่ยับยั้งเฉพาะราย (Specific Deterrence)

หมายถึง ผลจากกฎหมายและกระบวนการยุติธรรมที่ทำให้บุคคลที่เคยได้รับโทษตามกฎหมายหรือผ่านกระบวนการยุติธรรมของรัฐมาแล้ว เกิดความรู้สึกกลัวหากจะต้องกลับมารับโทษอีกครั้งจนทำให้เกิดความคิดในกระบวนการตัดสินใจว่าจะไม่กลับไปกระทำผิดซ้ำอีก

ทฤษฎีการป้องกันหรือการข่มขู่ยับยั้งนี้ สามารถนำมาใช้ในการกำหนดแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้ว่า หากต้องการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ภาครัฐจะต้องมีกฎหมายและระบบกระบวนการยุติธรรมที่มีความพร้อม ที่จะสามารถใช้บังคับใช้และลงโทษผู้กระทำผิดได้อย่างเหมาะสม รวดเร็ว เพียงพอที่จะทำให้ตัวผู้รับโทษเองเกรงกลัวและเข็ดหลาบจนไม่หวนกลับมากระทำผิดอีก เช่น มีแนวทางการติดตามสืบสวนที่รวดเร็ว มีบทลงโทษที่ร้ายแรงเหมาะสม มีระบบการยึดอายัดสกุลเงินเข้ารหัสที่เด็ดขาด ทั้งนี้ยังส่งผลให้สังคมส่วนรวมรับทราบและตระหนักถึงโทษหรือผลร้ายที่จะได้รับหากกระทำความผิดที่เกี่ยวกับสกุลเงินเข้ารหัสซึ่งถือเป็นแนวทางในการเพิ่มประสิทธิภาพการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสด้วย

2.8 ทฤษฎีบังคับใช้กฎหมาย (Law Enforcement Theory)

ทฤษฎีการบังคับใช้กฎหมายเป็นทฤษฎีที่เกิดจากแนวความคิดในการพยายามที่จะหาวิธีป้องกันอาชญากรรมที่เกิดขึ้นเป็นจำนวนมากในประเทศอังกฤษ ในช่วงสมัยศตวรรษที่ 19 ที่มีการปฏิวัติเปลี่ยนแปลงสภาพสังคมจากสังคมเกษตรกรรมเข้าสู่สังคมอุตสาหกรรม ทำให้เกิดการอพยพย้ายถิ่นฐานเพื่อเดินทางเข้าสู่เมืองใหญ่ซึ่งเป็นฐานการผลิตต่างๆ โดยการเคลื่อนย้ายของประชากรเข้าสู่ตัวเมืองนั้นส่งผลให้เกิดการขยายตัวทางเศรษฐกิจและสังคมอย่างรวดเร็ว จนทำให้ภาครัฐไม่สามารถปรับตัวหรือปรับเปลี่ยนแนวทางการดำเนินงานให้เท่าทันสถานการณ์ที่เปลี่ยนไปนี้ได้ทัน ส่งผลทำให้สภาพสังคมเกิดความไร้ระเบียบ และส่งผลให้เกิดอาชญากรรมขึ้นเป็นจำนวนมาก จึงทำให้เซอร์โรเบิร์ต พีล (Sir Robert Peel) ผู้ที่ได้รับการยกย่องให้เป็นบิดาแห่งตำรวจยุคใหม่ ได้มีดำริที่จะจัดตั้งกองบัญชาการตำรวจนครลอนดอน ประเทศอังกฤษขึ้น โดยได้วางหลักการสำคัญเกี่ยวกับแนวนโยบายไว้ 9 ข้อ ได้แก่ (ประเสริฐ เมฆมณี, 2517,น.44-45 อ้างถึงใน กองวิจัยและพัฒนา สำนักงานตำรวจแห่งชาติ, 2550)

1) การป้องกันปราบปรามเป็นภารกิจพื้นฐานของตำรวจ

2) ตำรวจต้องได้รับความเคารพนับถือและยกย่องจากประชาชนอย่างแท้จริง

3) การที่ประชาชนเคารพและปฏิบัติตามกฎหมายเป็นการชักนำให้ประชาชนเคารพยำเกรงตำรวจ

4) การปฏิบัติหน้าที่เชิงบังคับขู่เข็ญของตำรวจจะเป็นผลให้ประชาชนสนับสนุนกิจการตำรวจลดน้อยลงเป็นสัดส่วน

5) ตำรวจจะต้องปฏิบัติหน้าที่ในการบังคับใช้กฎหมายด้วยความเที่ยงธรรม

6) ตำรวจพึงใช้กำลังอาวุธในกรณีที่จำเป็นสุดวิสัยซึ่งไม่อาจหลีกเลี่ยงได้

7) ตำรวจและประชาชนเสมือนหนึ่งเป็นบุคคลคนเดียวกัน

8) ตำรวจเป็นตัวแทนของกฎหมาย

9) สังคมที่ปลอดจากอาชญากรรมและความยุ่งเหยิงย่อมเป็นสิ่งที่แสดงให้เห็นศักยภาพการทำงานของตำรวจ

หลักการดังกล่าวของพีลได้ถูกนำมาพัฒนาเป็นแนวคิดของทฤษฎีการบังคับใช้กฎหมาย กล่าวคือ เพื่อให้ประชาชนเกิดความยำเกรงต่อกฎหมาย**เจ้าหน้าที่ตำรวจจะต้องออกตรวจตราไปตามพื้นที่ต่างๆโดยจะต้องปรากฏกายให้ประชาชนและสังคมได้เห็นอย่างชัดเจน** เช่น จะต้องใช้การ

แต่งเครื่องแบบและใช้ยานพาหนะที่มีสัญลักษณ์หรือเครื่องหมายที่ทำให้สังเกตุเห็นได้โดยง่าย เพื่อผลสำคัญในการข่มขู่ยับยั้งผู้ที่จะกระทำผิดและแสดงให้ประชาชนทั่วไปได้เห็นว่ามีเจ้าหน้าที่ตำรวจรักษาความปลอดภัยในพื้นที่รับผิดชอบอยู่ตลอดเวลา จึงจะสามารถป้องกันไม่ให้เกิดอาชญากรรมได้ (ปุระชัย เปี่ยมสมบูรณ์, 2526 อ้างถึงใน กองวิจัยและพัฒนา สำนักงานตำรวจแห่งชาติ, 2550) โดยหลักการดังกล่าวถูกนำไปใช้ในการวางนโยบายในการป้องกันอาชญากรรมของเจ้าหน้าที่ตำรวจอย่างแพร่หลายจนเกิดเป็นการจัด “ตำรวจสายตรวจ” ออกตรวจตราพื้นที่รับผิดชอบอย่างในปัจจุบัน

โดยสรุปแล้วแนวคิดที่เป็นหลักการสำคัญของทฤษฎีบังคับใช้กฎหมายนี้คือ **“การปรากฏตัวของเจ้าหน้าที่ตำรวจ เพื่อผลในการข่มขู่ยับยั้งผู้กระทำผิด”** ซึ่งนำเอาหลักการดังกล่าวไปใช้ในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส จำเป็นจะต้องนำแนวคิดไปประยุกต์ใช้เพื่อให้เหมาะสมกับสภาพปัญหาเนื่องจากการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำผิดนั้น ไม่ได้เกิดขึ้นตามสภาพภูมิประเทศตามปกติแต่เกิดขึ้นบนระบบคอมพิวเตอร์ที่มีลักษณะเป็นสังคมเสมือนจริง

2.9 แนวคิดเกี่ยวกับนโยบายสาธารณะและตัวแบบนโยบายสาธารณะแบบกลุ่ม (Group Model)

2.9.1 ความหมายของนโยบายสาธารณะ

นโยบายสาธารณะถือเป็นกลไกสำคัญที่รัฐใช้ในการบริหารจัดการปัญหาต่างๆ ภายในประเทศ โดยเฉพาะอย่างยิ่งการกำหนดแนวนโยบายที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่จำเป็นจะต้องอาศัยแนวคิดเกี่ยวกับการกำหนดนโยบายสาธารณะ มาใช้เป็นแนวทางในการศึกษา วิเคราะห์เพื่อให้สามารถกำหนดนโยบายของรัฐที่เหมาะสมกับสภาวการณ์ของสังคมได้ โดยได้มีนักวิชาการได้ให้ความหมายของนโยบายสาธารณะ โดยแบ่งเป็นความหมายต่างๆ 3 ประเภท คือ (กุลธน ธนาพงศธร, 2520 อ้างถึงใน มยุรี อนุมานราชธน, 2556)

1) ความหมายในมิติที่เป็นกิจกรรมหรือการกระทำของรัฐบาล

นโยบายสาธารณะในความหมายนี้ หมายถึง แนวทางการบริหารงานของรัฐที่มีเป้าหมายหรือเป้าประสงค์อย่างใดอย่างหนึ่ง ซึ่งเป็นเรื่องที่เกี่ยวกับผลประโยชน์หรือส่งผลกระทบต่อสังคมโดยรวม เช่น การออกกฎหมาย การบังคับใช้กฎหมาย ทั้งนี้นโยบายอาจเป็นได้ทั้งในลักษณะของการกระทำหรืองดเว้นการกระทำใดๆ โดยอาศัยอำนาจของรัฐหรืออำนาจทางกฎหมายในการรับรองและให้อำนาจแก่เจ้าหน้าที่

2) **ความหมายในมิติที่เป็นทางเลือกสำหรับการตัดสินใจของรัฐบาล**

นโยบายสาธารณะในความหมายนี้ ได้มีนักวิชาการหลายท่านได้ให้ความหมายไว้ สามารถสรุปได้ว่า การตัดสินใจของรัฐบาลเพื่อกำหนดทิศทางให้แก่หน่วยงานต่างๆ เพื่อนำไปกำหนดแนวทางการปฏิบัติงานให้เกิดความสอดคล้องกับการทิศทางดังกล่าว โดยที่การตัดสินใจนี้เป็นลักษณะของการตกลงใจที่มีความถาวร มั่นคง ไม่ใช่ลักษณะของการตัดสินเพื่อแก้ปัญหาเพียงชั่วคราว หรือเป็นลักษณะของการตัดสินใจที่ส่งผลต่อสังคมส่วนรวมในระยะยาว

3) ความหมายในมิติที่เป็นแนวทางในการกระทำของรัฐบาล

นโยบายสาธารณะในความหมายนี้ มีลักษณะของความเป็นรูปธรรมที่ชัดเจน เช่น การกำหนดแผนงาน โครงการหรือการบัญญัติแนวทางการดำเนินงานต่างๆของรัฐ

นอกจากนี้ยังมีนักวิชาการได้ให้ความหมายของคำว่า “นโยบายสาธารณธะ” ต่างๆ ได้แก่ ศุภชัย ยาวะประภาษ (2550) ได้ให้ความหมายว่าหมายถึง แนวทางดำเนินกิจกรรมต่างๆที่รัฐได้ดำเนินการมาแล้ว กำลังดำเนินการอยู่ หรือกำลังจะดำเนินการหรือกิจกรรมที่จะกระทำในอนาคต ในขณะที่ ทศพร ศิริสัมพันธ์ (2539) อธิบายว่า “นโยบายสาธารณะ” หมายถึง นโยบายที่กำหนดโดยรัฐบาล ซึ่งหมายความรวมถึงหน่วยงานหรือองค์กรต่างๆที่ดำเนินกิจการภายใต้รัฐบาล ที่มีอำนาจหน้าที่เกี่ยวกับการกำหนดนโยบายนั้นๆ ทั้งนี้การกำหนดนโยบายต่างๆจะมีลักษณะของการตัดสินใจไปในทิศทางใดทิศทางหนึ่ง เพื่อให้เกิดการสร้างความสมดุลระหว่างองค์ประกอบต่างๆ

จากที่มีนักวิชาการได้ให้ความหมายของนโยบายสาธารณะไว้ในแนวทางต่างๆนั้น สามารถสรุปได้ว่า นโยบายสาธารณะคือการกระทำของรัฐหรือผู้มีอำนาจปกครองรูปแบบหนึ่งที่เป็นการแสดงออกถึงเจตนารมณ์หรือทิศทางการบริหารราชการในเรื่องที่เกี่ยวข้องกับผลประโยชน์ส่วนรวม โดยจะกำหนดกรอบแนวทางการปฏิบัติอย่างกว้าง หรือจะกำหนดหลักการและวิธีปฏิบัติที่ชัดเจนไว้ก็ได้ ทั้งนี้การกำหนดนโยบายจะต้องมีลักษณะของความมั่นคงและยั่งยืน รวมทั้งจะต้องสามารถแบ่งสรรปันส่วนทรัพยากรต่างๆให้เกิดความเหมาะสมในทุกๆด้าน

2.9.2 กระบวนการกำหนดนโยบายสาธารณะ

กระบวนการกำหนดนโยบายสาธารณะ สามารถแบ่งออกได้เป็น 5 ขั้นตอน ได้แก่ (James E. Anderson, 1975 อ้างถึงใน สนธิกาญจน์ เพื่อนสงคราม, 2560)

ขั้นตอนที่ 1 ขั้นการก่อตัวของปัญหาของนโยบายสาธารณะ (Public Policy Problem) เป็นการพิจารณาของภาครัฐว่าปัญหาที่เกิดขึ้น เป็นปัญหาในระดับที่เป็นปัญหาของประเทศชาติหรือสังคมส่วนรวมที่รัฐบาลจะต้องเข้าไปจัดการหรือจะต้องจัดให้ปัญหาดังกล่าวเป็นวาระของรัฐที่จะต้องกระทำการอย่างใดอย่างหนึ่งหรือไม่

ขั้นตอนที่ 2 ขั้นการก่อรูปนโยบายสาธารณะ (Public Policy Formation) เป็นขั้นตอนของการนำปัญหามาวิเคราะห์ เพื่อกำหนดทางเลือกของนโยบาย (Policy Alternatives) เพื่อการแก้ไขปัญหาว่ารัฐสามารถกระทำการไปในทิศทางใดบ้าง โดยใช้การวิเคราะห์ร่วมกันของผู้มีส่วนร่วมในการกำหนดนโยบายจากการพิจารณาข้อดี ข้อเสียของแต่ละทางเลือก

ขั้นตอนที่ 3 ขั้นการตัดสินใจนโยบายสาธารณะ (Public Policy Adoption) เป็นขั้นตอนภายหลังจากที่ได้วิเคราะห์ข้อดี ข้อเสียและประเมินผลที่จะได้รับแล้ว (Cost - Benefit) แล้วรัฐบาลจึงจะได้เลือกหรือตัดสินใจว่าจะใช้ทางเลือกแนวนโยบายใดในการแก้ปัญหา

ขั้นตอนที่ 4 ขั้นการนำนโยบายไปสู่การปฏิบัติ (Public Policy Implementation) โดยเมื่อได้ตัดสินใจเลือกนโยบายที่เหมาะสมแล้ว ก็จะต้องมีการนำไปปฏิบัติตามแนวทางหรือหลักการที่กำหนดไว้ ให้บรรลุเป้าหมาย

ขั้นตอนที่ 5 ขั้นการประเมินผลนโยบายสาธารณะ (Public Policy Evaluation) เป็นขั้นตอนภายหลังจากที่ได้มีการนำนโยบายไปปฏิบัติแล้ว จะต้องมีการศึกษาถึงปัญหา อุปสรรค และผลของการดำเนินนโยบายว่าสามารถนำไปใช้แก้ปัญหาที่เป็นปัญหาตั้งต้นได้หรือไม่ หรือจำเป็นจะต้องปรับปรุงพัฒนาแนวนโยบายอย่างไร หรือหากนโยบายไม่สามารถนำไปใช้แก้ปัญหาได้ ก็จำเป็นจะต้องกำหนดเป็นปัญหาเพื่อเข้าสู่กระบวนการนโยบายและกำหนดทางเลือกใหม่ เพื่อให้สามารถแก้ปัญหาได้ในที่สุด

2.9.3 ตัวแบบเกี่ยวกับการกำหนดนโยบายสาธารณะ (Public Policy Model)

ตัวแบบนโยบายสาธารณะเป็นเครื่องมือหรือกลไกที่ใช้ในการกำหนดนโยบายสาธารณะ ซึ่งมีลักษณะเป็นแนวคิดและหลักการต่างๆที่ที่สามารถนำไปประยุกต์ใช้กับปัญหาต่างๆ ตามแต่สถานการณ์ หรืออาจใช้ในการศึกษาวิเคราะห์นโยบายสาธารณะต่างๆ โดยมีตัวแบบนโยบายสาธารณะดังนี้ (สนธิกาญจน์ เพื่อนสงคราม, 2560) (มยุรี อนุมานราชธน, 2556)

1) ตัวแบบชนชั้นนำ (Elite Model)

เป็นลักษณะของการกำหนดนโยบายสาธารณะตามความเชื่อหรือค่านิยมของชนชั้นนำหรือชนชั้นปกครองมากกว่าการตอบสนองต่อความต้องการของสังคมส่วนรวม จนส่งผลทำให้ค่านิยมของชนชั้นนำกลายเป็นค่านิยมของสังคมด้วย ตัวแบบนโยบายแบบชนชั้นนำนี้มักจะเกิดขึ้นในสังคมที่ชนชั้นปกครองมีอำนาจมาก จึงทำให้แนวทางการกำหนดนโยบายในลักษณะนี้ เป็นแบบการกำหนดนโยบายจากบนลงล่างกล่าวคือรัฐบาลกำหนดแนวทางให้ประชาชนปฏิบัติตามเป็นหลัก

2) ตัวแบบสถาบัน (Institution Model)

สถาบันในที่นี้หมายถึง หมายถึงองค์การที่ใช้อำนาจรัฐในการตอบสนองต่อความต้องการของประชาชนส่วนรวมในสังคม โดยที่สถาบันจะต้องมีสถานภาพที่ชัดเจน มีการกำหนดความสัมพันธ์ภายในองค์การด้วยกฎระเบียบที่ชัดเจน โดยมักจะหมายถึงสถาบันที่มีอำนาจหลักภายในรัฐ เช่น สถาบันนิติบัญญัติ สถาบันบริหาร สถาบันตุลาการ โดยการใช้อำนาจของสถาบันต่างๆนี้จะเป็นไปเพื่อการกำหนดนโยบายต่างๆในรูปแบบของกฎหมาย มติคณะรัฐมนตรี คำพิพากษาของศาล หรือการตีความทางกฎหมาย รวมทั้งการกำหนดรูปแบบโครงสร้างความสัมพันธ์หรือพฤติกรรมของคนในสังคมผ่านการใช้อำนาจต่างๆ

3) ตัวแบบระบบ (System Model)

ตัวแบบนี้สะท้อนความหมายของระบบในทางการเมือง ที่มีขั้นตอนการแก้ปัญหาอย่างมีความสัมพันธ์ต่อกัน เพื่อให้สามารถจัดการหรือกำหนดทิศทางของนโยบายให้ตอบสนองต่อข้อเรียกร้องต่างๆ หรืออาจกล่าวได้ว่าเป็นการดำเนินการของกลุ่มองค์ประกอบต่างๆในสังคมที่มีความเกี่ยวข้องเชื่อมโยงกัน โดยองค์ประกอบของระบบจะประกอบด้วย สภาพแวดล้อมซึ่งหมายถึงสิ่งต่างๆที่อยู่ภายนอกระบบ ปัจจัยนำเข้าซึ่งเป็นรูปแบบของข้อเรียกร้องหรือความต้องการรวมทั้งการสนับสนุนต่างๆ จากนั้นจะเกิดกระบวนการทางการเมืองเพื่อสร้างผลผลิตออกเป็นแนวนโยบายหรือการตัดสินใจกระทำการอย่างใดอย่างหนึ่ง เพื่อตอบสนองต่อข้อเรียกร้องต่างๆ ซึ่งมีสถานะเป็นปัจจัยนำออก ซึ่งปัจจัยนำออกนี้จะย้อนกลับเข้าสู่การเป็นปัจจัยนำเข้าอีกครั้ง

4) ตัวแบบหลักเหตุผล (Rational Model)

ตัวแบบนี้นโยบายสาธารณะนี้ เป็นตัวแบบที่มุ่งเน้นการกำหนดนโยบายให้สอดคล้องกับความต้องการของประชาชนหรือสังคมสูงสุด รวมทั้งการที่รัฐบาลจะกำหนดนโยบายใดๆยังจำเป็นจะต้องพิจารณาการใช้งบประมาณและทรัพยากรอย่างสมเหตุสมผล โดยการดำเนินการกำหนด

นโยบายสาธารณะตามหลักการและเหตุผลจะมีขั้นตอนประกอบด้วย การกำหนดเป้าหมายของแผนปฏิบัติการและลำดับความสำคัญของเป้าหมาย กำหนดค่านิยมและทรัพยากรให้สอดคล้องกับเป้าหมาย ศึกษาทางเลือกทั้งหมดที่สอดคล้องกับนโยบาย วิเคราะห์ผลและความเสี่ยงของทางเลือกจากการพยากรณ์ผลที่จะเกิดขึ้น ชั่งน้ำหนักอัตราส่วนของผลที่จะได้รับในแง่ของต้นทุนกำไรของแต่ละทางเลือก และสุดท้ายคือการเปรียบเทียบผลได้ของแต่ละทางเลือก และพิจารณาเลือกทางเลือกที่ให้ประโชยน์มีความคุ้มค่าสูงสุด

5) ตัวแบบการเปลี่ยนแปลงในส่วนเพิ่ม (Incremental Model)

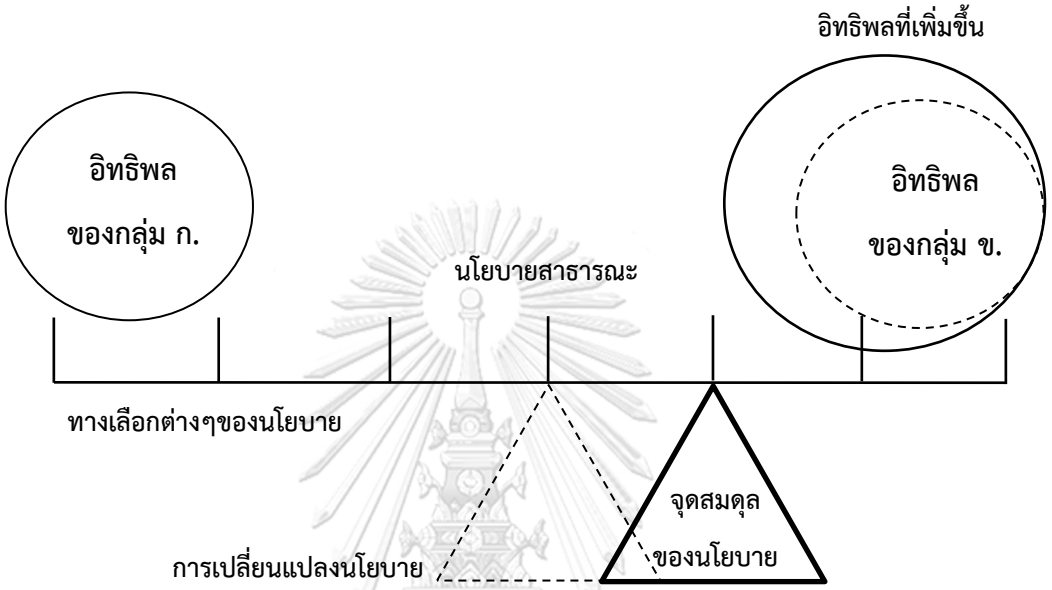
แนวทางการกำหนดนโยบายสาธารณะตามตัวแบบนี้ คือการนำเอานโยบายสาธารณะที่ดำเนินการหรือเคยดำเนินการอยู่ก่อนแล้ว มาพิจารณาต่อยอดการดำเนินการโดยอาจมีการเปลี่ยนแปลงแก้ไขปรับปรุงอย่างค่อยเป็นค่อยไป โดยเป็นการแสดงออกถึงแนวคิดเชิงอนุรักษ์นิยมประกอบกับแนวคิดว่าการเริ่มศึกษาตั้งแต่ต้นตอของปัญหาและการพิจารณาตัวเองอย่างละเอียดของรัฐบาลนั้น ทำให้ใช้ระยะเวลาและทรัพยากรเป็นจำนวนมาก จึงอาจทำให้การแก้ปัญหาล่าช้า ดังนั้นการกำหนดนโยบายตามตัวแบบนี้จึงมีหลักการสำคัญ คือ นโยบายสาธารณะจะต้องไม่เกิดจากการตัดสินใจเพียงครั้งเดียวแต่จะต้องเกิดจากการนำประสบการณ์จากนโยบายเดิมมาสำรวจข้อผิดพลาดเพื่อให้สามารถปรับปรุงและนำนโยบายไปปฏิบัติได้อย่างต่อเนื่อง

นอกจากตัวแบบการกำหนดนโยบายสาธารณะที่กล่าวมานี้แล้ว ยังมีอีกหนึ่งตัวแบบสำคัญที่สามารถนำมาใช้ในการกำหนดนโยบายสาธารณะในประเด็นด้านการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้ คือ **ตัวแบบกลุ่ม (Group Model)** ดังจะได้กล่าวต่อไป

2.9.4 ตัวแบบนโยบายสาธารณะแบบกลุ่ม (Group Model)

ตัวแบบการกำหนดนโยบายสาธารณะแบบกลุ่มนี้ ผู้วิจัยเห็นว่าสามารถนำไปใช้ในการวิเคราะห์แนวนโยบายที่เกี่ยวกับสกุลเงินเข้ารหัส โดยหลักการของตัวแบบดังกล่าวนี้มีนักวิชาการที่สำคัญคือ อาเธอร์ เอฟ. เบนท์ลีย์ (Arthur F. Bently) และ เดวิด บี. ทรูแมน (David B. Truman) กล่าวว่า นโยบายสาธารณะเป็นผลมาจากการเรียกร้องผลประโยชน์ของกลุ่มทางสังคมต่างๆ เช่น กลุ่มผู้มีอิทธิพล และกลุ่มการเมืองต่างๆ ซึ่งกลุ่มต่างๆเหล่านี้จะทำหน้าที่เสมือนเป็นตัวเชื่อมระหว่างประชาชนกับรัฐบาล เมื่อเกิดการเรียกร้องผลประโยชน์ของกลุ่มต่างๆแล้ว รัฐบาลจึงมีหน้าที่ในการประนีประนอมความต้องการของกลุ่มผลประโยชน์ต่างๆ และนโยบายสาธารณะที่กำหนดก็เป็นไปเพื่อการจัดสรรผลประโยชน์ให้แก่กลุ่มทางสังคมต่างๆให้เกิดความสมดุลมากที่สุด ทั้งนี้แนวนโยบายอาจ

เกิดการโน้มเอียงไปในทิศทางของกลุ่มทางสังคมที่มีอิทธิพลต่อรัฐบาลหรือผลประโยชน์ของสังคมส่วนรวม หรือในกรณีที่มีการเปลี่ยนแปลงอิทธิพลดังกล่าวดังนั้นจึงอาจกล่าวได้ว่าแนวนโยบายที่กำหนดอาจถูกเปลี่ยนแปลงไปได้เสมอ ตามสถานการณ์และข้อเรียกร้องของกลุ่มสังคมต่างๆ โดยสามารถแสดงแนวคิดของตัวแบบกลุ่มได้ตามภาพดังนี้



ภาพที่ 5 แนวทางการกำหนดนโยบายสาธารณะตามตัวแบบกลุ่ม (Group Model)
(Dye , 1984 อ้างถึงใน มยุรี อนุมานราชธน, 2556)

แนวคิดตัวแบบกลุ่มในการกำหนดนโยบายสาธารณะนั้น สามารถนำมาวิเคราะห์นโยบายที่เกี่ยวกับสกุลเงินเข้ารหัสได้ เนื่องจากในการกำหนดทิศทางการกำกับหรือควบคุมดูแลสกุลเงินเข้ารหัสซึ่งถือเป็นสินทรัพย์ดิจิทัลนั้น จำเป็นจะต้องคำนึงถึงผลประโยชน์ของกลุ่มทางสังคมต่างๆ ได้แก่ กลุ่มผู้ประกอบธุรกิจที่จะนำสกุลเงินเข้ารหัสไปใช้ในการพัฒนาเพื่อส่งเสริมให้เกิดการขยายตัวทางธุรกิจ ในขณะที่กลุ่มผู้มีส่วนได้เสียอีกกลุ่มหนึ่งคือกลุ่มผู้บังคับใช้กฎหมายที่จำเป็นจะต้องระงับยับยั้งหรือควบคุมความเสี่ยงที่จะมีการนำนวัตกรรมสมัยใหม่นี้ไปใช้ในการก่ออาชญากรรม ดังนั้น รัฐในฐานะตัวกลางตามตัวแบบกลุ่มนี้ จะต้องประเมินสถานการณ์และสภาพปัญหาต่างๆอย่างรอบคอบ เพื่อให้สามารถกำหนดแนวนโยบายที่เหมาะสมและสร้างสมดุลให้เกิดขึ้นทั้งในแง่ของการพัฒนาระบบเศรษฐกิจและการรักษาความงสบเรียบร้อยควบคู่กันไป

2.10 แนวคิดเกี่ยวกับมาตรการทางกฎหมาย

กฎหมายถือเป็นเครื่องมือสำคัญที่รัฐใช้ในการควบคุมและกำกับดูแลการกระทำต่างๆของคนในสังคม โดยฉพาะอย่างยิ่งการเป็นเครื่องมือหลักในการป้องกันอาชญากรรมและการกระทำความผิดต่างๆ เพื่อให้เกิดความสงบสุขและความเป็นระเบียบเรียบร้อยของสังคมส่วนรวม โดยในการกำหนดมาตรการทางกฎหมายเพื่อใช้บังคับยับยั้งการกระทำต่างๆของคนในสังคมนั้น จะมีความแตกต่างกันออกไปตามความเหมาะสมของเรื่อง โดยสามารถแบ่งรูปแบบของมาตรการทางกฎหมายออกเป็น 8 รูปแบบ ดังนี้ (อภิชน จันทรเสน, 2561)

1) การบังคับและควบคุมด้วยการลงโทษ (Command and Control Regulation) คือมาตรการที่รัฐกำหนดให้พฤติกรรมใดเป็นความผิดและห้ามมิให้ประชาชนประพฤติปฏิบัติ รวมทั้งการกำหนดมาตรการขั้นต่ำให้ประชาชนต้องปฏิบัติตาม โดยหากประชาชนฝ่าฝืนข้อกำหนดดังกล่าวก็จะต้องได้รับโทษทางกฎหมาย ซึ่งมาตรการนี้เป็นมาตรการทางกฎหมายที่มีการใช้อย่างแพร่หลายมากที่สุด เช่น มาตรการทางกฎหมายอาญาที่กำหนดให้พฤติกรรมต่างๆเป็นความผิดและหากฝ่าฝืนก็จะต้องได้รับโทษทางอาญา เป็นต้น จุดเด่นของมาตรการนี้คือการที่รัฐสามารถควบคุมการกระทำต่างๆของประชาชนได้ในทันที รวมทั้งสามารถใช้การลงโทษเพื่อทำให้การบังคับใช้กฎหมายเกิดความเด็ดขาด อีกทั้งยังเป็นการแสดงออกให้สังคมส่วนรวมได้เห็นถึงความพยายามในการที่จะหยุดยั้งพฤติกรรมที่ไม่พึงประสงค์ได้อย่างชัดเจน ซึ่งการดำเนินการตามมาตรการดังกล่าวก็สามารถทำได้โดยอาศัยเพียงขั้นตอนการร่างกฎหมายและกำหนดบทลงโทษเท่านั้น

แต่ในทางกลับกันมาตรการในลักษณะนี้ก็ยังคงมีข้อควรระวังในการบังคับใช้ เช่น ความเหมาะสมของการกำหนดให้พฤติกรรมใดๆเป็นความผิด เนื่องจากหากมีการกำหนดมาตรฐานที่ไม่เหมาะสมก็จะทำให้ประชาชนไม่สามารถปฏิบัติตามได้ ทำให้กฎหมายไม่เกิดสภาพบังคับได้จริง นอกจากนี้ยังต้องพึงระวังการกำหนดบทลงโทษให้มีความสอดคล้องเหมาะสมกับการกระทำความผิด รวมทั้งการจะบังคับใช้กฎหมายตามมาตรการการบังคับและควบคุมด้วยการลงโทษนี้ให้เกิดผลจะต้องพิจารณาถึงประสิทธิภาพของหน่วยงานที่บังคับใช้ว่ามีจำนวนคนและงบประมาณ ตลอดจนมีขั้นตอนวิธีการดำเนินงานที่สอดคล้องและรองรับที่จะสามารถดำเนินการบังคับใช้กฎหมายได้หรือไม่อีกด้วย ข้อควรระวังอีกประการหนึ่งคือ ความเสี่ยงต่อการเกิดการทุจริตประพฤติมิชอบของเจ้าหน้าที่ที่มีหน้าที่บังคับใช้กฎหมาย เนื่องจากการดำเนินการบังคับใช้กฎหมายนั้นส่วนมากจะขึ้นอยู่กับดุลยพินิจของเจ้าหน้าที่ผู้รับผิดชอบ จึงอาจเป็นช่องว่างให้ผู้กระทำผิดเสนอเงินสินบนเพื่อให้ตนเองรอดพ้นจาก

การถูกบังคับใช้กฎหมาย จึงจะเห็นได้ว่าแม้มาตรการดังนี้ จะเป็นเครื่องมือหลักในทางกฎหมายที่รัฐใช้ในการควบคุมและรักษาความสงบเรียบร้อยในสังคม แต่การจะบังคับใช้กฎหมายตามมาตรการนี้ให้เป็นผลก็จำเป็นจะต้องอาศัยปัจจัยต่างๆด้วย

2) การกำหนดคุณสมบัติและลักษณะต้องห้าม (Qualifications and Prohibitive Characteristics) เป็นมาตรการทางกฎหมายที่เกิดจากแนวคิดของการบริหารจัดการความเสี่ยง (Risk Management) ด้วยการประเมินความเสี่ยงและแนวโน้มของการฝ่าฝืนกฎเกณฑ์ของรัฐไว้ล่วงหน้า โดยรัฐจะทำการกำหนดคุณสมบัติและลักษณะต้องห้ามของกลุ่มบุคคลที่มีความเสี่ยงไว้ เพื่อเป็นการป้องปรามหรือตัดโอกาสก่อนที่ผู้กระทำผิดจะได้ลงมือกระทำผิด เช่น การกำหนดคุณสมบัติและลักษณะต้องห้ามเกี่ยวกับประสบการณ์การถูกฟ้องร้องดำเนินคดี ประวัติการต้องโทษคดีอาญา ประวัติการเป็นบุคคลล้มละลาย เป็นต้น

มาตรการการกำหนดคุณสมบัติและลักษณะต้องห้ามนี้ ถ้าได้มีการกำหนดไว้อย่างเหมาะสมแล้วจะส่งผลให้เกิดการบังคับใช้กฎหมายที่มีลักษณะเป็นทางอ้อม แต่มีประสิทธิภาพสูง เนื่องจากเป็นมาตรการที่ใช้งบประมาณน้อย อีกทั้งยังมีความชัดเจนและง่ายต่อการทำความเข้าใจของประชาชนทั่วไป แต่อย่างไรก็ตามในการกำหนดคุณสมบัติต้องห้ามต่างๆนั้น จำเป็นจะต้องพิจารณาถึงหลักสำคัญเกี่ยวกับสิทธิเสรีภาพภายใต้รัฐธรรมนูญด้วย

3) ระบบอนุญาต จดทะเบียน และจดแจ้ง (Licensing and Registration) หมายถึง การกำหนดให้ประชาชนที่มีความประสงค์จะดำเนินการกิจการบางประเภท จะต้องได้รับอนุญาตจากหน่วยงานของรัฐที่รับผิดชอบก่อนที่จะเริ่มดำเนินการได้ โดยหน่วยงานของรัฐที่รับผิดชอบในเรื่องนั้นๆ จะเป็นผู้กำหนดหลักเกณฑ์วิธีการตลอดจนเอกสารหลักฐานต่างๆให้แก่ประชาชน โดยมาตรการทางกฎหมายลักษณะนี้มักจะอยู่ในรูปแบบของการขอใบอนุญาตประเภทต่างๆ เช่น ใบอนุญาตประกอบกิจการสถานบริการ ตาม พ.ร.บ.สถานบริการ หรือ ใบอนุญาตจำหน่ายสุรา ตามกฎหมายที่เกี่ยวข้อง เป็นต้น

นอกจากใบอนุญาตแล้ว มาตรการทางกฎหมายรูปแบบนี้ยังรวมถึงระบบการจดทะเบียน ซึ่งมีลักษณะคล้ายกันกับการขอใบอนุญาตเพียงแต่เมื่อผู้ใดได้รับการจดทะเบียนแล้วไม่จำเป็นต้องมาต่ออายุเหมือนในกรณีของการขอใบอนุญาต หรืออีกนัยหนึ่งคือสามารถดำเนินกิจการต่างๆได้จนกว่าจะถูกเพิกถอนทะเบียน รวมทั้งระบบการจดแจ้งซึ่งมีลักษณะเพียงกำหนดให้ประชาชนจะต้องแจ้งให้หน่วยงานของรัฐทราบว่าจะดำเนินกิจการใดๆ เพื่อให้รัฐสามารถตรวจสอบได้ ซึ่ง

มาตรการในการจดทะเบียนและการจดแจ้งนี้ เป็นมาตรการควบคุมทางกฎหมายที่ลดหลั่นกันมาจากการขออนุญาตตามลำดับความสำคัญในการควบคุมกิจการต่างๆของรัฐ

4) การให้ควบคุมกันเองของภาคเอกชน (Self – Control / Self – Regulation) เป็นมาตรการที่รัฐมอบหมายหน้าที่ให้ประชาชนที่ดำเนินกิจการในลักษณะเดียวกัน ทำหน้าที่ในการควบคุมกำกับดูแลกันเองในลักษณะของกลุ่ม โดยอาจอยู่ในรูปแบบของสมาคมหรือองค์กรของผู้ที่ประกอบวิชาชีพเดียวกัน เช่น สภาทนายความ หอการค้า หรือ สมาคมร้านค้าทอง เป็นต้น โดยกลุ่มหรือองค์กรเหล่านี้สามารถกำหนดข้อบังคับต่างๆเพื่อใช้บังคับกับผู้ที่เข้าร่วมเป็นสมาชิก โดยหากสมาชิกฝ่าฝืนหรือไม่ปฏิบัติตามข้อบังคับก็อาจมีบทลงโทษเฉพาะกลุ่ม ยกเว้นในกรณีที่การดำเนินการของกลุ่มองค์กรใดที่อาจกระทบต่อประชาชนส่วนรวม รัฐก็อาจจะเข้าไปแทรกแซงหรือควบคุมกำกับดูแลในลักษณะต่างๆ เช่น การรับรองสถานะของกลุ่มผ่านการอนุญาตให้จัดตั้งหรือการพิจารณาเห็นชอบข้อบังคับของกลุ่มต่างๆ เป็นต้น การใช้มาตรการดังกล่าวจะทำให้เกิดการกำกับดูแลที่เหมาะสมและสอดคล้องกับการดำเนินกิจการของภาคเอกชน ได้มากกว่าการที่รัฐเป็นผู้ออกมาตรการบังคับเอง

5) การให้ความรู้และการบังคับให้เปิดเผยข้อมูลสำคัญ (Education and Disclosure Regulation) เกิดจากแนวคิดพื้นฐานที่ว่า “หากประชาชนไม่รู้กฎหมาย ก็ย่อมที่เป็นการยากที่จะสามารถปฏิบัติตามกฎหมายได้อย่างถูกต้องครบถ้วน” ดังนั้น มาตรการดังกล่าวจึงถือเป็นมาตรการสำคัญที่หน่วยงานที่มีหน้าที่ในการบังคับใช้กฎหมาย จะต้องดำเนินการประชาสัมพันธ์ให้ประชาชนได้รับทราบทั้งในส่วนของเนื้อหาสาระและข้อมูลที่เกี่ยวข้องกับการบังคับใช้กฎหมาย เช่น การประชาสัมพันธ์ให้ประชาชนได้รับทราบเมื่อมีการแก้ไขปรับปรุงตัวบทกฎหมาย ที่อาจกระทบต่อการใช้ชีวิตตามปกติของประชาชน การจัดอบรมให้ความรู้เกี่ยวกับกฎหมายต่างๆ หรือแม้กระทั่งการรายงานข่าวหรือเผยแพร่ผลการจับกุมและการลงโทษต่างๆ

นอกจากเจ้าหน้าที่ของรัฐที่มีหน้าที่บังคับใช้กฎหมายแล้ว มาตรการทางกฎหมายนี้ยังหมายความรวมถึง การกำหนดให้ผู้ประกอบการต่างๆจะต้องเปิดเผยข้อมูลสำคัญให้ประชาชนได้รับรู้อย่างครบถ้วน เพื่อให้ผู้บริโภคหรือผู้รับบริการมีข้อมูลเพียงพอสำหรับการพิจารณาตัดสินใจเลือกใช้สินค้าหรือบริการใดๆ เช่น ข้อมูลเกี่ยวกับสินค้า วัสดุหรือวัตถุดิบที่ใช้ในการผลิต ความเหมาะสมของราคากับคุณภาพสินค้า ตลอดจนสามารถพิจารณาถึงข้อดีข้อเสีย หรือความเสี่ยงภัยหรืออันตรายที่อาจเกิดขึ้นจากการใช้สินค้าหรือบริการนั้นๆ ซึ่งหากรัฐมีการกำหนดให้ผู้ประกอบการต่างๆเปิดเผย

ข้อมูลสำคัญเหล่านี้ ก็จะส่งผลให้ประชาชนทั่วไปได้รับความคุ้มครองและทำให้ประชาชนสามารถเข้าถึงข้อมูลสำคัญได้อย่างทั่วถึง

6) การให้สิทธิประโยชน์และสิ่งจูงใจ (Incentive – Based Regime) เป็นมาตรการทางกฎหมายรูปแบบหนึ่งที่เป็นการจูงใจให้ประชาชนกระทำการต่างๆไปในทิศทางที่ก่อให้เกิดประโยชน์ต่อส่วนรวม โดยอาศัยการให้รางวัลหรือสิ่งตอบแทนต่างๆ เพื่อเป็นการเสริมแรงจูงใจ โดยการให้สิทธิประโยชน์ดังกล่าวนี้อาจอยู่ในรูปแบบต่างๆ เช่น จากปัญหาฝุ่นมลพิษ PM 2.5 รัฐบาลอาจนำรูปแบบมาตรการทางกฎหมายนี้ มาจูงใจให้แก่ผู้ประกอบการโรงงานต่างๆ โดยการยกเว้นภาษีหรือลดภาษีให้กับโรงงานที่มีการควบคุมระบบการดำเนินการจนสามารถจัดการเรื่องปัญหาฝุ่นมลภาวะได้อย่างเป็นรูปธรรมและได้ผลสัมฤทธิ์ หรือ ในกรณีของการตั้งรางวัลนำจับ สำหรับผู้แจ้งเบาะแสกรณีมีกลุ่มวัยรุ่นจับกลุ่มแข่งรถในทาง เพื่อช่วยเหลือเจ้าหน้าที่ในการสืบสวนจับกุมผู้กระทำผิด เป็นต้น

มาตรการดังกล่าวนี้เปิดโอกาสให้ประชาชนหรือภาคเอกชน สามารถตัดสินใจได้ด้วยตนเองว่าจะกระทำการอันเป็นการสอดคล้องต่อนโยบายให้สิทธิประโยชน์นี้หรือไม่ โดยปราศจากสภาพบังคับตามกฎหมาย ซึ่งหากมาตรการดังกล่าวเป็นไปอย่างมีประสิทธิภาพก็จะส่งผลทำให้ภาครัฐประหยัดเวลาและงบประมาณในขั้นตอนการบังคับใช้กฎหมายต่างๆได้เป็นอย่างดีอีกด้วย อย่างไรก็ตามด้วยรูปแบบของมาตรการนี้ที่ไม่มีสภาพบังคับที่เด็ดขาดจึงอาจทำให้การนำไปใช้บังคับไม่สามารถควบคุมหรือจัดการกับเหตุการณ์ต่างๆที่จำเป็นจะต้องได้รับการควบคุมอย่างเข้มงวดได้

7) การให้สัมปทานและการกำหนดเงื่อนไขในกระบวนการจัดซื้อจัดจ้าง (Franchising and Public Procurement) มาตรการในรูปแบบนี้มีลักษณะเป็นการให้สัมปทานแก่ภาคเอกชนเพียงรายเดียวเพื่อดำเนินกิจการของรัฐบางประเภท ซึ่งมักจะเป็นกิจการที่มีลักษณะเป็นการผูกขาด หรือมีลักษณะที่มีผู้ผลิตรายเดียวจะเกิดประสิทธิภาพสูงสุด หรือเป็นกิจการที่มีขนาดใหญ่จนหากรัฐปล่อยให้มีการแข่งขันกันจะทำให้เกิดความสิ้นเปลืองต่อทรัพยากรเป็นจำนวนมาก โดยรัฐจะกำหนดให้ภาคเอกชนรายที่ได้รับสัมปทานมีสิทธิและหน้าที่ในการควบคุมกำกับดูแลมิให้ภาคเอกชนรายอื่นประกอบกิจการในลักษณะเดียวกัน ซึ่งมาตรการนี้ถือเป็นการบังคับใช้กฎหมายในทางอ้อมหรืออาจกล่าวได้ว่าเป็นการมอบอำนาจและหน้าที่ในการบังคับใช้กฎหมายให้กับผู้ได้รับสัมปทานไปโดยปริยาย อันเกิดจากแนวคิดที่ว่าภาคเอกชนที่ได้รับสัมปทานจากรัฐย่อมที่จะต้องรักษาผลประโยชน์สูงสุดแห่งตนไว้ จึงทำให้เกิดแรงจูงใจที่จะเป็นกลไกในการควบคุมและบังคับใช้กฎหมายแทนภาครัฐได้อย่างมีประสิทธิภาพ

อีกมาตรการหนึ่งที่มีลักษณะเป็นการบังคับใช้ในทางอ้อมคือ มาตรการในการกำหนดเงื่อนไขต่างๆในกระบวนการจัดซื้อจัดจ้างของหน่วยงานภาครัฐ โดยการกำหนดเงื่อนไขเหล่านี้ถือเป็นสภาพบังคับในทางอ้อม เพื่อให้ภาคเอกชนจำเป็นจะต้องจัดการกิจการต่างๆให้มีลักษณะตรงตามที่รัฐกำหนด จึงจะมีสิทธิ์เข้าเสนอราคาเพื่อทำการจัดซื้อจัดจ้างกับหน่วยงานภาครัฐได้ เช่น การห้ามผู้ประกอบการที่มีประวัติการฝ่าฝืนกฎหมายแรงงานเข้าทำสัญญากับรัฐ ซึ่งจะส่งผลให้ผู้ประกอบการทั่วไปเกิดแรงจูงใจที่จะปฏิบัติตามข้อกำหนดของกฎหมายมากขึ้น

8) การให้สิทธิแก่ประชาชนและการสร้างระบบความรับผิด (Rights and Liabilities) เป็นมาตรการที่มีลักษณะเป็นการมุ่งให้ประชาชนเกิดความตระหนักและคุ้มครองสิทธิของตนด้วยตนเอง หรือสามารถกล่าวอีกนัยหนึ่งได้ว่าเป็นการมอบภาระให้ภาคเอกชนบังคับใช้กฎหมายแทนรัฐ เช่น ประชาชนมีสิทธิตามกฎหมายที่จะใช้ทรัพยากรธรรมชาติเพื่ออุปโภคบริโภคได้ (ที่ไม่ได้มีลักษณะเป็นทรัพยากรที่มีจำกัดและควบคุมโดยรัฐ) ดังนั้น หากมีโรงงานหรือผู้ประกอบการใดๆ ประกอบกิจการอันเป็นการกระทบกับสิทธิของประชาชนส่วนรวม เช่น มีการปล่อยน้ำเสียลงในแม่น้ำลำคลองจนทำให้ชาวบ้านโดยรอบไม่สามารถใช้น้ำอุปโภคบริโภคได้ กรณีนี้ประชาชนที่ได้รับผลกระทบก็อาจฟ้องร้องเรียกค่าเสียหายได้ ก่อให้เกิดผลเป็นสภาพบังคับที่จะทำให้ผู้ประกอบการต่างๆจำจะต้องรักษามาตรฐานการดำเนินการให้เป็นไปตามกฎหมายเพื่อไม่ให้เกิดความเสียหายต่อรัฐและสังคมส่วนรวม

แม้การดำเนินการตามมาตรการนี้จะส่งผลให้ภาครัฐประหยัดงบประมาณและบุคลากรในการบังคับใช้กฎหมายได้ก็ตาม แต่ก็มีลักษณะคล้ายเป็นการผลักภาระให้กับภาคเอกชนที่จะต้องแบกรับค่าใช้จ่ายในการฟ้องร้องไว้แทน จนอาจทำให้ประชาชนตัดสินใจไม่นำคดีเข้าสู่กระบวนการยุติธรรมส่งผลให้ไม่เกิดสภาพบังคับตามกฎหมาย อีกทั้งยังขาดความแน่นอนในการบังคับใช้เนื่องจากกรณีพิพาทต่างๆที่เกิดขึ้นมีลักษณะแตกต่างกันไป จึงอาจทำให้ไม่เกิดความคุ้มครองได้อย่างแท้จริง โดยเฉพาะอย่างยิ่งมาตรการดังกล่าวนี้จะไม่สามารถใช้บังคับได้กับกรณีที่ ผลประโยชน์อันเกิดจากการประกอบกิจการแบบผิดกฎหมายนั้น มีมากกว่าการชดใช้ค่าเสียหายให้แก่ประชาชนผู้ได้รับความเดือดร้อน เป็นต้น

จะเห็นได้ว่าการป้องกันอาชญากรรมในมิติของกฎหมายนั้น มีมาตรการทางกฎหมายหลายรูปแบบ ดังนั้นเพื่อให้เกิดประสิทธิภาพสูงสุดในการบังคับใช้กฎหมายเพื่อยับยั้งการกระทำความผิดได้นั้น จำเป็นจะต้องพิจารณาว่าควรจะนำมาตรการรูปแบบใดมาบังคับใช้กับสถานการณ์ใด

หรือกรณีปัญหาใดให้มีความเหมาะสมสอดคล้องกัน โดยในการวิจัยครั้งนี้จะได้ศึกษาและวิเคราะห์ว่าในการป้องกันอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัสในประเทศไทยนั้น ควรจะมีการกำหนดทิศทางของมาตรการทางกฎหมายรูปแบบใดต่อไป

2.11 งานวิจัยที่เกี่ยวของ

2.11.1 งานวิจัยที่เกี่ยวกับสกุลเงินเข้ารหัสและบิทคอยน์

J. R. Clark, M. Scott Niederjohn, and William C. Wood (2018) ได้ศึกษาเกี่ยวกับความหมายและลักษณะการทำงานของบิทคอยน์ โดยได้อธิบายว่า “บิทคอยน์” คือสกุลเงินเสมือนจริง (Virtual Currency) ที่มีรูปแบบของการกระจายข้อมูล (Decentralized) ที่ใช้ระบบบล็อคเชนในการยืนยันและบันทึกข้อมูลทางธุรกรรมต่างๆ บิทคอยน์ถูกสร้างขึ้นโดยนักพัฒนา (หรือกลุ่มนักพัฒนา) นิรนามที่ใช้ชื่อว่า ซาโตชิ นากาโมโตะ (Satoshi Nakamoto) และเริ่มมีการนำมาใช้ตั้งแต่ ค.ศ. 2009 โดยที่มูลค่าของบิทคอยน์นั้นเป็นอิสระ ไม่ขึ้นอยู่กับรัฐบาล ธนาคารกลาง หรือแม้กระทั่งสถาบันทางการเงินต่างๆ โดยผู้ใช้งานสามารถใช้บิทคอยน์ในการทำธุรกรรมต่างๆเช่น การโอน – รับบิทคอยน์กันได้โดยตรง โดยไม่จำเป็นต้องแสดงตัวตนผู้ใช้งานที่แท้จริงแต่อย่างใด

ธุรกรรมต่างๆของบิทคอยน์จะถูกตรวจสอบยืนยันโดยการใช้ฉันทามติของผู้ใช้งานทุกคนในระบบ (A System of Network Consensus) กล่าวคือ เมื่อมีการทำธุรกรรมเกิดขึ้นในแต่ละครั้ง รายการทำธุรกรรมนั้นๆจะถูกประกาศให้ผู้ใช้งานในระบบทุกคนทราบผ่านรูปแบบการเข้ารหัสข้อมูลคอมพิวเตอร์ โดยผู้ใช้งานที่ต้องการจะเข้าร่วมการตรวจสอบความถูกต้องของธุรกรรมดังกล่าวก็จะต้องใช้ศักยภาพของเครื่องคอมพิวเตอร์ในการคำนวณเพื่อถอดรหัสข้อมูลดังกล่าวแข่งขันกับผู้ใช้งานคนอื่นๆ และผู้ที่สามารถถอดรหัสและเข้าทำการตรวจสอบยืนยันข้อมูลทางธุรกรรมได้เป็นคนแรกก็จะได้รับรางวัลเป็นบิทคอยน์ ทำให้ผู้ที่เข้าร่วมการตรวจสอบยืนยันทางธุรกรรมดังกล่าวถูกเรียกว่า “กลุ่มนักขุด” (Miners) โดยที่กระบวนการตรวจสอบยืนยันธุรกรรมด้วยระบบฉันทามตินี้จะเกิดขึ้นหมุนเวียนไปเพื่อให้บิทคอยน์สามารถทำงานต่อไปได้ จนกระทั่งมีบิทคอยน์ถูกสร้างขึ้นในระบบครบ 21 ล้านบิทคอยน์ตามที่ผู้ออกแบบระบบได้กำหนดไว้ ซึ่งมีการประมาณการกันว่าบิทคอยน์จะถูกสร้างขึ้นครบตามจำนวนดังกล่าวในปี ค.ศ. 2041 ซึ่งเมื่อถึงเวลานั้นบิทคอยน์จะกลายเป็นของหายากและจะส่งผลให้บิทคอยน์มีมูลค่าสูงในลักษณะเดียวกันกับทองคำหรือสินทรัพย์อื่นๆ แต่ในขณะเดียวกันด้วยลักษณะการทำงานของบิทคอยน์ โดยเฉพาะอย่างยิ่งสถานภาพของผู้ใช้งานบิท

คอยน์ที่มีลักษณะเป็นบุคคลนิรนาม (Anonymous) ก็ส่งผลทำให้ บิทคอยน์ถูกนำไปใช้ในการก่ออาชญากรรมออนไลน์ผ่านเว็บไซต์ใต้ดินต่างๆ เช่น ถูกใช้ในการลักลอบซื้อขายยาเสพติดและการลักลอบค้าประเวณี เป็นต้น

นอกจากนี้ยังได้มีการกล่าวถึง สถานภาพความเป็นสินทรัพย์ของบิทคอยน์ จากการพิจารณาเปรียบเทียบบิทคอยน์ (Bitcoin) กับสินทรัพย์อื่นๆอย่าง สกุลเงินดอลลารสหรัฐ (U.S. Dollar) สกุลเงินยูโรของสหภาพยุโรป (Euro) และทองคำ (Gold) โดยพิจารณาจากหลักเกณฑ์ของความเป็นเงินหรือสินทรัพย์ต่างๆ 3 ประการได้แก่ 1) การเป็นสื่อกลางในการแลกเปลี่ยน (Medium of Exchange) 2) การเป็นที่เก็บมูลค่า (Store of Value) และ 3) การเป็นหน่วยของมูลค่า (Unit of Account) โดยมีผลการเปรียบเทียบตามภาพดังนี้

	Medium of Exchange	Store of Value	Unit of Account
U.S. dollar	Excellent; accepted around the world	Good as long as U.S. inflation remains low.	Near-universal use in keeping accounts
Euro	Excellent; accepted throughout Europe and many other places	Good, as long as inflation remains low in the European Union	Widely used in keeping accounts
Gold	Slow and relatively costly to exchange for other goods and services	Highly dependent on world conditions, but best when world conditions	Not frequently used as a unit of account
Bitcoin	Slow to exchange for other goods and services, though it may improve with technological change	Highly dependent on future values of Bitcoin	Not frequently used as a unit of account

ภาพที่ 6 เปรียบเทียบความเป็นสินทรัพย์ระหว่างบิทคอยน์และทรัพย์สินประเภทต่างๆ
(J. R. Clark, M. Scott Niederjohn, and William C. Wood, 2018)

จากภาพดังกล่าวสามารถอธิบายได้ว่าผู้วิจัยนำเสนอว่า สกุลเงินดอลลารสหรัฐ (U.S. Dollar) มีคุณลักษณะของความเป็นเงินหรือสินทรัพย์ทั้งสามประการได้เป็นอย่างดี กล่าวคือ สกุลเงินดอลลารสหรัฐได้รับการยอมรับให้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการได้ทั่วโลก แม้กระทั่งบัตรเครดิตของสถาบันการเงินต่างๆยังมีความยึดโยงอยู่กับสกุลเงินดอลลาร์สหรัฐ รวมทั้งการเป็นที่เก็บมูลค่าที่ดีเนื่องจากมีภาวะความเป็นเงินเฟ้อต่ำ ทำให้คงอำนาจของการซื้อขายให้แก่ผู้ที่ครอบครองไว้ได้เป็นอย่างดี ประกอบกับการที่สกุลเงินดอลลาร์สหรัฐสามารถทำหน้าที่เป็นหน่วยวัดมูลค่าของสินค้า

และบริการต่างๆได้อย่างเป็นสากลเกือบจะทั่วโลก เช่นเดียวกันกับสกุลเงินยูโรของสหภาพยุโรป (Euro) ที่ได้รับการยอมรับให้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการในภูมิภาคยุโรปและภูมิภาคต่างๆ ทั้งยังมีภาวะเป็นเงินเฟ้อต่ำ และถูกใช้เป็นหน่วยวัดทางมูลค่าของสินค้าและบริการต่างๆอย่างแพร่หลาย

ในขณะที่ทองคำ (Gold) มีลักษณะที่แตกต่างจากสกุลเงินทั้งสองสกุล โดยทองคำนั้นไม่เหมาะกับการเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการโดยตรงเนื่องจากร้านค้า ผู้ประกอบการหรือผู้ให้บริการทั่วไปไม่มีความสามารถในการตรวจสอบคุณภาพและความบริสุทธิ์ของทองคำได้อย่างแม่นยำ อีกทั้งด้วยราคาทองคำมีความผกผันสูงหรือมีการเปลี่ยนแปลงไปตามเหตุการณ์สำคัญต่างๆของโลก จึงทำให้ทองคำนั้นยังทำหน้าที่เป็นที่เก็บมูลค่าได้ไม่ดีเท่าที่ควรเมื่อเทียบกับสกุลเงินทั้งสอง นอกจากนี้ในสังคมโลกยังไม่นิยมนำทองคำไปใช้ในการกำหนดมูลค่าของสินค้าและบริการต่างๆเท่าใดนัก ส่วนในกรณีของบิทคอยน์ (Bitcoin) นั้นก็ยังไม่สามารถทำหน้าที่เป็นเงินหรือสินทรัพย์ได้อย่างสมบูรณ์ เมื่อเทียบกับสกุลเงินทั้งสองสกุล ทั้งในแง่ของการเป็นสื่อกลางในการแลกเปลี่ยนที่ยังมีร้านค้าหรือผู้ประกอบการที่ยอมรับให้สามารถใช้บิทคอยน์ชำระแทนมูลค่าของสินค้าและบริการไม่มากนัก ประกอบกับมูลค่าของบิทคอยน์ที่ไม่ได้ยึดโยงอยู่กับรัฐบาล ธนาคารกลางหรือสินทรัพย์อื่นใด แต่ขึ้นอยู่กับปริมาณความต้องการของผู้สนใจครอบครอง (Demand-Supply) เป็นหลัก จึงทำให้มูลค่าของบิทคอยน์ไม่แน่นอน อีกทั้งเมื่อพิจารณาเปรียบเทียบมูลค่าของบิทคอยน์กับทองคำก็จะเห็นได้ว่า แม้ในอนาคตทองคำอาจไม่เป็นที่ต้องการในการเก็บสะสมอีกต่อไป แต่มูลค่าของทองคำอาจไม่ได้รับผลกระทบเท่าใดนัก เนื่องจากทองคำยังมีความจำเป็นในการใช้ในภาคธุรกิจและอุตสาหกรรม ในขณะที่หากความต้องการถือครองบิทคอยน์ในฐานะสินทรัพย์หมดลงไปในอนาคต ก็จะทำให้บิทคอยน์กลายเป็นเพียงข้อมูลคอมพิวเตอร์ที่ไม่มีคุณค่าและไม่สามารถจับต้องได้ ด้วยลักษณะที่กล่าวมานี้จึงทำให้บิทคอยน์ยังขาดคุณสมบัติการเป็นที่เก็บมูลค่าที่ดี รวมทั้งในประเด็นของการเป็นหน่วยวัดมูลค่าที่สังคมโลกยังไม่นิยมนำไปกำหนดมูลค่าของสินค้าและบริการต่างๆ ดังนั้น จึงพอสรุปได้ว่าบิทคอยน์มีลักษณะเป็นสินทรัพย์ที่ยังมีความเป็นสินทรัพย์ที่ยังไม่สมบูรณ์เท่าใดนัก

อัญชนา เหมือนคิด, ธนพล พุกเส็ง, ระดม เจือจันทร์ และ ศิรปัฐช์ บุญครอง (2557) ศึกษาเรื่อง Bitcoin: สกุลเงินของการเข้ารหัสลับที่น่าจับตามอง โดยมีวัตถุประสงค์ในการวิจัยเพื่อศึกษาและนำเสนอข้อมูลเกี่ยวกับการทำงานของบิทคอยน์และการใช้งานด้านต่างๆรวมทั้งปัญหาในด้านความปลอดภัยของบิทคอยน์ โดยในประเด็นด้าน**ข้อมูลเกี่ยวกับการทำงานของบิทคอยน์**นั้น

ผู้วิจัยกล่าวว่า บิทคอยน์เป็นสกุลเงินเข้ารหัสที่ใช้การยืนยันความถูกต้องของธุรกรรมและการป้องกันปัญหาการจ่ายเงินซ้ำซ้อน (Double Spending) ด้วยระบบการเข้ารหัสแบบ Public-Key Cryptography มาประยุกต์ใช้ โดยหากผู้ใช้งานต้องการใช้งานจะต้องสร้างกุญแจส่วนตัว (Private Key) ซึ่งต้องเก็บรักษาไว้เป็นความลับและกุญแจสาธารณะ (Public Key) ซึ่งสามารถประกาศให้ผู้อื่นทราบได้ การใช้งานบิทคอยน์จะต้องทำการเปิดบัญชีกระเป๋าเงิน หรือ Bitcoin Wallet เพื่อใช้เป็นโปรแกรมสำหรับการใช้แลกเปลี่ยนสินค้าและบริการ โดยกระเป๋าเงินดังกล่าวจะอยู่ในรูปแบบอิเล็กทรอนิกส์ ทำหน้าที่ในการแสดงยอดคงเหลือ เก็บประวัติการทำธุรกรรมต่างๆ แต่จะไม่มีการเปิดเผยข้อมูลของเจ้าของบัญชี และในการใช้งานบิทคอยน์ก็ไม่จำเป็นต้องยืนยันตัวบุคคลแต่อย่างใด

การทำธุรกรรมของบิทคอยน์ทำได้โดยระบบจะส่งข้อมูลของธุรกรรมพร้อมลายเซ็นดิจิทัล (Digital Signature) ซึ่งมีความสัมพันธ์กับกุญแจส่วนตัว (Private Key)และกุญแจสาธารณะ (Public Key) ของผู้ใช้งาน เข้าสู่โครงข่ายที่มีผู้ใช้งานบิทคอยน์ทั่วโลกเชื่อมต่ออยู่ เพื่อให้ผู้ใช้งานรายอื่นทำการตรวจสอบลายเซ็นและอนุมัติการทำธุรกรรม โดยกระบวนการตรวจสอบธุรกรรมนี้จะเป็นกระบวนการที่สำคัญมาก เนื่องจากข้อมูลทางธุรกรรมต่างๆจะถูกเข้ารหัสด้วยระบบค่า Hash แบบ SHA256 ดังนั้นผู้ใช้งานจะต้องตรวจสอบข้อมูลความถูกต้องของธุรกรรมผ่านการถอดรหัส และยังต้องสุ่มเพื่อแก้โจทย์ทางคณิตศาสตร์เพื่อคำนวณค่า Nonce ตามโจทย์ที่ระบบกำหนด จึงจะสามารถเก็บบันทึกข้อมูลทางธุรกรรมลงในบล็อคได้ ซึ่งการเก็บข้อมูลในแต่ละบล็อคก็จะมีการเข้ารหัสข้อมูลของบล็อคก่อนหน้าเอาไว้ทำให้การเก็บข้อมูลมีลักษณะเป็นลูกโซ่ไปข้างหน้าทางเดียว ซึ่งระบบการเก็บข้อมูลในลักษณะนี้จึงถูกเรียกว่า “บล็อคเชน” (Blockchain)

ประเด็นในด้านของการใช้งานบิทคอยน์นั้น ผลการศึกษาพบว่ามีการใช้งานบิทคอยน์ในการชำระค่าสินค้าและบริการทั่วไป และในขณะเดียวกันก็มีการนำบิทคอยน์ไปใช้ในทางผิดกฎหมาย เช่น ตัวอย่างของกรณีตลาดมืดออนไลน์ (Silk Road) และใน**ประเด็นเรื่องปัญหาด้านความปลอดภัย**จากผลการศึกษาพบว่ามีประเด็นที่ผู้ใช้งานต้องระมัดระวังเกี่ยวกับการเก็บรักษาข้อมูลกุญแจส่วนตัวไว้เป็นความลับ มิเช่นนั้นอาจถูกโจรกรรมบิทคอยน์ได้ นอกจากนี้ยังมีประเด็นความเสี่ยงทางเทคนิคและระบบคอมพิวเตอร์ เช่น ความเสี่ยงที่อาจจะถูกมิจฉาชีพที่เป็นแฮกเกอร์เข้ามาโจมตีระบบ จนทำให้บิทคอยน์ได้รับความเสียหายอย่างในกรณีของบริษัท Mt.GOX ในประเทศญี่ปุ่น เป็นต้น

ลักษนันท์ พลอยวัฒนาวงศ์ (2561) ศึกษาเรื่อง บิทคอยน์และเทคโนโลยีบล็อคเชน โดยได้ศึกษาถึง**คุณสมบัติของบิทคอยน์** ว่ามีลักษณะเหมือนสกุลเงินแบบดั้งเดิมในด้านการเป็นเครื่องมือที่

ใช้ในการแลกเปลี่ยนซื้อขายและการลงทุน โดยบิทคอยน์มีคุณลักษณะพิเศษคือการกระจายอำนาจการเก็บข้อมูลและไม่อยู่ภายใต้การควบคุมขององค์กรปกครองหรือสถาบันใดๆ อีกทั้งการทำธุรกรรมในระบบบิทคอยน์ไม่ได้เชื่อมโยงไปยังข้อมูลส่วนบุคคลหรือไม่มีการระบุตัวตนผู้ใช้งานที่แท้จริงแต่อย่างใด นอกจากนี้บิทคอยน์ยังใช้ระบบการเก็บข้อมูลแบบบล็อคเชนทำให้ข้อมูลมีความปลอดภัยมากกว่าการเก็บข้อมูลไว้ที่ส่วนกลางอย่างธนาคารหรือสถาบันการเงินต่างๆ โดยในการใช้งานบิทคอยน์จะต้องกระทำผ่านซอฟท์แวร์บิทคอยน์หรือกระเป๋าสตางค์บิทคอยน์ (Bitcoin Wallet) ที่มีด้วยกัน 4 รูปแบบ ได้แก่ 1) กระเป๋าสตางค์แบบฮาร์ดแวร์ (Hardware Wallet), กระเป๋าสตางค์แบบออนไลน์ (Web Wallet), กระเป๋าสตางค์สำหรับโทรศัพท์มือถือ (Mobile Wallet) และ กระเป๋าสตางค์บนเครื่องคอมพิวเตอร์ (Desktop Wallet) โดยในการทำธุรกรรมแต่ละครั้ง ผู้ใช้งานจะต้องระบุเงื่อนไขและรายละเอียดการทำธุรกรรมที่ต้องการผ่านกระเป๋าสตางค์ดังกล่าว

นอกจากนี้ผู้วิจัยยังกล่าวถึงส่วนประกอบของระบบการทำงานของบิทคอยน์ ได้แก่ **เทคโนโลยีบล็อคเชน** ว่าเป็นสายโซ่ของกล่องหรือก้อนข้อมูลที่ถูกจัดเก็บเรียงต่อกัน โดยเทคโนโลยีบล็อคเชนเกิดจากการทำงานร่วมกันของแนวคิดของเทคโนโลยีต่างๆ ได้แก่ ระบบการเข้ารหัสข้อมูลด้วยรหัสผ่านส่วนตัว (Private Key Cryptography), การติดต่อสื่อสารกันโดยตรงระหว่างผู้ใช้งาน (Peer-to-Peer) และโปรแกรมการทำงาน (Blockchain's Protocol) บล็อคเชนได้เปลี่ยนระบบการเงินจากที่มีธนาคารเป็นศูนย์กลางกลายเป็นการสร้างเครือข่ายข้อมูลในรูปแบบของระบบบัญชีสาธารณะ เพื่อให้เกิดความโปร่งใสและปลอดภัยมากยิ่งขึ้นด้วยการกระจายให้ผู้ใช้งานมีส่วนร่วมในการช่วยกันหรือแข่งขันกันตรวจสอบความถูกต้องของข้อมูลธุรกรรมต่างๆที่เกิดขึ้นในระบบ นอกจากนี้ในการจัดเก็บข้อมูลทางธุรกรรมของบิทคอยน์จะเก็บในลักษณะรวมข้อมูลไว้ในกล่องหรือบล็อคข้อมูลทางธุรกรรมจากนั้น จะทำการเข้ารหัสทางเดียวเพื่อเป็นการอ้างอิงว่าบล็อคปัจจุบัน มีข้อมูลหรือเชื่อมต่อมาจากบล็อคใดก่อนหน้า ซึ่งความเชื่อมโยงนี้กระทำผ่านการเข้ารหัสข้อมูลทางเดียวจึงทำให้ข้อมูลที่ได้เรียงต่อกันอย่างสามารถระบุที่มาของข้อมูลได้ และจะมีการเก็บข้อมูลไปในลักษณะอ้างอิงต่อกันไปคล้ายสักษณะของห่วงโซ่การเก็บข้อมูล โดยระบบบล็อคเชนนี้ยังสามารถนำไปประยุกต์ใช้กับการทำงานต่างๆ เช่น การซื้อขายหุ้น การซื้อขายอสังหาริมทรัพย์ การจัดการเอกสารด้วยลายเซ็นดิจิทัล เป็นต้น นอกจากนี้ผู้ศึกษายังได้กล่าวถึงข้อได้เปรียบของการใช้งานบิทคอยน์ว่าการใช้บิทคอยน์เป็นการทำธุรกรรมที่ถูกและรวดเร็ว และเมื่อมีการโอนบิทคอยน์ไปแล้วจะไม่สามารถเรียกคืนได้ (ไม่เหมือนในกรณีของการยกเลิกการซื้อสินค้าจากบัตรเครดิต เป็นต้น) รวมทั้งการทำ

ธุรกรรมบิทคอยน์ไม่ต้องใช้เอกสารใดๆ จึงทำให้ง่ายและสะดวกต่อการใช้งาน และด้วยลักษณะพิเศษตามที่ได้กล่าวมานี้ จึงอาจทำให้บิทคอยน์และบล็อคเชน เป็นอีกเทคโนโลยีหนึ่งที่อาจเปลี่ยนแปลงระบบการเงินการธนาคาร รวมทั้งระบบการจัดการฐานข้อมูลต่างๆที่เกี่ยวข้องในอนาคต

จะเห็นได้ว่าทั้งงานวิจัยของ **อัญชนา เหมือนคิด, ธนพล พุกเส็ง, ระดม เจือจันทร์ และศิรปัฐช์ บุญครอง (2557)** และ **ลักษนันท์ พลอยวัฒนาวงศ์ (2561)** ได้กล่าวถึงคุณลักษณะพิเศษของบิทคอยน์เช่นเดียวกัน รวมทั้งกล่าวถึงระบบบล็อคเชนซึ่งเป็นระบบการเก็บรักษาข้อมูลการทำธุรกรรมของบิทคอยน์ แต่ในงานวิจัยของ **ลักษนันท์ พลอยวัฒนาวงศ์ (2561)** ได้อธิบายให้เข้าใจได้ว่า บิทคอยน์และบล็อคเชนไม่ใช่สิ่งเดียวกัน และบล็อคเชนไม่ได้เป็นเทคโนโลยีที่ถูกสร้างมาเพื่อเป็นระบบเบื้องหลังบิทคอยน์เท่านั้น แต่ยังสามารถนำไปใช้เป็นกลไกในการออกแบบระบบการทำงานได้อีกหลากหลายรูปแบบ

2.11.2 งานวิจัยที่เกี่ยวกับการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรม

Sean Foley, Jonathan R. Karlsen and Talis J. Putnins (2018) ศึกษาเกี่ยวกับ **ปริมาณการใช้สกุลเงินเข้ารหัสในกิจกรรมที่ผิดกฎหมาย** (Sex, Drugs, and Bitcoin: How much illegal activity is financed through cryptocurrencies) โดยมีวัตถุประสงค์เพื่อต้องการจะทราบถึงปริมาณของการนำสกุลเงินเข้ารหัสโดยเฉพาะอย่างยิ่งบิทคอยน์ไปใช้ในกิจกรรมที่ผิดกฎหมายต่างๆ ที่เกี่ยวกับเรื่องทางเพศ ยาเสพติด และกิจกรรมที่ผิดกฎหมายต่างๆ โดยใช้การออกแบบโปรแกรมคอมพิวเตอร์ผนวกกับหลักคณิตศาสตร์เพื่อใช้ในการคำนวณและวิเคราะห์ผล

ผลการศึกษาปรากฏว่ามีผู้ใช้งานบิทคอยน์ (Bitcoin User) มากถึง 1 ใน 4 ของจำนวนผู้ใช้งานบิทคอยน์ ทั้งหมดที่ใช้บิทคอยน์ในกิจกรรมที่ผิดกฎหมาย และมีการทำธุรกรรมของบิทคอยน์ที่เกี่ยวกับกิจกรรมที่ผิดกฎหมายมากถึง 37 ล้านธุรกรรม คิดเป็นมูลค่าที่เกี่ยวข้องกับกิจกรรมที่ผิดกฎหมายต่างๆเหล่านี้มากถึง 76,000 ล้านเหรียญสหรัฐ (เท่ากับ ร้อยละ 46 ของมูลค่าการทำธุรกรรมทั้งหมดของบิทคอยน์) ซึ่งมูลค่านี้มีความใกล้เคียงกับมูลค่าความเสียหายที่เกิดขึ้นจากตลาดการลักลอบซื้อขายยาเสพติดในสหรัฐอเมริกาและยุโรป

ทั้งนี้ผู้วิจัยได้กล่าวว่า ลักษณะการใช้งานของผู้ใช้งานบิทคอยน์ที่ไม่ต้องแสดงตัวตนหรือมีลักษณะเป็นบุคคลนิรนาม (Anonymity) ทำให้เกิดการขยายตัวของการใช้งานบิทคอยน์ในทางผิดกฎหมายไปอย่างรวดเร็ว ทั้งนี้บิทคอยน์ยังกลายเป็นแม่แบบที่ส่งผลทำให้เกิดการพัฒนาของสกุลเงิน

เข้ารหัสอื่นๆเพื่อออกมารองรับการใช้งานที่ผิดกฎหมาย เช่น มีการปกปิดทั้งข้อมูลทางธุรกรรมและตัวตนผู้ใช้งาน จนทำให้สกุลเงินเข้ารหัสในช่วงหลังบิทคอยน์ (Alternative Cryptocurrencies) ที่มีลักษณะเอื้อต่อการใช้ในกิจกรรมที่ผิดกฎหมายเหล่านี้ถูกเรียกว่า “Shadow Cryptocurrencies” ซึ่งผู้วิจัยก็ยังพบว่า สัดส่วนการเติบโตของสกุลเงินเข้ารหัสกลุ่มนี้ยังแปรผันตรงกันกับสัดส่วนการเติบโตของการใช้บิทคอยน์ในกิจกรรมที่ผิดกฎหมายอีกด้วย

นอกจากนี้ผู้วิจัยยังได้ให้ความเห็นถึงปัญหาการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในกิจกรรมที่ผิดกฎหมายโดยเปรียบเทียบกับการใช้เงินสด (Cash) ว่า เมื่อพิจารณาเปรียบเทียบกันจากข้อเท็จจริงก็จะพบว่าเงินสดยังคงถูกใช้ในกิจกรรมที่ผิดกฎหมายสูงสุดมาตั้งแต่อดีตจนถึงปัจจุบัน เนื่องจากการตรวจสอบติดตามก็ยังคงทำได้เพียงการตรวจสอบจากเลขธนบัตรเท่านั้น แต่ความแตกต่างที่สำคัญระหว่างการใช้เงินสดและสกุลเงินเข้ารหัสคือ การที่การใช้สกุลเงินเข้ารหัสมีลักษณะเป็นการทำธุรกรรมดิจิทัล (Digital Transaction) ทำให้การกระทำผิดกฎหมายสามารถกระทำได้โดยไม่ติดข้อจำกัดทางพรมแดนหรือขอบเขตของรัฐ ไม่จำเป็นต้องเผชิญความเสี่ยงจากการตรวจสอบผ่านเจ้าหน้าที่ในแบบดั้งเดิมหรืออาจกล่าวได้ว่า การนำสกุลเงินเข้ารหัสมาใช้เป็นสื่อกลางในกิจกรรมที่ผิดกฎหมายต่างๆ ทำให้ตลาดมืด (Black Market) ถูกยกระดับเป็น ตลาดมืดอิเล็กทรอนิกส์ (Black E-commerce) ที่จะก่อความเสียหายให้กับสังคมโลกได้มากกว่าการกระทำความผิดด้วยเงินสดในอนาคต

Adam Turner and Angela Samantha Maitland Irwin (2018) ได้ศึกษาเกี่ยวกับแนวทางในการวิเคราะห์พฤติกรรมการใช้บิทคอยน์ในทางผิดกฎหมาย (Bitcoin transactions: a digital discovery of illicit activity on the blockchain) โดยมีวัตถุประสงค์ในการศึกษาเพื่อต้องการแสวงหาวิธีการในการตรวจสอบพฤติกรรมการใช้งานบิทคอยน์ที่ผิดกฎหมายและแนวทางในการเปิดเผยตัวตนที่แท้จริงของผู้ที่ใช้บิทคอยน์ในการกระทำความผิดกฎหมาย โดยอาศัยการวิเคราะห์ข้อมูลที่เกี่ยวกับพฤติกรรมการทำธุรกรรมที่เกี่ยวกับบิทคอยน์ด้วยโปรแกรมคอมพิวเตอร์ประเภทต่างๆด้วยหลักการทางสถิติและความรู้เฉพาะทางทางด้านข้อมูลคอมพิวเตอร์ โดยที่การศึกษาครั้งนี้มีแนวคิดมาจากการพบข้อมูลบ่งชี้ว่าสกุลเงินเข้ารหัสต่างๆโดยเฉพาะอย่างยิ่ง “บิทคอยน์” เป็นตัวเลือกที่ถูกนำไปใช้เป็นสื่อกลางในการก่ออาชญากรรมประเภทต่างๆ เช่น ใช้ในการซื้อขายยาเสพติด ใช้ในการสร้างโปรแกรมมัลแวร์ (Malware) หรือ เครื่องมือสอดแนม (Spying Tools) ในทางคอมพิวเตอร์ ใช้ในการเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการผิดกฎหมายต่างๆในตลาดมืดออนไลน์ ใช้ใน

การฟอกเงินผ่านเกมออนไลน์และการสนับสนุนเงินให้แก่กลุ่มผู้ก่อการร้าย ซึ่งสาเหตุที่บิทคอยน์ถูกนำไปใช้เป็นสื่อกลางในการกระทำความผิดดังกล่าวเป็นเพราะ ระบบการทำงานของบิทคอยน์ที่เปิดเผยข้อมูลทางธุรรรมแต่ไม่มีการลงทะเบียนหรือเก็บข้อมูลเพื่อยืนยันตัวตนผู้ใช้งานบิทคอยน์ในแต่ละบัญชีที่แท้จริง (Personally Identifiable Information [PPI]) จนทำให้สำนักงานสอบสวนกลางสหรัฐอเมริกา (FBI) กล่าวถึงประเด็นปัญหาจากลักษณะดังกล่าวนี้ว่า “บิทคอยน์” จะกลายเป็นสวรรค์ของการฟอกเงินและอาชญากรรมประเภทต่างๆ เพราะการติดตามและสืบสวนเพื่อยืนยันตัวตนผู้ใช้งานบิทคอยน์ในการกระทำผิดกฎหมายจะเป็นไปอย่างยากลำบากและมีโอกาสน้อยมากที่จะประสบความสำเร็จแม้จะอาศัยเทคโนโลยีในปัจจุบันก็ตาม

ทั้งนี้ผู้ศึกษาซึ่งเป็นผู้ที่มีความเชี่ยวชาญทางด้านโปรแกรมคอมพิวเตอร์ ได้ศึกษาและทำความเข้าใจหลักการทำงานของบิทคอยน์เชิงลึกจนเกิดสมมติฐานว่า แม้บิทคอยน์จะไม่ได้มีการระบุตัวตนผู้ใช้งานที่แท้จริง (PPI) ก็ตาม แต่ผู้ใช้งานบิทคอยน์ไม่ได้ไร้ตัวตนอย่างสมบูรณ์แบบเสมอไป แต่มีโอกาสที่จะสามารถถูกระบุตัวตนได้จากการวิเคราะห์และจำแนกพฤติกรรมการใช้บิทคอยน์อย่างละเอียดถี่ถ้วน ด้วยการเฝ้าสังเกตุข้อมูลการใช้งานกุญแจสาธารณะ (Public Key) ที่ใช้ในการทำธุรกรรมบิทคอยน์ในแต่ละครั้ง แล้วนำไปวิเคราะห์เพื่อสร้างรูปแบบของพฤติกรรมในการใช้งานบิทคอยน์ทำธุรกรรมต่างๆ (A Pattern of Behavior) โดยโปรแกรมคอมพิวเตอร์เฉพาะทาง จากนั้นเมื่อสามารถจำแนกรูปแบบของพฤติกรรมการใช้งานได้แล้ว เมื่อพบพฤติกรรมที่น่าสงสัยก็จะนำข้อมูลการใช้งานเหล่านั้นไปตรวจสอบเชิงลึกว่าในพฤติกรรมการใช้งานนั้นๆ มีความเกี่ยวข้องเชื่อมโยงกับธุรกรรมภายนอกระบบบิทคอยน์ ที่มีการลงทะเบียนข้อมูลยืนยันตัวบุคคลไว้หรือไม่ต่อไป ซึ่งแนวคิดและการวิจัยดังกล่าวจำเป็นจะต้องอาศัยความรู้ความเข้าใจในด้านวิศวกรรมคอมพิวเตอร์ชั้นสูง

การทดลองเพื่อทดสอบสมมติฐานดังกล่าว ผู้ศึกษาได้ใช้โปรแกรมคอมพิวเตอร์ประเภทต่างๆ ได้แก่ โปรแกรมไวร์ชาร์ค (Wireshark) ซึ่งเป็นโปรแกรมที่ใช้ในการติดตามข้อมูลที่แสดงความเชื่อมโยงในการใช้งานของบิทคอยน์ (Bitcoin Protocol) และโปรแกรมบิทคอยน์คอร์ (Bitcoin Core) ซึ่งเป็นโปรแกรมที่จำเป็นสำหรับการใช้งานบิทคอยน์เต็มรูปแบบ ประกอบกับการใช้เว็บเบราซ์เซอร์ (Web Browser) ทั่วไปเพื่อใช้ในการสมัครใช้งานกระเป๋าเงินบิทคอยน์ (Bitcoin Wallet) โดยจากผลการศึกษาพบว่า สามารถใช้โปรแกรมคอมพิวเตอร์ดังกล่าวติดตามการทำธุรกรรมที่เกี่ยวกับบิทคอยน์ได้จริง อีกทั้งยังสามารถใช้ในการวิเคราะห์และจำแนกพฤติกรรมการใช้งาน จนสามารถพบรูปแบบพฤติกรรมการใช้งานและสามารถระบุบัญชีผู้ใช้งาน (Bitcoin Address) ที่มีพฤติกรรมต้อง

สงสัยได้ในเบื้องต้น แต่ก็ยังไม่สามารถนำข้อมูลพฤติกรรมดังกล่าวไปใช้ยืนยันตัวตนบุคคลผู้ใช้งานที่แท้จริงได้แต่อย่างใด เพราะแม้จะทราบบัญชีผู้ใช้งานต้องสงสัยหรือพบธุรกรรมที่ต้องสงสัย แต่ก็ไม่มีหลักฐานหรือข้อมูลใดๆที่จะเชื่อมโยงไปถึงบุคคลผู้กระทำความผิดได้จริงแต่อย่างใด อย่างไรก็ตามในทางทฤษฎีแล้วการพัฒนาทางด้านสถาปัตยกรรมคอมพิวเตอร์ในอนาคต มีโอกาสที่จะทำให้นักพัฒนาหรือเจ้าหน้าที่ของรัฐสามารถสร้างโปรแกรมที่สามารถตรวจจับพฤติกรรมการใช้งานบิทคอยน์ที่ผิดกฎหมายได้อย่างมีประสิทธิภาพมากยิ่งขึ้นจนแนวโน้มสูงที่นำไปสู่การตรวจสอบยืนยันตัวตนผู้ใช้งานบิทคอยน์ในการกระทำความผิดได้

2.11.3 งานวิจัยที่เกี่ยวกับแนวทางการกำกับดูแลสกุลเงินเข้ารหัส

Aneta Vondráčková (2016) ได้ศึกษาเกี่ยวกับ **มาตรการในการกำกับดูแลสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสของสหภาพยุโรป (Regulation of Virtual Currency in the European Union)** โดยกล่าวว่า จากปริมาณการใช้งานสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสที่มีจำนวนเพิ่มขึ้นอย่างรวดเร็ว ทำให้เกิดความเสี่ยงที่จะมีการนำสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสต่างๆ ไปใช้ในการก่ออาชญากรรม เช่น การฟอกเงิน การเลี่ยงภาษี การสนับสนุนเงินทุนให้กลุ่มผู้ก่อการร้าย รวมถึงอาชญากรรมรูปแบบอื่นๆ ทำให้สหภาพยุโรปตระหนักถึงปัญหาดังกล่าวและมีความพยายามที่จะกำหนดมาตรการต่างๆเพื่อกำกับดูแลสกุลเงินเสมือนหรือสกุลเงินเข้ารหัส โดยกระบวนการศึกษาและพัฒนามาตรการดังกล่าวของสหภาพยุโรป ได้เริ่มต้นขึ้นตั้งแต่ปี ค.ศ. 2012 จากรายงานของธนาคารกลางยุโรป (The 2012 European Central Bank Report) โดยในรายงานดังกล่าวได้มีการศึกษาและให้คำนิยาม “สกุลเงินเสมือน (Virtual Currency)” เป็นครั้งแรกโดยให้ความหมายว่าเป็นเงินดิจิทัลที่ไม่อยู่ภายใต้การกำกับดูแลของหน่วยงานของรัฐที่ผู้พัฒนามีเจตนาสร้างขึ้นเพื่อใช้งานภายในเฉพาะกลุ่มบุคคลในชุมชนเสมือน ซึ่งจากการให้คำจำกัดความดังกล่าวของธนาคารกลางแห่งยุโรป ทำให้สหภาพยุโรปมีมุมมองเริ่มแรกต่อสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสว่าจะถูกใช้งานในวงแคบเท่านั้น

แต่ต่อมาในปี ค.ศ. 2013 หน่วยงานกำกับการธนาคารแห่งยุโรปได้ออกแถลงการณ์ (The European Banking Authority Statement) เพื่อแจ้งเตือนถึงความเสี่ยงต่างๆที่เกี่ยวกับสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสและยังมีการเรียกร้องไปยังผู้นำด้านการเงินการธนาคารของแต่ละประเทศเพื่อขอความร่วมมือให้สถาบันการเงินของชาติสมาชิกที่ดำเนินการเกี่ยวกับระบบการจ่ายเงินและ

ระบบเครดิต งดเว้นการซื้อ ถือครองหรือรับแลกเปลี่ยนสกุลเงินเสมือนหรือสกุลเงินเข้ารหัส และยังมีการเรียกร้องให้สภานิติบัญญัติแห่งยุโรป (EU Legislative) ขยายขอบเขตการป้องกันและปราบปรามการฟอกเงินให้ครอบคลุมการซื้อขายแลกเปลี่ยนสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสด้วย ผนวกกับการเกิดเหตุการณ์การก่อการร้ายในกรุงปารีส ประเทศฝรั่งเศสในปี ค.ศ.2015 ที่กระตุ้นให้สหภาพยุโรปมีแนวคิดเกี่ยวกับการป้องกันการโจมตีระบบการเงินของรัฐและการลักลอบสนับสนุนทางด้านการเงินแก่กลุ่มผู้ก่อการร้ายซึ่งมีความเกี่ยวข้องกับการใช้งานสกุลเงินเสมือนหรือสกุลเงินเข้ารหัส

จนกระทั่งในปี ค.ศ. 2016 สภายุโรป (European Parliament) ได้ผลักดันให้คณะกรรมาธิการยุโรป (European Commission) ตั้งคณะทำงานร่วมกันระหว่างชาติสมาชิกเพื่อกำหนดกฎหมายหรือแนวทางการปฏิบัติ ทั้งในด้านการเฝ้าระวังและควบคุมกำกับดูแลการใช้งานสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสที่ชัดเจน จนต่อมาได้มีการกำหนดข้อปฏิบัติที่เป็นแนวทางการควบคุมการใช้งานสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสไว้ใน กฎหมายยุโรปเกี่ยวกับการต่อต้านการฟอกเงินฉบับที่ 4 (The Fourth Anti – Money Laundering Directive) โดยมีแนวคิดหลักในการดำเนินการคือ เจตจำนงในการลดหรือแก้ปัญหาเรื่องคุณลักษณะของสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสที่มีการปกปิดตัวตนที่แท้จริงของผู้ใช้งาน (Anonymous) และมุ่งตรวจสอบและสร้างความโปร่งใสให้กับเส้นทางการเงินต่างๆ เพื่อป้องกันการฟอกเงิน การปกปิดเส้นทางการเงิน และการลักลอบสนับสนุนเงินทุนให้แก่กลุ่มผู้ก่อการร้าย โดยมีกรอบการปฏิบัติคือ

1) การกำหนดให้การประกอบธุรกิจเกี่ยวกับสกุลเงินเสมือนหรือสกุลเงินเข้ารหัส ทั้งในส่วนของผู้ประกอบธุรกิจการรับซื้อขายแลกเปลี่ยน และผู้ให้บริการเกี่ยวกับกระเป๋าเงินอิเล็กทรอนิกส์ที่ใช้กับสกุลเงินเสมือน (Virtual Wallets and Exchange Platforms) จะต้องอยู่ภายใต้การควบคุมดูแลของรัฐ ในลักษณะเดียวกันกับผู้ประกอบธุรกิจเกี่ยวกับการเงิน โดยจะต้องทำการกำหนดมาตรการในการตรวจสอบลูกค้าของตน และต้องรายงานให้เจ้าหน้าที่ของรัฐทราบกรณีที่พบการทำธุรกรรมที่เกี่ยวกับสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสที่มีลักษณะต้องสงสัย นอกจากนี้ในการทำธุรกรรมต่างๆของสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสจะต้องถูกตรวจสอบเส้นทางการเงินและความโปร่งใสของที่มาของเงินเช่นเดียวกันกับสกุลเงินปกติ

2) สร้างและพัฒนาระบบที่จะทำการกำกับดูแลและคุ้มครองผู้ใช้งานในการทำธุรกรรม การซื้อขายแลกเปลี่ยนสกุลเงินเสมือน ให้มีความน่าเชื่อถือ รวมทั้งออกแบบระบบการรักษา

ความปลอดภัยของระบบคอมพิวเตอร์หรือระบบอิเล็กทรอนิกส์ที่เกี่ยวข้องกับสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสเพื่อป้องกันการถูกโจมตี

ชาติสมาชิกสหภาพยุโรปได้นำกรอบแนวทางนี้ไปพิจารณาดำเนินการให้เหมาะสมกับกฎหมายภายในของตนเอง โดยผู้วิจัยได้ยกตัวอย่างถึงสาธารณรัฐเช็ก (The Czech Republic) ซึ่งได้มีการกำหนดมาตรการให้ผู้ประกอบธุรกิจเกี่ยวกับการซื้อขายแลกเปลี่ยนสกุลเงินเสมือนจะต้องอยู่ภายใต้กฎหมายที่เกี่ยวกับการฟอกเงินของชาติรวมทั้งจะถูกตรวจสอบด้วยมาตรการต่างๆเพื่อแก้ปัญหาการไม่ระบุตัวตน (Anonymity) โดยผู้ประกอบธุรกิจรับแลกเปลี่ยนสกุลเงินเสมือนหรือสกุลเงินเข้ารหัส รวมทั้งผู้ให้บริการเกี่ยวกับกระเป๋าเงินดิจิทัลสำหรับสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสจะต้องทำการยืนยันตัวบุคคลผู้ใช้งานทุกกรณี รวมทั้งจะต้องตรวจสอบเส้นทางการเงินของผู้ใช้บริการในกรณีที่มีการซื้อขายแลกเปลี่ยนในช่วงมูลค่าตั้งแต่ 1000 ยูโร (ประมาณ 35,000 บาท) ขึ้นไป โดยหากเจ้าหน้าที่ของรัฐตรวจพบว่าผู้ให้บริการไม่ได้ดำเนินการตามมาตรการดังกล่าว จะถือว่าการซื้อขายแลกเปลี่ยนครั้งนั้นเป็นโมฆะและมีความผิดตามกฎหมาย ซึ่งผลจากมาตรการดังกล่าวทำให้ปัจจุบันทำให้สาธารณรัฐเช็กมีการใช้งานสกุลเงินเสมือนจริงหรือสกุลเงินเข้ารหัสนี้อย่างแพร่หลายและยังไม่กระทบต่อความมั่นคงหรือความสงบสุขภายในประเทศ ทั้งยังป้องกันจากการฟอกเงินและการสนับสนุนเงินทุนแก่กลุ่มผู้ก่อการร้ายได้อย่างมีประสิทธิภาพ

จุฑารัตน์ ชวดนุช (2557) ศึกษาเรื่อง ปัญหากฎหมายในการนำบิทคอยน์มาใช้สำหรับทำธุรกรรมออนไลน์ในประเทศไทย ผลการศึกษาพบว่า บิทคอนย์เริ่มเป็นที่สนใจของสังคมโลกมากขึ้นและมีแนวโน้มที่จะได้รับการยอมรับให้ใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการมากขึ้น เช่น มีการเพิ่มขึ้นของจำนวนร้านค้าหรือผู้ประกอบธุรกิจต่างๆที่ยอมรับให้ผู้ใช้บริการชำระเป็นบิทคอยน์ได้ ส่งผลทำให้เกิดความนิยมในการใช้งานบิทคอยน์ออกไปในวงกว้างทั่วโลก อีกประเด็นหนึ่งที่ทำให้บิทคอยน์เป็นที่นิยมคือแนวคิดในการออกแบบบิทคอยน์ที่ต้องการสร้างให้บิทคอยน์เป็นสื่อกลางในการแลกเปลี่ยนที่มีลักษณะในการลดอุปสรรคและต้นทุนในการทำธุรกรรมทางการเงินต่างๆอันจะช่วยส่งเสริมกิจกรรมการค้าผ่านช่องทางออนไลน์ที่เข้ากับยุคดิจิทัลไร้พรมแดนได้เป็นอย่างดี แต่ในขณะเดียวกันกลไกการทำงานของบิทคอยน์ที่ยังขาดความยอมรับในแง่ของกฎหมายและด้วยสถานภาพของบิทคอยน์ที่ไม่ถูกควบคุมด้วยกติกามาตรฐานก็เป็นปัจจัยสำคัญที่ผู้ที่สนใจเข้ามาใช้งานบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆจะต้องพิจารณาอย่างรอบคอบ เนื่องจากบิทคอยน์ยังคงมีความเสี่ยงอยู่มาก เช่น ในเรื่องมูลค่าที่มีความผันผวนสูงเนื่องจากราคาของบิทคอยน์ขึ้นอยู่กับความต้องการ

ของตลาดในลักษณะของกลไกอุปสงค์อุปทาน หรือ ในเรื่องความเสี่ยงด้านความปลอดภัยเนื่องจากบิทคอยน์มีลักษณะเป็นเงินเสมือน (Virtual Currency) ไม่มีตัวตน จึงอาจส่งผลให้การเก็บรักษาอาจจะเผชิญกับภัยคุกคามในโลกไซเบอร์ไม่ว่าจะเป็นการถูกแฮกเกอร์โจรกรรมข้อมูล ภัยจากไวรัสคอมพิวเตอร์ รวมทั้งความเสี่ยงที่มิจฉาชีพจะนำสกุลเงินเข้ารหัสไปใช้ในการฟอกเงินหรือใช้เป็นเครื่องมือในการหลีกเลี่ยงภาษีจากการขายสินค้าและบริการเนื่องจากไม่สามารถตรวจสอบได้และยังไม่มีกฎหมายใดควบคุมกำกับดูแล อีกทั้งยังไม่มีการยอมรับให้บิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ สามารถนำไปชำระหนี้กันได้ตามกฎหมาย จากประเด็นปัญหาที่กล่าวมาจึงได้มีการเสนอข้อเสนอแนะดังนี้

1) ควรมีการออกกฎ ระเบียบ กำกับดูแล และกำหนดให้เว็บไซต์ต่างๆที่ยอมรับการทำธุรกรรมด้วยบิทคอยน์ในการซื้อขายสินค้าและบริการต่างๆ จะต้องขออนุญาตในการประกอบธุรกิจรวมถึงธุรกิจอื่นๆ เช่น โรงแรม ร้านหนังสือ ร้านอาหาร เพื่อประโยชน์ในการจัดเก็บภาษีและเพื่อความสะดวกในการบังคับใช้กฎหมายที่เกี่ยวข้อง

2) ควรกำหนดให้การทำธุรกรรมบิทคอยน์อยู่ภายใต้การดูแลของสถาบันการเงินและสำนักงานป้องกันและปราบปรามการฟอกเงิน และสถาบันการเงินมีหน้าที่ต้องรายงานการทำธุรกรรมต่อสำนักงานป้องกันและปราบปรามการฟอกเงิน

3) ควรกำหนดให้สถาบันการเงินของรัฐ เป็นผู้ให้บริการรับแลกเปลี่ยนบิทคอยน์เท่านั้น รวมถึงบริการรับแลกเปลี่ยนผ่านเครื่องกดเงินอัตโนมัติ (Bitcoin ATM)

4) ควรกำหนดให้สำนักงานป้องกันและปราบปรามการฟอกเงินมีอำนาจหน้าที่ในการวางหลักเกณฑ์และกำกับดูแลให้มีการปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน รวมทั้งรับรายงานการทำธุรกรรมจากสถาบันการเงิน เพื่อดำเนินการวิเคราะห์ตรวจสอบเพื่อป้องกันไม่ให้มีการนำบิทคอยน์ไปใช้ในการฟอกเงิน รวมทั้งมีควรกำหนดให้อำนาจในการ ยึด อายัดบิทคอยน์ด้วย

5) หน่วยงานอื่นๆที่เกี่ยวข้อง ควรให้การสนับสนุนการดำเนินการในเรื่องการป้องกันการฟอกเงิน เช่น ธนาคารแห่งประเทศไทยควรออกมาตรการกำกับดูแลให้สถาบันการเงินส่งรายงานการทำธุรกรรมให้กับสำนักงานป้องกันและปราบปรามการฟอกเงิน

6) ควรกำหนดให้หน่วยงานอื่นๆ เช่น กรมการปกครอง กรมศุลกากร กรมสรรพากร ต้องให้ความร่วมมือในการให้ข้อมูลที่เป็นประโยชน์ในการตรวจสอบบุคคลหรือเส้นทางการเงินที่อาจ

เกี่ยวข้องกับการกระทำผิดหากได้รับการร้องขอจาก สำนักงานป้องกันและปราบปรามการฟอกเงิน และหน่วยงานที่มีหน้าที่ในการปราบปรามอาชญากรรม เช่น สำนักงานตำรวจแห่งชาติ หรือ กรมสอบสวนคดีพิเศษ

7) ควรกำหนดให้การใช้บิทคอยน์ในการเล่นเกมรูแปแบบต่างๆ เช่น การพนัน เป็นสิ่งผิดกฎหมายเพื่อป้องกันการฟอกเงินผ่านการเล่นการพนันเนื่องจากยากแก่การตรวจสอบ

8) ควรกำหนดให้มีการสร้างเครือข่ายเฝ้าระวังเว็บพนันผิดกฎหมาย

9) ควรกำหนดให้หน่วยงานที่เกี่ยวกับการควบคุมดูแลการกระทำผิดบนเครือข่ายอินเทอร์เน็ต มีอำนาจในการควบคุมดูแลและตรวจสอบ

10) ควรกำหนดให้ผู้ใช้บิทคอยน์ ต้องมีการระบุชื่อนามสกุลจริงในการใช้งาน เพื่อเป็นการ เพื่อเป็นการเปิดเผยตัวตนเพื่อความสะดวกในการควบคุม

ณหทัย สุขเสนา (2560) ศึกษาเรื่อง มาตรการกำกับดูแลเงินสกุลดิจิทัลและการปรับใช้กฎหมายไทยกับเงินสกุลดิจิทัล: บิทคอยน์ โดยผลการศึกษาพบว่า ผลการศึกษาเกี่ยวกับ**ความหมายและสถานะทางกฎหมายของบิทคอยน์**นั้น แม้แต่ละประเทศจะให้คำนิยามของบิทคอยน์แตกต่างกันออกไป แต่แนวคิดหลักที่ทุกประเทศเห็นพ้องต้องกันคือ ยังไม่มีประเทศใดยอมรับให้บิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆเป็นเงินตราจริง รวมทั้งยังไม่รับรองให้เป็นสิ่งที่ใช้ชำระหนี้กันได้ตามกฎหมาย (Legal Tender) อีกด้วย ในส่วนของสถานะทางกฎหมายของบิทคอยน์ในขณะที่ทำการวิจัยนั้น ในประเทศไทยยังไม่มีการออกกฎหมายหรือมาตรการใดๆมากำกับดูแลการใช้บิทคอยน์ มีเพียงประกาศแจ้งเตือนประชาชนเกี่ยวกับการใช้บิทคอยน์จากธนาคารแห่งประเทศไทยว่าบิทคอยน์ไม่ได้อยู่ภายใต้การกำกับดูแลของทางการและไม่อยู่ภายใต้กฎหมายของประเทศไทย การใช้หรือการถือครองบิทคอยน์จึงไม่ได้รับการคุ้มครองจากหน่วยงานของรัฐ แต่ในขณะเดียวกันแม้ว่าจะยังไม่มีสถานะเป็นเงินตราและไม่ได้อยู่ภายใต้การกำกับดูแลโดยทางการของก็ตาม แต่ยังมีผู้นิยมใช้บิทคอยน์ในการทำธุรกรรมต่าง ๆ ดังนั้น ผู้ศึกษาจึงได้นำเสนอผลการศึกษา**สภาพปัญหาและอุปสรรคที่เกิดจากการใช้บิทคอยน์ในประเทศไทย** ว่ามีประเด็นปัญหาอยู่สองประการคือ

1) ความเสี่ยงจากการใช้บิทคอยน์ในการทำธุรกรรมต่าง ๆ เนื่องจากการใช้บิทคอยน์ในประเทศไทย(ในขณะนั้น)ยังไม่มีกฎหมายใดออกมาเพื่อรองรับการทำธุรกรรมดังกล่าวและเนื่องจากบิทคอยน์ยังไม่ถือเป็นเงินตราตามกฎหมาย ดังนั้นการทำธุรกรรมต่างๆที่เกี่ยวกับบิทคอยน์จึงไม่ได้รับการคุ้มครอง การใช้บิทคอยน์ซื้อขายแลกเปลี่ยนจึงเป็นเพียงข้อตกลงร่วมกันระหว่างผู้ซื้อกับผู้ขาย

และหากเกิดกรณีปัญหาต่างๆขึ้นการนำคดีฟ้องร้องต่อศาลก็จะเป็นไปอย่างยากลำบาก เพราะการทำธุรกรรมของบิทคอยน์นั้น ไม่จำเป็นต้องเปิดเผยข้อมูลของคู่ค้าหรือผู้ทำธุรกรรมต่อกัน เช่น ชื่อ ที่อยู่ ประวัติการทำธุรกรรมและไม่จำเป็นต้องแสดงตัวตนในการใช้บริการ ดังนั้น หากเกิดความเสียหายแล้วย่อมเป็นการยากที่จะหาตัวผู้กระทำความผิดและผู้เสียหายอาจไม่ได้รับการเยียวยาในกรณีนี้ นอกจากนี้ถึงแม้คดีขึ้นสู่ศาลก็อาจมีปัญหาในการพิจารณาคดีเนื่องจากบิทคอยน์ยังไม่มีนิยามหรือสถานะทางกฎหมายทำให้การจะนำกฎหมายมาปรับใช้นั้นย่อมทำได้ยากหรือไม่อาจจะกระทำได้

2) ปัญหาในการกำกับดูแลบิทคอยน์ในประเทศไทย เนื่องจากบิทคอยน์ไม่ได้ออกโดยธนาคารหรือสถาบันการเงินของรัฐและไม่ได้อยู่ภายใต้การควบคุมหรือกำกับดูแลในลักษณะเดียวกันกับเงินตราที่ใช้กันอยู่ในระบบแต่บิทคอยน์ถูกควบคุมด้วยระบบกลไกของเทคโนโลยีบล็อคเชน ซึ่งหากรัฐต้องการจะกำกับดูแลบิทคอยน์โดยตรงก็จำเป็นจะต้องทำการศึกษาในระบบการทำงานของบล็อคเชนที่เป็นเรื่องทางเทคนิคคอมพิวเตอร์ขั้นสูงซึ่งอาจต้องใช้ระยะเวลานาน อย่างไรก็ตาม หากรัฐยังไม่มีการออกมาตรการต่างๆเพื่อใช้กำกับดูแลบิทคอยน์ในประเทศไทยในเบื้องต้นแล้ว อาจมีการนำบิทคอยน์ไปใช้ในทางที่ผิดกฎหมายได้ อย่างเช่น การใช้บิทคอยน์ในการฟอกเงินหรือการนำบิทคอยน์ไปใช้เพื่อชำระค่าสินค้าที่ไม่ถูกกฎหมาย เช่น อาวุธปืนที่ไม่มีใบอนุญาต หรือยาเสพติด เป็นต้น

จากประเด็นปัญหาที่กล่าวมาข้างต้น ผู้ศึกษาจึงได้เสนอแนะว่าประเทศไทยควรพิจารณากำหนดสถานะทางกฎหมายให้กับบิทคอยน์ให้ชัดเจน เพื่อจะได้สามารถออกมาตรการต่างๆมากำกับดูแลได้อย่างชัดเจน อีกทั้งยังจะสามารถนำกฎหมายต่างๆที่เกี่ยวข้องมาปรับใช้กับบิทคอยน์ และควรจะมีการศึกษามาตรการในการป้องกันและปราบปรามใช้บิทคอยน์ไปในทางที่ผิดกฎหมายในประเทศไทย เพื่อให้สอดรับกับสถานการณ์ทางด้านสังคมและเทคโนโลยีที่เปลี่ยนแปลงไป จึงมีความสอดคล้องกับงานวิจัยของ จุฑารัตน์ ชวดนุช (2557) ที่เสนอแนวทางและมาตรการต่างๆเพื่อกำกับดูแลและควบคุมการใช้เงินเข้ารหัสในประเด็นต่างๆเพื่อป้องกันไม่ให้เกิดการนำสกุลเงินเข้ารหัสไปเป็นเครื่องมือในการกระทำผิดกฎหมายตามที่ได้กล่าวมาแล้ว

สิรวิศ ศรีวิลาส (2561) ศึกษาเรื่อง มาตรการในการกำกับดูแลสินทรัพย์ดิจิทัล โดยผลการศึกษาพบว่า ประเทศไทยได้ออกกฎหมายที่เกี่ยวกับสกุลเงินเข้ารหัส คือ พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 มีวัตถุประสงค์เพื่อกำกับดูแลการประกอบธุรกิจสินทรัพย์ดิจิทัลและกำหนดมาตรการทางกฎหมายเกี่ยวกับการเสนอขายโทเคนดิจิทัลแก่ประชาชน (ICO) เพื่อเพิ่มความเชื่อมั่นและเป็นการคุ้มครองนักลงทุนให้ได้รับความคุ้มครองตามกฎหมาย โดยกฎหมาย

ดังกล่าวได้มีการระบุให้ สกุลเงินเข้ารหัสหรือคริปโทเคอร์เรนซี (Cryptocurrency) และ โทเคนดิจิทัล (Digital Token) เป็น “สินทรัพย์ดิจิทัล”(Digital Asset) และยังได้บัญญัติถึงความหมายของการประกอบธุรกิจสินทรัพย์ดิจิทัลว่า หมายถึง การประกอบธุรกิจได้แก่ 1) ศูนย์ซื้อขายสินทรัพย์ดิจิทัล 2) นายหน้าซื้อขายสินทรัพย์ดิจิทัล และ 3) ผู้ค้าสินทรัพย์ดิจิทัล ซึ่งผู้ที่ประสงค์จะประกอบธุรกิจดังกล่าวจะต้องได้รับอนุญาตจากสำนักงานคณะกรรมการหลักทรัพย์และตลาดหลักทรัพย์(ก.ล.ต.) ทั้งนี้ ธุรกิจสินทรัพย์ดิจิทัลดังกล่าวจะถือเป็นสถาบันการเงินที่มีหน้าที่ต้องปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินด้วย

นอกจากกฎหมายดังกล่าวจะกำหนดหลักเกณฑ์เกี่ยวกับการประกอบธุรกิจสินทรัพย์ดิจิทัลแล้ว ยังได้กำหนดหลักเกณฑ์เกี่ยวกับการระดมทุนผ่านการเสนอโทเคนดิจิทัล หรือ Initial Coin Offering (ICO) ด้วย โดยกำหนดให้การเสนอขายโทเคนดิจิทัลต่อประชาชน จะต้องอยู่ภายใต้กฎหมายดังกล่าวในหมวด 3 โดยก่อนจะมีการเสนอขายประชาชนจะต้องมีการยื่นขออนุญาตต่อ ก.ล.ต. และยังมีการจำกัดปริมาณการลงทุนของผู้ลงทุน โดยแบ่งผู้ลงทุนเป็น 2 ประเภท ได้แก่ 1) ผู้ลงทุนรายใหญ่ เช่น สถาบันการเงิน ผู้ลงทุนรายใหญ่ตามประกาศ ก.ล.ต. และนิติบุคคลร่วมลงทุนหรือกิจการร่วมลงทุน เป็นต้น โดยกลุ่มผู้ลงทุนรายใหญ่นี้สามารถลงทุนได้โดยไม่จำกัดจำนวน 2) ผู้ลงทุนรายย่อย จะถูกจำกัดการลงทุนไว้เพียงรายละไม่เกิน 3 แสนบาทต่อการเสนอขายครั้งนั้น ทั้งนี้รวมกันไม่เกิน 4 เท่าของส่วนของผู้ถือหุ้นของผู้ออกโทเคนดิจิทัล หรือไม่เกินร้อยละ 70 ของมูลค่าทั้งหมดที่เสนอขายต่อครั้ง

แม้กฎหมายดังกล่าว จะมีการกำหนดแนวทางการประกอบธุรกิจดิจิทัลและการเสนอขายโทเคนให้แก่ประชาชนตามเพื่อเป็นการกำกับดูแลการใช้งานสกุลเงินเข้ารหัสในเบื้องต้นตามที่ได้กล่าวมาแล้ว แต่จากการพิจารณาข้อกฎหมายดังกล่าวทำให้พบว่า กฎหมายดังกล่าวกำกับดูแลเฉพาะการประกอบธุรกิจเท่านั้น ซึ่งอาจ**ไม่ครอบคลุมถึงกรณีที่ภาคประชาชนหรือภาคเอกชนทำการถือครองและแลกเปลี่ยนสกุลเงินเข้ารหัสด้วยกันเองโดยตรง ซึ่งทำให้การซื้อขายแลกเปลี่ยนสกุลเงินเข้ารหัสด้วยกันเองโดยตรงลักษณะนี้ไม่ถูกตรวจสอบโดยกลไกภาครัฐจนอาจทำให้เกิดเป็นช่องว่างและเป็นช่องทางไปสู่การนำสกุลเงินเข้ารหัสไปใช้ในการก่ออาชญากรรมได้ รวมทั้ง**แม้จะมีการกำหนดให้การประกอบธุรกิจสินทรัพย์ดิจิทัลถือเป็นสถาบันการเงินและมีหน้าที่ตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงินก็ตาม แต่ปรากฏว่าความผิดมูลฐานที่บัญญัติไว้ในกฎหมายฟอก

เงินดังกล่าวยังไม่ครอบคลุมถึงการก่ออาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอีกด้วย จากประเด็นปัญหาที่กล่าวมานี้ ผู้ศึกษาจึงเสนอแนะดังนี้

1) คำจัดความของ “คริปโทเคอร์เรนซี” และ “โทเคนดิจิทัล” ที่บัญญัติไว้ในพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 มีลักษณะกว้างขวางจนอาจก่อให้เกิดปัญหาในการตีความและการบังคับใช้กฎหมายได้ เช่น หากพิจารณาตามความหมายตามกฎหมายแล้ว กรณีของเงินสกุลในเกม หรือโปรแกรมต่างๆอาจถูกตีความเป็นสกุลเงินเข้ารหัส หรือ โทเคนดิจิทัลด้วย ดังนั้น จึงควรมีการแก้ไขคำนิยามดังกล่าวให้เกิดความชัดเจน เช่น จำกัดเฉพาะเหรียญคริปโทเคอร์เรนซี หรือ โทเคนดิจิทัลที่สร้างขึ้นภายใต้ระบบบล็อคเชนเท่านั้น เป็นต้น

2) ในประเด็นด้านการเสนอขายโทเคนดิจิทัลหรือการระดมทุนผ่าน ICO ผู้ศึกษาเสนอให้มีการผ่อนผันในเรื่องของค่าธรรมเนียมตามกฎหมายให้กับผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลรายย่อย หรือ กลุ่มสตาร์ทอัพ เพื่อเป็นการส่งเสริมภาคธุรกิจระดับเล็กให้มีโอกาสเติบโตในตลาด อีกทั้งยังมีการเสนอให้ลดข้อจำกัดในการลงทุนเพื่อเพิ่มความเท่าเทียมและสร้างโอกาสให้นักลงทุนได้เกิดการแข่งขันกันอย่างเป็นธรรมมากยิ่งขึ้น

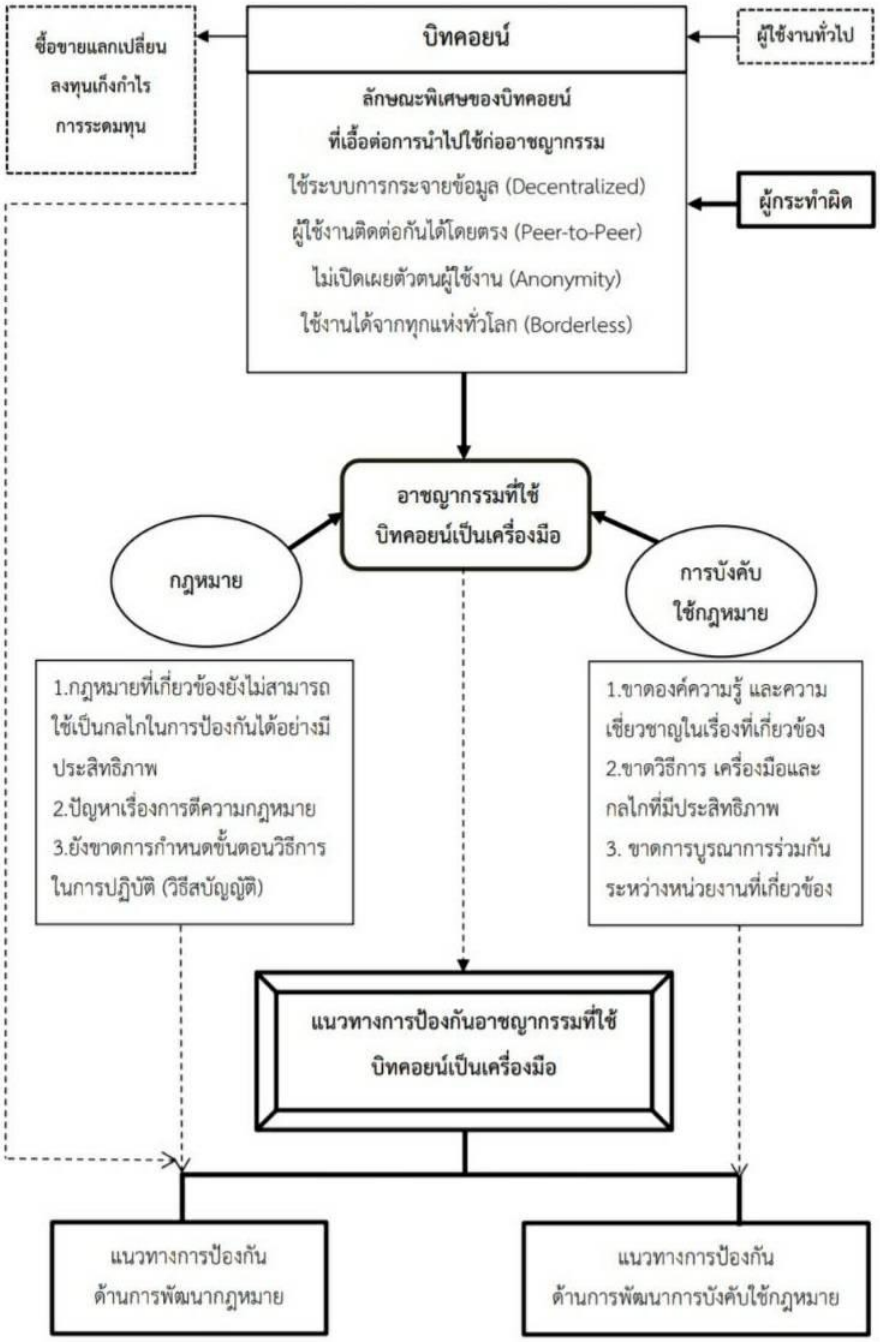
3) ในประเด็นด้านระบบการจัดให้ลูกค้าแสดงตน ผู้ศึกษาเสนอว่าควรจะให้สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ผ่อนผันให้มีการแสดงตนผ่านทางช่องทางอิเล็กทรอนิกส์ หรือระบบ Electronic – Know Your Customer (E-KYC) ซึ่งเป็นลักษณะเดียวกันกับที่ธนาคารแห่งประเทศไทยได้ยอมรับการแสดงตัวตนด้วยวิธีดังกล่าวตั้งแต่ปี พ.ศ. 2559 เนื่องจากในการลงทุนในสกุลเงินเข้ารหัสในประเทศไทย จะมีชาวต่างชาติเข้ามาลงทุนเป็นจำนวนมาก หากไม่มีการผ่อนผันตามลักษณะดังกล่าว อาจเกิดผลกระทบทำให้ประเทศเสียแหล่งเงินทุนไปเป็นจำนวนมาก

4) นอกจากนี้ยังจำเป็นจะต้องพัฒนากฎหมายเกี่ยวกับสกุลเงินเข้ารหัสเพื่อให้ครอบคลุมและสามารถป้องกันการนำสกุลเงินเข้ารหัสไปใช้ในการก่ออาชญากรรม เช่น ป้องกันการนำสกุลเงินเข้ารหัสไปใช้ในการฟอกเงิน รวมทั้ง ผู้ศึกษายังเสนอให้แก้ไขกฎหมายที่เกี่ยวกับการฟอกเงินในประเด็นเรื่องการเพิ่มความผิดมูลฐานเพื่อให้สอดคล้องกับสถานการณ์ในยุคปัจจุบันที่เปลี่ยนแปลงไป เช่น ควรมีการเพิ่มความผิดมูลฐานเกี่ยวกับการลักลอบเจาะระบบรักษาความปลอดภัยเพื่อกระทำต่อสกุลเงินเข้ารหัส เป็นต้น

งานวิจัยดังกล่าว แม้จะมีแนวทางการวิเคราะห์ที่แตกต่างจากงานวิจัยของ ณหทัย สุขเสนา (2560) เนื่องจากในการศึกษาของ สิรวิศ ศรีวิลาส (2561) เป็นการศึกษาภายหลังจากที่ประเทศไทย

ได้ออกพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 แล้วก็ตาม แต่ในขณะเดียวกัน งานวิจัยทั้งสองเรื่องยังมีข้อเสนอแนะไปในแนวทางเดียวกันในประเด็นเรื่องการป้องกันการนำสกุลเงินเข้ารหัสไปใช้ในการก่ออาชญากรรม โดย ณหทัย สุขเสนา (2560) กล่าวว่า หากรัฐยังไม่มีการออกมาตรการต่างๆเพื่อใช้กำกับดูแลบิทคอยน์ ในประเทศไทยในเบื้องต้นแล้ว อาจมีการนำบิทคอยน์ไปใช้ในทางที่ผิดกฎหมายได้ ในขณะที่ สิรวิศ ศรีวิลาส (2561) เสนอแนะว่าแม้จะมีกฎหมายมากำกับดูแลสกุลเงินเข้ารหัสแล้วก็ตาม แต่ยังต้องพัฒนากฎหมายเกี่ยวกับสกุลเงินเข้ารหัสเพื่อให้ครอบคลุมและสามารถป้องกันการนำสกุลเงินเข้ารหัสไปใช้ในการก่ออาชญากรรมได้อย่างมีประสิทธิภาพมากยิ่งขึ้น แสดงให้เห็นว่าประเด็นปัญหาเรื่องการป้องกันการนำสกุลเงินเข้ารหัสไปใช้ในการก่ออาชญากรรมยังเป็นประเด็นสำคัญที่จะต้องทำการศึกษาต่อไป

2.12 กรอบแนวคิดการวิจัย



หมายถึง สภาพปัญหาและสาเหตุที่ทำให้เกิดอาชญากรรมที่ใช้บิทคอยน์เป็นเครื่องมือ

หมายถึง การนำสภาพปัญหาและสาเหตุที่ทำให้เกิดอาชญากรรมที่ใช้บิทคอยน์เป็นเครื่องมือ มาใช้ในการวิเคราะห์และกำหนดแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์เป็นเครื่องมือ

บทที่ 3
บิทคอยน์กับอาชญากรรมและกลไกการป้องกันของรัฐ

ในบทนี้ผู้วิจัยจะได้ศึกษาถึงองค์ความรู้ที่เกี่ยวกับบิทคอยน์ ทั้งในประเด็นเรื่องความหมาย ความเป็นมา คุณลักษณะพิเศษ ขั้นตอนการทำธุรกรรม วิธีการได้มา มูลค่าและสถานภาพของบิทคอยน์ ตลอดจนการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมรูปแบบต่างๆและจะได้ศึกษาถึงแนวนโยบาย กฎหมายและมาตรการต่างๆที่เกี่ยวข้องกับสกุลเงินเข้ารหัสทั้งในต่างประเทศและในประเทศไทย ตลอดจนศึกษาถึงแนวทางการปฏิบัติหน้าที่ของหน่วยงานที่มีหน้าที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในปัจจุบัน ดังนี้

3.1 องค์ความรู้เกี่ยวกับบิทคอยน์

3.1.1 ความหมายของบิทคอยน์

ได้มีผู้ให้ความหมายของบิทคอยน์ ทั้งในส่วนของหน่วยงานภาครัฐ ภาคธุรกิจ นักวิชาการและผู้ที่สนใจศึกษาทั้งจากในประเทศไทยและในต่างประเทศ ดังนี้

หน่วยงานบังคับใช้กฎหมายของสหรัฐอเมริกาอย่างสำนักงานสอบสวนกลาง (Federal Bureau of Investigation หรือ FBI) ได้ให้ความหมายของบิทคอยน์ว่า บิทคอยน์คือสกุลเงินเสมือนจริง (Virtual Currency) ที่มีลักษณะพิเศษ คือ ไม่ใช้ระบบการรวมข้อมูลไว้ที่ศูนย์กลาง แต่ใช้การกระจายข้อมูล (Decentralized) มีลักษณะการทำงานแบบให้ผู้ใช้บริการติดต่อกันได้โดยตรงโดยไม่จำเป็นต้องผ่านตัวกลาง (Peer-to-Peer) และทำงานภายใต้ระบบโครงข่าย (Network-Based) ด้วยลักษณะดังนี้ จึงทำให้บิทคอยน์เหมาะแก่การนำไปใช้ในการเคลื่อนย้ายถ่ายโอน รวมถึงการฟอกเงินสกปรกภายใต้สภาวะที่ไม่สามารถยืนยันตัวบุคคลผู้กระทำผิดได้ (Anonymity) และด้วยลักษณะดังที่กล่าวมา จึงทำให้การสืบสวนในเรื่องที่เกี่ยวกับบิทคอยน์เป็นไปด้วยความซับซ้อน (Federal Bureau of Investigation [FBI], 2012)

ศูนย์ข้อมูลอาชญากรรมองค์การระดับภูมิภาคของสหรัฐอเมริกา (Regional Organized Crime Information Center หรือ ROCIC) ได้ศึกษาวิจัยแนวทางการสืบสวนอาชญากรรมเกี่ยวกับบิทคอยน์และได้ให้คำจำกัดความว่า บิทคอยน์คือสกุลเงินเข้ารหัส (Cryptocurrency) ชนิดหนึ่ง ที่ถูก

นำมาใช้เป็นสื่อกลางในการแลกเปลี่ยน โดยบิทคอยน์ถูกสร้างและเก็บรักษาอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ด้วยระบบบล็อคเชน โดยอาศัยเทคนิคการเข้ารหัสข้อมูลเพื่อประโยชน์ในการสร้างและตรวจสอบยืนยันการทำธุรกรรมทางการเงินของบิทคอยน์ (Regional Organized Crime Information Center [ROCIC], 2018, pp.2)

ในมิติทางด้านการธนาคารและการลงทุนก็ได้มีการให้ความหมายของบิทคอยน์ไว้ โดยธนาคารกลางแห่งยุโรป (European Central Bank) ได้อธิบายว่า บิทคอยน์เป็นสกุลเงินเสมือนจริงที่ไม่สามารถจับต้องได้ โดยบิทคอยน์ถูกสร้างและจัดเก็บด้วยระบบเครือข่ายคอมพิวเตอร์และสมการทางคณิตศาสตร์ แม้บิทคอยน์จะไม่ใช่สกุลเงินจริง แต่ก็ถือเป็นทรัพย์สินชนิดหนึ่งที่สามารถใช้เพื่อเก็งกำไรในด้านการลงทุนได้ (European Central Bank, 2018)

สำหรับในประเทศไทยนั้นหน่วยงานของรัฐที่เกี่ยวข้องอย่าง ธนาคารแห่งประเทศไทย (2557) ได้ออกประกาศฉบับที่ 8/2557 เรื่อง ข้อมูลเกี่ยวกับ Bitcoin และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่น ๆ ที่ลักษณะใกล้เคียง โดยได้ให้ข้อมูลเกี่ยวกับความหมายของบิทคอยน์ว่า บิทคอยน์และหน่วยข้อมูลทางอิเล็กทรอนิกส์ที่ลักษณะใกล้เคียงกัน คือหน่วยข้อมูลที่เกิดจากกลไกคอมพิวเตอร์ที่ถูกกำหนดไว้โดยคนกลุ่มหนึ่งที่มุ่งหวังจะใช้หน่วยข้อมูลดังกล่าวเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการ รวมถึงการแลกเปลี่ยนกับเงินตราสกุล ต่าง ๆโดยมีการจัดเก็บข้อมูลในระบบคอมพิวเตอร์

สำนักงานเลขาธิการสภาผู้แทนราษฎร (2561, หน้า 2) ได้อธิบายความหมายของ “บิทคอยน์ (Bitcoin)” ว่าเกิดจากการผสมคำระหว่างคำว่า “บิท (Bit)” ที่ย่อมาจากคำว่า Binary Digit ซึ่งหมายถึง ตัวเลขในระบบดิจิทัลซึ่งเป็นเลขฐานสองและเป็นหน่วยข้อมูลที่เล็กที่สุดในระบบคอมพิวเตอร์ทั่วไป ผสมกับคำว่า “คอยน์ (Coin)” ซึ่งหมายถึง เหรียญกษาปณ์ ดังนั้น บิทคอยน์ จึงหมายถึงเงินเสมือนหรือเงินดิจิทัลที่สามารถนำไปแลกเปลี่ยนสินค้าและบริการได้ แต่ไม่มีรูปร่างและไม่สามารถจับต้องได้เหมือนธนบัตรหรือเหรียญทั่วไป

หน่วยงานบังคับใช้กฎหมายอย่างกรมสอบสวนคดีพิเศษโดย พรรณทิพย์ เต็มเจริญ (2561, หน้า 69) ได้ให้ความหมายไว้ว่า บิทคอยน์คือสกุลเงินชนิดใหม่ในรูปดิจิทัลที่มีการคิดค้นขึ้นมาเพื่อที่จะหาวิธีการทำธุรกรรมทางการเงินที่ไม่ต้องผ่านตัวกลางอย่างธนาคาร เพื่อหลีกเลี่ยงการเสียค่าธรรมเนียม ป้องกันความไม่ปลอดภัยจากการถูกโจรกรรมข้อมูลทางการเงิน รวมทั้งเพื่อหลีกเลี่ยงความเสี่ยงจากการล้มของสถาบันทางการเงินหลัก

ในส่วนของภาคธุรกิจเองก็ได้ให้ความสนใจในการศึกษาเกี่ยวกับบิทคอยน์เช่นกัน โดย สำนักการค้าบริการและการลงทุน กรมเจรจาการค้าระหว่างประเทศ โดย สุชาญ ไวชีตา (2560, หน้า 23) ได้กล่าวว่า บิทคอยน์ คือ สกุลเงินดิจิทัลซึ่งอยู่ภายใต้การดูแลของระบบเครือข่ายคอมพิวเตอร์ ซึ่งเกิดขึ้นเพื่อมุ่งหวังที่จะให้เป็นสื่อกลางในการแลกเปลี่ยนเสมือนเป็นเงินตรา เพื่อใช้ในการจ่ายเงินเพื่อซื้อขายสินค้าและบริการ สำหรับทดแทนเงินตราสกุลดั้งเดิมต่าง ๆ โดยมีวัตถุประสงค์ให้เป็นสกุลเงินกลางที่ไม่ต้องกระทำธุรกรรมผ่านธนาคาร เพื่อหลีกเลี่ยงปัญหาเรื่องค่าธรรมเนียมและการตรวจสอบบัญชี

นอกจากหน่วยงานภาครัฐและภาคธุรกิจแล้ว ยังมีนักวิชาการและผู้ที่สนใจศึกษาในเรื่องที่เกี่ยวกับบิทคอยน์ รวมทั้งสื่อต่าง ๆ ได้ให้ความหมายหรือคำนิยามของบิทคอยน์ไว้ อาทิ

Gulled and Hossain (2018) ได้ให้ความหมายว่าบิทคอยน์คือสกุลเงินเข้ารหัสที่ใช้ระบบจ่ายเงินแบบกระจายข้อมูล ผ่านระบบโครงข่ายที่เชื่อมต่อกันโดยตรง ทำให้ผู้ใช้งานสามารถทำธุรกรรมระหว่างกันได้เอง โดยธุรกรรมต่าง ๆ จะถูกตรวจสอบความถูกต้องโดยเทคโนโลยีการเข้ารหัสและข้อมูลที่ถูกตรวจสอบแล้วจะถูกบันทึกด้วยเทคโนโลยีบล็อคเชน (Blockchain) ที่มีลักษณะแบบเปิดเผยหรือเป็นบัญชีสาธารณะ

ทวีชัย มีลาภ (2559, หน้า 107) กล่าวว่า บิทคอยน์คือเงินเสมือน (Virtual Currency) ที่อยู่ในรูปแบบอิเล็กทรอนิกส์โดยอาศัยโปรแกรมที่ทำงานบนระบบเครือข่ายอินเทอรเน็ตและบันทึกการทำธุรกรรมในบัญชีแบบแยกประเภทบนเครือข่ายอินเทอร์เน็ตสาธารณะ

จุฑารัตน์ ชวดนุช (2556, หน้า 5) ได้ให้ความหมายของบิทคอยน์ว่าเป็นหน่วยเงินใช้ชื่อสกุลเงินว่า BTC ตัวเงินจะสามารถแบ่งย่อยไปได้ถึงทศนิยมแปดหลัก เรียกหน่วยย่อยที่สุดว่า Satoshi ตามชื่อผู้ให้กำเนิดบิทคอยน์ อย่างไรก็ตามบิทคอยน์ยังเป็นเหมือนสิ่งที่เป็นรูปธรรม เป็นตัวเลขที่อยู่ใน Bitcoin Address หรือเป็นสิ่งสมมติขึ้นเพื่อให้เหมือนวัตถุอย่างเช่น เหรียญ โดยสามารถนำไปใช้ซื้อสิ่งของผ่านทางธุรกรรมทางอิเล็กทรอนิกส์

จากการศึกษาทำให้สามารถสรุปความหมายได้ว่า **“บิทคอยน์” คือสกุลเงินเข้ารหัสที่อยู่ในรูปแบบของข้อมูลทางคอมพิวเตอร์ที่ถูกสร้างขึ้นเพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการในลักษณะเดียวกันกับเงินตราจริง แต่ไม่มีรูปร่างและไม่สามารถจับต้องได้ โดยมีการทำงานและจัดเก็บข้อมูลทางธุรกรรมบนเครือข่ายคอมพิวเตอร์สาธารณะ**

3.1.2 ความเป็นมาของบิทคอยน์

แนวคิดซึ่งถือเป็นที่มาของการสร้างบิทคอยน์ คือแนวคิดเกี่ยวกับการพัฒนาสกุลเงินดิจิทัล (Digital Currency) ภายใต้พื้นฐานความคิดที่ต้องการนำเอาเทคโนโลยีคอมพิวเตอร์มาใช้ในการสร้างสื่อกลางในการแลกเปลี่ยนสินค้าและบริการรูปแบบใหม่ ซึ่งแนวคิดดังกล่าวเริ่มมาตั้งแต่ช่วงปี ค.ศ. 1980 โดยในช่วงแรกนั้นนักพัฒนาหรือนักวิศวกรรมคอมพิวเตอร์จะต้องพบกับความท้าทายที่จะต้องออกแบบให้สกุลเงินดิจิทัลที่อยู่ในรูปแบบข้อมูลอิเล็กทรอนิกส์นี้ มีความน่าเชื่อถือเทียบเท่ากับเงินสกุลจริงที่มีรูปร่างและสามารถจับต้องได้ เพื่อให้สามารถนำไปใช้ในการแลกเปลี่ยนสินค้าและบริการได้จริง โดยประเด็นปัญหาสำคัญที่นักพัฒนาจะต้องแก้ปัญหาให้ได้ มีอยู่ 3 ประเด็น ได้แก่ (Andreas M. Antonopoulus, 2017)

1) จะทำอย่างไรให้สกุลเงินดิจิทัลที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ได้รับการยอมรับและเชื่อถือว่าเป็นทรัพย์สินที่สามารถครอบครองและถือเอาได้ สามารถนำไปใช้งานได้จริงตลอดจนจะไม่ถูกปลอมแปลงข้อมูลในอนาคตเนื่องจากเป็นข้อมูลที่ไม่สามารถจับต้องได้

2) ภายใต้สภาพของสกุลเงินดิจิทัลที่จำเป็นจะต้องมีการทำธุรกรรมผ่านระบบเครือข่ายคอมพิวเตอร์ ซึ่งเป็นระบบการติดต่อสื่อสารขนาดใหญ่และเปิดกว้าง ทำให้เกิดช่องว่างที่ผู้ใช้งานอาจลักลอบทำธุรกรรมซ้อนกันหลายรายการในเวลาเดียวกัน (Double-Spend) เช่น นาย ก. มีเงินดิจิทัลอยู่เพียง 10 บาท แต่ได้เจตนาทำการโอนเงินดิจิทัล จำนวน 10 บาทนี้ ผ่านระบบคอมพิวเตอร์ให้กับทั้ง นาย ข. และ นาย ค. ในเวลาเดียวกัน (ทำให้กลายเป็นว่านาย ก. มีเงินทั้งหมด 20 บาท ซึ่งไม่ตรงกับความเป็นจริง) ซึ่งอาจทำให้เกิดความผิดพลาดของระบบได้ ซึ่งหากนักพัฒนาต้องการจะสร้างความน่าเชื่อถือให้กับเงินดิจิทัลก็จำเป็นจะต้องออกแบบระบบให้สามารถป้องกันปัญหาดังกล่าวด้วย

3) นอกจากนี้นักพัฒนายังต้องแก้ปัญหาสำคัญอีกประการหนึ่งคือ จะออกแบบสกุลเงินดิจิทัลอย่างไรเพื่อไม่ให้เกิดการโต้เถียงทางกรรมสิทธิ์ระหว่างผู้ใช้งาน หรือจะทำให้ผู้ใช้งานมั่นใจได้อย่างไรว่า เมื่อผู้ใดผู้หนึ่งครอบครองสกุลเงินดิจิทัลแล้ว จะไม่มีผู้อื่นมาอ้างสิทธิ์ครอบครองในตัวเงินเดียวกัน

ประเด็นปัญหาต่างๆเหล่านี้ **จึงทำให้แนวคิดเกี่ยวกับสกุลเงินดิจิทัลยังไม่ถูกนำมาพัฒนาและสร้างออกมาให้สามารถใช้งานได้จริงในขณะนั้น** ซึ่งจากประเด็นปัญหาเมื่อเปรียบเทียบกับ **ธนบัตร**แล้วจะพบว่า หากเป็นกรณีของธนบัตรจะสามารถสร้างความน่าเชื่อถือได้โดย ธนบัตรสามารถ

ถือครองและจับต้องได้จริง มีการป้องกันการปลอมแปลงด้วยการใช้กระดาษและหมึกพิมพ์พิเศษที่ปลอมแปลงได้ยาก มีการป้องกันข้อพิพาทของการถือครองกรรมสิทธิ์ด้วยการระบุตัวเลขประจำธนบัตร และสามารถป้องกันการจ่ายเงินซ้ำซ้อนได้ เนื่องจากโดยสภาพของธนบัตรหนึ่งใบย่อมไม่อาจถูกใช้งานได้จากหลากหลายสถานที่ จึงทำให้สื่อกลางในการแลกเปลี่ยนสินค้าและบริการอย่างธนบัตรไม่ได้รับผลกระทบจากประเด็นปัญหาดังกล่าว

ความก้าวหน้าในการพัฒนาแนวคิดเกี่ยวกับสกุลเงินดิจิทัลได้ปรากฏชัดขึ้นในปี ค.ศ. 1998 ที่นายเหวย ได่ (Wei Dai) นักวิศวกรรมคอมพิวเตอร์ ได้เสนอแนวคิดเกี่ยวกับสกุลเงินดิจิทัลชื่อ “บี - มันนี่ (B-money)” ซึ่งเป็นแนวคิดที่สามารถแก้ไขและอุดช่องว่างที่เป็นประเด็นปัญหาตามที่ได้กล่าวมาแล้ว ด้วยการนำเอาระบบการเข้ารหัสข้อมูลคอมพิวเตอร์ (Cryptography) มาใช้ในการสร้างความปลอดภัยให้กับสกุลเงินดิจิทัลนี้ โดยการนำเอาข้อมูลสำคัญของผู้ใช้งานมาเข้ารหัสทางคอมพิวเตอร์เพื่อให้เกิดเป็นลายเซ็นเฉพาะตัวแบบดิจิทัล (Digital Signature) ลงบนสกุลเงินดิจิทัล เพื่อแสดงความเป็นเจ้าของ ป้องกันการปลอมแปลง ตลอดจนสามารถนำไปใช้ยืนยันการทำธุรกรรมด้วยสกุลเงินดิจิทัลเพื่อให้เกิดความน่าเชื่อถือมากยิ่งขึ้น โดยแนวคิดนี้ได้รับความสนใจอย่างแพร่หลายจนทำให้แนวคิดเกี่ยวกับสกุลเงินดิจิทัลที่ใช้การเข้ารหัสนี้จึงถูกเรียกว่า **“สกุลเงินเข้ารหัส” หรือ “Cryptocurrency”** ขณะที่ในปีเดียวกันนี้ นายนิค ซาโบ (Nick Szabo) นักวิศวกรรมคอมพิวเตอร์อีกท่านหนึ่ง ก็ได้นำเสนอแนวคิดเกี่ยวกับการสร้างสกุลเงินเข้ารหัสชื่อ “บิทโกลด์ (Bit Gold)” ด้วยแนวคิดในการกระจายข้อมูล (Decentralized) เพื่อต้องการให้เกิดความโปร่งใสในการทำธุรกรรมต่างๆ โดยไม่จำเป็นต้องมีการเก็บข้อมูลไว้ที่ส่วนกลาง (Server) แต่อย่างใด แม้ในท้ายที่สุดแนวคิดของสกุลเงินเข้ารหัสทั้งสองสกุลนี้ จะไม่ได้ถูกสร้างออกมาใช้งานจริงก็ตาม แต่แนวคิดดังกล่าวก็ได้รับความสนใจและถือเป็นแนวคิดต้นแบบสำคัญในการพัฒนาสกุลเงินเข้ารหัสรวมทั้งบิทคอยน์ในเวลาต่อมา (Pasupol Bunsaen, 2018)

จนกระทั่งในปี ค.ศ.2009 ชื่อของ “บิทคอยน์” จึงได้ถูกกล่าวถึงและเผยแพร่เป็นครั้งแรก ในบทความ เรื่อง “Bitcoin: A Peer-to-Peer Electronic Cash System” โดยผู้เขียนที่ใช้ชื่อว่านายซาโตชิ นากาโมโตะ (Satoshi Nakamoto) ในบทความดังกล่าวได้มีการกล่าวถึง**แนวคิดหลักที่เป็นที่มาของการสร้างบิทคอยน์**ไว้ว่า เกิดจากปัญหาต่าง ๆ ที่เกิดขึ้นจากระบบการเงินการธนาคารแบบเดิมที่มีการดำเนินการในลักษณะการรวมศูนย์อำนาจ (Centralization) กล่าวคือ การตรวจสอบยืนยันความถูกต้องของธุรกรรม การอนุมัติดำเนินการธุรกรรมรวมทั้งการเก็บบันทึกข้อมูลการทำ

ธุรกรรมทางการเงินต่าง ๆ จะถูกดำเนินการโดยตัวกลาง เช่น ธนาคารหรือสถาบันทางการเงินต่าง ๆ ที่ได้รับความเชื่อถือ ซึ่งด้วยระบบการรวมศูนย์อำนาจนี้ทำให้เกิดประเด็นปัญหาหลายประการ ดังนี้ (Satoshi Nakamoto, 2008)

1) การทำธุรกรรมต่าง ๆ ผ่านตัวกลาง มีโอกาสที่เกิดความผิดพลาดได้ เนื่องจากสถาบันทางการเงินที่เป็นตัวกลางอาจเกิดความขัดแย้งระหว่างกัน ทำให้การจ่ายเงินไม่ได้รับการอนุมัติ เช่น ปัญหาการปฏิเสธการจ่ายเงินตามเช็ค หรือ ปัญหาบัตรเครดิตหมดอายุ เป็นต้น

2) เมื่อข้อมูลทั้งหมด ไม่ว่าจะเป็นข้อมูลทางบัญชีหรือข้อมูลทางธุรกรรมต่าง ๆ ซึ่งถือเป็นข้อมูลสำคัญของผู้ใช้บริการ ถูกเก็บรวบรวมไว้ที่ศูนย์เก็บข้อมูลส่วนกลางของธนาคารหรือสถาบันการเงินต่าง ๆ จึงเกิดความเสี่ยงที่ข้อมูลนั้นอาจถูกเปลี่ยนแปลง แก้ไข ทั้งจากความผิดพลาด ขาดเจตนา หรืออาจถูกกระทำโดยทุจริต

หรืออาจจะเกิดการโจมตีระบบฐานข้อมูลเพื่อเข้าไปทำลายข้อมูลต่าง ๆ หรือ ความเสี่ยงที่อาจจะเกิดกรณีที่มีการลักลอบเข้าถึงฐานข้อมูลเพื่อเข้าไปแก้ไขตัวเลขจำนวนเงินในบัญชี จนอาจทำให้เกิดความเสียหายและเกิดความไม่ถูกต้องของข้อมูลได้

3) การมีตัวกลางในการดำเนินการต่าง ๆ ทำให้ต้นทุนในการทำธุรกรรมสูงขึ้น เนื่องจากตัวกลางมีการเรียกเก็บค่าธรรมเนียมในการดำเนินการ ทำให้ธุรกรรมขนาดเล็กไม่สามารถเกิดขึ้นได้ เนื่องจากต้นทุนในการดำเนินการแพงกว่าจำนวนเงินในการทำธุรกรม

4) การดำเนินการทางธุรกรรมที่จะต้องกระทำผ่านตัวกลางอยู่เสมอ ทำให้เกิดความล่าช้าในการทำธุรกรรม เพราะจะต้องรอให้ตัวกลางทำการตรวจสอบและอนุมัติธุรกรรมนั้น ๆ

5) การดำเนินการทางธุรกรรมที่จะต้องกระทำผ่านตัวกลาง ทำให้ขาดอิสรภาพในทางการเงินไปบางส่วน อันเป็นผลมาจากการที่จำเป็นจะต้องถูกตรวจสอบการทำธุรกรรมอยู่เสมอ เช่น การถูกระงับการจ่ายเงินชั่วคราว หรือ การถูกอายัดเงินในบัญชี เป็นต้น

6) ปัญหาความเสี่ยงในการควบคุมการใช้ข้อมูลส่วนบุคคล อันเนื่องมาจากการที่ข้อมูลส่วนบุคคลของผู้ใช้บริการถูกเก็บไว้กับตัวกลางอย่างธนาคาร จึงอาจมีโอกาสที่ข้อมูลสำคัญอาจถูกลักลอบนำไปใช้โดยมิชอบเช่น การนำข้อมูลส่วนบุคคลไปเปิดเผยโดยไม่ได้รับอนุญาต เป็นต้น

จากประเด็นปัญหาต่าง ๆ ในข้างต้นทำให้นายซาโตชิ นากาโมโตะ เสนอแนวทางการแก้ปัญหาด้วยการ**คิดค้นและออกแบบแนวคิดของ “บิทคอยน์”** ขึ้นเพื่อให้เป็นระบบการจ่ายเงินแบบอิเล็กทรอนิกส์ด้วยรูปแบบของสกุลเงินเข้ารหัสที่ให้ผู้ใช้งานสามารถทำธุรกรรมต่อกันได้โดยตรง

(Peer-to-Peer) มีระบบการตรวจสอบความถูกต้องและอนุมัติการดำเนินการธุรกรรมอย่างเปิดเผยในรูปแบบของการกระจายข้อมูลภายใต้การทำงานของระบบบัญชีสาธารณะที่ไม่ต้องอาศัยตัวกลางในการดำเนินการ มีระบบการป้องกันการจ่ายเงินซ้ำซ้อน (Double Spending) รวมทั้งยังมีการเก็บข้อมูลทางธุรกรรมด้วยระบบบล็อคเชน (Blockchain) ที่มีความปลอดภัยสูงเนื่องจากจะไม่สามารถย้อนกลับไปแก้ไขหรือลักลอบเข้าไปเปลี่ยนแปลงข้อมูลทางธุรกรรมที่ถูกตรวจสอบยืนยันแล้วได้ ซึ่งจะได้อธิบายถึงรายละเอียดคุณลักษณะต่าง ๆ ของบิทคอยน์ที่ได้กล่าวมานี้ในหัวข้อต่อไป

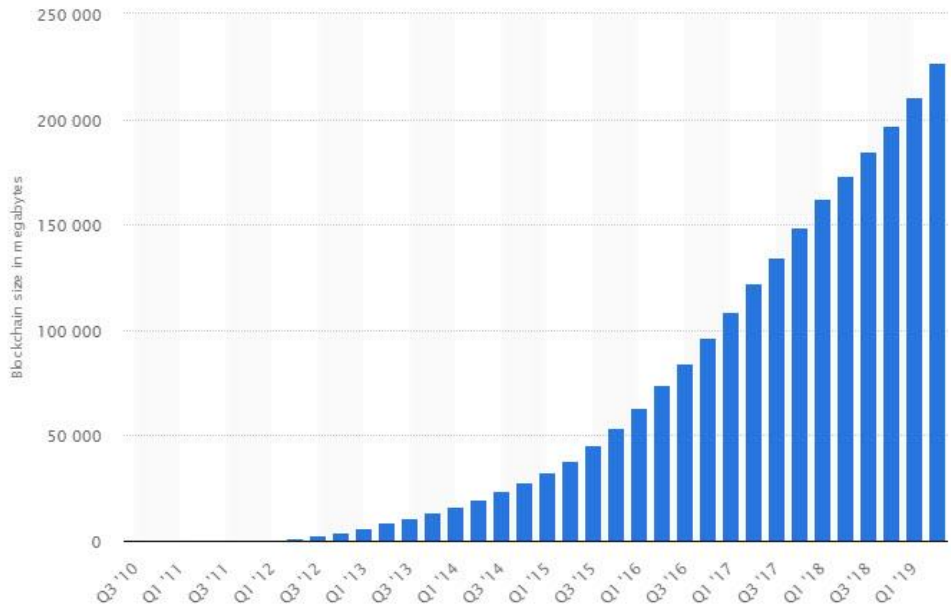
หลังจากที่หลักการและแนวคิดของบิทคอยน์ได้ถูกเผยแพร่ออกมาก็ส่งผลให้มีผู้สนใจและวิพากษ์วิจารณ์ไปอย่างหลากหลาย จนกระทั่งในปี พ.ศ.2552 จึงได้มีการ**เปิดตัวบิทคอยน์หน่วยแรก** รวมทั้งมีการแจกจ่ายโปรแกรมสำหรับการสร้างพัฒนาระบบบิทคอยน์ และมีการสร้างเว็บไซต์สำหรับการใช้งานบิทคอยน์เป็นครั้งแรก คือ www.bitcoin.org ขึ้น โดยในช่วงแรกนั้นบิทคอยน์ยังไม่เป็นที่นิยมเท่าใดนักเนื่องจากไม่ได้มีการค้ำประกันมูลค่าของบิทคอยน์ด้วยสินทรัพย์หรือสถาบันการเงินใด ๆ และการถือกำเนิดของสกุลเงินเข้ารหัสในลักษณะนี้ยังถือเป็นเรื่องใหม่ของสังคมโลกในขณะนั้น (พรชัย ชุนหจินดา, 2561) จนกระทั่งในปี พ.ศ. 2553 จึงปรากฏหลักฐานว่าได้เกิด**การนำบิทคอยน์ไปใช้ในการซื้อสินค้าขึ้นเป็นครั้งแรกของโลก** โดยสำนักข่าวซีบีเอส (CBS News) ได้กล่าวถึงเหตุการณ์ดังกล่าวว่า เมื่อวันที่ 22 พฤษภาคม 2553 นายลาซโล่ ฮานเยค (Laszlo Hanyecz) อาชีพนักโปรแกรมคอมพิวเตอร์ ได้ใช้บิทคอยน์จำนวน 10,000 บิทคอยน์เพื่อซื้อพิซซ่า จำนวน 2 ถาด ซึ่งหากคำนวณจากมูลค่าของบิทคอยน์ในปัจจุบัน (กรกฎาคม 2562) จะทำให้ราคาพิซซ่าทั้ง 2 ถาดดังกล่าวมีมูลค่าสูงถึงประมาณ 3,200 ล้านบาท (Evie Salomon, 2019)

เหตุการณ์สำคัญที่ทำให้ทั่วโลกเริ่มให้ความสนใจกับบิทคอยน์มากยิ่งขึ้น คือ การก่อตั้งบริษัทรับแลกเปลี่ยนบิทคอยน์ชื่อดังคือบริษัท Mt.Gox ในปี ค.ศ. 2010 มีที่ตั้งอยู่ในย่านชิบูย่า กรุงโตเกียว ประเทศญี่ปุ่น มีการให้บริการรับแลกเปลี่ยนสกุลเงินจริงทั่วโลกกับบิทคอยน์ผ่านการดำเนินการบนโลกอินเทอร์เน็ต ซึ่งภายในระยะเวลาสามปีหลังจากที่เปิดทำการ บริษัท Mt.Gox ก็ได้กลายเป็นบริษัทรับแลกเปลี่ยนบิทคอยน์ที่ใหญ่ที่สุดในโลก โดยกว่า 70% ของการทำธุรกรรมที่เกี่ยวกับบิทคอยน์ทั้งหมดในโลกอยู่ภายใต้ความดูแลของ Mt.Gox ทั้งสิ้น แต่เหตุการณ์ที่ทำให้บิทคอยน์เป็นที่สนใจของทั้งโลกอีกครั้ง ก็คือเหตุการณ์ในปี ค.ศ.2014 ที่บริษัท Mt.Gox ถูกคนร้ายลักลอบเข้าไปในระบบ (Hack) และขโมยบิทคอยน์ไปกว่า 740,000 บิทคอยน์ คิดเป็นมูลค่า 460 ล้านเหรียญสหรัฐ โดยเหตุการณ์ดังกล่าวทำให้มีผู้ได้รับความเสียหายเป็นจำนวนมากและปัจจุบันยังมีการฟ้องร้องต่อสู้คดีที่

เกี่ยวกับการชดใช้ค่าเสียหายระหว่างผู้ใช้บริการกับบริษัท Mt.Gox ในประเทศญี่ปุ่น แม้ว่าจากเหตุการณ์ดังกล่าวจะทำให้ราคาของบิทคอยน์พุ่งต่ำลง แต่ภายหลังจากที่ข่าวเหตุการณ์ดังกล่าวได้แพร่ออกไปกลับยิ่งทำให้มีผู้สนใจศึกษาและใช้งานบิทคอยน์มากยิ่งขึ้นจนราคาของบิทคอยน์กลับมาสูงขึ้น (Andrew Norry, 2019)

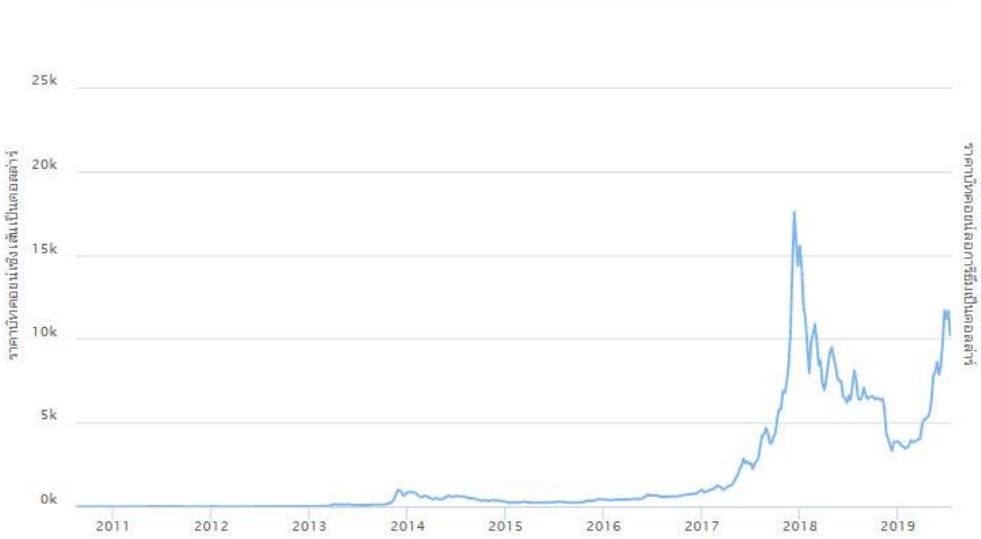
อีกเหตุการณ์หนึ่งที่เกิดขึ้นในช่วงเวลาใกล้เคียงกันและส่งผลให้เกิดความสนใจและมีการใช้บิทคอยน์มากขึ้น คือ เหตุการณ์ในปี ค.ศ.2013 ที่สำนักงานสอบสวนกลางสหรัฐอเมริกา (FBI) ได้ทำการจับกุมตัวนายเบลค เบนท์ฮอล์ (Blake Benthall) ผู้ดูแลตลาดมืดออนไลน์ซิลค์โร้ด (Silk Road) ซึ่งเป็นแหล่งซื้อขายสินค้าผิดกฎหมายหลายประเภทที่อยู่บนอินเท็อรเน็ต โดยสินค้าที่มีการซื้อขายกันในซิลค์โร้ดได้แก่ ยาเสพติด อาวุธปืน อวัยวะมนุษย์ เอกสารราชการปลอม และสิ่งของผิดกฎหมายอื่น ๆ อีกมากมาย **โดยในการซื้อขายสิ่งของดังกล่าวจะใช้บิทคอยน์แทนเงินสดเพื่อต้องการปกปิดตัวตนที่แท้จริงของผู้ซื้อขาย ทำให้ซิลค์โร้ดเป็นตลาดมืดออนไลน์ที่แรกที่มีการใช้บิทคอยน์ในการซื้อขายสินค้าผิดกฎหมาย** ภายหลังการจับกุมได้มีการรายงานข้อมูลว่า มีผู้เข้ามาใช้บริการเว็บไซต์ซิล์คโร้ดกว่า 150,000 ราย มีสินค้าผิดกฎหมายประกาศขายกว่า 13,000 ชนิด และมีเงินหมุนเวียนอยู่ในตลาดมืดออนไลน์ดังกล่าวกว่า 8 ล้านเหรียญสหรัฐต่อเดือน (Dominic Rushe, 2014) การจับกุมครั้งสำคัญดังกล่าวทำให้เกิดเสียงวิพากษ์วิจารณ์ว่าบิทคอยน์ถูกสร้างขึ้นเพื่อเป็นเครื่องมือชั้นดีให้กับอาชญากร แต่ในทางกลับกันกลับทำให้เกิดความสนใจในบิทคอยน์มากยิ่งขึ้นทั่วโลก

จากเหตุการณ์ของบริษัท Mt.Gox และการปิดตัวลงของตลาดมืดซิลค์โร้ด ส่งผลทำให้บิทคอยน์เป็นที่สนใจและเริ่มมีการใช้งานมากยิ่งขึ้น โดยจากรายงานสถิติการใช้งานบิทคอยน์ของเว็บไซต์ www.statista.com ที่แสดงข้อมูลการใช้งานบิทคอยน์ด้วยการสำรวจจำนวนการทำธุรกรรมทั้งหมดที่ถูกบันทึกด้วยระบบบล็อคเชน (Blockchain) ตั้งแต่ปี ค.ศ.2010 – 2019 ดังภาพต่อไปนี้ (Shanhong Liu, 2019)



ภาพที่ 7 ปริมาณการเก็บข้อมูลการทำธุรกรรมของบิทคอยน์ในระบบบล็อคเชน (Blockchain) ตั้งแต่ปี ค.ศ.2010 – 2019 โดยแบ่งเป็นไตรมาส

จากภาพดังกล่าวจะเห็นได้ว่า ในปี ค.ศ. 2010 มีปริมาณการบันทึกข้อมูลธุรกรรมในระบบบล็อคเชนไม่ถึง 0 เมกะไบท์ จนถึงปัจจุบันในปี ค.ศ. 2019 ที่มีการบันทึกข้อมูลธุรกรรมในระบบบล็อคเชนสูงถึงกว่า 200,000 – 250,000 เมกะไบท์ ทำให้สามารถอธิบายได้ว่า**มีความนิยมในการใช้งานบิทคอยน์เพิ่มขึ้นเป็นจำนวนมาก** และสืบเนื่องจากปริมาณการใช้งานและความต้องการถือครองบิทคอยน์ที่มากขึ้น ก็ส่งผลทำให้มูลค่าของบิทคอยน์เพิ่มขึ้นอย่างมหาศาล ดังที่ปรากฏในภาพต่อไปนี้ (Bitcoin Price History, 2019)



ภาพที่ 8 มูลค่าของบิทคอนย์(เหรียญสหรัฐ) ตั้งแต่ ปี ค.ศ. 2011 ถึง 2019

จะเห็นว่าจากเมื่อปี ค.ศ. 2011 – 2013 ที่บิทคอยน์ยังไม่ได้รับความสนใจเท่าใดนัก ขณะนั้นบิทคอยน์จำนวน 1 บิทคอยน์ยังมีมูลค่าไม่ถึง 1 เหรียญสหรัฐ แต่ในช่วงปลายปี ค.ศ. 2013 มูลค่าของบิทคอยน์ก็เริ่มปรับตัวสูงขึ้น และมีมูลค่าสูงสุดเมื่อเดือน ธันวาคม ค.ศ. 2017 ที่บิทคอยน์จำนวน 1 บิทคอยน์ มีมูลค่าสูงถึง 19,783.06 เหรียญสหรัฐ และหลังจากนั้นมูลค่าของบิทคอยน์ก็มีความผันผวนขึ้นลงไปตามกระแสข่าวและเป็นไปตามความต้องการของตลาดซื้อขาย โดยในปัจจุบัน (กรกฎาคม ค.ศ.2019) 1 บิทคอยน์ มีมูลค่าเท่ากับ 10649.40 เหรียญสหรัฐ หรือเท่ากับ 327,958.92 บาท

นอกจากการที่ “บิทคอยน์” เป็นสื่อกลางในการแลกเปลี่ยนรูปแบบใหม่ที่อยู่ในสภาพของข้อมูลอิเล็กทรอนิกส์ที่มีความทันสมัยและน่าสนใจ ประกอบกับเหตุการณ์สำคัญที่เกี่ยวกับบิทคอยน์ตามที่ได้กล่าวมาแล้ว ปัจจัยสำคัญที่ทำให้บิทคอยน์ได้รับความนิยมในการใช้งานจนทำให้บิทคอยน์มีมูลค่าสูงขึ้นเป็นจำนวนมากนั้นก็คือ คุณ**ลักษณะพิเศษของบิทคอยน์** ที่ทำให้บิทคอยน์เป็นสกุลเงินเข้ารหัสที่แตกต่างจากสกุลเงินเข้ารหัสประเภทอื่น มีความโปร่งใสและปลอดภัยสูงสุดในเวลาเดียวกัน ตลอดจนยังไม่จำเป็นต้องอาศัยคนกลางในการตรวจสอบยืนยันธุรกรรม อีกทั้งยังไม่สามารถถูกโจมตีจากผู้ไม่หวังดีได้

3.1.3 คุณลักษณะพิเศษของบิทคอยน์

สาเหตุสำคัญที่ทำให้ “บิทคอยน์” เป็นสกุลเงินเข้ารหัสที่ได้รับความนิยมสูงสุด คือการที่บิทคอยน์มีระบบการทำงานที่มีความปลอดภัยและมีความน่าเชื่อถือสูง อันเกิดจากคุณลักษณะพิเศษต่าง ๆ ดังนี้

3.1.3.1 การเข้ารหัสเพื่อรักษาความปลอดภัย (Cryptography)

คุณลักษณะพิเศษของบิทคอยน์ ที่ถือเป็นหัวใจสำคัญในด้านการรักษาความปลอดภัยของข้อมูลคือ **ระบบการเข้ารหัสข้อมูล(Cryptography)** ซึ่งหมายถึง การเปลี่ยนให้ข้อความตามปกติที่สามารถเข้าใจได้ทั่วไป ไปอยู่ในรูปของตัวอักษรและตัวเลข หรือสัญลักษณ์ต่าง ๆ ที่มีรูปแบบเฉพาะตามเงื่อนไขที่กำหนดไว้ ตัวอย่างเช่น หากกำหนดเงื่อนไขว่าให้ทำการเข้ารหัสข้อมูลด้วยการเปลี่ยนตัวอักษรภาษาอังกฤษตามปกติ ให้เลื่อนไปอีก 4 ตัวอักษร ดังนั้น หากกำหนดให้ข้อมูลสำคัญ คือ “AAAA” ข้อมูลดังกล่าวจะถูกเข้ารหัสเป็น “EEEE” และหากกำหนดให้ข้อมูลสำคัญคือ “TEST” ข้อมูลนี้จะถูกเข้ารหัสเป็น “XIWX” เป็นต้น ด้วยระบบการเข้ารหัสข้อมูลนี้จะทำให้บุคคลภายนอกที่ไม่มีส่วนเกี่ยวข้องหรือผู้ที่ไม่ได้รับอนุญาต ไม่สามารถเข้าใจข้อมูลดังกล่าวได้ เพื่อจุดประสงค์ในการรักษาความปลอดภัยของข้อมูล

ในกรณีของบิทคอยน์ ใช้วิธีการเข้ารหัสข้อมูลด้วยค่าแฮช (Hash Function) แบบ **SHA-256** ที่เป็นระบบการเข้ารหัสด้วยตรรกะทางคอมพิวเตอร์ด้วยการเปลี่ยนรูปแบบจากข้อมูลปกติไปเป็นรูปแบบของตัวอักษรภาษาอังกฤษและตัวเลขผสมกัน มีขนาด 64 ตัวอักษร ตามตัวอย่างดังต่อไปนี้ (พรชัย ชุนหจินดา, 2561,หน้า 5)

ข้อมูลต้นทาง : Test

ข้อมูลที่ผ่านการเข้ารหัสด้วยรูปแบบ SHA–256 :

532eaabd9574880dbf76b9b8cc00832c20a6ec113d682299550d7a6e0f345e25

ภาพที่ 9 ตัวอย่าง ผลการเข้ารหัสข้อมูลค่าแฮช ด้วยรูปแบบ SHA-256
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2562)

การเข้ารหัสด้วยข้อมูลด้วยค่าแฮชตามรูปแบบของ SHA-256 นี้ ไม่ว่าจะนำข้อมูลต้นทางเดิมมาทำการเข้ารหัสกี่ครั้ง ก็จะให้ข้อมูลปลายทาง (Output) เหมือนเดิมทุกครั้ง นอกจากนี้แม้ข้อมูลต้นทางจะแตกต่างกันเพียงเล็กน้อยแต่ข้อมูลที่เป็นผลลัพธ์ที่ได้จากการเข้ารหัสจะไม่ซ้ำกัน ตามตัวอย่างดังต่อไปนี้

ข้อมูลต้นทาง : Test
ข้อมูลที่ผ่านการเข้ารหัสด้วยรูปแบบ SHA–256 :
532eaabd9574880dbf76b9b8cc00832c20a6ec113d682299550d7a6e0f345e25

ข้อมูลต้นทาง : test
ข้อมูลที่ผ่านการเข้ารหัสด้วยรูปแบบ SHA–256 :
9f86d081884c7d659a2feaa0c55ad015a3bf4f1b2b0b822cd15d6c15b0f00a08

ภาพที่ 10 ตัวอย่างการเปรียบเทียบผลการเข้ารหัสข้อมูลค่าแฮช ด้วยรูปแบบ SHA-256
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2562)

จากตัวอย่างดังกล่าว จะเห็นได้ว่าข้อมูลต้นทาง คือ “Test” และ “test” แตกต่างกันเพียงตัวสะกดตัวพิมพ์ใหญ่ ตัวพิมพ์เล็กของตัวอักษรตัวแรกเท่านั้น แต่ปรากฏว่า ภายหลังจากทำการเข้ารหัสข้อมูลด้วยระบบ SHA-256 แล้วผลลัพธ์ที่ได้จะมีค่าแตกต่างกันเป็นอย่างมาก

นอกจากนี้ การเข้ารหัสข้อมูลด้วยค่าแฮชตามรูปแบบของ SHA-256 นี้ยังมีลักษณะเป็นการเข้ารหัสแบบสมการทางเดียว (One – Way Function) กล่าวคือ เมื่อทำการเข้ารหัสข้อมูลต้นทางผ่านรูปแบบ SHA-256 จนได้ผลลัพธ์ออกมาแล้ว จะ**ไม่สามารถนำค่าที่เป็นผลลัพธ์มาคำนวณกลับไปหาข้อมูลต้นทางได้** (ชาลี ธรรมรัตน์, 2554) ดังนั้นจึงกล่าวได้ว่า การเก็บรักษาข้อมูลด้วยวิธีการเข้ารหัสด้วยค่าแฮชตามรูปแบบ SHA-256 ของบิทคอยน์นี้ทำให้ข้อมูลต่าง ๆ มีความปลอดภัยสูงมาก โดยวิธีการเดียวที่ผู้ไม่หวังดีจะค้นพบข้อมูลต้นทางที่แท้จริงได้ คือการสุ่มเดาข้อมูลต้นทางไปเรื่อย ๆ จนกว่าจะมีค่าการเข้ารหัสตรงกับค่าผลลัพธ์ที่ต้องการทราบ หรือที่ภาษาทางด้านคอมพิวเตอร์ระบบ เรียกว่า “Brute Force” ซึ่งในทางปฏิบัติจริงแล้วมีความเป็นไปได้น้อยมากจนแทบจะเป็นไปไม่ได้

บิทคอยน์ได้นำการเข้ารหัสข้อมูลมาใช้ในการทำงานของระบบดังนี้

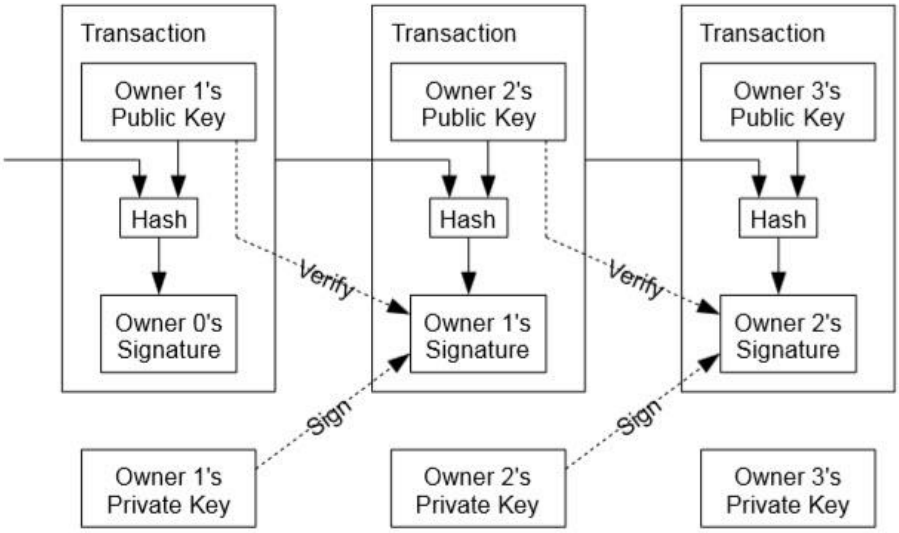
1) ใช้ในการสร้างรหัสผ่านส่วนตัวและเลขบัญชีประจำตัว (ดลพร ประสงค์สุทธิพร, 2557) โดยเมื่อผู้ใช้บริการต้องการจะใช้บริการระบบบิทคอยน์ จะต้องลงทะเบียนสมัครใช้งาน จากนั้นระบบจะกำหนดค่าแฮชมาให้ชุดหนึ่งเพื่อใช้เป็น **รหัสผ่านส่วนตัว (Private Key)** โดยรหัสผ่านนี้เป็นรหัสเฉพาะตัวเพื่อใช้สำหรับยืนยันตัวบุคคลว่าเป็นเจ้าของบัญชีผู้ใช้งานจริง และจำเป็นต้องใช้รหัสผ่านนี้เพื่ออนุมัติการโอนและรับเงินบิทคอยน์ โดยรหัสผ่านส่วนตัวนี้จะถูกเข้ารหัสอยู่ในรูปแบบของค่าแฮชตามรูปแบบของ SHA-256 ทำให้ปลอดภัยต่อการถูกลักลอบเข้าบัญชี

ภายหลังจากที่ระบบกำหนดค่ารหัสผ่านส่วนตัวให้กับผู้ใช้งานแล้วเพื่อให้เกิดความเชื่อมโยงกัน ระบบจะนำค่ารหัสผ่านส่วนตัวไปทำการเข้ารหัสข้อมูลค่าแฮชอีกครั้งหนึ่งเพื่อสร้างเป็น **เลขที่บัญชี (Bitcoin Address/Public Key)** ที่มีลักษณะเหมือนเลขที่บัญชีธนาคารทั่วไปที่สามารถนำไปใช้แจ้งให้ผู้อื่นทราบในกรณีที่ต้องการทำธุรกรรมได้และ การที่บิทคอยน์ใช้การเข้ารหัสเพื่อสร้างรหัสผ่านส่วนตัว (Private Key) และเลขที่บัญชี (Bitcoin Address/Public Key) ตามที่กล่าวมานี้ทำให้เกิดความปลอดภัยสูงเนื่องจาก ทั้งรหัสผ่านและเลขที่บัญชีมีความเชื่อมโยงกันผ่านการเข้ารหัส แต่ในขณะเดียวกันการแจ้งเลขที่บัญชีให้ผู้อื่นทราบกลับไม่เป็นอันตรายต่อผู้ใช้งานแต่อย่างใด เพราะแม้จะทราบเลขที่บัญชีก็ไม่สามารถคำนวณกลับไปหาค่าต้นทางที่เป็นรหัสผ่านส่วนตัวได้ปรากฏตามตัวอย่างดังต่อไปนี้

รหัสผ่านส่วนตัว (Private Key) :
0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF0123456789ABCDEF
เลขที่บัญชีบิทคอยน์ (Bitcoin Address/Public Key) :
1Dk9L8FiXXar7Rk2mJzxEZjcBeVFGdh2Jz

ภาพที่ 11 ตัวอย่างรหัสผ่านส่วนตัวและเลขที่บัญชีบิทคอยน์
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2562)

2) ใช้ในการทำธุรกรรม โดยหากผู้ใช้งานต้องการทำธุรกรรม เช่น การโอน-รับบิทคอยน์ จำเป็นจะต้องใช้ทั้งเลขที่บัญชีและรหัสผ่านส่วนตัวเพื่อให้ระบบตรวจสอบยืนยันความถูกต้องด้วยการเข้ารหัสข้อมูลดังปรากฏตามภาพต่อไปนี้ (Satoshi Nakamoto, 2008)



ภาพที่ 12 การใช้การเข้ารหัสข้อมูลสำหรับการทำธุรกรรมของบิทคอยน์

จากภาพสามารถอธิบายได้ว่า **เมื่อผู้ใช้ที่ 1 (Owner 1) ต้องการโอนบิทคอยน์ให้กับผู้ใช้ที่ 2 (Owner 2)** จะต้องสร้างคำสั่งการโอนเงิน (Transaction) ขึ้น จากนั้นจะต้องใช้ทั้งเลขที่บัญชี (Owner 1's Public Key) และรหัสผ่านส่วนตัว (Owner 1's Private Key) ประกอบกันเพื่อ**เข้ารหัสคำสั่งการโอนเงินและสร้างลายเซ็นดิจิทัล** (Owner 1's Signature) เพื่อยืนยันตัวตนแล้วจึงส่งข้อมูลไปให้ผู้ใช้ที่ 2 ตามเลขที่บัญชีของผู้ใช้ที่ 2 (Owner 2's Public Key)

และเมื่อคำสั่งการโอนดังกล่าวถูกส่งเข้ามาในระบบแล้ว จะถูกตรวจสอบยืนยันว่าผู้ใช้ที่ 1 เป็นผู้ส่งเงินมาจริงหรือไม่ **ด้วยการถอดรหัส**ระหว่างเลขที่บัญชีของผู้ใช้ที่ 1 (Owner 1's Public Key) กับลายเซ็นดิจิทัล (Owner 1's Signature) ที่ประทับอยู่ และเมื่อผ่านการตรวจสอบแล้ว ผู้ใช้ที่ 2 จึงสามารถรับบิทคอยน์ได้ด้วยการใช้รหัสผ่านส่วนตัว (Owner 2's Private Key) ของตนเอง**ถอดรหัสข้อความดังกล่าวเพื่อยืนยันความเป็นเจ้าของบัญชีปลายทาง**

สามารถสรุปให้เข้าใจได้โดยง่ายว่า **ในการทำธุรกรรมของบิทคอยน์นั้น ต้องใช้รหัสผ่านส่วนตัว (Private Key) และเลขที่บัญชี (Public Key) ประกอบกันเพื่อเข้ารหัสข้อมูลและถอดรหัสข้อมูล เพื่อใช้ในการยืนยันความเป็นเจ้าของบัญชีและเพื่ออนุมัติการทำธุรกรรมการโอนและรับบิทคอยน์**

3) ใช้ในการรักษาความปลอดภัยในการเก็บข้อมูล ภายหลังจากที่มีการตรวจสอบความถูกต้องและยืนยันการทำธุรกรรมแล้ว ระบบของบิทคอยน์จะทำการเก็บข้อมูลด้วยระบบบล็อคเชน (Blockchain) ซึ่งมีลักษณะคล้ายกล่องเก็บข้อมูลที่อยู่ในรูปแบบอิเล็กทรอนิกส์ โดยระบบจะทำการจัดกลุ่มและเก็บรวบรวมข้อมูลประวัติทางธุรกรรมไว้ในรูปแบบของบล็อค (Block) ต่อเนื่องกันไปเป็นห่วงโซ่ (Chain) ตามลำดับเวลา **โดยในแต่ละบล็อคจะมีการอ้างอิงข้อมูลจากบล็อคก่อนหน้าเพื่อยืนยันความถูกต้องและป้องกันความผิดพลาดของห่วงโซ่การเก็บข้อมูล ด้วยการนำข้อมูลจากบล็อคก่อนหน้ามาเข้ารหัสและบรรจุไว้ในบล็อคปัจจุบันเสมือนเป็นค่าลายพิมพ์นิ้วมือดิจิทัลประจำบล็อค** ดังนั้น จึงไม่สามารถมีการเปลี่ยนแปลงแก้ไขข้อมูลภายในบล็อคที่ถูกตรวจสอบยืนยันแล้วได้ เพราะจะทำให้ค่าที่ระบุไว้ในแต่ละบล็อคเปลี่ยนแปลงไปและระบบจะปฏิเสธการแก้ไขเปลี่ยนแปลงนั้นทันที ทำให้บิทคอยน์มีความปลอดภัยในการเก็บรักษาข้อมูลสูง (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561) โดยจะได้อธิบายรายละเอียดของระบบบล็อคเชนเพิ่มเติมในหัวข้อต่อไป

การที่ผู้พัฒนาบิทคอยน์นำระบบการเข้ารหัสข้อมูลมาใช้ในการขั้นตอนการทำงานต่างๆของบิทคอยน์ทำให้บิทคอยน์ถูกเรียกว่าเป็น **“สกุลเงินเข้ารหัส (Cryptocurrency)”** และการเข้ารหัสข้อมูลนี้ยังเป็นคุณลักษณะพิเศษหนึ่งที่ทำให้บิทคอยน์ได้รับความเชื่อถือในประเด็นด้านความปลอดภัยในการเก็บรักษาข้อมูล ส่งผลทำให้เกิดความมั่นใจที่จะถือครองบิทคอยน์ไว้และทำให้มูลค่าของบิทคอยน์เพิ่มสูงขึ้นมาโดยตลอด

3.1.3.2 การทำธุรกรรมระหว่างกันโดยตรง (Peer-to-Peer)

คุณลักษณะสำคัญอีกประการของบิทคอยน์ที่ ซาโตชิ นากาโมโตะ ได้นำมาใช้เป็นแนวคิดหลักในการออกแบบการทำงานของบิทคอยน์คือ การที่ผู้ใช้งานบิทคอยน์สามารถทำธุรกรรมระหว่างกันได้โดยตรง โดยไม่ต้องดำเนินการผ่านตัวกลางอย่างธนาคารหรือสถาบันการเงินต่างๆ (พรชัย ชุนหจินดา, 2561) ด้วยระบบการทำธุรกรรมระหว่างกันโดยตรงนี้ ส่งผลทำให้การใช้งานบิทคอยน์เป็นการทำธุรกรรมที่สะดวกรวดเร็วและยังมีค่าธรรมเนียมต่ำเมื่อเทียบกับวิธีการทางธุรกรรมอื่นๆ เช่น ในกรณีของการโอนบิทคอยน์ไปให้ผู้รับทางไกลจะมีค่าธรรมเนียมประมาณ 0.0005 บิทคอยน์หรือคิดเป็นมูลค่าไม่ถึงหนึ่งบาท แต่หากเป็นการดำเนินการผ่านธนาคารหรือสถาบันการเงินต่าง ๆ จะเกิดค่าธรรมเนียมที่ต้องชำระประมาณ 700 – 1,300 บาท ต่อรายการธุรกรรม หรือหากเป็นการ

ดำเนินการด้วยบัตรเครดิต ผู้ใช้งานจะต้องเสียค่าธรรมเนียมประมาณ 3 – 5% นอกจากนี้หากเป็นการทำธุรรมทางไกลที่ผ่านการดำเนินการของตัวกลาง จะมีระยะเวลาในการดำเนินการประมาณ 2-3 วัน ในขณะที่หากเป็นการทำธุรกรรมด้วยบิทคอยน์สามารถทำธุรกรรมให้เสร็จสิ้นได้ภายในไม่กี่ชั่วโมงเท่านั้น (ลักษนันท์ พลอยวัฒนาวงศ์, 2561)

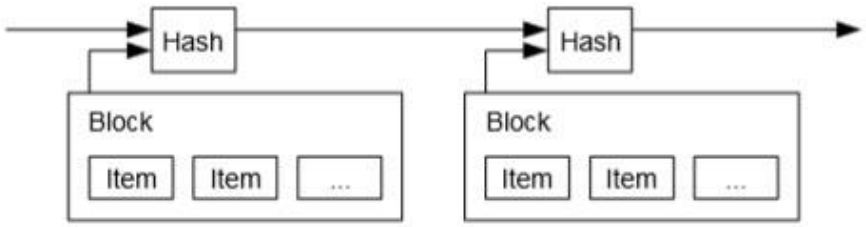
3.1.3.3 การกระจายอำนาจในการตรวจสอบยืนยันธุรกรรม (Decentralized and Public Ledger)

แนวคิดในการสร้างบิทคอยน์นั้นเกิดจากการตระหนักถึงปัญหาของระบบการเงินการธนาคารแบบดั้งเดิมที่ใช้ตัวกลางที่ไว้ใจได้อย่างธนาคารและสถาบันการเงินต่าง ๆ ในการตรวจสอบยืนยันและเก็บบันทึกข้อมูลทางธุรกรรมต่าง ๆ ซึ่งการใช้ระบบการรวบรวมที่ศูนย์กลางลักษณะนี้ทำให้เกิดปัญหาขึ้นในหลายประเด็นตามที่ได้กล่าวมาแล้ว ดังนั้นผู้พัฒนาบิทคอยน์จึงใช้ระบบการตรวจสอบยืนยันทางธุรกรรมแบบใหม่ที่ไม่ต้องอาศัยตัวกลาง แต่ใช้ระบบการกระจายอำนาจ (**Decentralize**) ที่ให้ผู้ใช้งานบิทคอยน์ทุกคนในระบบสามารถตรวจสอบความถูกต้องของธุรกรรมที่เกิดขึ้นได้ทุกธุรกรรม **โดยระบบจะนำข้อมูลที่เป็นคำร้องขออนุมัติทำธุรกรรมจากผู้ใช้งานบิทคอยน์ทุกราย มาแสดงไว้ในบัญชีสาธารณะ (Public Ledger)** ที่เปรียบเสมือนเป็นบัญชีบันทึกข้อมูลธุรกรรมทั้งหมดในระบบบิทคอยน์ โดยที่ผู้ใช้งานบิทคอยน์ทุกรายจะได้รับสำเนาข้อมูลบัญชีสาธารณะดังกล่าวนี้ เพื่อเปิดโอกาสให้ผู้ใช้งานสามารถร่วมกันตรวจสอบยืนยันธุรกรรมต่างๆที่เกิดขึ้นในระบบได้ อีกทั้งระบบยังจูงใจให้ผู้ใช้งานเกิดการแข่งขันกันตรวจสอบยืนยันธุรกรรมโดยผู้ใช้งานที่สามารถตรวจสอบยืนยันธุรกรรมด้วยวิธีการและเงื่อนไขที่ระบบกำหนดไว้ได้สำเร็จเป็นคนแรกจะได้รับบิทคอยน์เป็นค่าตอบแทน หรือที่กลุ่มผู้ใช้งานนิยมเรียกการแข่งขันกันตรวจสอบยืนยันความถูกต้องเพื่อแลกกับค่าตอบแทนเป็นบิทคอยน์นี้ว่า การขุดหรือการทำเหมืองบิทคอยน์ (Mining) ซึ่งจะได้อธิบายถึงวิธีการในการขุดโดยละเอียดต่อไป

การตรวจสอบยืนยันความถูกต้องของธุรกรรมด้วยการกระจายอำนาจในลักษณะนี้มีจุดประสงค์เพื่อทำให้การธุรกรรมของบิทคอยน์เป็นไปอย่างโปร่งใส เพราะไม่ถูกผูกขาดอำนาจการตรวจสอบไว้ที่ตัวกลางซึ่งอาจจะเกิดความผิดพลาดได้ อีกทั้งการที่ข้อมูลถูกตรวจสอบยืนยันจากหลายบุคคล ทำให้การทำธุรกรรมของบิทคอยน์มีความถูกต้องแม่นยำและน่าเชื่อถือเป็นอย่างยิ่ง (ลักษนันท์ พลอยวัฒนาวงศ์, 2561)

3.1.3.4 การเก็บข้อมูลแบบบล็อคเชน (Blockchain)

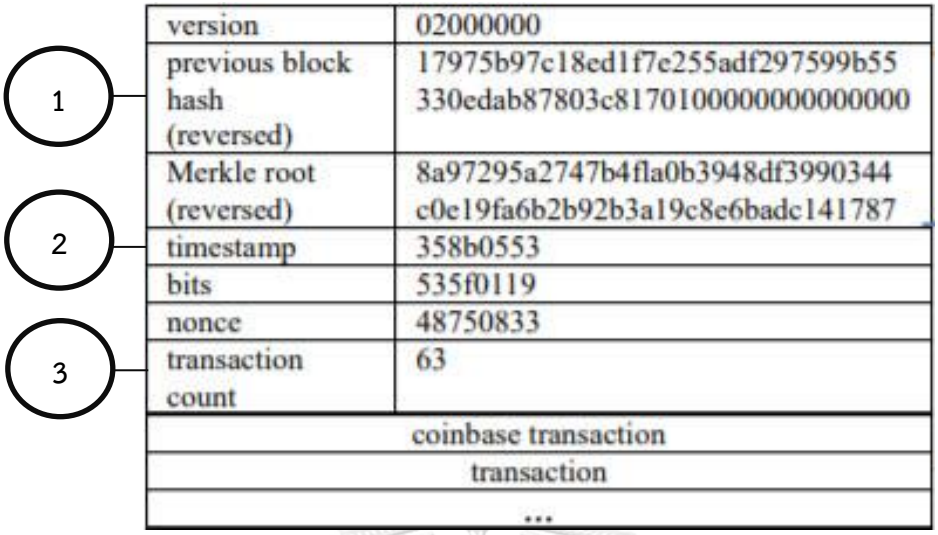
ระบบการเก็บข้อมูลแบบบล็อคเชน (Blockchain) เกิดจากการที่ ซาโตชิ นากาโมโตะ ได้นำเสนอ วิธีการเก็บรักษาข้อมูลทางธุรกรรมของบิทคอยน์ให้อยู่ในรูปแบบของบล็อคข้อมูล (Block) ที่เชื่อมต่อกันเป็นห่วงโซ่ (Chain) ตามลำดับเวลา โดยภายหลังจากที่มีการตรวจสอบยืนยันธุรกรรมแล้ว ระบบจะรวบรวมข้อมูลธุรกรรมแล้วใส่ลงในบล็อคข้อมูลที่สร้างขึ้น ลักษณะคล้ายกับการเก็บข้อมูลลงในกล่องข้อมูลอิเล็กทรอนิกส์ โดยในแต่ละบล็อคจะมีการอ้างอิงข้อมูลจากบล็อคก่อนหน้าเพื่อยืนยันความถูกต้องและป้องกันความผิดพลาดของห่วงโซ่การเก็บข้อมูล ด้วยการนำข้อมูลจากบล็อคก่อนหน้ามาเข้ารหัสทางเดียว (One-way function) ด้วยค่าแฮช (Hash) แล้วนำเอาค่าที่ได้มาใช้เสมือนเป็นค่าลายพิมพ์นิ้วมือดิจิทัลประจำบล็อคข้อมูลแต่ละบล็อค ดังปรากฏตามภาพ (Satoshi Nakamoto, 2008)



ภาพที่ 13 แนวคิดการเก็บข้อมูลด้วยระบบบล็อคเชน (Blockchain)

ในแต่ละบล็อคจะมีการเก็บข้อมูลทางธุรกรรมไว้หลายรายการเสมือนเป็นฐานข้อมูลที่เก็บข้อมูลทางธุรกรรมของบิทคอยน์ไว้ทั้งหมด และในขณะเดียวกันระบบจะนำบล็อคข้อมูลที่ถูกสร้างขึ้นใหม่ไปต่อท้ายสายโซ่ที่ยาวที่สุดเพียงสายเดียว จึงทำให้ไม่เกิดความซ้ำซ้อนในการเก็บข้อมูล และยังทำให้ฐานข้อมูลมีลักษณะเหมือนกันทั้งระบบ (ดลพร ประสงค์สุทธิพร, 2557)

นอกจากนี้ในแต่ละบล็อคยังมีการระบุค่าที่เป็นเสมือน **ตราประทับเวลา (Timestamp)** เพื่อระบุว่าบล็อคข้อมูลใดถูกสร้างขึ้นก่อนหรือหลัง เพื่อเหตุผลในการป้องกันปัญหาการสั่งจ่ายเงินซ้ำซ้อน หรือที่นิยมเรียกว่า **Double Spending** (หมายถึงการที่ผู้ใช้งานสั่งจ่ายเงินก้อนเดียวกัน ให้กับผู้รับหลายคนในเวลาเดียวกัน เช่น นาย ก. มีบิทคอยน์จำนวน 1 บิทคอยน์ แต่สร้างคำสั่งการโอนเงินจำนวน 1 บิทคอยน์ ให้กับทั้ง นาย ข. และ นาย ค. ในเวลาเดียวกัน) อีกด้วย โดยรูปแบบของบล็อคเชนที่เกิดขึ้นในระบบบิทคอยน์จริง จะมีลักษณะดังนี้ (ลักษนันท์ พลอยวัฒนาวงศ์, 2561)



ภาพที่ 14 ส่วนประกอบของข้อมูลภายในบล็อคเก็บข้อมูลบิทคอยน์ 1 บล็อค

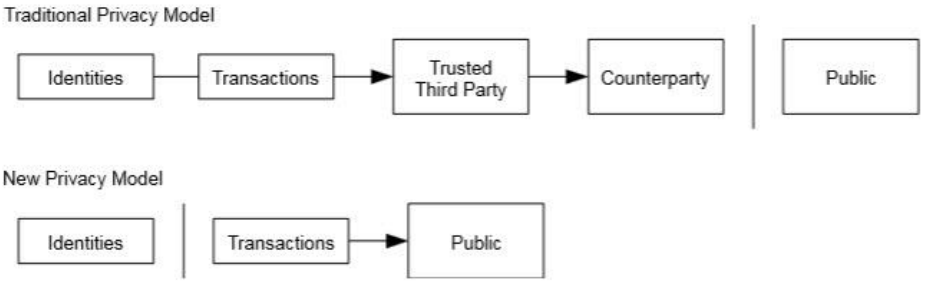
จากภาพตัวอย่าง **หมายเลข 1** คือ ค่าแฮช (Hash) ของบล็อคก่อนหน้าเพื่ออ้างอิงว่าบล็อคตัวอย่างตามภาพนี้เป็นบล็อคที่ต่อมาจากบล็อคดังกล่าว **หมายเลข 2** คือค่าที่เป็น**ตรา**ประทับเวลา (Timestamp) และ**หมายเลข 3** คือ ตัวเลขบอกจำนวนว่า ในบล็อคนี้มีการเก็บข้อมูลธุรกรรมบิทคอยน์ไว้ จำนวน 63 ธุรกรรม

การเก็บบันทึกข้อมูลทางธุรกรรมของบิทคอยน์ด้วยระบบบล็อคเชนดังกล่าวนี้ทำให้เกิดความปลอดภัยสูงเนื่องจาก **ไม่สามารถเกิดการลักลอบแก้ไขเปลี่ยนแปลงข้อมูลที่ถูกบันทึกไว้ในแต่ละบล็อคได้** เพราะหากมีการเปลี่ยนแปลงแก้ไขข้อมูลภายในบล็อค จะทำให้ค่าแฮชที่ระบุไว้ในแต่ละบล็อคเปลี่ยนแปลงไปและไม่สามารถนำไปอ้างอิงถึงบล็อคก่อนหน้าได้ ซึ่งหากเกิดกรณีดังกล่าวนี้ขึ้นระบบจะตรวจพบและไม่อนุมัติการลักลอบแก้ไขเปลี่ยนแปลงข้อมูลทันทีเพื่อป้องกันไม่ให้ห่วงโซ่การเก็บข้อมูลเสียหายทั้งระบบ

3.1.3.5 ไม่สามารถระบุตัวตนเจ้าของบัญชีได้ (Anonymity)

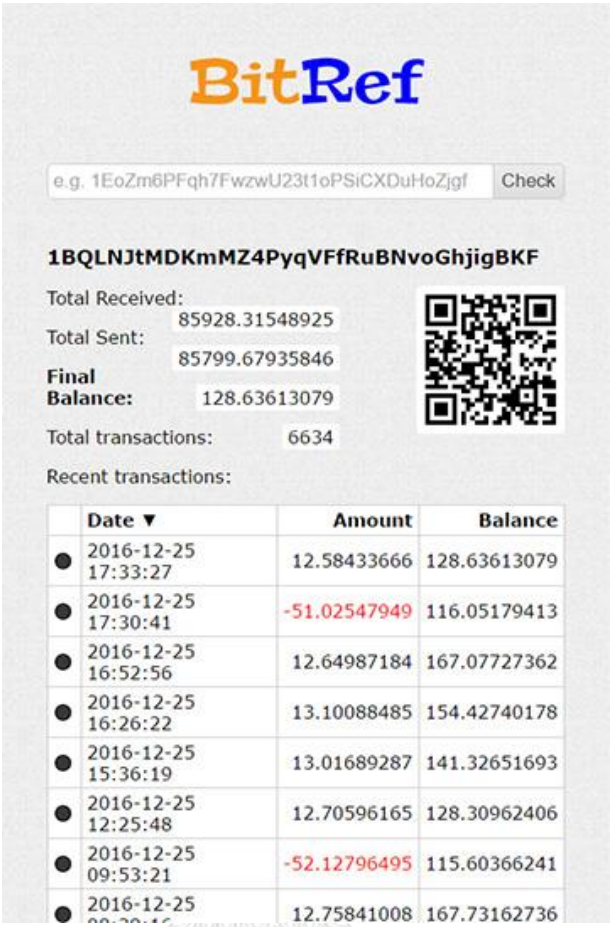
คุณลักษณะพิเศษของบิทคอยน์อีกประการหนึ่งที่เป็นประเด็นที่น่าสนใจเป็นอย่างยิ่ง คือ แม้จะมีการเปิดเผยรายละเอียดข้อมูลที่เกี่ยวกับการทำธุรกรรมบิทคอยน์ที่เกิดขึ้นทุกธุรกรรม ได้แก่ ข้อมูลเลขที่บัญชีบิทคอยน์และข้อมูลความเคลื่อนไหวทางธุรกรรมของผู้ใช้งานบิทคอยน์ทั้งหมดทุกคนทั่วโลกผ่านระบบบัญชีสาธารณะ (Public Ledger) เพื่อกระจายอำนาจการตรวจสอบและ

ยืนยันความถูกต้องของธุรกรรมตามที่ได้กล่าวมาแล้ว แต่ระบบบิทคอยน์**ไม่ได้ระบุตัวตนที่แท้จริงของเจ้าของบัญชีแต่อย่างใด** โดยแนวคิดในการรักษาความลับด้วยการไม่ระบุตัวตนของเจ้าของบัญชีบิทคอยน์นั้น ปรากฏอยู่ในแนวคิดของซาโตชิ นากาโมโตะ มาตั้งแต่ต้นตามภาพดังนี้ (Satoshi Nakamoto, 2008)



ภาพที่ 15 แนวคิดการไม่เปิดเผยตัวตนเจ้าของบัญชีผู้ใช้งานบิทคอยน์

จากภาพดังกล่าวสามารถอธิบายได้ว่า ในขณะที่ระบบการเงินการธนาคารแบบดั้งเดิมจะมีการตรวจสอบตัวตนเจ้าของบัญชีโดยตัวกลางที่ได้รับความไว้วางใจอย่างธนาคารและสถาบันการเงินต่างๆ ภายหลังจากที่ได้รับการยืนยันตัวตนแล้วจึงจะสามารถทำธุรกรรมทางการเงินได้ แต่ในกรณีของบิทคอยน์นั้นผู้ใช้งานสามารถทำธุรกรรมได้ทันที โดย**ไม่มีการตรวจสอบยืนยันตัวตนที่แท้จริงว่าบุคคลใดเป็นผู้ทำธุรกรรม แต่จะตรวจสอบยืนยันเพียงว่าธุรกรรมดังกล่าวเป็นการทำธุรกรรมระหว่างเลขที่บัญชีใดเท่านั้น** เนื่องจากต้องการรักษาความเป็นส่วนตัวให้กับผู้ใช้งาน ดังนั้นแม้จะมีการเปิดเผยข้อมูลรายละเอียดเกี่ยวกับการทำธุรกรรมทั้งหมดสู่สาธารณะก็ไม่สามารถทราบได้ว่าผู้ใดเป็นผู้ทำธุรกรรมดังกล่าว ดังตัวอย่างต่อไปนี้



ภาพที่ 16 ตัวอย่างข้อมูลประวัติการทำธุรกรรมบิทคอยน์
ของเลขที่บัญชี 1BQLNJtMDKmMZ4PyqVFfRuBNvoGhjigBKF
(*Blockchain for Geek ... เบื้องหลังการทำงานฉบับ Technical ตัวอย่างจาก Bitcoin*, 2559)

ข้อมูลรายละเอียดที่เกี่ยวกับประวัติและบันทึกการทำธุรกรรมบิทคอยน์นั้นเป็นข้อมูลเปิดที่สามารถค้นหาและตรวจสอบได้จากผู้ให้บริการทั่วไป โดยภาพตัวอย่างที่ยกมานี้เป็นการตรวจสอบข้อมูลทางธุรกรรมของผู้ใช้งานเลขที่บัญชี 1BQLNJtMDKmMZ4PyqVFfRuBNvoGhjigBKF ผ่านผู้ให้บริการชื่อเว็บไซต์บิทเรฟ (www.bitref.com) โดยบุคคลทั่วไปจะสามารถทราบได้ทันทีว่า ผู้ใช้งานบัญชีบิทคอยน์ดังกล่าวครอบครองบิทคอยน์จำนวนเท่าใด ทำธุรกรรมบิทคอยน์ไปแล้วกี่ครั้ง มีมูลค่าการโอน-รับบิทคอยน์เท่าใด รวมทั้งสามารถทราบความเคลื่อนไหวทางบัญชีได้จากประวัติการใช้งาน **แต่จะไม่สามารถทราบได้ว่าผู้ใดเป็นเจ้าของบัญชีนั้น และในระบบบิทคอยน์เองก็ไม่ได้มีตรวจสอบยืนยันและบันทึกข้อมูลตัวตนที่แท้จริงของผู้ใช้งานแต่อย่างใด**

คุณลักษณะพิเศษที่ไม่มีการระบุตัวตนของเจ้าของบัญชีดังกล่าว เป็นปัจจัยสำคัญที่ทำให้อาชญากรอาจนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมประเภทต่างๆ ใช้เป็นเครื่องมือในการฟอกเงิน หรือใช้เป็นทางเลือกใหม่ในการเก็บรักษารายได้ที่ได้จากการกระทำความผิดต่างๆได้ เพราะเจ้าหน้าที่ของรัฐไม่สามารถตรวจสอบได้ว่าผู้ใดเป็นเจ้าของบัญชีบิทคอยน์ต่างๆ (อภินพ อติพิบูลย์สิน, 2557) ดังนั้นจึงถือได้ว่า คุณลักษณะพิเศษนี้ เป็นประเด็นปัญหาสำคัญที่จะต้องนำมาพิจารณาเพื่อหาแนวทางในการป้องกันการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมต่อไป

3.1.3.6 จำนวนและหน่วยของบิทคอยน์

ผู้สร้างบิทคอยน์ออกแบบให้ระบบสามารถสร้างบิทคอยน์ได้มากที่สุดจำนวน 21 ล้านบิทคอยน์เท่านั้น ด้วยเหตุผลในการต้องการจำกัดปริมาณอุปทานเพื่อคงมูลค่าให้แก่บิทคอยน์ แต่เนื่องจากมูลค่าของบิทคอยน์ 1 บิทคอยน์นั้นมีมูลค่าสูง จึงทำให้ต้องมีการกำหนดหน่วยของบิทคอยน์ให้มีขนาดเล็กลง เพื่อลดข้อจำกัดในการใช้งานและยังทำให้ระบบราคามีประสิทธิภาพ อีกทั้งยังสร้างให้เกิดความเป็นธรรมในการทำธุรกรรมมากขึ้น (พรชัย ชุนหจินดา, 2561) โดยตัวย่อแทน 1 หน่วยบิทคอยน์ คือ BTC และสามารถแบ่งบิทคอยน์เป็นหน่วยย่อยได้ดังนี้ (จุฑารัตน์ ชวดนุช, 2556)

1 BTC = 1 บิทคอยน

0.01 BTC = 1 cBTC = 1 เซนติบิทคอยน

0.001 BTC = 1 mBTC = 1 มิลลิบิทคอยน

0.000 001 BTC = 1 mBTC = 1 ไมโครบิทคอยน

0.000 000 01 BTC = 1 ซาโตชิ

3.1.4 มูลค่าของบิทคอยน์

บิทคอยน์ถูกสร้างขึ้นเพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการในลักษณะเดียวกันกับเงินสกุลจริง ดังนั้นจึงจำเป็นจะต้องมีการกำหนดมูลค่าให้กับบิทคอยน์ โดยบิทคอยน์ไม่ได้มีการกำหนดมูลค่าจากการค้ำประกันด้วยสินทรัพย์หรือสถาบันการเงินใดๆ แต่ใช้วิธีการจำกัดให้มีการสร้างบิทคอยน์ได้ทั้งหมดจำนวน 21 ล้านบิทคอยน์ อีกทั้งยังมีการป้องกันไม่ให้มีการทำซ้ำหรือลอกเลียนแบบบิทคอยน์เพื่อเพิ่มจำนวนได้ มูลค่าของบิทคอยน์จึงเป็นไปตามกลไกของอุปสงค์อุปทาน

(Demand and Supply) กล่าวคือ เมื่อมีผู้ต้องการซื้อบิทคอยน์มากขึ้นแต่จำนวนบิทคอยน์มีจำกัด มูลค่าของบิทคอยน์ก็จะสูงขึ้น ในทางกลับกันหากระดับความต้องการซื้อบิทคอยน์ลดลงมูลค่าของบิทคอยน์ก็ลดลงด้วย โดยมีปัจจัยต่าง ๆ ที่จะส่งผลต่อมูลค่าของบิทคอยน์ดังนี้ (สำนักงานเลขาธิการสภาผู้แทนราษฎร, 2561)

ปัจจัยที่ทำให้มูลค่าของบิทคอยน์เพิ่มขึ้น

1) จำนวนของบิทคอยน์ที่มีจำนวนจำกัดเพียง 21 ล้านบิทคอยน์ ทำให้เมื่อเวลาผ่านไประบบจะปรับกลไกให้เกิดการสร้างบิทคอยน์ได้ยากขึ้น ทำให้โอกาสที่จะสามารถถือครองบิทคอยน์น้อยลงซึ่งสวนทางกับความต้องการใช้บิทคอยน์ ส่งผลให้มูลค่าของบิทคอยน์สูงขึ้น

2) ความเชื่อมั่นในแง่ของการลงทุนเก็งกำไร ที่นักลงทุนมีความเชื่อว่าบิทคอยน์จะมีมูลค่าสูงขึ้นโดยไม่มีขีดจำกัด ประกอบกับการขยายตัวของตลาดการลงทุนบิทคอยน์ในปัจจุบัน ทำให้เกิดกระแสความต้องการครอบครองบิทคอยน์เป็นจำนวนมากและส่งผลให้มีบิทคอยน์มูลค่าสูงขึ้น

3) ความนิยมในบิทคอยน์ที่เกิดจากความสะดวกสบายในการใช้งานแทนเงินสกุลจริงที่มีความรวดเร็ว ไร้ขอบเขต ประกอบกับการที่สังคมโลกเริ่มมีการยอมรับและเชื่อมั่นในบิทคอยน์ให้สามารถใช้แลกเปลี่ยนสินค้าและบริการได้มากขึ้น ทำให้เกิดความต้องการในการครอบครองและมีปริมาณการใช้บิทคอยน์เพิ่มมากขึ้นจึงส่งผลให้มูลค่าของบิทคอยน์สูงขึ้น

ปัจจัยที่ทำให้มูลค่าของบิทคอยน์ลดลง

1) มูลค่าของบิทคอยน์อาจลดลง หากเกิดการซื้อ-ขายบิทคอยน์ในตลาดซื้อขายเป็นปริมาณมาก ซึ่งเป็นไปตามกลไกของตลาด

2) หากระดับความเชื่อมั่นในบิทคอยน์ลดลง มูลค่าของบิทคอยน์ก็จะลดต่ำลงด้วย เช่น หากเกิดกระแสข่าวในทางลบที่เกี่ยวกับบิทคอยน์ ก็จะส่งผลให้ระดับความต้องการถือครองบิทคอยน์ลดลง

3) การแข่งขันกันเองในตลาดสกุลเงินเข้ารหัส เนื่องจากในปัจจุบันมีสกุลเงินเข้ารหัสกว่า 1,500 ชนิด และยังมีการสร้างและพัฒนาสกุลเงินเข้ารหัสชนิดใหม่อยู่เสมอ จึงอาจทำให้เกิดการแข่งขันจากกันระหว่างสกุลเงินเข้ารหัสจนส่งผลกระทบต่อมูลค่าของบิทคอยน์ได้

3.1.5 วิธีการได้มาซึ่งบิทคอยน์

จากการศึกษางานวิจัย (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561) (จุฑารัตน์ ชวดนุช, 2557) สามารถสรุปการได้มาซึ่งบิทคอยน์สามารถกระทำได้ 3 วิธี ได้แก่

1) การแลกเปลี่ยน (Exchange) โดยผู้ที่ต้องการถือครองบิทคอยน์สามารถนำเงินสกุลจริงไปแลกเปลี่ยนเป็นบิทคอยน์ได้ทั้งจากการแลกเปลี่ยนกันเองโดยตรงกับผู้ที่ถือครองบิทคอยน์อยู่แล้ว (Local Exchange) หรือ การแลกเปลี่ยนจากสกุลเงินจริงเป็นบิทคอยน์ผ่านการดำเนินการของผู้ให้บริการรับแลกเปลี่ยน (Exchange Center) ต่างๆ ตามราคาแลกเปลี่ยนที่กำหนด ในลักษณะคล้ายกันกับการแลกเปลี่ยนสกุลเงินต่างๆตามปกติ

2) โดยการซื้อขายแลกเปลี่ยนสินค้าหรือบริการ (Payment) โดยผู้ใช้งานอาจได้รับบิทคอยน์ได้ด้วยการรับโอนบิทคอยน์แทนการรับชำระค่าสินค้าและบริการด้วยการใช้สกุลเงินจริง

3) โดยการขุดหรือการทำเหมืองบิทคอยน์ (Mining) วิธีการขุดหรือการทำเหมืองบิทคอยน์นั้นเกิดขึ้นสืบเนื่องมาจากแนวคิดการกระจายอำนาจในการตรวจสอบความถูกต้องของข้อมูลธุรกรรมบิทคอยน์ที่ไม่ต้องอาศัยตัวกลางอย่างธนาคารหรือสถาบันการเงินต่างๆ แต่ให้ผู้ใช้งานบิทคอยน์ (Nodes) ที่เชื่อมต่อกับระบบอยู่แล้ว เป็นผู้ทำหน้าที่ในการตรวจสอบความถูกต้องของธุรกรรมแล้วนำข้อมูลที่ได้รับการตรวจสอบแล้วไปบันทึกลงในบล็อคข้อมูล (Block) ตามที่ได้อธิบายไปแล้วในหัวข้อการเก็บข้อมูลแบบบล็อคเชน โดยเพื่อให้ระบบการตรวจสอบข้อมูลด้วยผู้ใช้งานด้วยกันเองนี้สามารถทำงานได้อย่างมีประสิทธิภาพ **ระบบบิทคอยน์จึงมีการจูงใจให้เกิดการแข่งขันกันตรวจสอบยืนยันความถูกต้องของธุรกรรมขึ้น ด้วยการจ่ายค่าตอบแทนเป็นบิทคอยน์จำนวนหนึ่งให้กับผู้ที่สามารถตรวจสอบยืนยันความถูกต้องของธุรกรรมแล้วบันทึกข้อมูลไว้ในบล็อคได้เป็นคนแรก** ทั้งนี้ในการตรวจสอบความถูกต้องของธุรกรรมดังกล่าว จะต้องมีการแก้สมการทางคณิตศาสตร์ที่ถูกเข้ารหัสซึ่งจำเป็นจะต้องกระทำผ่านการคำนวณด้วยระบบคอมพิวเตอร์ที่มีศักยภาพสูง จึงทำให้ต้องอาศัยต้นทุนและระยะเวลาเป็นจำนวนมาก จึงทำให้วิธีการได้มาซึ่งบิทคอยน์ในรูปแบบนี้ถูกเรียกว่าการขุดหรือการทำเหมือง

ขั้นตอนในการขุดหรือการทำเหมืองบิทคอยน์ สามารถทำได้โดยนักขุด (Miner) จะต้องติดตั้งโปรแกรมคำสั่งให้คอมพิวเตอร์ทำการสุ่มค่าเฉพาะที่ถูกเรียกว่าค่า Nonce ขึ้น แล้วนำไปคำนวณร่วมกับค่าแฮช (Hash) ของบล็อคปัจจุบัน (Current Block) ด้วยวิธีการทางคณิตศาสตร์ ซึ่ง

กระบวนการนี้จะเกิดขึ้นซ้ำไปมาอย่างต่อเนื่องจนกว่าจะสามารถคำนวณหาค่าผลลัพธ์ที่มีค่าต่ำกว่าหรือเท่ากับค่าเป้าหมาย (Target) ที่ระบบกำหนดไว้ได้ ซึ่งในการแก้ปัญหาสมการทางคณิตศาสตร์ดังกล่าวจะต้องใช้พลังงานคอมพิวเตอร์เป็นจำนวนมากอย่างมหาศาล จึงทำให้ซาโตชิ นากาโมเตะเรียกหลักการใช้พลังงานและศักยภาพทางคอมพิวเตอร์เพื่อแข่งขันกันแก้ปัญหาสมการทางคณิตศาสตร์นี้ว่า Proof-of-Work (Satoshi Nakamoto, 2008)

นอกจากนี้ระบบบิทคอยน์ยังได้ออกแบบให้เกิดความสมดุลในการขุดบิทคอยน์ด้วยการกำหนดค่าความยากในการแก้สมการ (Difficulty) ขึ้น โดยค่าความยากดังกล่าวจะเป็นตัวควบคุมว่าหากในระบบมีผู้ขุดบิทคอยน์เป็นจำนวนมาก ก็จะทำให้มีการตรวจสอบยืนยันธุรกรรมและสร้างจำนวนบล็อคเพื่อเก็บข้อมูลมากขึ้น ระยะเวลาเฉลี่ยในการขุดบิทคอยน์ก็จะลดลง เมื่อเป็นเช่นนั้นระบบจะปรับค่าความยากให้เพิ่มขึ้น ส่งผลให้การแก้สมการยากขึ้น ความสามารถในการที่จะตรวจสอบยืนยันและสร้างบล็อคเพื่อเก็บข้อมูลก็จะลดลง ทำให้ปริมาณการสร้างบล็อคกลับสู่ภาวะปกติ ส่งผลให้มีผู้ขุดบิทคอยน์มากขึ้นเป็นวงจรเช่นนี้ไป โดยระบบจะปรับสมดุลอัตโนมัติด้วยการปรับค่าความยากใหม่ทุกๆ 2,016 บล็อค หรือประมาณ 2 สัปดาห์ (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

3.1.6 ขั้นตอนการทำธุรกรรมของบิทคอยน์

ภายหลังจากที่ผู้ใช้งานได้ทำการสมัครใช้งานผ่านช่องทางต่างๆและได้รับ รหัสผ่านส่วนตัว (Private Key) และเลขที่บัญชี (Bitcoin Address/Public Key) แล้ว เมื่อต้องการทำธุรกรรม เช่น การโอนบิทคอยน์ให้ผู้ใดผู้หนึ่งสามารถกระทำได้ตามขั้นตอนดังต่อไปนี้ (Satoshi Nakamoto, 2008)

1) เมื่อผู้ใช้งานต้องการจะโอนบิทคอยน์ให้ผู้ใดผู้หนึ่ง ก็จะต้องสร้างคำสั่งการโอนบิทคอยน์โดยระบุข้อมูลที่เกี่ยวข้องได้แก่ เลขที่บัญชีของตนเอง เลขที่บัญชีของผู้ที่จะรับการโอนบิทคอยน์ จำนวนบิทคอยน์ที่ต้องการโอน โดยข้อมูลต่างๆเหล่านี้จะถูกเข้ารหัสด้วยค่าแฮชเอาไว้ รวมทั้งคำสั่งการโอนเงินนี้จะถูกปิดผนึกด้วยลายเซ็นดิจิทัล (Digital Signature) ที่เกิดจากการนำรหัสผ่านส่วนตัวของผู้โอนมาเข้ารหัสเพื่อรักษาความปลอดภัยอีกชั้นหนึ่ง

2) จากนั้นคำสั่งการโอนบิทคอยน์ดังกล่าว จะถูกเผยแพร่ไปในระบบบัญชีสาธารณะ (Public ledger) เพื่อให้ผู้ใช้งานในระบบ (Nodes) ร่วมทำการตรวจสอบยืนยันความถูกต้องของคำสั่งธุรกรรมดังกล่าว เช่น ผู้โอนกับข้อมูลส่วนตัวที่ถูกเข้ารหัสไว้ในคำสั่งโอนเงินดังกล่าวสอดคล้องกัน

หรือไม่ ผู้โอนมีจำนวนบิทคอยน์เพียงพอสำหรับการโอนครั้งนั้นหรือไม่ โดยการตรวจสอบจะเป็นลักษณะของการแข่งขันกันคำนวณเพื่อแก้โจทย์สมการทางคณิตศาสตร์และถอดรหัสข้อมูลที่ถูกเข้ารหัสไว้ (ดังจะได้อธิบายรายละเอียดในหัวข้อ วิธีการได้มาซึ่งบิทคอยน์ ในเรื่องการทำเหมืองหรือการขุดบิทคอยน์) แล้วจึงตรวจสอบข้อมูลความถูกต้องของคำสั่งดังกล่าว

3) หลังจากที่มีผู้สามารถตรวจสอบความถูกต้องของข้อมูลการโอนบิทคอยน์และสามารถแก้โจทย์สมการทางคณิตศาสตร์ได้เป็นคนแรกแล้ว ระบบจะส่งข้อมูลดังกล่าวไปให้ผู้ใช้งานอื่นๆตรวจสอบซ้ำ

4) หากได้รับฉันทามติ (Consensus) จากผู้ใช้งานอื่นๆว่าข้อมูลดังกล่าวถูกต้องแล้ว คำสั่งการโอนบิทคอยน์ดังกล่าวจะถูกนำไปรวมกับคำสั่งทางธุรกรรมบิทคอยน์อื่นๆ แล้วนำไปเก็บไว้ในบล็อคข้อมูลใหม่ (Block) ที่ถูกสร้างขึ้น จากนั้นบล็อคข้อมูลใหม่นี้ก็จะถูกนำไปต่อในสายโซ่บล็อคข้อมูล (Blockchain) เพื่อเก็บรักษาข้อมูลต่อไป

5) เมื่อคำสั่งโอนบิทคอยน์ดังกล่าวถูกจัดเก็บในระบบบล็อคเชนแล้ว ก็จะทำให้กระบวนการโอนบิทคอยน์ตามคำสั่งโอนดังกล่าวเสร็จสิ้น

3.1.7 สถานภาพของบิทคอยน์ในประเทศไทย

จากการศึกษาความเป็นมาของบิทคอยน์ทำให้ทราบถึงเจตนาของผู้พัฒนาที่ต้องการให้บิทคอยน์เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการในลักษณะเดียวกันกับเงินสกุลจริง และถึงแม้ในปัจจุบันจะมีการนำบิทคอยน์ไปใช้ในการทำธุรกรรม ติดต่อซื้อขายแลกเปลี่ยนสินค้าและบริการกันได้จริงแล้วก็ตาม แต่ก็ยังมีประเด็นที่จำเป็นจะต้องศึกษาและทำความเข้าใจถึงสถานภาพของบิทคอยน์ในแง่มุมต่างๆ ดังนี้

3.1.7.1 สถานภาพของบิทคอยน์ในแง่ของการทำหน้าที่เป็นเงินแม้จะมีการนำบิทคอยน์ไปใช้ในการแลกเปลี่ยนสินค้าและบริการระหว่างกัน ในลักษณะที่คล้ายกันกับเงินสกุลจริงก็ตาม **แต่ในปัจจุบันยังไม่ถือว่าบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เป็นเงินที่ชำระหนี้ได้ตามกฎหมายไทย** เนื่องจากยังไม่มีคุณลักษณะพื้นฐานของเงินครบทั้ง 3 ประการ ดังต่อไปนี้ (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

1) การเป็นสื่อกลางในการแลกเปลี่ยน (Medium of Exchange) หมายถึงการทำหน้าที่เป็นสื่อกลางในการแลกเปลี่ยนหรือการชำระเงินเพื่อซื้อสินค้าและบริการหรือการชำระ

หนี้ตามสัญญาต่างๆ ซึ่งถึงแม้จะมีการนำบิทคอยน์ไปใช้ในการแลกเปลี่ยนสินค้าและบริการในบางสังคมที่มีการยอมรับในคุณค่าของบิทคอยน์แล้วก็ตาม แต่ก็ยังปรากฏว่ายังมีอีกหลายสังคมที่ยังไม่ให้การยอมรับเชื่อถือบิทคอยน์เช่นกัน ดังนั้น จึง**ยังไม่อาจกล่าวได้โดยชัดเจนว่าบิทคอยน์มีสถานะเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการได้เทียบเท่ากับเงินตราสกุลจริง เนื่องจากยังขาดความน่าเชื่อถือ ยังไม่เป็นสากล และยังขึ้นอยู่กับการยอมรับของผู้ซื้อและผู้ขายซึ่งแตกต่างกันไปในแต่ละสังคมอีกด้วย**

2) หน่วยของมูลค่า (Unit of Account) หมายถึง การทำหน้าที่เป็นหน่วยในการวัดมูลค่าของสินค้าและบริการ โดยสามารถเปรียบเทียบมูลค่าได้ด้วยการเปรียบเทียบปริมาณของสื่อกลางนั้น และสามารถรวบรวมกันเพื่อให้มีมูลค่ามากขึ้น และแบ่งแยกออกเพื่อให้มีมูลค่าลดลงได้ ด้วยหลักการของการเป็นหน่วยของมูลค่าดังกล่าวยิ่งช่วยให้เกิดการลดต้นทุนทางธุรกรรมและเกิดความสะดวกในทางเศรษฐกิจมากขึ้นซึ่งถือได้ว่าบิทคอยน์มีคุณลักษณะนี้

3) ที่เก็บมูลค่า (Store of Value) หมายถึง การทำหน้าที่เก็บและรักษามูลค่าไว้ในตนเองหรือการเก็บกำลังซื้อของผู้ถือครองเอาไว้ ทำให้ผู้ถือครองสามารถเก็บสะสมตัวเก็บมูลค่าไว้ ไม่จำเป็นจะต้องเร่งรีบใช้กำลังซื้อนั้นเพื่อแลกเปลี่ยนสินค้าและบริการในทันที ซึ่งในคุณลักษณะข้อนี้นั้นยังถือไม่ได้ว่าบิทคอยน์เป็นที่เก็บมูลค่าได้อย่างมั่นคงเท่ากับเงิน สาเหตุเพราะมูลค่าของบิทคอยน์ไม่ได้ถูกยึดโยงหรืออ้างอิงกับสินทรัพย์ใดแต่เกิดจากระดับอุปสงค์อุปทาน กล่าวคือเมื่อมีผู้ต้องการถือครองมากบิทคอยน์ก็จะมีมูลค่าสูงในขณะเดียวกันหากมีผู้ต้องการถือครองน้อยบิทคอยน์ก็จะมีมูลค่าลดลง ทั้งนี้ยังต้องอาศัยความเชื่อถือในมูลค่าบิทคอยน์ด้วย ประกอบกับการที่บิทคอยน์อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ที่ปราศจากการดูแลจากตัวกลางอย่างธนาคารหรือสถาบันการเงินต่างๆ อีกทั้งยังไม่มีรูปร่างและไม่สามารถจับต้องได้ ทำให้เกิดความเสี่ยงที่บิทคอยน์จะถูกยกเลิกหรือปิดระบบไปอีกด้วย ดังนั้น จึง**ยังไม่อาจกล่าวได้โดยชัดเจนว่าบิทคอยน์มีสถานะเป็นที่เก็บมูลค่าได้เทียบเท่ากับเงินตราสกุลจริง**

นอกจากนี้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ยังไม่เข้าลักษณะตามคำนิยามของกฎหมายเงินตราจึงทำให้ยังไม่สามารถนำไปใช้ชำระหนี้ได้ตามกฎหมาย อีกทั้งกฎหมายที่เกี่ยวกับการป้องกันปราบปรามการฟอกเงินก็ยังไม่สามารถตรวจสอบการทำธุรกรรมทางการเงินของบิทคอยน์ที่เกี่ยวข้องกับการกระทำผิดกฎหมายได้ จากเหตุผลที่กล่าวมาทั้งหมดนี้จึงทำให้**บิทคอยน์ยังไม่มีสถานภาพเป็นเงิน**แต่อย่างใด

3.1.7.2 สถานภาพของบิทคอยน์ในแง่ของการเป็นสินทรัพย์ในพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 มาตรา 3 ได้ให้ความหมายของคำว่า “สินทรัพย์ดิจิทัล” ไว้ว่า

“สินทรัพย์ดิจิทัล” หมายความว่า คริปโทเคอร์เรนซีและโทเคนดิจิทัล

“คริปโทเคอร์เรนซี” หมายความว่า หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้าบริการหรือสิทธิอื่นใดหรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และให้หมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นใดตามที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด”

“โทเคนดิจิทัล” หมายความว่า หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่าย อิเล็กทรอนิกส์โดยมีวัตถุประสงค์เพื่อ

(1) กำหนดสิทธิของบุคคลในการเข้าร่วมลงทุนในโครงการหรือกิจการใด ๆ

(2) กำหนดสิทธิในการได้มาซึ่งสินค้าหรือบริการหรือสิทธิอื่นใดที่เฉพาะเจาะจง ทั้งนี้ ตามที่กำหนดในข้อตกลงระหว่างผู้ออกและผู้ถือและให้หมายความรวมถึงหน่วยแสดงสิทธิอื่นตามที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด

เมื่อนำนิยามความหมายดังกล่าวมาพิจารณาจะสามารถเข้าใจได้ว่า บิทคอยน์เป็นคริปโทเคอร์เรนซีประเภทหนึ่ง เพราะบิทคอยน์มีสถานะเป็นหน่วยข้อมูลอิเล็กทรอกนิกส์ที่ใช้เป็นสื่อกลางในการแลกเปลี่ยน ส่วนในความหมายของการเป็นโทเคนดิจิทัลนั้นบิทคอยน์อาจมีลักษณะเข้าเงื่อนไขการเป็นโทเคนดิจิทัลได้ หากมีการใช้บิทคอยน์ในการระดมทุนจากประชาชนในลักษณะของ ICO หรือ Initial Coin Offering อีกทั้งในปัจจุบันสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ได้ประกาศอนุญาตให้สามารถนำบิทคอยน์ไปใช้ในการพิจารณาแลกเป็นโทเคนดิจิทัลเพื่อใช้ในการระดมทุนได้ (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2561) ดังนั้น หากพิจารณาจากความหมายตามกฎหมายดังกล่าวข้างต้น **บิทคอยน์จึงมีสถานภาพเป็นสินทรัพย์ ในรูปแบบของสินทรัพย์ดิจิทัล**

3.1.7.3 สถานภาพของบิทคอยน์ในแง่มุมของกฎหมายและอาชญากรรม ในแง่ของกฎหมายและอาชญากรรมนั้น ในทางกฎหมายอาญาหรือกฎหมายที่มีโทษต่างๆในทางอาญายังไม่ได้มีการกำหนดหรือให้คำนิยามหรือมีบทเฉพาะกาลที่เกี่ยวกับบิทคอยน์ไว้โดยเฉพาะ ดังนั้น ในการ

นำกฎหมายทางอาญาและกฎหมายอื่นๆมาปรับใช้ในกรณีที่เกิดข้อพิพาทที่เกี่ยวกับบิทคอยน์ขึ้นจึงจำเป็นจะต้องใช้การปรับข้อกฎหมายที่ใกล้เคียงมาใช้โดยอนุโลมเท่านั้น นอกจากนี้ด้วยเจตนาของผู้สร้างหรือผู้พัฒนาที่ต้องการให้บิทคอยน์ทำหน้าที่เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการเท่านั้น จึงทำให้ผู้วิจัยวิเคราะห์ได้ว่า **บิทคอยน์ไม่ได้มีความผิดหรือไม่ได้มีความชั่วร้ายในตัวเอง** เหมือนในกรณีของยาเสพติดหรือสิ่งผิดกฎหมายต่างๆ ดังนั้น การครอบครองบิทคอยน์จึงไม่ได้ถูกระบุว่าเป็นความผิด แต่ในขณะเดียวกันก็มีโอกาสสูงที่บิทคอยน์จะถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรมรูปแบบต่างๆดังจะได้กล่าวในหัวข้อต่อไป

3.2 บิทคอยน์กับอาชญากรรม

ด้วยคุณลักษณะพิเศษและหลักการทำงานของบิทคอยน์ ที่มีลักษณะของการไม่เปิดเผยตัวตนเจ้าของบัญชีผู้ใช้ที่แท้จริง (Anonymity) การเข้ารหัสข้อมูลสำคัญทางธุรกรรมต่างๆ (Cryptography) ระบบการทำงานที่ผู้ใช้งานสามารถติดต่อสื่อสารและทำธุรกรรมต่อกันได้เองโดยตรง (Peer–to-Peer) โดยไม่ผ่านตัวกลางหรือไม่ผ่านกลไกการควบคุมของเจ้าหน้าที่รัฐ รวมทั้งมูลค่าของบิทคอยน์ที่มีความผันผวนสูงขึ้นอยู่กับระดับอุปสงค์อุปทาน ประกอบกับสถานภาพในทางกฎหมายของบิทคอยน์ที่ยังคลุมเครือไม่ชัดเจน จึงทำให้บิทคอยน์มีคุณลักษณะที่เหมาะแก่การนำไปเป็นเครื่องมือในการก่ออาชญากรรมรูปแบบต่างๆ เพราะเมื่อมีการนำบิทคอยน์ไปใช้ในการประกอบอาชญากรรมแล้ว การดำเนินการในการติดตามสืบสวนสอบสวนรวบรวมพยานหลักฐานและรายละเอียดในการกระทำความผิดโดยเจ้าหน้าที่ของรัฐจะเป็นไปด้วยความซับซ้อน ยากลำบาก จำเป็นจะต้องอาศัยเจ้าหน้าที่ที่มีทักษะความชำนาญในด้านเทคโนโลยีคอมพิวเตอร์ขั้นสูง ซึ่งจากการศึกษารวบรวมข้อมูลของผู้ศึกษาพบว่ามีการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมด้วยกัน 2 ลักษณะ คือ **การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรง** เป็นลักษณะของการนำบิทคอยน์ไปใช้เป็นเครื่องมือแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมายหรือใช้เป็นสื่อกลางในการกระทำความผิดแทนสกุลเงินจริงเพื่อหลีกเลี่ยงการถูกตรวจสอบย้อนกลับของเจ้าหน้าที่ของรัฐ เช่น การใช้บิทคอยน์ซื้อขายยาเสพติด การใช้บิทคอยน์ซื้อขายอาวุธเถื่อน การใช้บิทคอยน์ในการจ้างวานให้ผู้อื่นไปกระทำความผิด รวมทั้ง การนำบิทคอยน์ไปใช้ในการระดมทุนของกลุ่มผู้ก่อการร้าย และการเรียกค่าไถ่ด้วยการเรียกร้องให้จ่ายค่าไถ่ด้วยบิทคอยน์ เป็นต้น และ **การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่อ**

อาชญากรรมทางอ้อม เป็นลักษณะของการนำเอาชื่อ “บิทคอยน์” ไปใช้ในการโฆษณาชวนเชื่อหรือหลอกลวงให้เหยื่อหลงเชื่อว่าจะมีการลงทุนและเก็งกำไรจากมูลค่าของบิทคอยน์ที่มีความผันผวนตามกลไกและความต้องการของตลาดเพื่อให้เกิดผลกำไรมาแบ่งปันให้แก่สมาชิกผู้เข้าร่วม และเมื่อเหยื่อหลงเชื่อและนำเงินมาลงทุนแล้ว คนร้ายก็จะนำเงินไปใช้ในการกระทำความผิดในลักษณะของแชร์ลูกโซ่ หรือกระทำความผิดในรูปแบบอื่นๆที่มีลักษณะคล้ายกัน โดยจะได้อธิบายถึงลักษณะและรูปแบบของการกระทำความผิดที่เกิดขึ้นจริงดังนี้

3.2.1 การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรง

จากการศึกษารวบรวมข้อมูลพบว่า มีการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมในลักษณะนำไปใช้เป็นสื่อกลางในการซื้อขายสิ่งของผิดกฎหมาย การนำไปใช้ในการชำระเงินค่าจ้างวานให้ผู้อื่นไปกระทำความผิด รวมทั้งการนำบิทคอยน์ไปใช้เป็นสื่อกลางในการแลกเปลี่ยนผลประโยชน์กันระหว่างผู้กระทำความผิดในรูปแบบต่างๆ ดังนี้

3.2.1.1 การลักลอบซื้อขายยาเสพติดโดยการชำระเงินด้วยบิทคอยน์

การลักลอบซื้อขายยาเสพติดมีประวัติศาสตร์มาอย่างยาวนานและถือเป็นประเด็นปัญหาหลักที่ทุกประเทศทั่วโลกให้ความสำคัญมาโดยตลอด แต่สาเหตุหนึ่งที่ทำให้ปัญหาการลักลอบซื้อขายยาเสพติดยังไม่หมดไปคือ ผู้กระทำผิดได้มีการพัฒนา วิวัฒนาการ และมีความพยายามในการแสวงหาวิธีการกระทำผิดใหม่ๆ เพื่อหลบเลี่ยงกระบวนของรัฐอยู่เสมอ ในสังคมปัจจุบันที่มีการใช้เทคโนโลยีสมัยใหม่อย่างแพร่หลาย **บิทคอยน์จึงกลายเป็นเครื่องมือชั้นดีของผู้กระทำผิดที่จะนำมาใช้ในชำระค่ายาเสพติดแทนสกุลเงินจริง** เพราะจากเดิมนั้นการใช้สกุลเงินจริง ไม่ว่าจะเป็นเงินสดหรือแม้กระทั่งการโอนเงินเข้าบัญชีของกลุ่มขบวนการลักลอบค้ายาเสพติด จะทำให้เจ้าหน้าที่ของรัฐสามารถตรวจสอบเส้นทางการเงินได้ ถึงแม้จะใช้ตัวแทนเชิด หรือ นอมินี ในการรับเงิน ส่งเงิน หรือแม้จะมีการจ้างให้ผู้ที่ไม่เกี่ยวข้องมาเปิดบัญชีธนาคารให้ก็ตาม แต่เจ้าหน้าที่ของรัฐก็สามารถตรวจสอบเส้นทางการเงินและสืบสวนสอบสวนจนสามารถพบตัวกลุ่มผู้กระทำผิดที่แท้จริงได้ในที่สุด แต่ในกรณีของการใช้บิทคอยน์ในการซื้อขายยาเสพติดแล้ว จะสร้างปัญหาให้เจ้าหน้าที่ของรัฐเป็นอย่างมาก เนื่องจากไม่สามารถระบุตัวตนของเจ้าของบัญชีได้ แม้จะสามารถติดตามเส้นทางการเงินทางอิเล็กทรอนิกส์ของบิทคอยน์จนทราบเลขที่บัญชีที่ต้องสงสัยแล้วก็ตาม ดังตัวอย่างเหตุการณ์ที่

เกิดขึ้นในประเทศออสเตรเลีย เมื่อวันที่ 13 เมษายน 2561 ที่ผ่านมากองกำลังรักษาเขตแดน หรือ Australian Border Force (ABF) ได้ออกมาเปิดเผยว่า ได้บูรณาการกำลังร่วมกับสำนักงานตำรวจแห่งชาติออสเตรเลีย หรือ Australian Federal Police (AFP) ร่วมกันจับกุมตัวผู้ต้องหาหญิงซึ่งได้ทำการสั่งซื้อยาเสพติดผ่านเว็บไซต์ใต้ดินหรือ ดาร์คเว็บ (Dark web) **โดยมีการชำระเงินค่ายาเสพติดด้วยบิทคอยน์** ใช้การจัดส่งยาเสพติดผ่านทางเรือมาจากสหราชอาณาจักร (United Kingdoms) โดยประเภทของยาเสพติดที่ตรวจยึดได้ได้แก่ MDMA หรือที่รู้จักว่า เอ็กซ์ตาซี (Ecstacy) รวมทั้งยาเสพติดประเภทที่เป็นกลุ่มโอปิออยด์ (The Opioids Oxycodone and Fentanyl) ที่มีความเข้มข้นกว่ายาเสพติดปกติถึง 50 – 100 เท่า ซึ่งทำให้ผู้เสพยาเสพติดประเภทนี้มักจะไม่สามารถควบคุมปริมาณการเสพได้ โดยในกรณีของการจับกุมครั้งนี้นั้น เจ้าหน้าที่สืบทราบมาจากการใช้งานเว็บไซต์ใต้ดินและได้สืบทราบเส้นทางการนำเข้าทางเรือ จึงได้ร่วมกันขอออกหมายค้นและหมายจับและทำการจับกุมตัวและยึดของกลางดังกล่าว (Australian Federal Police [AFP] , 2018)

อย่างไรก็ตามแม้จะมีการกล่าวอ้างของกองกำลังรักษาเขตแดนและเจ้าหน้าที่ตำรวจของประเทศออสเตรเลียว่า สามารถติดตามสืบสวนจับกุมการกระทำผิดที่มีการใช้สกุลเงินดิจิทัล (Cryptocurrency) ได้อันเกิดมาจากความร่วมมือกันระหว่างหน่วยงานก็ตาม แต่ก็ยังเป็นการติดตามสืบสวนจับกุมจากช่องทางอื่น ซึ่งไม่ใช่การติดตามจากเส้นทางการเงินหรือการทำธุรกรรมบิทคอยน์โดยตรง ซึ่งมีผู้กระทำผิดหรือผู้ลักลอบซื้อขายยาเสพติดอีกเป็นจำนวนมากที่ไม่ได้ติดต่อซื้อขายกันผ่านทางเว็บไซต์ใต้ดิน ซึ่งถ้าเป็นกรณีดังกล่าวนี้จะแทบจะเป็นไปไม่ได้เลยที่เจ้าหน้าที่ของรัฐจะตรวจสอบจนพบตัวผู้กระทำผิด

ในขณะเดียวกันในประเทศไทยปัญหาเกี่ยวกับการใช้บิทคอย์ในการลักลอบซื้อขายยาเสพติดได้เป็นที่สนใจของสำนักงานป้องกันและปราบปรามยาเสพติด (ป.ป.ส.) เช่นกัน โดยในการประชุมเชิงปฏิบัติการเครือข่ายข้อมูลเฝ้าระวังยาเสพติดอาเซียน ครั้งที่ 5 ระหว่างวันที่ 7 - 9 มีนาคม 2561 ที่ผ่านมานั้น นายชลัยสิน โพธิเจริญ รองเลขาธิการป.ป.ส. ได้กล่าวถึงประเด็นปัญหานี้ว่า (บุญชัย ธนะไพรินทร์, 2561)

> *“เริ่มมีข่าวการเชื่อมโยงบิทคอยน์ กับพฤติกรรมที่น่าสงสัย เช่น การใช้บิทคอยน์ซื้อยาเสพติดในตลาดมืด รวมทั้งมีการซื้อขายยาเสพติดผ่านทางออนไลน์และการขนส่งยาเสพติดผ่านบริษัทขนส่งเอกชน ของไทย สิงคโปร์ และเกาหลีใต้ เป็นต้น จึงควรเริ่มมีการเฝ้าระวังในภูมิภาคอาเซียน"*

จากคำกล่าวดังกล่าวของผู้บริหารระดับสูงของสำนักงานป้องกันและปราบปรามยาเสพติด (ป.ป.ส.) ทำให้ตระหนักได้ว่า ขบวนการลักลอบค้ายาเสพติดกำลังก้าวเข้าสู่วิวัฒนาการใหม่ในการลักลอบซื้อขายยาเสพติดโดยใช้นวัตกรรมสมัยใหม่อย่างบิทคอยน์เป็นเครื่องมือ ซึ่งจะสามารถสร้างปัญหาให้กับหน่วยงานของรัฐที่มีหน้าที่เกี่ยวข้องในการป้องกันปราบปรามยาเสพติดทั้งในประเทศไทยและทุกประเทศทั่วโลกเป็นอย่างมาก

3.2.1.2 ซื้อขายอาวุธเถื่อนโดยการชำระเงินด้วยบิทคอยน์

การลักลอบซื้อขายอาวุธเถื่อน เป็นกิจกรรมที่เกิดขึ้นอยู่เสมอในกลุ่มอาชญากร การลักลอบซื้อขายอาวุธเถื่อนในอดีต จะต้องอาศัยความรู้จักคุ้นเคยกับ “คนกลาง” ที่จะสามารถจัดหาอาวุธมาให้กับอาชญากรได้ โดย “คนกลาง” ดังกล่าวก็จะต้องแบกรับความเสี่ยงที่จะถูกสืบสวนจับกุมและอาจจะถูกตรวจสอบเส้นทางการเงินไปจนพบเจ้าของผู้รับมอบอาวุธต่อไปก็เป็นได้ แต่ในปัจจุบันอาชญากรได้สร้าง ดาร์คเว็บ (Dark web) หรือ เว็บไซต์ใต้ดินที่เป็นจุดศูนย์รวมของการแลกเปลี่ยนสินค้าผิดกฎหมายโดยเฉพาะอาวุธเถื่อน เป็นโครงข่ายที่อาชญากรสามารถติดต่อซื้อขายกันได้โดยตรง แต่ถึงอย่างไรก็ซื้อขายอาวุธเถื่อนผ่านดาร์คเว็บเหล่านี้ ก็ยังจำเป็นจะต้องชำระเงินค่าสิ่งของกันเป็นเงินสกุลจริงผ่านการโอนเงินด้วยวิธีต่างๆ ซึ่งยังคงมีความเสี่ยงที่เจ้าหน้าที่ของรัฐจะสามารถติดตามเส้นทางการเงินของกลุ่มผู้กระทำผิดได้ไม่มากก็น้อยอยู่เช่นเดิม

แต่ภายหลังจากที่บิทคอยน์เริ่มเป็นที่แพร่หลาย อาชญากรก็ได้เล็งเห็นประโยชน์ของสกุลเงินเข้ารหัสชนิดนี้ และนำมาใช้ในการชำระเงินเพื่อซื้อขายแลกเปลี่ยนอาวุธเถื่อนกัน ดังตัวอย่างเหตุการณ์ที่เกิดขึ้นในประเทศสหรัฐอเมริกา ที่มีการจับกุมตัวนายเบนจามิน เจมส์ แคนซ์ (Benjamin James Cance) ในข้อหา “ลักลอบขายและจัดส่งอาวุธผิดกฎหมายผ่านทางเรือและฟอกเงิน” โดยจากข้อมูลการสืบสวนพบว่า นายเบนจามินได้รับการสั่งซื้ออาวุธปืนเถื่อนผ่านทางดาร์คเว็บ และ**ได้มีการให้ผู้ซื้อชำระค่าอาวุธปืนดังกล่าวด้วยบิทคอยน์** เพื่อต้องการหลีกเลี่ยงไม่ให้เจ้าหน้าที่ตรวจสอบความเคลื่อนไหวทางการเงิน โดยเจ้าหน้าที่ตำรวจได้เปิดเผยว่า สามารถสืบสวนคดีดังกล่าวนี้ได้เนื่องจากพบว่า นายเบนจามินมีการฟอกเงินผ่านการซื้อบ้านจึงทำให้เจ้าหน้าที่พบความผิดปกติจากการครอบครองเงินเป็นจำนวนมาก (*Illegal Weapons Dealer Used Bitcoin for Transaction,* 2015)

นอกจากนี้ยังมีการรายงานข่าวว่าในประเทศสก็อตแลนด์ก็ได้เกิดการกระทำผิดในรูปแบบนี้เช่นกัน โดยจากการรายงานของเว็บไซต์ซีซีเอ็น (www.ccn.com) ว่า นายเดวิด มิทเชล

(David Mitchell) อายุ 43 ปี ได้ถูกศาลพิพากษาลงโทษจำคุกเป็นเวลา 5 ปี จากการกระทำความผิดที่นายเดวิดได้สั่งซื้ออาวุธปืนขนาด 9 มม. พร้อมด้วยลูกกระสุนปืนกว่า 150 นัด โดยชำระเงินด้วยบิทคอยน์ผ่านทางเว็บไซต์ใต้ดินหรือดาร์คเว็บ และสั่งให้ผู้ขายทำการจัดส่งอาวุธปืนและเครื่องกระสุนปืนเถื่อนดังกล่าวทางเรือโดยมีต้นทางจากประเทศสหรัฐอเมริกามาส่งยังปลายทางที่ประเทศสก็อตแลนด์ แต่ถูกเจ้าหน้าที่ร่วมกันสืบสวนและจับกุมตัวได้ก่อน ตามรายงานดังกล่าวระบุว่าการสั่งซื้ออาวุธปืนดังกล่าว **นายเดวิดได้ใช้บิทคอยน์จำนวน 0.74 เหรียญบิทคอยน์ (0.74 BTC) คิดเป็นเงินจำนวน 2,750 เหรียญสหรัฐ หรือราว 85,000 บาท ชำระเป็นค่าอาวุธและค่าขนส่งอาวุธปืนเถื่อน**ดังกล่าว (David Hundeyin, 2019) โดยในรายงานดังกล่าวไม่ได้กล่าวถึงว่าเจ้าหน้าที่ของรัฐสืบทราบการกระทำผิดจากข้อมูลใด

จากกรณีตัวอย่างดังกล่าวทำให้ผู้ศึกษาเชื่อว่า ในปัจจุบันยังมีการลักลอบซื้อขายอาวุธเถื่อนข้ามประเทศโดยใช้บิทคอยน์เป็นเครื่องมืออีกเป็นจำนวนมากทั่วโลก ทั้งนี้การสืบสวนปราบปรามจับกุมยังจำเป็นจะต้องอาศัยข้อมูลแวดล้อมต่างๆประกอบจึงจะทำให้สามารถจับกุมผู้กระทำผิดในลักษณะนี้ได้ แต่หากเจ้าหน้าที่ของรัฐมีเพียงข้อมูลทางธุรกรรมของบิทคอยน์เพียงเท่านั้นก็จะทำให้เกิดความยากลำบากเพราะยังไม่สามารถยืนยันตัวบุคคลเจ้าของบัญชีบิทคอยน์ได้

3.2.1.3 การว่าจ้างผู้อื่นให้กระทำผิดกฎหมาย โดยชำระค่าจ้างด้วยบิทคอยน์

ได้มีการรายงานว่า หญิงสาวผู้หนึ่งได้มีการจ้างวานผ่านเว็บไซต์ใต้ดิน (Dark Web) ให้คนร้ายไปสังหารภรรยาของชายชู้ที่เธอมีความสัมพันธ์อยู่ด้วย โดยมีการตกลงจ่ายค่าจ้างกันเป็นบิทคอยน์คิดเป็นเงินค่าจ้างกว่า หนึ่งหมื่นเหรียญสหรัฐ โดยเว็บไซต์สื่อมวลชนท้องถิ่นของเมืองชิคาโก คือ ชิคาโก ซัน ไทม์ (Chicago Sun Times) ได้เผยแพร่เนื้อหาของเหตุการณ์ดังกล่าว เมื่อวันที่ 18 เมษายน 2561 ว่า นางสาวทีน่า โจนส์ (Tina Jones) วัย 31 ปี ถูกจับกุมในข้อหาจ้างวานฆ่าโดยเจ้าหน้าที่ตำรวจได้รับเบาะแสว่า ทีน่า จ่ายเงินค่าจ้างให้คนร้ายไปสังหารหญิงสาวผู้หนึ่งในเมืองวู้ดริจก์ (Woodridge) เมื่อประมาณเดือน มกราคม 2561 โดยเธอได้เข้าไปใน**เว็บไซต์ใต้ดินที่มีผู้รับจ้างกระทำผิดกฎหมายต่างๆ และรับค่าจ้างเป็นบิทคอยน์** เนื่องจากเป็นการปกปิดตัวตนที่แท้จริงได้ดีที่สุด โดยเมื่อมีการโอนจ่ายบิทคอยน์กันแล้ว ก็จะไม่มีผู้ใดล่วงรู้เส้นทางการเงิน หรือแม้กระทั่งผู้ที่ติดต่อจ้างวานกันก็แทบจะไม่รู้จักตัวตนที่แท้จริงของกันและกัน และประเด็นปัญหาด้านการปกปิดตัวตนของอาชญากรนี้ทำให้บิทคอยน์เป็นที่นิยมเป็นอย่างมากในการใช้ชำระค่าจ้างต่าง ๆ ในการ

กระทำผิดกฎหมายของอาชญากร (Luke Wilusz, 2018) อีกเหตุการณ์หนึ่งที่มีลักษณะคล้ายกันเกิดขึ้นในประเทศเดนมาร์ก จากการเปิดเผยของเว็บไซต์คอยน์เทเลกราฟ (www.cointelegraph.com) เมื่อวันที่ 16 ธันวาคม 2560 ว่า หญิงชาวอิตาเลียนถูกศาลตัดสินจำคุก 6 ปี ในข้อหา**จ้างวานฆ่าแฟนเก่าของตนเอง โดยชำระเงินค่าจ้างเป็นบิทคอยน์จำนวน 4.1 บิทคอยน์** ซึ่งคิดเป็นเงินกว่า 4,000 เหรียญสหรัฐ หรือประมาณ 120,000 บาท (Jon Buck, 2017)

จากตัวอย่างที่ยกมานี้จะเห็นได้ว่าบิทคอยน์ถูกนำไปใช้เป็นสื่อกลางโดยผู้กระทำผิดและอาชญากรต่างๆได้นำบิทคอยน์ไปใช้ในการชำระเงินค่าจ้างแทนสกุลเงินจริงเพื่อแลกกับผลประโยชน์ในทางที่ผิดกฎหมาย เพื่อหลีกเลี่ยงการถูกตรวจสอบและสืบสวนจับกุมจากเจ้าหน้าที่ของรัฐ

3.2.1.4 การใช้บิทคอยน์เพื่อการซื้อขายสื่อลามกอนาจาร

การกระทำผิดในลักษณะของการเข้าถึงและเผยแพร่สื่อลามกอนาจารทั้งรูปแบบของภาพนิ่งและภาพเคลื่อนไหวในปัจจุบันสามารถทำได้ง่ายกว่าในอดีต เนื่องจากระบบเทคโนโลยีสารสนเทศและการสื่อสารมีความก้าวหน้าไปมาก ไม่ว่าจะเป็นการเกิดขึ้นของระบบอินเทอร์เน็ต รวมทั้งการพัฒนาของอุปกรณ์คอมพิวเตอร์และโทรศัพท์มือถือสมาร์ทโฟนแบบต่างๆ ส่งผลทำให้ปัญหาด้านสื่อลามกอนาจารแพร่ไปอย่างรวดเร็ว ถึงแม้ในปัจจุบันจะมีหน่วยงานต่างๆของรัฐเข้ามาควบคุม สอดส่องดูแล และป้องกันปราบปรามการกระทำผิดลักษณะนี้ แต่ก็ยังปรากฏว่ายังมีการลักลอบเข้าถึงและเผยแพร่สื่อลามกอนาจารอยู่เป็นจำนวนมาก

ในหลายประเทศทั่วโลกการครอบครองหรือเข้าถึงสื่อลามกอนาจารโดยเฉพาะอย่างยิ่งสื่อลามกอนาจารเกี่ยวกับเด็กเป็นสิ่งผิดกฎหมาย ดังนั้น ผู้กระทำผิดจึงพยายามแสวงหาช่องทางหรือวิธีการที่สามารถครอบครองหรือเข้าถึงสื่อลามกอนาจารได้โดยไม่ถูกตรวจสอบจากเจ้าหน้าที่ของรัฐ ดังนั้น การใช้บิทคอยน์เพื่อเข้าถึงสื่อลามกอนาจารจึงเป็นทางเลือกที่ผู้กระทำผิดเหล่านี้เลือกใช้ โดยข้อมูลจากเว็บไซต์คอยน์เนาซ์ (www.coinnounce.com) ระบุว่า เว็บไซต์ชื่อดังที่เผยแพร่สื่อลามกอนาจาร จำนวน 6 เว็บไซต์ได้แก่ Naughty America , Pornhub , Chaturbate , Livejasmin , Playboy Plus และ Xotika ได้ประกาศยอมรับให้**ผู้ที่ต้องการจะเข้าถึงสื่อลามกอนาจาร สามารถซื้อสิทธิ์การเข้าถึงข้อมูลด้วยการชำระเงินเป็นบิทคอยน์**ได้แล้ว โดยการนำบิทคอยน์มาใช้ในการกระทำผิดลักษณะนี้เกิดจากแนวคิดว่า จากเดิมที่ผู้ที่ต้องการจะเข้าถึงข้อมูลสื่อลามกอนาจารต่างๆเหล่านี้ต้องการจะเข้าชมภาพหรือภาพเคลื่อนไหวภายในเว็บไซต์ก็จะต้องชำระเงินด้วยการโอนเงินหรือการชำระด้วยบัตรเครดิต ซึ่งนอกจากจะทำให้เกิดความอับอาย เมื่อหลักฐานการชำระเงินจาก

ทางธนาคารปรากฏรายละเอียดการเข้าถึงสื่อลามกอนาจารดังกล่าวแล้ว ยังทำให้ผู้ที่เข้าถึงสื่อลามกอาจถูกตรวจสอบเส้นทางการเงินจนทราบตัวตนและถูกตั้งข้อสงสัยว่าจะครอบครองสื่อลามกอนาจารได้ ดังนั้น เพื่อหลีกเลี่ยงปัญหาดังกล่าวการนำบิทคอนย์ที่มีจุดเด่นที่ไม่สามารถระบุตัวตนผู้ใช้งานได้จึงเป็นช่องทางที่เกิดประโยชน์ต่อการเผยแพร่และเข้าถึงสื่อลามกอนาจารในปัจจุบันเป็นอย่างมาก (Coinnounce, 2018)

ในมุมมองของผู้ศึกษาเชื่อว่า ในอนาคตจะมีการซื้อขายหรือใช้บิทคอยน์ในการเข้าถึงสื่อลามกอนาจารบนโลกออนไลน์นี้เป็นจำนวนมากขึ้นเรื่อยๆ ซึ่งจะส่งผลทำให้ปัญหาอาชญากรรมที่เกี่ยวกับสื่อลามกอนาจารจะทวีความรุนแรงมากยิ่งขึ้น

3.2.1.5 การเรียกค่าไถ่

นอกจากบิทคอยน์จะถูกนำไปใช้เป็นสื่อกลางในการซื้อขายแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมายแล้ว บิทคอยน์ยังถูกนำมาใช้แทนสกุลเงินจริงในการเรียกค่าไถ่ของอาชญากรอีกด้วย โดยการเรียกค่าไถ่แบบดั้งเดิมนั้น หากมีการเรียกร้องให้ชำระเงินค่าไถ่เป็นเงินสด ก็จำเป็นจะต้องมีการนัดหมายเวลาและสถานที่ในการส่งมอบเงินซึ่งมีโอกาสสูงที่จะถูกเจ้าหน้าที่ของรัฐพบตัวหรือติดตามไปจนพบที่ซ่อนตัวได้ หรือในกรณีของการโอนเงินค่าไถ่ อาชญากรก็จะต้องเสี่ยงจากการติดตามกระแสการเงินของเจ้าหน้าที่ของรัฐซึ่งจะสามารถตรวจสอบไปจนถึงตัวการผู้กระทำผิดได้ ดังนั้นหลังจากที่มีการสร้างบิทคอยน์ขึ้นอาชญากรได้มองเห็นประโยชน์จากลักษณะพิเศษของบิทคอยน์ที่ไม่สามารถติดตามตรวจสอบกระแสทางการเงินของบิทคอยน์เพื่อระบุตัวตนเจ้าของบัญชีได้ จนเกิดเป็นการเรียกค่าไถ่แบบใหม่ที่เรียกร้องให้มีการชำระค่าไถ่เป็นบิทคอยน์เพื่อหลีกเลี่ยงโอกาสที่อาจจะถูกตรวจสอบจากเจ้าหน้าที่ของรัฐได้ ดังตัวอย่างที่เกิดขึ้นจริงที่สำนักข่าว เดอะการ์ดเดี้ยน (The Guardian) ได้เผยแพร่รายละเอียดเกี่ยวกับเหตุการณ์ที่มีกลุ่มคนร้ายลักพาตัวเด็กอายุ 13 ปี ไป ขณะที่เด็กคนนั้นกำลังเล่นอยู่กับเพื่อนอีกสองคนที่สนามเด็กเล่นในย่านวิทแบงค์ (Witbank) เมืองพูมาลังกา (Mpumalanga) ประเทศแอฟริกาใต้ โดยพยานที่เห็นเหตุการณ์เล่าว่า มีกลุ่มคนร้ายทำการลักพาตัวและจับเด็กคนดังกล่าวเข้าไปในรถยี่ห้อ โตโยต้า แล้วก็ขับหลบหนีไป โดยกลุ่มคนร้ายได้ทิ้งกระดาษโน๊ตไว้ในที่เกิดเหตุก่อนจะหลบหนีไปโดยระบุข้อความให้พ่อแม่ของเด็กผู้เคราะห์ร้าย **จะต้องจ่ายค่าไถ่เป็นบิทคอยน์เป็นจำนวน 15 เหรียญบิทคอยน์ หรือคิดเป็นเงินกว่า 123,000 เหรียญสหรัฐ** ซึ่งเหตุการณ์ที่เกิดขึ้นนี้ ถือเป็นครั้งแรกที่มีการเรียกค่าไถ่เป็นสกุลเงินอิเล็กทรอนิกส์เกิดขึ้นในประเทศแอฟริกาใต้ (Jason Burke, 2018)

เหตุการณ์เช่นเดียวกันนี้เคยเกิดขึ้นในประเทศยูเครน โดยสำนักข่าวรอยเตอร์ (Reuters) ได้เผยแพร่ว่าเมื่อวันที่ 26 ธันวาคม 2560 กลุ่มคนร้ายติดอาวุธจำนวน 6 คน ได้ทำการลักพาตัว นายพาเวล เลอเนอร์ (Pavel Lerner) หัวหน้านักวิเคราะห์ทางการเงินและผู้เชี่ยวชาญระบบบล็อคเชนของบริษัทชื่อดังทางด้านการเงินแห่งหนึ่งของประเทศยูเครน โดยคนร้ายได้จับตัวนายพาเวลขึ้นไปบนรถบัสขนาดเล็กแล้วเรียกร้องให้มีการจ่ายค่าไถ่เป็นบิทคอยน์ ซึ่งต่อมา**กลุ่มคนร้ายได้ปล่อยตัวประกันออกมาภายหลังจากที่ได้รับค่าไถ่เป็นบิทคอยน์ไปแล้วคิดเป็นมูลค่ากว่าหนึ่งล้านเหรียญสหรัฐ** (Pavel Polityuk, 2017) จากตัวอย่างที่ได้กล่าวมาแล้วทำให้สามารถคาดการณ์ได้ในเบื้องต้นว่า ในอนาคตกลุ่มอาชญากรที่ทำการลักพาตัวเพื่อเรียกค่าไถ่น่าจะมีการเรียกร้องให้จ่ายเงินค่าไถ่เป็นบิทคอยน์มากยิ่งขึ้น

นอกจากการเรียกค่าไถ่ในแบบดั้งเดิมแล้ว ในสภาวะสังคมโลกปัจจุบันอุปกรณ์อิเล็กทรอนิกส์โดยเฉพาะอย่างยิ่งเครื่องคอมพิวเตอร์นั้น ถือเป็นอุปกรณ์สำคัญที่มนุษย์ใช้ในการทำงานและเก็บข้อมูลสำคัญต่างๆ จนทำให้อาชญากรอาศัยความต้องการใช้เครื่องคอมพิวเตอร์และข้อมูลต่างๆ ประกอบกับการใช้ความเชี่ยวชาญทางด้านการเขียนโปรแกรมคอมพิวเตอร์มาใช้ในการเรียกค่าไถ่ด้วยรูปแบบใหม่โดยการสร้าง**โปรแกรมสำหรับเรียกค่าไถ่ (Ransomware)** ขึ้น โดยโปรแกรมชนิดนี้จะถูกปล่อยหรือทำให้ระบาดในลักษณะเดียวกันกับไวรัสคอมพิวเตอร์ (Virus) เพื่อให้ตัวโปรแกรมลักลอบเข้าไปติดตั้งอยู่ในเครื่องคอมพิวเตอร์ของเหยื่อ และเมื่อโปรแกรมดังกล่าวได้เข้าสู่ระบบแล้ว จะทำการนำข้อมูลทั้งหมดที่อยู่ภายในเครื่องของเหยื่อ ไปเข้ารหัสลับและทำการปิดกั้นข้อมูลไว้ ทำให้เหยื่อไม่สามารถเข้าถึงข้อมูลของตนเองได้ ส่งผลให้เกิดความเสียหาย หลังจากนั้นคนร้ายจะทำการเรียกค่าไถ่ให้ชำระด้วยวิธีต่างๆ โดยหากเหยื่อยอมชำระค่าไถ่ตามที่ต้องการ คนร้ายจะให้รหัสหรือวิธีในการแก้ไขเพื่อยกเลิกโปรแกรมดังกล่าว แต่หากเหยื่อไม่ยินยอมจ่ายค่าไถ่หรือไม่จ่ายค่าไถ่ภายในเวลาที่กำหนด คนร้ายก็จะทำการข่มขู่ว่าจะลบข้อมูลทั้งหมดในเครื่องคอมพิวเตอร์ของเหยื่อ จนทำให้ในท้ายที่สุดผู้ที่ตกเป็นเหยื่อส่วนใหญ่ก็จะยินยอมเสียค่าไถ่ เพื่อไม่ให้เกิดความเสียหายต่อข้อมูลสำคัญต่างๆที่อยู่ภายในเครื่องคอมพิวเตอร์

ในช่วงแรกที่คนร้ายใช้โปรแกรมเรียกค่าไถ่ดังกล่าว การจ่ายค่าไถ่จะอยู่ในรูปแบบของการโอนเงินผ่านบัญชีธนาคาร ซึ่งมีความเสี่ยงจากการติดตามกระแสการเงินของเจ้าหน้าที่รัฐซึ่งจะสามารถตรวจสอบไปจนถึงตัวการผู้กระทำผิดได้ แต่หลังจากที่บิทคอยน์ได้ถูกใช้งานอย่างแพร่หลายแล้ว ก็ปรากฏว่า**มีการใช้โปรแกรมเรียกค่าไถ่นี้บังคับให้เหยื่อชำระค่าไถ่เป็นบิทคอยน์** เพื่อประโยชน์

ในการปกปิดตัวตนของผู้กระทำผิดและเพื่อให้เกิดความยากลำบากในการติดตามเส้นทางการเงินที่ได้รับเป็นค่าไถ่ดังกล่าว โดยหนึ่งในโปรแกรมเรียกค่าไถ่ที่ระบาดไปทั่วโลก และสร้างความเสียหายเป็นจำนวนมูลค่ามหาศาลจนกลายเป็นที่รู้จักโปรแกรมหนึ่งคือ **“WannaCry”** (กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม, 2560) โดยโปรแกรมเรียกค่าไถ่ดังกล่าวได้เริ่มระบาดทางระบบเครือข่ายคอมพิวเตอร์ในช่วงเดือนพฤษภาคม พ.ศ.2560 ผ่านช่องโหว่ของระบบปฏิบัติการไมโครซอฟท์วินโดวส์ (Microsoft Windows) ที่มีการใช้กันอย่างแพร่หลาย จนทำให้เครื่องคอมพิวเตอร์ที่ถูกโปรแกรมนี้โจมตีไม่สามารถใช้งานได้ **โดยคนร้ายได้กำหนดให้เหยื่อชำระค่าไถ่เป็นบิทคอยน์ จำนวน 300 เหรียญสหรัฐ (ต่อ 1 เครื่องคอมพิวเตอร์)** พร้อมกำหนดระยะเวลานับถอยหลังเพื่อเป็นการข่มขู่และบีบบังคับให้ต้องยอมจ่ายค่าไถ่ให้กับคนร้าย

โดยโปรแกรม Wannacry นี้ ได้แพร่ระบาดไปสู่เครื่องคอมพิวเตอร์กว่า 100,000 เครื่อง ใน 150 ประเทศทั่วโลก ซึ่งเป็นเครื่องคอมพิวเตอร์ทั้งของหน่วยงานของรัฐ สถานประกอบการ โรงพยาบาล รวมทั้งภาคเอกชนและภาคธุรกิจต่างๆ จนทำให้มีการประเมินมูลค่าความเสียหายที่เกิดจากการเรียกค่าไถ่เป็นบิทคอยน์ด้วยโปรแกรม Wannacry นี้ไว้สูงถึง 4,000 พันล้านเหรียญสหรัฐ (Jonathan Berr , 2017) แม้ในเวลาต่อมาจะมีผู้เชี่ยวชาญทางด้านโปรแกรมคอมพิวเตอร์ สามารถหยุดยั้งการทำงานของโปรแกรมดังกล่าวนี้ไว้ได้ก็ตาม แต่ผลกระทบจากเหตุการณ์นี้ก็ส่งผลทำให้เกิดพฤติกรรมเลียนแบบและทำให้มีการสร้างโปรแกรมเรียกค่าไถ่เป็นบิทคอยน์หรือสกุลเงินเข้ารหัสสกุลอื่นๆในลักษณะเดียวกันนี้เกิดขึ้นตามมาอีกเป็นจำนวนมาก

จะเห็นได้ว่าการเรียกค่าไถ่ทั้งในแบบดั้งเดิมและแบบที่ใช้โปรแกรมเรียกค่าไถ่ (Ransomware) ตามที่ได้กล่าวมาข้างต้น มีการพัฒนาเปลี่ยนแปลงลักษณะการกระทำความผิดโดยการที่อาชญากรได้นำบิทคอยน์มาใช้เป็นช่องทางหรือวิธีการในการเรียกค่าไถ่ เพื่อให้มีโอกาสรอดพ้นจากการตรวจสอบเส้นทางการเงินจากเจ้าหน้าที่ของรัฐมากยิ่งขึ้น

3.2.1.6 การระดมเงินทุนของกลุ่มผู้ก่อการร้ายด้วยบิทคอยน์

ถึงแม้การก่อวินาศกรรมหรือการสร้างสถานการณ์ความรุนแรงของกลุ่มผู้ก่อการร้ายกลุ่มต่างๆทั่วโลก จะมีวัตถุประสงค์หรือข้อเรียกร้องอันเป็นต้นเหตุของการก่อการร้ายที่แตกต่างกัน มีลักษณะและวิธีการในการก่อเหตุแตกต่างกัน แต่ปัจจัยสำคัญที่กลุ่มผู้ก่อการร้ายกลุ่มต่างๆ จำเป็นจะต้องใช้เหมือนกันทุกกลุ่มก็คือ **“เงินทุน”** เนื่องจากในการก่อเหตุแต่ละครั้งจำเป็นจะต้องใช้เงินทุนไม่ว่าจะเป็นการจัดหาอาวุธยุทโธปกรณ์ต่างๆ การจ่ายเงินเป็นค่าตอบแทนหรือค่าเหนื่อยให้กับผู้ก่อ

เหตุ การติดสินบนเจ้าหน้าที่ของรัฐ ตลอดจนการใช้จ่ายเพื่อการบริหารภายในกลุ่มผู้ก่อการร้าย ดังนั้น จึงอาจกล่าวได้ว่าการก่อการร้ายจะสำเร็จหรือไม่นั้นขึ้นอยู่กับเงินทุนเป็นสำคัญด้วย

การหาเงินทุนของกลุ่มผู้ก่อการร้ายกระทำด้วยกันหลายวิธี เช่น กรณีของกลุ่มไอเอส (IS) จะใช้วิธีการลักพาตัวเพื่อเรียกค่าไถ่ การขู่กรรโชกทรัพย์ การปล้นธนาคารและร้านค้าทอง การค้าของเถื่อน นอกจากนี้ในส่วนของเงินสนับสนุนเพิ่มเติมจะอยู่ในรูปแบบของการบริจาค ไม่ว่าจะเป็นการบริจาคอย่างเปิดเผยของผู้ที่มีแนวคิดอุดมการณ์ตรงกันกับกลุ่มผู้ก่อการร้าย หรือเป็นการบริจาคแบบไม่เปิดเผยจากบุคคลต่างๆ รวมทั้งยังมีการกล่าวหาว่ามีบริจาคสนับสนุนในทางลับจากรัฐบาลของประเทศที่ได้ประโยชน์จากการก่อการร้ายแม้จะไม่มีหลักฐานยืนยันอย่างชัดเจนก็ตาม (ยอดชาย วิถีพานิช, 2558)

การระดมทุนด้วยการบริจาคนั้นหากเป็นการบริจาคด้วยสกุลเงินจริง จะทำให้สามารถสืบสวนติดตามเส้นทางการเงินจนพบตัวผู้สนับสนุนกลุ่มผู้ก่อการร้ายได้ในที่สุด ดังนั้นจึงมีการนำบิทคอยน์มาใช้ในการรับบริจาคหรือระดมทุนให้กับกลุ่มผู้ก่อการร้ายต่างๆ ดังที่ปรากฏในการรายงานของสำนักข่าวรอยเตอร์ว่า กลุ่มกบฏฮามาสได้พัฒนากลยุทธ์ในการระดมเงินทุนด้วยการยกระดับวิธีการบริจาคจากเดิมมาเป็นบิทคอยน์ด้วยการสร้างกระเป๋าเงินดิจิทัล (Digital Wallet) เพื่อให้สะดวกต่อการระดมทุนจากทั่วทุกมุมโลกทำให้เกิดความรวดเร็วในการรวบรวมเงินทุน อีกทั้งยังเป็นการหลบเลี่ยงการถูกตรวจสอบของหน่วยงานด้านความมั่นคงและหน่วยข่าวกรองต่างๆได้เป็นอย่างดี นอกจากนี้ข้อมูลจากการวิจัยของบริษัท เอลลิปทิค จำกัด (Elliptic Co.) ซึ่งเป็นบริษัทที่ทำงานเกี่ยวกับการค้นคว้าและวิจัยเพื่อป้องกันการใช้งานสกุลเงินเข้ารหัสโดยมิชอบ ซึ่งมีที่ทำการอยู่ในประเทศอังกฤษและประเทศสหรัฐอเมริกา ได้เปิดผลการศึกษาว่า ตั้งแต่วันที่ 26 มีนาคม – 16 เมษายน 2562 มีบิทคอยน์จำนวนกว่า 0.6 บิทคอยน์ คิดเป็นมูลค่าประมาณ 3,300 เหรียญสหรัฐ หรือคิดเป็นเงินจำนวนกว่า 100,000 บาท ได้ถูกบริจาคให้แก่กระเป๋าเงินดิจิทัลของกลุ่มผู้ก่อการร้ายนี้ และภายในระยะเวลาสี่เดือนที่กลุ่มผู้ก่อการร้ายทำการระดมทุนจากบิทคอยน์นั้น ได้รับการบริจาคเงินไปแล้วกว่า 7,400 เหรียญสหรัฐ หรือคิดเป็นเงินจำนวน 220,000 บาท (Reuters, 2019)

3.2.1.7 การฟอกเงินผ่านบิทคอยน์

ด้วยสาเหตุที่บิทคอยน์ถูกสร้างให้มีลักษณะคล้ายสกุลเงิน กล่าวคือมีมูลค่าในตนเองและสามารถนำไปใช้ในการแลกเปลี่ยนสินค้าและบริการได้ อีกทั้งยังสามารถเปลี่ยนจากสกุลเงินจริงเป็น

บิทคอยน์และเปลี่ยนจากสกุลเงินบิทคอยน์กลับไปเป็นสกุลเงินต่างๆ ประกอบกับการที่บิทคอยน์มีคุณลักษณะพิเศษคือการปกปิดตัวตนบัญชีผู้ใช้งาน ทำให้บิทคอยน์มีคุณสมบัติที่เหมาะสมกับการฟอกเงินเป็นอย่างยิ่ง เพราะเจ้าหน้าที่ของรัฐที่เกี่ยวข้องกับการตรวจสอบการฟอกเงินจะไม่สามารถตรวจสอบที่มาที่ไปของบิทคอยน์ได้โดยง่าย ดังนั้น บิทคอยน์จึงถือเป็นแหล่งฟอกเงินชั้นดีของเหล่าอาชญากรอีกด้วย ตามที่ปรากฏในรายงานข่าวของเว็บไซต์คอยน์เทเลกราฟ(www.cointelegraph.com) เมื่อวันที่ 24 เมษายน 2562 ว่า เจ้าหน้าที่ตำรวจประเทศบราซิลได้จับกุมตัวผู้ต้องสงสัยกรณีที่มีการฟอกเงินผ่านบิทคอยน์ โดยเจ้าหน้าที่ตำรวจได้สืบทราบว่าผู้ต้องสงสัยมีความเกี่ยวข้องกับขบวนการค้ายาเสพติด จึงได้ทำการตรวจสอบภายในบ้านพักของผู้ต้องสงสัย และพบว่าภายในบ้านนั้นมีการติดตั้งเครื่องคอมพิวเตอร์ที่มีลักษณะเป็นชุดคอมพิวเตอร์ที่มีดัดแปลงพิเศษที่ผู้ต้องสงสัยอ้างว่าเป็นเครื่องคอมพิวเตอร์สำหรับทำการขุดบิทคอยน์ ซึ่งเจ้าหน้าที่ตำรวจบราซิลเชื่อว่าผู้ต้องสงสัยได้ใช้การขุดบิทคอยน์บังหน้าสำหรับการนำผลประโยชน์ที่ได้จากการค้ายาเสพติดมาฟอกเงินด้วยบิทคอยน์ (Ana Alexandre, 2019)

ขณะที่ในประเทศเดนมาร์ค ได้มีการตัดสินลงโทษจำคุกชายชาวเดนมาร์คเป็นเวลา 4 ปี 3 เดือน จากข้อหาที่ได้ทำการฟอกเงินด้วยบิทคอยน์เป็นเงินมูลค่ากว่า 450,000 เหรียญสหรัฐ ซึ่งเงินจำนวนนี้เป็นเงินที่ได้มาจากการกระทำผิดกฎหมายทั้งสิ้น โดยเจ้าหน้าที่ตำรวจได้ทำการสืบสวนทราบว่าผู้ต้องหามีพฤติกรรมเกี่ยวกับการขมขู่กรรโชกทรัพย์และปลอมแปลงบัตรเครดิต จึงได้ขยายผลจนตรวจสอบพบบัญชีการเงินที่มีการใช้สำหรับเรียกรับเงินจากการแบล็คเมล์และการขู่กรรโชกทรัพย์ทางอินเทอร์เน็ต ประกอบกับการได้รับแจ้งเบาะแสว่าผู้ต้องหามีพฤติกรรมการใช้บิทคอยน์เป็นจำนวนมาก จึงสามารถสืบสวนและติดตามจับกุมตัวได้ (Helen Partz, 2019)

วิธีการที่คนร้ายใช้บิทคอยน์ในการฟอกเงินนั้นมีสามารถทำได้โดย การนำเอาเงินที่ได้จากการกระทำผิดไปซื้อหรือแลกเปลี่ยนเป็นบิทคอยน์ จากนั้นก็ทำการโอนย้ายถ่ายเทบิทคอยน์ดังกล่าวไปแยกเก็บไว้หลายบัญชีเพื่อให้เกิดความยุ่งยากซับซ้อนในการตรวจสอบ จากนั้น เมื่อถึงเวลาที่ต้องการก็จะทยอยเปลี่ยนบิทคอยน์กลับไปเป็นสกุลเงินจริงโดยอ้างว่าเป็นเงินกำไรที่ได้จากการเก็งกำไรมูลค่าบิทคอยน์ที่มีความผันผวนอยู่ตลอดเวลา (David Canellis, 2018)

จากตัวอย่างที่ได้กล่าวมานี้ ทำให้เชื่อได้ว่าหากบิทคอยน์ยังคงมีมูลค่าและยังเป็นที่ต้องการในหมู่ผู้ใช้งานและนักลงทุนต่างๆ ตลอดจนยังสามารถนำไปใช้เป็นสื่อกลางในการแลกเปลี่ยน

สินค้าและบริการได้ การฟอกเงินด้วยบิทคอยน์ก็มีความเป็นไปได้ที่จะเกิดขึ้นอย่างต่อเนื่องหากยังไม่มีมาตรการป้องกันการฟอกเงินด้วยสกุลเงินเข้ารหัสโดยเฉพาะอย่างยิ่งบิทคอยน์ที่เหมาะสม

จากการศึกษาการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรงรูปแบบต่างๆตามที่ได้กล่าวมาแล้ว ทำให้เข้าใจได้ว่าสาเหตุสำคัญที่ทำให้บิทคอยน์ถูกนำไปใช้ในกิจกรรมที่ผิดกฎหมายไม่ว่าจะเป็นการใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย การเรียกค่าไถ่เป็นบิทคอยน์ การระดมทุนของกลุ่มผู้ก่อการร้ายไปจนถึงการฟอกเงินด้วยบิทคอยน์นั้น เป็นเพราะ**ลักษณะพิเศษของบิทคอยน์ที่มีการปกปิดตัวตนเจ้าของบัญชี (Anonymity)** การนำบิทคอยน์ไปใช้ในการกระทำความผิดเช่นนี้ ทำให้การตรวจสอบติดตาม การป้องกันปราบปรามและการสืบสวนจับกุมการผู้กระทำผิดโดยเจ้าหน้าที่ของรัฐเป็นไปด้วยความยากลำบาก มีความซับซ้อน ต้องอาศัยความรู้ความเชี่ยวชาญในด้านเทคโนโลยีคอมพิวเตอร์ชั้นสูง ส่งผลทำให้อาชญากรหรือผู้กระทำผิดต่างๆมีโอกาสรอดพ้นจากการถูกจับกุมดำเนินคดีมากกว่าการใช้สกุลเงินทั่วไปในการกระทำความผิด ซึ่งในมุมมองของผู้ศึกษานั้น หากต้องการที่จะป้องกันอาชญากรรมที่มีการใช้สกุลเงินเข้ารหัสที่มีลักษณะของการปกปิดตัวตนเจ้าของบัญชีเช่นนี้จำเป็นจะต้องแสวงหามาตรการต่างๆเพื่อให้สามารถยืนยันตัวตนเจ้าของบัญชีผู้ใช้งานบิทคอยน์ ซึ่งจะได้ทำการศึกษาต่อไป

3.2.2 การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมทางอ้อม

นอกจากการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย การใช้แทนสกุลเงินจริงในการเรียกค่าไถ่ การใช้ในการระดมทุนของกลุ่มผู้ก่อการร้าย รวมทั้งการใช้บิทคอยน์ในการฟอกเงินซึ่งถือเป็นการใช้บิทคอยน์ในการก่ออาชญากรรมโดยตรงแล้ว ยังมีผู้กระทำผิดที่นำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมในทางอ้อมอีกด้วย โดยการกระทำผิดในลักษณะนี้จะเป็นการอาศัยเอาชื่อ “บิทคอยน์” ไปใช้ในการโฆษณาชวนเชื่อหรือหลอกลวงให้เหยื่อหลงเชื่อว่าจะมีการลงทุนและเก็งกำไรจากมูลค่าของบิทคอยน์ที่มีความผันผวนตามกลไกและความต้องการของตลาดเพื่อให้เกิดผลกำไรมาแบ่งปันให้แก่สมาชิกผู้เข้าร่วม และเมื่อเหยื่อหลงเชื่อและนำเงินมาลงทุนแล้ว คนร้ายก็จะนำเงินไปใช้ในการกระทำความผิดในลักษณะของแชร์ลูกโซ่ หรือกระทำความผิดในรูปแบบอื่นๆที่มีลักษณะคล้ายกันดังตัวอย่างเหตุการณ์ที่เกิดขึ้นดังนี้

3.2.2.1 หลอกว่าจะมีการนำเงินไปลงทุนจากการเก็งกำไรในมูลค่าของบิทคอยน์

การหลอกลวงในลักษณะนี้ ในอดีตคือการที่มิจฉาชีพหรือคนร้าย ใช้วิธีการชักชวนให้เหยื่อร่วมลงทุนในผลิตภัณฑ์ทางการลงทุนต่างๆ เช่น หลอกว่าจะมีการระดมเงินเพื่อไปลงทุนในหุ้น เป็นต้น ซึ่งภายหลังจากที่เหยื่อหลงเชื่อและนำเงินไปร่วมลงทุน ในช่วงแรกจะได้รับผลตอบแทนเป็นจำนวนมากแต่เมื่อผ่านไปสักระยะเมื่อครบเวลาจ่ายเงินปันผลจะไม่สามารถติดต่อผู้ที่เกี่ยวข้องได้ และในที่สุดกลุ่มผู้กระทำผิดก็จะหลบหนีไป เพราะในการดำเนินการที่แท้จริงไม่มีการลงทุนใดๆ เป็นเพียงการนำเงินของเหยื่อหมุนเวียนกันจ่ายเป็นค่าตอบแทนในลักษณะของแชร์ลูกโซ่

ต่อมาเมื่อ**บิทคอยน์มีมูลค่าสูงขึ้นจนเป็นที่สนใจของนักลงทุนเป็นจำนวนมาก** เนื่องจากมีความผันผวนสูงเป็นไปตามกลไกการตลาด การลงทุนในมูลค่าของบิทคอยน์จึงกลายเป็นเป้าหมายที่มิจฉาชีพหรือคนร้ายนำไปใช้ในการหลอกลวงประชาชน ดังที่ปรากฏตามรายงานข่าวว่า เมื่อวันที่ 8 สิงหาคม 2561 เจ้าหน้าที่ตำรวจสังกัด กองกำกับการ 1 กองบังคับการปราบปราม ได้จับกุม นายบูม หรือ นายจิรัชพิสิษฐ์ จารวิจิต ดารานายแบบชื่อดัง ในข้อหาร่วมกันกับพวกฉ้อโกงและกระทำความผิดตาม พ.ร.บ.ฟอกเงิน สืบเนื่องจากการที่เจ้าหน้าที่ตำรวจได้รับแจ้งจากนักลงทุนชาวฟินแลนด์ว่า **ได้ถูกนายบูมกับพวกสบคบกันหลอกลวงให้ตนนำเงินมาลงทุนในสกุลเงินบิทคอยน์** โดยหลอกลวงว่าจะมีการนำเอาบิทคอยน์ไปเปลี่ยนเป็นอีกสกุลเงินหนึ่งเพื่อการลงทุนในตลาดหลักทรัพย์ รวมทั้งจะมีการแบ่งเงินจำนวนหนึ่งไปลงทุนในบ่อนการพนันที่ต่างประเทศ จนตนหลงเชื่อและร่วมลงทุนเป็นเงินบิทคอยน์จำนวนกว่า 5,500,000 บิทคอยน์ คิดเป็นจำนวนกว่า 797 ล้านบาท โดยภายหลังจากที่ตนได้โอนเงินบิทคอยน์จำนวนดังกล่าวไปแล้วตนก็ไม่เคยได้ส่วนแบ่งหรือไม่เคยได้รับแจ้งความคืบหน้าในการลงทุนดังกล่าวอีกเลย จากการสืบสวนของเจ้าหน้าที่ตำรวจทำให้ทราบว่า **เมื่อนายบูมกับพวกได้รับเงินบิทคอยน์จำนวนดังกล่าวแล้ว ไม่ได้มีการนำเอาไปลงทุนแต่อย่างใด แต่มีการนำไปใช้จ่ายภายในครอบครัวและนำไปใช้ซื้อที่ดิน และยังได้มีการแปลงบิทคอยน์มาเป็นเงินไทยแล้วโอนแบ่งส่วนให้กับผู้ร่วมขบวนการ**โดยเจ้าหน้าที่ตำรวจพบมีบัญชีการเงินที่เกี่ยวข้องกับการกระทำผิดครั้งนี้กว่า 40 บัญชี (สปริงนิวส์, 2561)

นอกจากเหตุการณ์ที่คนไทยเป็นผู้หลอกลวงเหยื่อชาวต่างชาติแล้ว ยังมีเหตุการณ์ที่คนไทยตกเป็นเหยื่อถูกหลอกลวงลงทุนในบิทคอยน์ด้วยตามที่ปรากฏจากการรายงานข่าวของสถานีโทรทัศน์ไทยทีวีสีช่อง 3 ที่ได้รายงานว่า มีกลุ่มคนไทยตกเป็นเหยื่อถูกคนร้ายชักชวนผ่านทาง

โปรแกรมไลน์ (Line) ให้ลงทุนในมูลค่าของบิทคอยน์ โดยคนร้ายหลอกลวงด้วยการออกแบบแผนการลงทุนในลักษณะเป็นแพ็คเกจ (Package) ดังปรากฏในภาพ

ภาพที่ 17 แพ็คเกจการลงทุนในมูลค่าบิทคอยน์ที่คนร้ายสร้างขึ้นเพื่อหลอกชักชวนให้เหยื่อหลงเชื่อ (สถานีโทรทัศน์ไทยทีวีสีช่อง 3, 2561)

จากแผนการลงทุนตามภาพ คนร้ายจะทำการหลอกลวงว่า หากเหยื่อทำการโอนเงินให้กับคนร้ายจำนวน 3,000 เหรียญสหรัฐ คนร้ายจะนำเงินไปลงทุนในมูลค่าของบิทคอยน์เพื่อทำการเก็งกำไร แล้วจะนำส่วนที่เป็นกำไรมาคืนให้กับเหยื่อ เป็นเงิน 108,000 บาท นอกจากนี้หากมีการชักชวนผู้อื่นมาร่วมลงทุนด้วยจะได้รับส่วนแบ่งจากผลกำไรอีก 10 เปอร์เซนต์ อีกทั้งยังมีการหลอกว่าหากมีผลประกอบการดีมากจะมีการพาเหยื่อผู้ร่วมลงทุนเดินทางไปท่องเที่ยวต่างประเทศอีกด้วย จึงทำให้เหยื่อหลงเชื่อและโอนเงินให้กับคนร้ายเป็นเงินจำนวนกว่า 3,000,000 บาท แต่ปรากฏว่าในท้ายที่สุดหลังจากที่เหยื่อโอนเงินไปแล้วก็ไม่สามารถติดต่อกับคนร้ายใด เมื่อตรวจสอบก็ปรากฏว่าเว็บไซต์ต่างๆที่คนร้ายทำขึ้นเพื่อหลอกลวงเหยื่อก็ถูกปิดไปด้วย

3.2.2.2 หลอกว่าจะมีการนำเงินไปลงทุนจากการขุดบิทคอยน์

ตามที่ผู้ศึกษาได้กล่าวถึงการได้มาของบิทคอยน์แล้วว่า ระบบของบิทคอยน์นั้นออกแบบให้การได้มาซึ่งบิทคอยน์มาจาก 2 วิธีการ คือ จากการทำธุรกรรมโอนให้กันไปมาในลักษณะเช่นเดียวกันกับเงินสกุลจริง และอีกวิธีการหนึ่งคือการขุด (Mining) ซึ่งเป็นการใช้พลังงานในการคำนวณสมการทางคณิตศาสตร์ที่จะต้องใช้คอมพิวเตอร์สมรรถนะสูงในการแข่งขันกันถอดสมการทางคณิตศาสตร์เพื่อตรวจสอบธุรกรรมต่างๆที่ถูกเข้ารหัสเพื่อแข่งขันกับนักขุดบิทคอยน์ทั่วโลกเพื่อยืนยัน

ความถูกต้องของการทำธุรกรรม โดยหากนักขุดคนใดแก้สมการสำเร็จเป็นคนแรกก็จะได้รับค่าตอบแทนเป็นบิทคอยน์ ดังนั้น จึงเกิดเป็นธุรกิจการรับจ้างและระดมทุนในการแข่งขันกันขุดบิทคอยน์ขึ้น โดยมีบริษัทหรือกลุ่มนักขุดเป็นจำนวนมากทั่วโลกที่มีการดำเนินการธุรกิจในลักษณะนี้ แต่ในขณะเดียวกัน มิจฉาชีพก็ได้เล็งเห็นผลประโยชน์จากการหลอกลวงว่าจะทำการขุดบิทคอยน์ดังกล่าว จึงมีการชักชวนหลอกลวงเหยื่อดังที่ปรากฏจากการรายงานของ เว็บไซต์กรุงเทพธุรกิจ (www.bangkokbiznews.com) ว่า เมื่อวันที่ 15 กุมภาพันธ์ 2562 ได้มีกลุ่มผู้เสียหายเข้าแจ้งความร้องทุกข์กับกองบังคับการปราบปรามการกระทำผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี หรือ บก. ปอท. กรณีได้ทำการ**ลงทุนกับบริษัทที่เปิดให้บริการลงทุนในการขุดบิทคอยน์** ซึ่งพบข้อพิรุธว่าอาจจะเป็นการกระทำผิดฐานฉ้อโกงประชาชน โดยบริษัทดังกล่าวได้มีการโฆษณาอยู่ตามสังคมออนไลน์ว่าเป็นบริษัทลูกของบริษัทรับขุดบิทคอยน์ซึ่งเป็นบริษัทใหญ่ในต่างประเทศ มีสาขาย่อยทั้งในกรุงเทพมหานครและจังหวัดเชียงใหม่จึงทำให้ผู้เสียหายหลงเชื่อ **ในการเข้าร่วมลงทุนนั้นผู้สนใจจะต้องสมัครเป็นสมาชิกของบริษัทผ่านทางเว็บไซต์ที่จัดทำขึ้น โดยจะต้องฝากเงินเข้าระบบในขั้นต้นเป็นเงินจำนวน 2,000 บาท จากนั้นบริษัทจะขุดบิทคอยน์มามอบให้กับผู้ร่วมลงทุน ซึ่งจะได้รับมากหรือน้อยนั้นขึ้นอยู่กับจำนวนเงินที่ร่วมลงทุน**

จากแผนการลงทุนดังกล่าวทำให้มีผู้เสียหายหลงเชื่อและโอนเงินให้บริษัทดังกล่าวกว่า 10,000,000 บาท โดยในช่วงแรกบริษัทดังกล่าวได้นำบิทคอยน์มามอบให้กับผู้เสียหายจริง เมื่อนำบิทคอยน์ไปตรวจสอบก็ปรากฏว่าเป็นบิทคอยน์ที่ใช้งานได้จริง จึงยิ่งทำให้ผู้เสียหายหลงเชื่อและร่วมโอนเงินลงทุนเพิ่มขึ้นอีกเป็นจำนวนมาก แต่ต่อมาในช่วงเดือนตุลาคม 2561 ทางบริษัทได้ออกประกาศเปลี่ยนแปลงและชะลอการถอนบิทคอยน์ออกจากระบบ จนกระทั่งเดือนมกราคม 2562 ได้ระงับการถอนบิทคอยน์ออกจากระบบทั้งหมดและเมื่อผู้เสียหายติดต่อไปยังบริษัทก็ไม่ได้รับคำตอบที่ชัดเจน ทำให้ผู้เสียหายเกิดความวิตกว่าบริษัทจะหลอกลวงและการดำเนินการทั้งหมดอาจเข้าข่ายเป็นการฉ้อโกงประชาชน ซึ่งจากการรวบรวมข้อมูลของผู้เสียหายปรากฏว่ามีการประมาณการความเสียหายแล้วอยู่ที่ประมาณ 500 ล้านบาท (กรุงเทพธุรกิจ, 2562)

พฤติกรรมการชักชวนให้ผู้อื่นมาลงทุนและลักษณะของการจ่ายค่าตอบแทนของบริษัทรับขุดบิทคอยน์ที่ปรากฏตามรายงานดังกล่าว มีลักษณะคล้ายกันกับการกระทำผิดในลักษณะแชร์ลูกโซ่ที่ในข้อเท็จจริงแล้วอาจไม่ได้มีการนำเงินไปลงทุนขุดบิทคอยน์จริง แต่เป็นการกระทำผิดในลักษณะที่นำเงินของเหยื่อรายหนึ่งไปซื้อบิทคอยน์แล้วนำบิทคอยน์ไปมอบให้เหยื่ออีกรายหนึ่ง

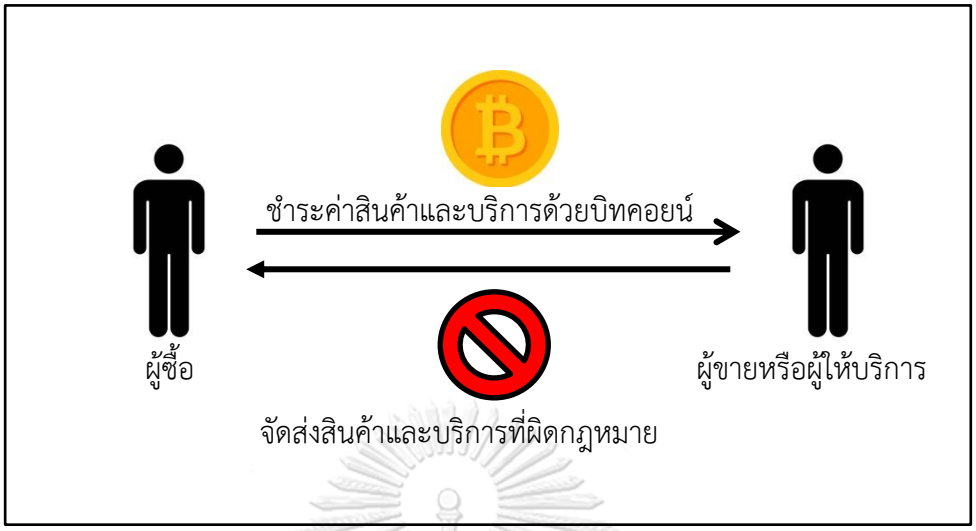
หมุนเวียนกันไปจนเกิดความน่าเชื่อถือ และเมื่อระดมทุนได้เงินจำนวนมากแล้วจึงปิดบริษัทหลบหนีไปในที่สุด

จากกรณีตัวอย่างลักษณะการกระทำผิดโดยใช้บิทคอยน์เป็นเครื่องมือในทางอ้อมที่ผู้ศึกษายกตัวอย่างมานี้ ทำให้เข้าใจได้ว่าอาชญากรได้ใช้ประโยชน์จากคุณลักษณะของบิทคอยน์ที่มีมูลค่าสูง มีราคาผันผวนตามความต้องการของตลาด มีผลตอบแทนที่จะได้รับจากการเก็งกำไรเป็นจำนวนมาก นำไปใช้ในการหลอกลวงชักจูงให้เหยื่อหลงเชื่อว่า หากนำเงินมาร่วมลงทุนแล้วจะได้รับผลตอบแทนเป็นจำนวนมาก ซึ่งในการดำเนินการรับลงทุนและร่วมลงทุนในลักษณะนี้ จำเป็นอย่างยิ่งที่รัฐจะต้องเข้าไปสอดส่องและกำกับดูแลการดำเนินธุรกิจในลักษณะเดียวกันนี้อย่างใกล้ชิด เนื่องจากเป็นการดำเนินธุรกิจที่มีความเสี่ยงที่จะมีลักษณะเป็นการฉ้อโกงประชาชนสูง ดังจะได้อธิบายถึงนโยบายมาตรการและกฎหมายต่างๆที่เกี่ยวข้องต่อไป

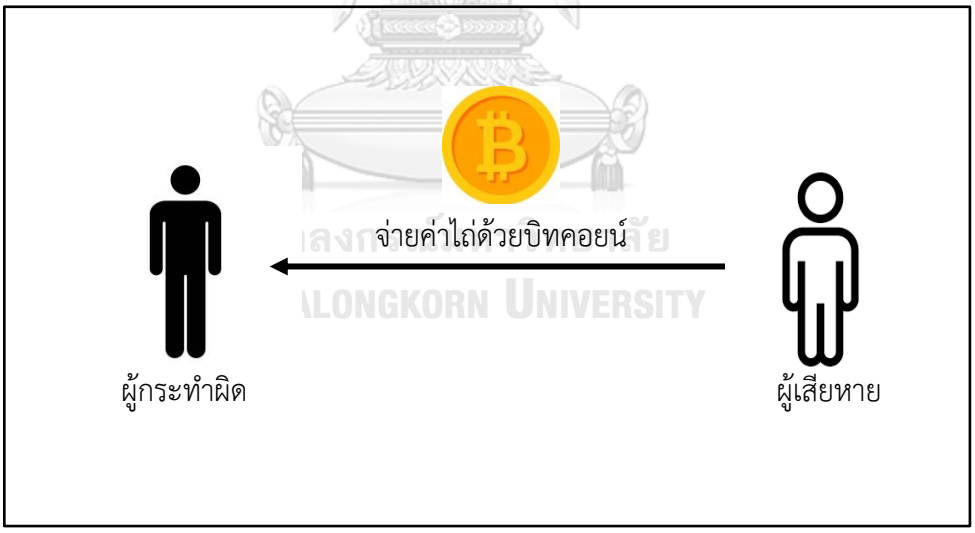
3.2.3 เปรียบเทียบรูปแบบการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรงและทางอ้อม

จากการศึกษาค้นคว้ารูปแบบของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมทั้งโดยทางตรงและทางอ้อม ทำให้พบข้อแตกต่างกันกล่าวคือ ในการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการกระทำผิดโดยตรงนั้น ผู้กระทำผิดจะมีการใช้บิทคอยน์ในการกระทำผิดจริง เช่น การนำบิทคอยน์ไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและการบริการที่ผิดกฎหมาย การใช้แทนสกุลเงินจริงในการเรียกค่าไถ่ ใช้เป็นตัวกลางในการระดมเงินทุนของกลุ่มผู้ก่อการร้าย รวมทั้งการใช้บิทคอยน์ในการฟอกเงิน แต่ในส่วนของการใช้บิทคอยน์ในการก่ออาชญากรรมทางอ้อมนั้น ผู้กระทำผิดไม่ได้นำบิทคอยน์มาใช้แต่อย่างใด แต่มักเป็นการนำชื่อ “บิทคอยน์” มาใช้เพื่อให้เหยื่อหลงเชื่อว่าจะมีการลงทุนในการเก็งกำไรมูลค่าของบิทคอยน์หรือเป็นการลงทุนเพื่อให้ได้มาซึ่งบิทคอยน์หรือการขุดบิทคอยน์เท่านั้น ซึ่งในข้อเท็จจริงแล้วไม่ได้มีการดำเนินการใดๆที่เป็นการลงทุนหรือกระทำกับบิทคอยน์โดยตรงแต่อย่างใด เพื่อให้เกิดความเข้าใจในรูปแบบของการกระทำผิดทั้งโดยตรงและทางอ้อม ผู้วิจัยจึงขออธิบายประกอบภาพแนวคิดดังนี้

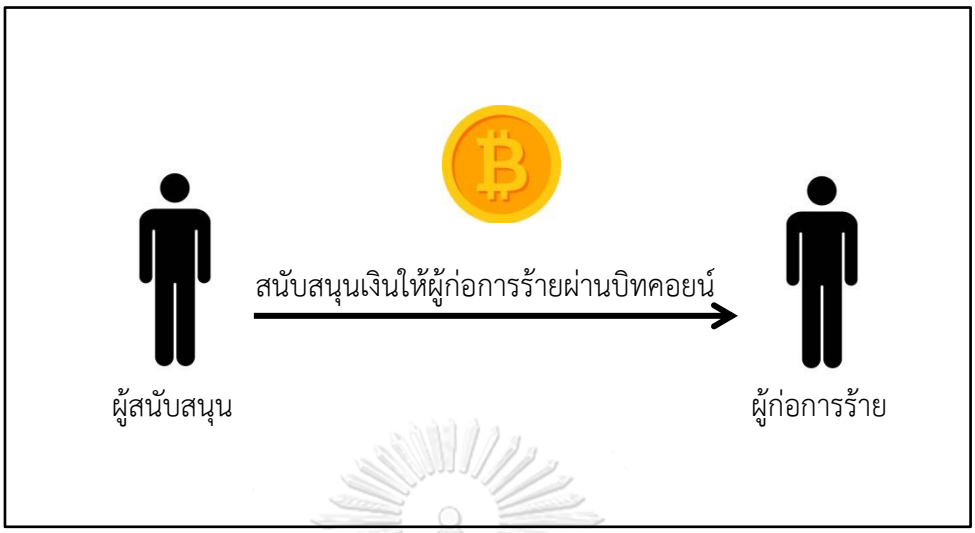
3.2.3.1 อธิบายรูปแบบการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยตรง



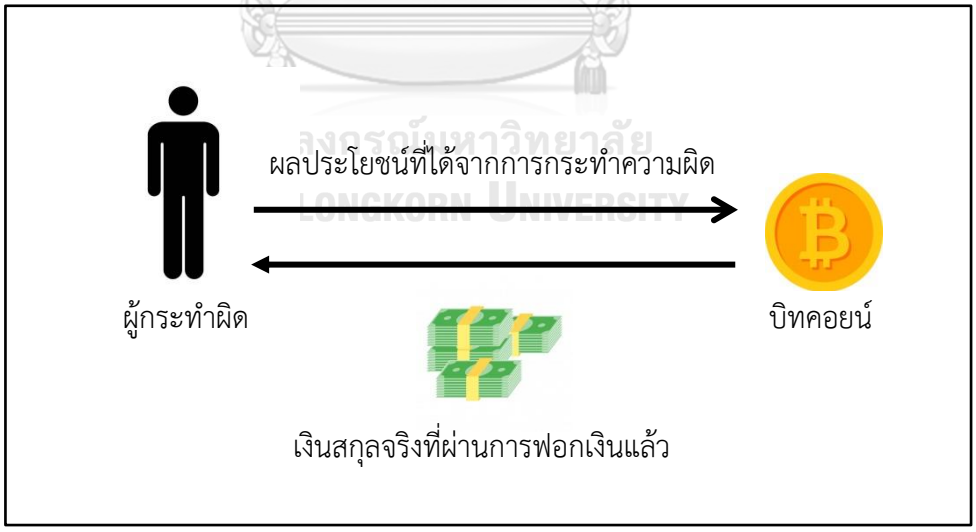
ภาพที่ 18 รูปแบบการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยตรงด้วยการใช้บิทคอยน์ในการซื้อขายแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2562)



ภาพที่ 19 รูปแบบการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยตรงด้วยการเรียกร้องให้จ่ายค่าไถ่ด้วยบิทคอยน์
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2562)

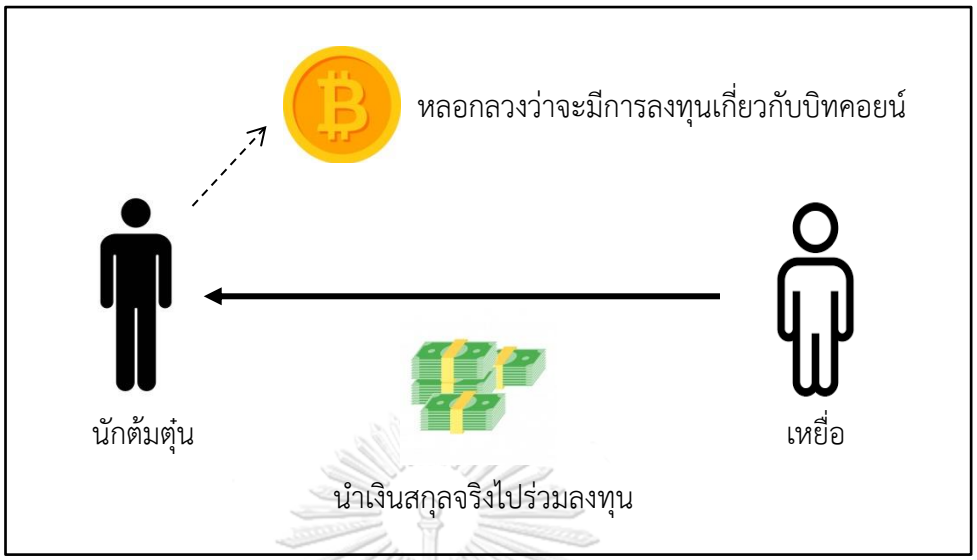


ภาพที่ 20 รูปแบบการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยตรงด้วยการใช้บิทคอยน์ในการระดมเงินทุนของกลุ่มผู้ก่อการร้าย
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2562)



ภาพที่ 21 รูปแบบการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยตรงด้วยการใช้บิทคอยน์ในการฟอกเงิน
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2562)

3.2.3.2 อธิบายรูปแบบการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมทางอ้อม



ภาพที่ 22 รูปแบบการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมทางอ้อม
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2562)

3.3 แนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสในต่างประเทศ

จากการศึกษารวบรวมข้อมูลในหัวข้อต่างๆที่ผ่านมา ทำให้เข้าใจได้ว่าบิทคอยน์และสกุลเงินเข้ารหัสสกุลต่างๆ ได้เริ่มเข้ามามีบทบาทในการเป็นเครื่องมือที่ใช้ในการแลกเปลี่ยนสินค้าและบริการระหว่างกัน เป็นเครื่องมือในการลงทุนในลักษณะของสินทรัพย์ดิจิทัล การระดมทุนในลักษณะของการใช้สกุลเงินเข้ารหัส (ICO) การทำเหมืองหรือการขุด (Mining) อีกทั้งยังถูกนำไปใช้ในการก่ออาชญากรรมรูปแบบต่างๆตามที่กล่าวมาแล้ว จึงทำให้ทั่วโลกเริ่มตระหนักถึงปัญหาต่างๆที่อาจเกิดขึ้นอันเป็นผลมาจากการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่มีความแพร่หลายมากยิ่งขึ้น จนนำไปสู่การกำหนดนโยบาย กฎหมาย หรือ มาตรการต่างๆเพื่อควบคุม กำกับดูแล การใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ แต่ทั้งนี้ด้วยความแตกต่างกันในด้านวัฒนธรรม วิถีชีวิต ความเชื่อ การเมือง ระบบเศรษฐกิจและบริบทต่างๆของแต่ละประเทศ จึงทำให้มีแนวทางการกำหนดนโยบาย กฎหมาย หรือมาตรการต่างๆที่แตกต่างกันออกไป ดังนี้

3.3.1 ประเทศญี่ปุ่น

ประเทศญี่ปุ่น เป็นประเทศที่มีชื่อเสียงในด้านการพัฒนาทางอุตสาหกรรม เทคโนโลยีสารสนเทศ และนวัตกรรมใหม่ๆอยู่เสมอ ภายหลังจากการกำเนิดของนวัตกรรมทางการเงินอย่างสกุลเงินเข้ารหัส ในประเทศญี่ปุ่นก็มีผู้นิยมใช้สกุลเงินเข้ารหัสเป็นจำนวนมากจนได้รับความนิยมเป็นที่แพร่หลาย มีการนำสกุลเงินเข้ารหัสไปใช้ในการซื้อขายแลกเปลี่ยนสินค้าและบริการในชีวิตประจำวันเป็นจำนวนมาก ส่งผลให้มีธุรกิจห้างร้านจนถึงร้านค้าทั่วไปยอมรับชำระเงินในรูปแบบของสกุลเงินเข้ารหัสเป็นจำนวนมาก จนทำให้รัฐบาลญี่ปุ่นเริ่มพิจารณาถึงความเป็นไปได้ที่จะมีการพัฒนาให้สกุลเงินเข้ารหัสมีสถานะเป็นทรัพย์สินที่สามารถใช้ชำระค่าสินค้าและบริการแก่กันได้ โดยในช่วงต้นปี ค.ศ. 2017 หน่วยงานเกี่ยวกับการบริการทางการเงิน หรือ Financial Services Agency (FSA) ซึ่งทำหน้าที่เกี่ยวกับการตรวจสอบและกำกับดูแลด้านการเงินของประเทศญี่ปุ่น ได้เสนอร่างแก้ไขพระราชบัญญัติการให้บริการชำระเงิน หรือ Payment Services Act (PSA) ต่อกระทรวงเทคโนโลยีข้อมูลและการสื่อสารของประเทศญี่ปุ่น โดยมีผลใช้บังคับตั้งแต่เดือน เมษายน ค.ศ. 2017 เป็นต้นมา **ส่งผลทำให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆถือเป็นทรัพย์สินที่มีมูลค่า สามารถใช้สำหรับชำระค่าสินค้าและบริการ ค่าเช่าต่างๆ ให้แก่บุคคลอื่นผ่านการโอน หรือ จำหน่ายผ่านวิธีการทางระบบอิเล็กทรอนิกส์ได้ แต่ทั้งนี้ยังไม่ถือว่าบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นเงินตราที่จะใช้ชำระหนี้กันได้ตามกฎหมาย (Legal Tender) แต่อย่างใด** (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

ภายหลังจากที่มีการแก้ไขกฎหมายดังกล่าว หน่วยงานเกี่ยวกับการบริการทางการเงิน(FSA) จึงได้รับมอบหมายให้ทำหน้าที่ในการออกกฎหมาย กำกับดูแล ควบคุมการใช้บิทคอยน์และสกุลเงินเข้ารหัส เช่น การออกใบอนุญาตให้กับผู้ที่ประกอบธุรกิจเป็นตัวกลางหรือเป็นนายหน้าในการซื้อขายหรือรับแลกเปลี่ยนสกุลเงินเข้ารหัส โดยมีหลักเกณฑ์สำคัญที่ควบคุมการใช้สกุลเงินเข้ารหัสคือ การใช้สกุลเงินเข้ารหัสจะต้องถูกตรวจสอบตามกฎหมายตรวจสอบการฟอกเงินของประเทศ และสถาบันการเงินรวมทั้งผู้ให้บริการซื้อขายแลกเปลี่ยนหรือทำธุรกิจรับเป็นนายหน้าในการจัดหา ซื้อขายแลกเปลี่ยนสกุลเงินเข้ารหัสจะต้องดำเนินนโยบายในการรู้จักและเก็บข้อมูลของลูกค้าของตน (Know–Your–Customer-Rules) เพื่อเป็นการป้องกันความเสียหายที่อาจเกิดขึ้นในทุกกรณี นอกจากนี้ในประเด็นด้านการจัดเก็บภาษี ปรากฏว่า เมื่อปี ค.ศ.2018 หน่วยงานด้านการจัดเก็บภาษีของประเทศญี่ปุ่น หรือ National Tax Agency ได้ระบุว่า**กำไรจากการซื้อขายสกุลเงินเข้ารหัสถือเป็นรายได้**

เบ็ดเตล็ด (Miscellaneous Income) ที่จะต้องเสียภาษีระหว่าง ร้อยละ 15 ถึง ร้อยละ 55 (พรชัย ชุนหจินดา, 2561)

ในประเด็นด้านการบังคับคดี ประเทศญี่ปุ่นได้มีมาตรการเกี่ยวกับการยึดอายัดบิทคอยน์ที่น่าสนใจ สืบเนื่องจากคดีล้มละลายของบริษัท Mt.Gox (บริษัทรับบริการแลกเปลี่ยนบิทคอยน์ที่มีที่ตั้งอยู่ในประเทศญี่ปุ่น ถูกโจรกรรมบิทคอยน์จนล้มละลาย) ที่เริ่มต้นจากการที่ศาลมีคำสั่งให้เริ่มกระบวนการพิจารณาคดีล้มละลายและแต่งตั้งเจ้าพนักงานพิทักษ์ทรัพย์ซึ่งมีหน้าที่ในการรวบรวมทรัพย์สินของลูกหนี้คดีล้มละลาย โดยในคดีนี้ได้มีการ**นำเอาทรัพย์สินที่เป็นบิทคอยน์รวมเข้ามาอยู่ในกองทรัพย์สินของลูกหนี้ล้มละลาย**เพื่อที่จะนำไปขายทอดตลาดและนำมาชำระหนี้ให้แก่ผู้เสียหายด้วย โดยในการยึดอายัดบิทคอยน์ในคดีนี้เจ้าพนักงานพิทักษ์ทรัพย์ได้ดำเนินการด้วยการยึดข้อมูลรหัสผ่านส่วนตัว (Private Key) ของบริษัท Mt.Gox และทำการโอนย้ายบิทคอยน์จำนวน 202,106.00072 บิทคอยน์ไปยังบัญชีบิทคอยน์ที่ถูกควบคุมโดยเจ้าพนักงานพิทักษ์ทรัพย์ จากกรณีดังกล่าวนี้จึงถือได้ว่าประเทศญี่ปุ่นมีมาตรการในการยึดอายัดทรัพย์สินที่เป็นบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่เป็นรูปธรรมและสามารถปฏิบัติได้จริง (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

นอกจากกรณีคดีล้มละลายของบริษัท Mt.Gox แล้วยังมีกรณีศึกษาเกี่ยวกับการยึดบิทคอยน์แทนค่าปรับในคดีจราจรในประเทศญี่ปุ่นด้วย โดยกรณีนี้เกิดจากเจ้าหน้าที่ตำรวจอำเภอโยโกของประเทศญี่ปุ่นได้นำพระราชบัญญัติการให้บริการชำระเงิน หรือ Payment Services Act (PSA) มาปรับใช้ในการยึดสกุลเงินเข้ารหัสแทนการยึดทรัพย์สินประเภทอื่นๆจากชายอายุ 59 ปีที่ค้างค่าปรับในความผิดเกี่ยวกับการจอดรถ เนื่องจากเจ้าหน้าที่ตำรวจไม่พบบัญชีธนาคารของผู้กระทำผิดและไม่ทราบว่าผู้กระทำผิดทำงานอยู่ที่ใด โดยเจ้าหน้าที่ตำรวจได้เข้าไปยังบัญชีสกุลเงินเข้ารหัสของชายดังกล่าวและทำการอายัดสกุลเงินเสมือนคิดเป็นมูลค่ากว่า 5,000 เยน (Nathalie Stucky, 2018 อ้างถึงใน ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

ในกรณีของประเทศญี่ปุ่นนี้ สามารถวิเคราะห์ได้ว่า ด้วยบริบทของประเทศญี่ปุ่นที่มีวิถีชีวิตตามวัฒนธรรมดั้งเดิมแต่ผสมผสานและมีการปรับตัวเปลี่ยนแปลงไปตามนวัตกรรมและเทคโนโลยีสมัยใหม่อยู่เสมอ ทำให้ประเทศญี่ปุ่นตระหนักถึงปัญหาต่างๆที่อาจเกิดขึ้นจากการใช้งานสกุลเงินเข้ารหัส แต่ในขณะเดียวกันก็มองเห็นโอกาสที่จะเกิดพัฒนาระบบเศรษฐกิจได้ จึงทำให้เกิดการกำหนดนโยบาย กฎหมาย และมาตรการต่างๆออกมารองรับให้สอดคล้องกับสถานการณ์การใช้งาน

สกุลเงินเข้ารหัสดังที่ได้กล่าวมานี้ ส่งผลทำให้การใช้งานสกุลเงินเข้ารหัสมีความปลอดภัย มีหน่วยงานที่กำกับดูแลรับผิดชอบอย่างชัดเจน มีมาตรการควบคุมอย่างเป็นรูปธรรม ส่งผลทำให้มีการใช้งานสกุลเงินเข้ารหัสอย่างแพร่หลายมากยิ่งขึ้น

3.3.2 ประเทศจีน

ประเทศจีนมีแนวนโยบายที่ชัดเจนและประกาศตัวว่าไม่ยอมรับสกุลเงินเข้ารหัสทุกชนิดทุกประเภท โดยจะเห็นได้จากการที่ในปี พ.ศ. 2552 รัฐบาลจีนได้ประกาศ**ห้ามใช้สกุลเงินเข้ารหัสในการซื้อขายแลกเปลี่ยนสินค้าและบริการในประเทศจีน** เนื่องจากยังไม่มั่นใจผลกระทบที่อาจเกิดขึ้นต่อระบบการเงินของประเทศ ต่อมาในปี พ.ศ. 2556 สถาบันการเงินหลักของประเทศจีนรวมทั้งผู้ให้บริการเกี่ยวกับธุรกิจการเงินประเภทบุคคลที่สามถูกรัฐบาลห้ามไม่ให้ยอมรับ สนับสนุน ใช้หรือเสนอการซื้อขายสกุลเงินเข้ารหัสทุกชนิด นอกจากนี้ในปี พ.ศ.2560 เป็นต้นมา ธนาคารกลางแห่งประเทศจีน (People's Bank of China หรือ PBoC) ยังได้มีการประกาศแจ้งไปยังสถาบันการเงินทั่วประเทศรวมทั้งแจ้งเตือนให้ประชาชนทราบว่า **การดำเนินการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัส หมายความรวมถึงการระดมทุนผ่านสกุลเงินเข้ารหัส หรือ Initial Coin Offering (ICO) เป็นสิ่งหลอกลวงและผิดกฎหมายและห้ามกระทำการระดมทุนในลักษณะดังกล่าวในประเทศจีนเป็นอันขาด** โดยการประกาศนี้ยังมีผลย้อนหลังถึงการระดมทุนผ่านสกุลเงินเข้ารหัส (ICO) ที่มีการขายไปแล้วจะต้องถูกยกเลิกและคืนเงินให้แก่นักลงทุนทุกราย นอกจากนี้ภายหลังจากที่มีการประกาศนโยบายนี้แล้ว ได้เกิดผลในทางปฏิบัติที่ชัดเจนคือมีการปิดตัวลงของเว็บไซต์ที่ทำหน้าที่เป็นตัวแทนหรือนายหน้าในการระดมทุนแบบ ICO รวมทั้งพวกกลุ่มนายหน้ารับแลกเปลี่ยนสกุลเงินเข้ารหัสสกุลต่างๆด้วย (พรชัย ชุนหจินดา, 2561)

แม้จะมีการกำหนดนโยบายที่ชัดเจนในการไม่ยอมรับและห้ามใช้สกุลเงินเข้ารหัสก็ตาม แต่ประเทศจีนยังคงตระหนักถึงความเสี่ยงที่อาจเกิดขึ้นต่อเสถียรภาพทางการเงินของประเทศ ในกรณีที่หากยังมีการใช้สกุลเงินเข้ารหัสในประเทศจีน ดังนั้น เพื่อเป็นการปกป้องความมั่นคงของค่าเงินหยวน ประเทศจีนจึงได้มีการออกนโยบายที่จะพัฒนาสกุลเงินเข้ารหัสของตนเอง โดยรัฐบาลได้มอบหมายให้ธนาคารกลางแห่งประเทศจีน (PBoC) ทำการศึกษาและพัฒนาสกุลเงินเข้ารหัสของประเทศจีนเอง โดยมีวัตถุประสงค์หลักในการปกป้องการคุกคามของค่าเงินหยวนจากสกุลเงินเข้ารหัสสกุลต่างๆ อีกทั้งยังเป็นการรักษาไว้ซึ่งเสถียรภาพและความมั่นคงทางการเงินของประเทศ ประกอบ

กับยังเป็นการกระตุ้นให้เกิดการพัฒนานวัตกรรมทางการเงินรูปแบบใหม่ที่อยู่ภายใต้ความควบคุมของรัฐเพื่อรักษาความมั่นคงภายในประเทศอีกด้วย (สยามบล็อคเชน, 2561)

จะเห็นได้ว่านโยบายที่เกี่ยวกับสกุลเงินเข้ารหัสของประเทศจีนนั้นเป็นไปในแนวทางที่ไม่ยอมรับสกุลเงินเข้ารหัสและมีการห้ามการใช้งานโดยเฉพาะในประเด็นของการใช้ในการซื้อขายแลกเปลี่ยนสินค้าและบริการและการระดมทุนด้วยสกุลเงินเข้ารหัส (ICO) อย่างชัดเจน โดยสามารถวิเคราะห์ได้ว่า ประเทศจีนมีพื้นฐานระบอบการปกครองในรูปแบบสังคมนิยม การกำหนดนโยบายในการบริหารปกครองประเทศนั้น มักจะเป็นไปในแนวทางในการรักษาความมั่นคงและผลประโยชน์ของประเทศในภาพรวมมาเป็นอันดับแรก จึงได้มีแนวนโยบายในการไม่ยอมรับสกุลเงินเข้ารหัสอันถือเป็นความเสี่ยงที่อาจก่อให้เกิดความเสียหายภายในประเทศได้ แต่ในขณะเดียวกันก็สามารถกล่าวได้ว่าประเทศจีนในปัจจุบันอยู่ในยุคของการพัฒนาอุตสาหกรรมและเทคโนโลยีสมัยใหม่ จนทำให้การสร้างสรรค์นวัตกรรมต่างๆของประเทศจีนในปัจจุบันนั้นเกิดความทัดเทียมกับนานาชาติ จึงทำให้วิสัยทัศน์ในการกำหนดนโยบายในเรื่องนี้มีการกำหนดนโยบายที่จะสร้างสกุลเงินเข้ารหัสของตนเอง ซึ่งในมุมมองของผู้วิจัยมองว่าเป็นการกำหนดนโยบายเชิงป้องกันและเชิงรุกในเวลาเดียวกัน ซึ่งเป็นผลดีให้กับประเทศจีนได้เป็นอย่างมาก

3.3.3 สหรัฐอเมริกา

สหรัฐอเมริกาเป็นประเทศที่เน้นหนักในนโยบายด้านความมั่นคงและความปลอดภัยภายในราชอาณาจักร ดังนั้น การกำหนดนโยบายเกี่ยวกับสกุลเงินเข้ารหัสจึงถูกพิจารณาอย่างละเอียดรอบคอบ เพื่อให้การเติบโตของการใช้สกุลเงินเข้ารหัสในสหรัฐเมริกาเป็นไปอย่างปลอดภัยสูงสุด โดยคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน สหรัฐอเมริกา หรือ Financial Action Task Force (FATF) ได้ให้คำนิยามของสกุลเงินเข้ารหัสว่า **เป็นตัวแทนของมูลค่าที่อยู่ในรูปแบบดิจิทัล (Digital Representation of Value)** ที่สามารถนำไปใช้ในการแลกเปลี่ยนกันทางดิจิทัล อีกทั้งยังมีลักษณะดังต่อไปนี้

1) เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการ (Medium of Exchange)

2) เป็นหน่วยของมูลค่า (Unit of Account)

3) เป็นที่เก็บมูลค่า (Store of Value)

แต่ทั้งนี้**สกุลเงินเข้ารหัสไม่ใช่สกุลเงินจริง (Fiat Currency) และยังไม่สามารถนำไปชำระหนี้กันตามกฎหมายเหมือนสกุลเงินจริงได้ (Legal Tender)** เนื่องจากสกุลเงินเข้ารหัสไม่ได้มีการ

ออกหรือรับรองจากรัฐบาล ไม่ได้ยึดโยงอยู่กับสินทรัพย์ใดๆ อีกทั้งในการใช้งานสกุลเงินเข้ารหัสนี้ยังแตกต่างกันไปตามแต่เงื่อนไขและข้อตกลงภายในของแต่ละชุมชนหรือสังคมนั้นๆ (Financial Action Task Force [FATF], 2015) นอกจากนี้ เครือข่ายการบังคับใช้กฎหมายอาชญากรรมทางการเงินสหรัฐอเมริกา หรือ Financial Crimes Enforcement Network (FinCEN) ได้ให้ความหมายของสกุลเงินเข้ารหัสไว้ว่า **"เป็นสื่อกลางในการแลกเปลี่ยนที่สามารถใช้ในการแลกเปลี่ยนสินค้าและบริการได้ในลักษณะคล้ายกันกับเงินในสภาพแวดล้อมบางลักษณะ แต่ไม่มีสถานะเป็นตราสารที่ใช้ชำระหนี้ได้ตามกฎหมาย"** (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561) จากการให้ความหมายของหน่วยงานที่เกี่ยวข้องตามที่ได้กล่าวมานี้ ทำให้พอเข้าใจได้ว่าสหรัฐอเมริกามีมุมมองว่าสกุลเงินเข้ารหัสเป็นสื่อกลางในการแลกเปลี่ยนรูปแบบหนึ่ง แต่ไม่สามารถนำมาใช้ชำระหนี้กันได้ตามกฎหมาย

ในปี ค.ศ.2013 เครือข่ายการบังคับใช้กฎหมายกับอาชญากรรมที่เกี่ยวกับการเงิน หรือ (FinCEN) ได้กำหนดให้ผู้ประกอบธุรกิจต่างๆที่มีลักษณะเป็นการบริการด้านการเงิน (Money Services Businesses: MSBs) ที่เกี่ยวข้องกับสกุลเงินเข้ารหัสที่ใช้ระบบการทำงานแบบกระจายศูนย์ (Decentralized) เช่น บิทคอยน์ ต้องถูกควบคุมด้วยกฎหมายต่อต้านการฟอกเงิน ส่งผลทำให้ผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสประเภทอื่นๆ ไม่ว่าจะมีวัตถุประสงค์เพื่อใช้ในการซื้อขายแลกเปลี่ยนสกุลเงินเข้ารหัส การทำเหมืองหรือการขุด หรือการทำธุรกรรมที่มีการแลกเปลี่ยนด้วยสกุลเงินดอลลาร์สหรัฐจะต้องขึ้นทะเบียนกับรัฐบาล

ต่อมาในปี ค.ศ. 2014 สหรัฐอเมริกาได้ผ่านกฎหมายต้นแบบเกี่ยวกับการกำกับดูแลผู้ประกอบธุรกิจที่เกี่ยวข้องกับเงินเสมือน หรือ US Uniform Regulation of Virtual-Currency Businesses ACT โดยกฎหมายนี้ได้กำหนดให้กิจกรรมดังต่อไปนี้ ถือเป็นการประกอบธุรกิจที่เกี่ยวข้องกับเงินเสมือน (Virtual-Currency Business Activity) ได้แก่ (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

1) การแลกเปลี่ยน การโอน หรือการจัดเก็บเงินเสมือน

2) การมีส่วนร่วมในการจัดการเงินเสมือน ไม่ว่าโดยทางตรงหรือโดยผ่านข้อตกลงกับผู้ให้บริการเงินเสมือน

3) การแลกเปลี่ยนมูลค่าทางดิจิทัล (Digital Representations of Value) ภายในเกมออนไลน์หรือเกมแพลตฟอร์มอื่นๆ เช่น เพื่อใช้เป็นเงินเสมือนหรือการชำระหนี้ตามกฎหมาย

นอกจากนี้ ในประเด็นด้านระดับการกำกับดูแล กฎหมายดังกล่าวนี้ยังได้แบ่งกลุ่มผู้ประกอบธุรกิจเงินเสมือนไว้ 3 ระดับ (Three-tier System) ดังนี้ (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

ระดับที่ 1 (Minor Activity) ผู้ประกอบการที่มีธุรกิจเกี่ยวกับเงินเสมือนไม่เกิน 5,000 ดอลลาร์ สหรัฐต่อปี (ประมาณ 163,000 บาท) ได้รับยกเว้นไม่ต้องอยู่ภายใต้การกำกับดูแล

ระดับที่ 2 (Intermediate Registration) ผู้ประกอบการที่มีธุรกิจเกี่ยวกับเงินเสมือนเกินกว่า 5,000 แต่ไม่เกิน 35,000 ดอลลาร์สหรัฐต่อปี (ประมาณ 1,140,000 บาท) ต้องจดทะเบียนกับรัฐและต้องปฏิบัติตามหลักเกณฑ์และวิธีการที่กำหนด โดยผู้ประกอบการกลุ่มนี้สามารถคงสถานะอยู่ในระดับนี้ได้นานถึง 2 ปี ตราบเท่าที่ยังมีมูลค่าการดำเนินธุรกิจไม่เกินเพดานที่กำหนดไว้ ผู้ประกอบการที่จดทะเบียนในรูปแบบนี้จะต้องจดทะเบียนกับ FinCEN ด้วย เนื่องจากในการประกอบธุรกิจดังกล่าวจะต้องอยู่ภายใต้มาตรการการดูแลผู้ให้บริการทางการเงิน (Money Services Businesses: MSBs) ตามที่ได้กล่าวมาแล้ว

ระดับที่ 3 (Full Licensure) ผู้ประกอบการที่มีธุรกิจเกี่ยวกับเงินเสมือนเกินกว่า 35,000 ดอลลาร์ (ประมาณ 1,140,000 บาท) สหรัฐขึ้นไป ต้องอยู่ภายใต้การกำกับดูแลเต็มรูปแบบ

ต่อมาในปี ค.ศ. 2015 คณะกรรมาธิการการซื้อขายสินค้าโภคภัณฑ์ซื้อขายล่วงหน้าของสหรัฐอเมริกา หรือCommodities Futures Trading Commission (CFTC) ได้ออกประกาศระบุว่าสกุลเงินเข้ารหัสหรือเงินเสมือนอาจถือเป็นสินค้า โภคภัณฑ์ หรือตราสารอนุพันธ์ (Derivatives Contracts) ดังนั้น จึงต้องอยู่ในความควบคุมของคณะกรรมาธิการดังกล่าวด้วยและในปี ค.ศ. 2017 ได้มีการระดมทุนผ่านการเสนอขายหรือจำหน่ายโทเคนดิจิทัลหรือสกุลเงินเข้ารหัส (ICO) เป็นจำนวนมาก สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์สหรัฐอเมริกา หรือ U.S. Securities and Exchange Commission (SEC) จึงได้พิจารณาว่าการขาย ICO อาจสามารถกำกับดูแลได้ด้วยการใช้กฎหมายหลักทรัพย์ (DAO Report of Investigation) มาปรับใช้ โดยการนำกฎหมายหลักทรัพย์ดังกล่าวมากำกับดูแลการระดมทุน ICO นี้ จะไม่เพียงมีผลกับการระดมทุนของบริษัทต่างๆในสหรัฐอเมริกาเท่านั้น แต่จะครอบคลุมไปถึงกิจการในต่างประเทศที่มีการระดมทุน ICO ที่มีการเสนอขายโทเคนดิจิทัลหรือสุลเงินเข้ารหัสให้กับนักลงทุนสหรัฐอเมริกาด้วย (พรชัย ชุนหจินดา, 2561)

ประเด็นด้านการบังคับคดีในสหรัฐอเมริกาผู้ที่ประสงค์จะทำการยึดทรัพย์นั้นจะต้องแสดงให้ศาลเห็นถึงข้อเท็จจริงที่เกี่ยวข้อง เช่น ลักษณะของทรัพย์สิน และตำแหน่งที่ตั้ง เป็นต้น เพื่อให้เจ้าพนักงานบังคับคดีสามารถทำการสืบค้นและตรวจสอบทรัพย์สินที่จะถูกยึดต่อไปได้ ในกรณีของสกุลเงินเข้ารหัสนั้น เจ้าหนี้อาจจะต้องทำการสืบเพื่อให้ทราบว่าลูกหนี้ตามคำพิพากษานั้นมีทรัพย์สินที่เป็นสกุลเงินเข้ารหัสเก็บไว้ในที่ใดบ้าง เช่น บัญชีที่เปิดไว้กับตลาดแลกเปลี่ยน (Exchange) หรือวอลเล็ท (Wallet) ต่างๆ

สำหรับขั้นตอนการยึดอายัดสกุลเงินเข้ารหัสนั้น เจ้าพนักงานบังคับคดีจะดำเนินการยึดรหัสผ่านส่วนตัว (Private Key) ของลูกหนี้ โดยจะมีการควบคุมให้เฉพาะบุคคลที่เกี่ยวข้องกับกระบวนการบังคับคดีเท่านั้นที่จะสามารถเข้าถึงรหัสผ่านส่วนตัว (Private Key) ดังกล่าว จากนั้นเจ้าพนักงานบังคับคดีจะใช้รหัสผ่านส่วนตัวของเจ้าหนี้เพื่อโอนสกุลเงินเข้ารหัสเข้าไปที่บัญชีของศาล โดยสามารถอธิบายได้ตามแผนภาพต่อไปนี้

ภาพที่ 23 ขั้นตอนการยึดอายัดสกุลเงินเข้ารหัสของสหรัฐอเมริกา
(ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

แม้สหรัฐอเมริกาจะให้สถานภาพของสกุลเงินเข้ารหัสเป็นเพียงแค่ทรัพย์สินประเภทหนึ่งที่สามารถนำมาใช้แลกเปลี่ยนสินค้าบริการและสามารถนำไปเก็งกำไรกันได้ โดยไม่ใช่วัตถุที่สามารถนำไปชำระหนี้กันได้ตามกฎหมายก็ตาม แต่สหรัฐอเมริกาก็ได้มีการออกนโยบาย กฎหมายและมาตรการต่างๆในการควบคุมกำกับดูแลสกุลเงินเข้ารหัสได้อย่างรอบคอบ ทั้งประเด็นในด้านธุรกิจการให้บริการเงินเสมือนและประเด็นในด้านการเป็นเครื่องมือในการลงทุน โดยภายใต้มาตรการต่างๆเหล่านี้ยังถูกควบคุมด้วยกลไกการตรวจสอบการฟอกเงินอีกชั้นหนึ่งด้วย อีกทั้งยังมีแนวทางการปฏิบัติในการบังคับคดีที่เกี่ยวกับสกุลเงินเข้ารหัส เช่น การยึด/อายัดสกุลเงินเข้ารหัสที่เป็นรูปธรรมสามารถปฏิบัติได้จริงอีกด้วย

3.3.4 สหพันธรัฐรัสเซีย

ในปี ค.ศ.2016 รัฐบาลรัสเซียประกาศเตือนว่าการซื้อขายสกุลเงินเข้ารหัสในประเทศรัสเซียเป็นสิ่งผิดกฎหมายเนื่องจากขัดกับมาตรา 140 ของประมวลกฎหมาย Russian Civil Code ที่วางหลักไว้ว่าการแสดงราคาและการชำระสินค้าและบริการในประเทศรัสเซียต้องใช้เงินตราสกุลรูเบิลเท่านั้น แต่ต่อมาในปี ค.ศ. 2017 หน่วยงานกลางที่มีหน้าเกี่ยวกับการจัดเก็บภาษีของรัสเซีย หรือ Federal Tax Service ได้มีการศึกษาและเสนอนโยบายและออกร่างกฎหมายรองรับการทำธุรกรรมด้วยสกุลเงินเข้ารหัส โดยร่างกฎหมายดังกล่าวระบุว่า **สกุลเงินเข้ารหัสเป็นสินทรัพย์ทางการเงินดิจิทัล (Digital Financial Asset) ประเภทหนึ่ง แต่ยังไม่รับรองให้ใช้เป็นสื่อกลางของระบบชำระเงินและยังไม่รับรองให้นำไปชำระหนี้ได้ตามกฎหมาย** ส่วนในประเด็นการด้านการระดมทุนผ่านการเสนอขายสกุลเงินเข้ารหัส หรือ ICO ร่างกฎหมายฉบับดังกล่าวยังมีการจำกัดให้นักลงทุนที่ไม่ได้รับการรับรองจากหน่วยงานของรัฐ เข้าร่วมการระดมทุนแบบ ICO ได้สูงสุดไม่เกิน 900 ดอลลาร์สหรัฐ รวมทั้งยังมีเป้าหมายจะขึ้นทะเบียนนักทำเหมืองหรือนักขุด (Miner) รวมถึงให้ทำการซื้อขายคริปโทเคอร์เรนซีใน ตลาดที่มีใบอนุญาตเท่านั้น (พรชัย ชุนหจินดา, 2561)

ส่วนแนวโน้มนโยบายเกี่ยวกับสกุลเงินเข้ารหัสของรัสเซีย เป็นไปในแนวทางที่จะมีการยอมรับและพัฒนาสกุลเงินเข้ารหัสมากขึ้น เห็นได้จากรายงานข่าวล่าสุดว่าประธานาธิบดีวลาดิมีร์ ปูติน (Vladimir Putin) ได้สั่งการให้รัฐบาลรัสเซียทำการปรับปรุงแก้ไขกฎหมายเพื่อให้สามารถนำมาใช้บังคับและกำกับดูแลสกุลเงินเข้ารหัสให้ครอบคลุมภายในเดือนกรกฎาคม ค.ศ.2019 โดยได้สั่งการให้รัฐบาลเร่งทำงานร่วมกันกับสภาดูมา (State Duma) ซึ่งเป็นสภาล่างของรัสเซียเพื่อร่วมกันพิจารณาออกกฎหมายต่างๆที่จะสนับสนุนและพัฒนาระบบเศรษฐกิจดิจิทัล (Digital Economy) ของรัสเซีย โดยแนวทางการออกกฎหมายดังกล่าวประกอบไปด้วย การพิจารณาแก้ไขเพิ่มเติมกฎหมายแพ่งและพาณิชย์เดิม ในการกำหนดขั้นตอนการทำธุรกรรมในรูปแบบอิเล็กทรอนิกส์ มาตรการควบคุมและกำกับดูแลสินทรัพย์ดิจิทัลรูปแบบต่างๆ ซึ่งหมายความรวมถึงสกุลเงินเข้ารหัสด้วย รวมถึงแนวทางการพัฒนาด้านการลงทุนและเพื่อดึงดูดให้นักลงทุนชาวต่างชาติเข้ามาลงทุนในรูปแบบดิจิทัลมากยิ่งขึ้น (Kevin Helms, 2019)

จากแนวนโยบาย กฎหมาย และมาตรการต่างๆของประเทศรัสเซียตามที่ได้กล่าวมานี้ทำให้สามารถวิเคราะห์ได้ว่ารัสเซียต้องการผลักดันให้เกิดการพัฒนาระบบเศรษฐกิจตามนโยบายเศรษฐกิจดิจิทัลเพื่อให้สามารถแข่งขันกับชาติมหาอำนาจคู่แข่งอย่างสหรัฐเมริกาได้ และด้วย

สถานการณ์การใช้สกุลเงินเข้ารหัสเป็นจำนวนมากทั่วโลกจึงทำให้รัสเซียมองเห็นโอกาสอันดีที่จะนำสกุลเงินเข้ารหัสมาเป็นเครื่องมือหนึ่งในการกระตุ้นให้เกิดการเติบโตของระบบเศรษฐกิจในยุคใหม่ จึงเร่งให้มีการศึกษาและออกกฎหมายเพื่อให้สอดคล้องและสามารถใช้กำกับดูแลสกุลเงินเข้ารหัสในฐานะสินทรัพย์ดิจิทัลประเภทหนึ่งได้อย่างมีประสิทธิภาพต่อไป

3.3.5 สวิตเซอร์แลนด์

สวิตเซอร์แลนด์เป็นประเทศที่มีชื่อเสียงด้านสถาบันทางการเงินและธนาคารเป็นอย่างมาก ดังนั้นจึงเป็นที่น่าสนใจที่จะศึกษาว่าสวิตเซอร์แลนด์มีแนวนโยบายเกี่ยวกับสกุลเงินเข้ารหัสอย่างไร โดยเริ่มตั้งแต่ปี ค.ศ. 2013 ที่สมาชิกรัฐสภาสวิตเพื่อความยั่งยืนทางดิจิทัล (Pardigli) จำนวน 45 คน ได้เรียกร้องให้รัฐบาลสวิตพิจารณาและประเมินโอกาสที่จะเกิดจากการใช้ประโยชน์บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เพื่อให้เกิดการกระตุ้นภาคการเงินของประเทศ นอกจากนี้ยังเสนอให้มีการกำหนดสถานภาพทางกฎหมายของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆให้ชัดเจน เนื่องจากการกำหนดสถานภาพที่ชัดเจนจะส่งผลต่อการกำกับดูแลในประเด็นที่เกี่ยวกับการจัดเก็บภาษี การลงทุนในตลาดหลักทรัพย์ และการจัดการเกี่ยวกับการฟอกเงินด้วย (Wiebel Thomas, 2013)

ต่อมาในปี ค.ศ. 2014 สภาสหพันธรัฐสวิต (The Swiss Federal Council) ได้เผยแพร่รายงานเกี่ยวกับสกุลเงินเข้ารหัสโดยได้อธิบายถึงความสำคัญในแง่ของการเป็นเครื่องมือกระตุ้นภาคเศรษฐกิจ การควบคุมกำกับดูแลด้วยกฎหมายและความเสี่ยงต่างๆ โดยในรายงานฉบับนี้มีการระบุว่าสกุลเงินเข้ารหัส (Cryptocurrency) มีความหมายทั่วไปเหมือน เงินเสมือน (Virtual Currency) คือเป็นตัวแทนที่ระบุมูลค่าที่อยู่ในรูปแบบอิเล็กทรอนิกส์ ใช้สำหรับซื้อขายแลกเปลี่ยนกันในลักษณะเดียวกันกับเงิน แต่ไม่สามารถนำไปใช้ชำระหนี้กันได้ตามกฎหมาย (Legal Tender) ดังนั้น สกุลเงินเข้ารหัสจึงอาจถูกจัดเป็นสินทรัพย์ประเภทหนึ่งได้ ภายหลังจากที่รายงานดังกล่าวถูกเผยแพร่ออกมาทำให้มุมมองในด้านนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศสวิตเซอร์แลนด์เปลี่ยนไป เพราะแม้ในรายงานดังกล่าวจะได้มีการประเมินและแจ้งเตือนถึงความเสี่ยงที่อาจเกิดขึ้นจากการใช้สกุลเงินเข้ารหัสไปเกี่ยวข้องกับการฟอกเงิน การสนับสนุนเงินทุนให้กับผู้ก่อการร้าย และยังมีประเด็นที่จะต้องคุ้มครองนักลงทุนอีกมากก็ตาม แต่ในขณะเดียวกันรายงานดังกล่าวก็ได้เน้นหนักไปถึงประโยชน์ในเชิงเศรษฐกิจที่จะเกิดขึ้นมากมายมหาศาลนำสกุลเงินเข้ารหัสซึ่งถือเป็นเทคโนโลยีสมัยใหม่มาใช้ ดังนั้น จึงมีความจำเป็นที่จะต้องปรับปรุงแก้ไขกฎหมายหรือกฎระเบียบของสถาบันทางการเงินต่างๆ ที่ยังมีส่วนในการขัดขวางไม่ให้มีการพัฒนาในด้านเทคโนโลยี

ทางการเงิน (Fintech) ได้ เช่น ผู้ให้บริการชำระเงินด้วยสกุลเงินเข้ารหัสผ่านโทรศัพท์มือถือและการบริการให้กู้ยืมเงินแบบ Peer-to-Peer เป็นต้น ในขณะเดียวกันหน่วยงานกำกับดูแลด้านการตลาดทางการเงินของสวิต หรือ The Swiss Financial Market Supervisory Authority (*FINMA*) ได้ออกมาประกาศว่าพระราชบัญญัติความผิดเกี่ยวกับการฟอกเงินจะขยายขอบเขตให้ครอบคลุมถึงสกุลเงินเข้ารหัสด้วย ต่อมาในปี ค.ศ. 2018 สำนักงานเลขาธิการแห่งรัฐสวิตว่าด้วยการเงินระหว่างประเทศ หรือ Staatssekretariat für internationale Finanzfragen (SIF) ได้รายงานว่าได้มีการตั้งคณะทำงานร่วมกันเพื่อทำการศึกษาเกี่ยวกับระบบบล็อคเชน (Blockchain) และการระดมทุนผ่านการเสนอขายสกุลเงินเข้ารหัสต่างๆ (Initial Coin Offering หรือ ICO) โดยคณะทำงานดังกล่าวจะทำงานร่วมกับกระทรวงยุติธรรมและหน่วยงานกำกับดูแลด้านการตลาดทางการเงินของสวิต (*FINMA*) รวมทั้งภาคธุรกิจต่างๆที่ให้ความสนใจเพื่อศึกษาเกี่ยวกับกรอบกฎหมายที่เกี่ยวข้องเพื่อเสนอความเห็นแก่สภาสูงและนำไปสู่การเสนอร่างกฎหมาย เพื่อให้สอดคล้องกับแนวนโยบายหลักของประเทศที่ต้องการให้เกิดนวัตกรรมทางการเงินสมัยใหม่ (Jenny Gesley, 2018)

ในประเด็นการการจัดเก็บภาษีนั้น สวิตเซอร์แลนด์ได้กำหนดมาตรการไว้อย่างชัดเจน เช่น หากผู้ได้รับเงินได้เป็นบิทคอยน์หรือสกุลเงินเข้ารหัสสกุลอื่นๆ ก็จะต้องนำมูลค่าของบิทคอยน์หรือสกุลเงินอื่นๆที่ได้รับขณะนั้นเทียบเป็นสกุลเงินของสวิตเซอร์แลนด์แล้วนำมาคำนวณเพื่อเสียภาษีเงินได้ตามปกติ หรือ กรณีของผู้ที่ทำเหมืองหรือทำการขุด (Miner) เมื่อได้รับบิทคอยน์หรือสกุลเงินเข้ารหัสสกุลต่างๆมา ก็จะต้องเสียภาษีเงินได้เพิ่มเติมตามมูลค่าของบิทคอยน์หรือสกุลเงินเข้ารหัสที่ได้รับมาด้วย อีกทั้ง มาตรการการจัดเก็บภาษีนี้ยังรวมถึงผู้ประกอบกิจการรับแลกเปลี่ยนสกุลเงินเข้ารหัสจะต้องนำผลกำไรมาคำนวณเพื่อเสียภาษีด้วย (Jenny Gesley, 2018)

3.4 แนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

3.4.1 แนวนโยบายเกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

ประเทศไทยเป็นประเทศหนึ่งที่มีผู้ใช้งานสกุลเงินเข้ารหัสเป็นจำนวนมากเช่นกัน โดยแนวนโยบายเกี่ยวกับสกุลเงินเข้ารหัสของประเทศไทยสามารถอธิบายตามช่วงเวลาได้ดังนี้

พ.ศ.2557 ธนาคารแห่งประเทศไทยได้มีประกาศฉบับที่ 8/2557 ลงวันที่ 18 มีนาคม 2557 เรื่องข้อมูลเกี่ยวกับ Bitcoin และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่นๆที่ลักษณะใกล้เคียงกัน โดยเนื้อหาในประกาศฉบับนี้นั้นได้ความรู้เกี่ยวกับความหมายของ บิทคอยน์และสกุลเงินเข้ารหัสสกุลอื่นๆ

รวมทั้งแจ้งเตือนถึงความเสี่ยงในการครอบครองสกุลเงินเข้ารหัสที่มีมูลค่าเปลี่ยนแปลงได้อย่างรวดเร็ว และอาจได้รับความเสียหายจากการปิดตัวไปอย่างกะทันหันของบริษัทตัวกลางที่ทำหน้าที่ในการแลกเปลี่ยนสกุลเงินเข้ารหัสเหล่านี้ นอกจากนี้ยังได้ระบุข้อแนะนำประชาชน ดังนี้ (ธนาคารแห่งประเทศไทย, 2557)

*"3.1 หน่วยข้อมูลทางอิเล็กทรอนิกส์นี้**ไม่ถือเป็นเงินที่ใช้ชำระหนี้ได้ตามกฎหมายไทย** การใช้หน่วยข้อมูลดังกล่าวในการชำระค่าสินค้าหรือบริการจึงอาจถูกปฏิเสธจากร้านค้าได้*

3.2 มีความเสี่ยงจากการที่มูลค่าหน่วยข้อมูลทางอิเล็กทรอนิกส์ผันแปรอย่างรวดเร็ว เนื่องจากมูลค่าของหน่วยข้อมูลอิเล็กทรอนิกส์เกิดจากความต้องการแลกเปลี่ยนในกลุ่มของผู้ใช้ด้วยกัน มูลค่าจึงมีความผันผวนสูงและไม่สัมพันธ์กับสภาพเศรษฐกิจจริง ผู้ถือครองหน่วยข้อมูลจึงมีความเสี่ยงที่จะสูญเสียเงินจากการที่มูลค่าของหน่วยข้อมูลลดลงอย่างรวดเร็ว และหากร้านค้าใดรับหน่วยข้อมูล ดังกล่าวเพื่อแลกเปลี่ยนกับสินค้าและบริการของตน ก็อาจมีความเสี่ยงที่หน่วยข้อมูลที่ได้รับมาและถือไว้นั้นอาจมีมูลค่าหรือราคาลดลงได้ตลอดเวลาอย่างรวดเร็วจากมูลค่าหรือราคาเดิม ณ ขณะที่ตนได้ รับมา

*3.3 มีความเสี่ยงจาก**การถูกขโมยข้อมูล** เนื่องจากหน่วยข้อมูลอิเล็กทรอนิกส์ดังกล่าว จะต้องจัดเก็บไว้ในอุปกรณ์คอมพิวเตอร์เท่านั้น จึงมีความเสี่ยงที่ผู้ถือครองอาจสูญเสียหน่วยข้อมูล ดังกล่าวได้จากการถูกลักลอบโจรกรรมข้อมูล*

*3.4 มีความเสี่ยงที่**ผู้ใช้ไม่ได้รับการคุ้มครอง** เนื่องจากหน่วยข้อมูลอิเล็กทรอนิกส์ดังกล่าว ไม่ได้เป็นสื่อการชำระเงินตามกฎหมาย ดังนั้น หากมีการใช้เป็นช่องทางในการหลอกลวงหรือฉ้อโกง หรือกรณีที่เกิดปัญหาในการใช้งาน เช่น การโอนไปยังผู้รับผิดคนหรือผิดจำนวน หรือโอนไปยังร้านค้า แล้วแต่ไม่ได้รับสินค้า การติดตามข้อมูลการโอนเพื่อใช้เป็นพยานหลักฐานอาจทำได้ยากหากต้องฟ้องร้องดำเนินคดี ซึ่งต่างจากการโอนเงินผ่านธนาคารพาณิชย์หรือผู้ให้บริการชำระเงินภายใต้การกำกับดูแลของทางการที่มีระบบติดตามได้"*

จะเห็นได้ว่า จากข้อแนะนำที่ทางธนาคารแห่งประเทศไทยแนะนำให้ประชาชนรับทราบนั้น ธนาคารแห่งประเทศไทยระบุชัดเจนว่า **สกุลเงินเข้ารหัสไม่ถือเป็นเงินที่ชำระหนี้ได้ตามกฎหมายไทย และผู้ใช้จะไม่ได้รับความคุ้มครอง**

พ.ศ.2561 เมื่อวันที่ 12 กุมภาพันธ์ 2561 ธนาคารแห่งประเทศไทยได้มีหนังสือแจ้งไปยังผู้จัดการสถาบันการเงินทุกแห่ง **เรื่อง ขอความร่วมมือสถาบันการเงินไม่ให้ทำธุรกรรมที่เกี่ยวข้อง**

กับคริปโตเคอเรนซี (Cryptocurrency) โดยมีใจความสำคัญว่า ธนาคารแห่งประเทศไทยเล็งเห็นประเด็นปัญหาที่อาจเกิดขึ้นจากการทำธุรกรรมที่เกี่ยวข้องกับคริปโตเคอเรนซี **โดยเฉพาะประเด็นที่ไม่สามารถระบุตัวตนผู้ออกได้อย่างชัดเจน** ไม่มีสินทรัพย์ค้ำประกันตามมูลค่าหรือไม่มีทรัพย์สินอ้างอิง โดยได้ขอความร่วมมือสถาบันการเงินต่างๆไม่ให้ทำธุรกรรมหรือมีส่วนร่วมในการสนับสนุนการทำธุรกรรมเกี่ยวกับสกุลเงินเข้ารหัส ดังนี้ (ธนาคารแห่งประเทศไทย, 2561)

"1.การเข้าไปลงทุนหรือซื้อขายในคริปโตเคอเรนซี่เพื่อผลประโยชน์ของสถาบันการเงินเองหรือผลประโยชน์ของลูกค้า

2.การให้บริการรับแลกเปลี่ยนคริปโตเคอเรนซี่ผ่านช่องทางให้บริการของสถาบันการเงิน

3.การสร้างแพลตฟอร์ม (Platform) เพื่อเป็นสื่อกลางให้ลูกค้าเข้าไปทำธุรกรรมเกี่ยวกับคริปโตเคอเรนซี่ระหว่างกัน

4.การให้ลูกค้าใช้บัตรเครดิตในการซื้อคริปโตเคอเรนซี่

5.การสนับสนุนหรือให้คำปรึกษากับลูกค้าเกี่ยวกับการลงทุนหรือการแลกเปลี่ยนคริปโตเคอเรนซี่"

จากการขอความร่วมมือดังกล่าวแสดงให้เห็นได้ว่า ธนาคารแห่งประเทศไทยต้องการให้สถาบันการเงินทุกแห่ง**ห้ามดำเนินการใดๆที่มีความเกี่ยวกับคริปโตเคอเรนซี หรือ สกุลเงินเข้ารหัสในทุกกรณี**

ภายหลังจากประกาศ 2 ฉบับดังกล่าวจากธนาคารแห่งประเทศไทย ทำให้สถานะของสกุลเงินเข้ารหัสในประเทศไทยตกอยู่ในสภาวะ**สุญญากาศ**ในทันที กล่าวคือ สกุลเงินเข้ารหัสไม่ถือเป็นเงินตามกฎหมายไทยและไม่สามารถชำระหนี้ตามกฎหมายได้ **แต่ไม่ได้ระบุว่าการครอบครองหรือการทำธุรกรรมหรือการซื้อขายเพื่อเก็งกำไรในมูลค่าสกุลเงินเข้ารหัสผิดกฎหมายหรือไม่** เพียงแต่มีการขอความร่วมมือไปยังสถาบันการเงินทุกสถาบันไม่ให้เข้าไปยุ่งเกี่ยวหรือแนะนำประชาชนทุกกรณี ดังนั้นผู้ศึกษาจึงมีมุมมองว่ารัฐบาลไทย ณ ขณะนั้นได้ผลักภาระความเสี่ยงให้กับผู้ต้องการถือครองสกุลเงินเข้ารหัส โดยที่รัฐและสถาบันการเงินปฏิเสธความเกี่ยวข้องในทุกกรณีถ้าเกิดปัญหาใดๆขึ้น

ต่อมาปรากฏว่า เมื่อวันที่ 10 พฤษภาคม 2561 (หลังจากที่ธนาคารแห่งประเทศไทยมีการประกาศขอความร่วมมือไปยังสถาบันการเงินต่างๆเพียง 2 เดือน) ได้มีการออก พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 ขึ้นมาบังคับใช้โดยมีวัตถุประสงค์หลักคือ เพื่อให้การประกอบธุรกิจ

สินทรัพย์ดิจิทัล (สกุลเงินเข้ารหัสและโทเคนดิจิทัลต่างๆ) อยู่ในความควบคุมดูแลของรัฐ โดยหากผู้ใดต้องการจะประกอบธุรกิจในการเป็นศูนย์ซื้อขายทรัพย์สินดิจิทัล เป็นนายหน้าซื้อขายทรัพย์สินดิจิทัล ผู้ค้าทรัพย์สินดิจิทัล รวมทั้งกิจการอื่นๆที่เกี่ยวกับทรัพย์สินดิจิทัล จะต้องได้รับอนุญาตจากคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และจะต้องดำเนินการตามที่กฎหมายนี้กำหนด โดยหากฝ่าฝืนจะมีโทษทั้งทางแพ่งและทางอาญา โดยเมื่อวิเคราะห์ถึงเจตนารมณ์ในการออกกฎหมายนี้แล้วก็จะพบว่า เป็นไปเพื่อการรักษาเสถียรภาพในทางการเงินของประเทศ และป้องกันความเสียหายที่อาจจะเกิดขึ้นในกรณีของการซื้อขายสกุลเงินเข้ารหัสหรือการระดมทุนโดยการใช้สกุลเงินเข้ารหัสในวงกว้างได้ โดยจะได้กล่าวถึงบทบัญญัติที่เป็นมาตรการสำคัญในกฎหมายนี้ต่อไป

จากข้อมูลที่กล่าวมานี้ทำให้สามารถวิเคราะห์ได้ว่าประเทศไทยมีการตื่นตัวต่อสถานการณ์การใช้งานสกุลเงินเข้ารหัสโดยทิศทางของแนวนโยบายในช่วงแรกจะเป็นไปในลักษณะของการคุ้มครองความปลอดภัยให้แก่ประชาชนด้วยการแจ้งเตือนถึงความเสี่ยง แต่ในขณะเดียวกันก็ยังไม่ได้ใช้มาตรการบังคับหรือการปฏิเสธอย่างเข้มแข็งต่อการใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ และภายหลังจากที่หน่วยงานภาครัฐที่เกี่ยวข้องได้ทำการศึกษาและประเมินสถานการณ์แล้วจึงได้เสนอออกกฎหมายเฉพาะขึ้นมากำกับดูแลบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ

3.4.2 พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561

ตามที่ได้กล่าวมาแล้วว่า กฎหมายดังกล่าวนี้ถือเป็นกฎหมายเฉพาะที่มุ่งจะควบคุมกำกับดูแลการใช้งานสกุลเงินเข้ารหัสต่างๆ ในส่วนที่เน้นหนักไปทางด้านการประกอบธุรกิจเป็นสำคัญ โดยมีสาระสำคัญและมาตรการต่างๆที่เกี่ยวข้อง ดังนี้

1) การบัญญัติรับรองให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆมีสถานะเป็นสินทรัพย์ดิจิทัล

โดยจะเห็นได้จากบทบัญญัติในมาตรา 3 ที่บัญญัติไว้ว่า *“คริปโทเคอร์เรนซี หมายความว่า หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และให้หมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นใดตามที่คณะกรรมการ ก.ล.ต.ประกาศกำหนด”* และ *“สินทรัพย์ดิจิทัล หมายถึง คริปโทเคอร์เรนซีและโทเคนดิจิทัล”* ซึ่งด้วยผลของบทบัญญัติตามกฎหมายดังกล่าวจึงทำให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆมี

สถานะเป็นทรัพย์สินตามกฎหมายในรูปแบบของสินทรัพย์ดิจิทัล แต่อย่างไรก็ตาม**กฎหมายนี้ยังไม่ได้บัญญัติให้สินทรัพย์ดิจิทัลถือเป็นเงินที่ชำระหนี้ได้ตามกฎหมายไทยแต่อย่างใด**

2) มีการกำหนดมาตรการที่เกี่ยวข้องกับการป้องกันการฟอกเงิน

โดยมาตรการดังกล่าวปรากฏอยู่ใน มาตรา 7 ที่บัญญัติไว้ว่า *"ให้ถือว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลและผู้ให้บริการระบบเสนอขายโทเคนดิจิทัลตามพระราชกำหนดนี้ เป็นสถาบันการเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน"* ซึ่งแสดงให้เห็นว่ากฎหมายนี้มีความพยายามที่จะเป็นกลไกสำคัญในการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการฟอกเงินด้วย

3) ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจะต้องได้รับอนุญาตจากรัฐ

เพื่อให้การประกอบธุรกิจสินทรัพย์ดิจิทัลอยู่ภายใต้การควบคุมกำกับดูแลของรัฐ กฎหมายนี้จึงได้บัญญัติให้ผู้ที่ต้องการจะประกอบธุรกิจสินทรัพย์ดิจิทัลจะต้องได้รับอนุญาตก่อน โดยได้บัญญัติหลักการดังกล่าวไว้ใน มาตรา 26 ว่า *"ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลต้องได้รับอนุญาตจากรัฐมนตรีตามข้อเสนอแนะของคณะกรรมการ ก.ล.ต."*

4) การกำหนดหลักเกณฑ์ต่างๆเพื่อควบคุมการประกอบธุรกิจสินทรัพย์ดิจิทัล

นอกจากมาตรการที่กำหนดให้การประกอบธุรกิจสินทรัพย์ดิจิทัลจะต้องได้รับอนุญาตจากรัฐแล้ว ภายหลังจากที่ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลได้รับอนุญาตแล้ว ยังจะต้องดำเนินการให้เป็นไปตามหลักเกณฑ์และวิธีการต่างๆที่กฎหมายกำหนดด้วย โดยในมาตรา 30 ได้บัญญัติถึงหลักเกณฑ์และวิธีการต่างๆ ดังนี้

"(1) การมีแหล่งเงินทุนที่เพียงพอสำหรับการรองรับการประกอบธุรกิจและความเสี่ยงในด้านต่างๆ

(2) ความปลอดภัยของทรัพย์สินของลูกค้า

(3) การรักษาความปลอดภัยจากการโจรกรรมทางอิเล็กทรอนิกส์เพื่อป้องกันระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ รวมถึงการบริหารจัดการความเสี่ยงที่เกิดจากการโจรกรรมหรือเหตุอื่นๆ

(4) การมีระบบบัญชีที่เหมาะสมกับกิจการและจักให้มีการสอบบัญชีโดยผู้สอบบัญชีที่สำนักงาน ก.ล.ต. ให้ความเห็นชอบ

(5) การมีมาตรการการรู้จักลูกค้า การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า และมาตรการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้ายหรือการฟอกเงิน"

5) การกำหนดมาตรการลงโทษทั้งในทางอาญาและทางแพ่ง

เพื่อให้การควบคุมกำกับดูแลการประกอบธุรกิจสินทรัพย์ดิจิทัล เป็นไปอย่างมีประสิทธิภาพ กฎหมายนี้จึงได้มีการกำหนดบทลงโทษกรณีที่ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลฝ่าฝืนหรือไม่ปฏิบัติตาม โดยมีมาตรการการลงโทษทั้งในทางอาญาและทางแพ่งดังปรากฏในหมวด 8 และหมวด 9 ของกฎหมายนี้ ตัวอย่างเช่น ในมาตรา 66 ที่บัญญัติไว้ว่า *"ผู้ใดประกอบธุรกิจสินทรัพย์ดิจิทัลโดยมิได้รับอนุญาตตามมาตรา 26 ต้องระวางโทษจำคุกตั้งแต่สองปีถึงห้าปี และปรับตั้งแต่สองแสนบาทถึงห้าแสนบาท และปรับอีกไม่เกินวันละหนึ่งหมื่นบาทตลอดเวลาที่ยังฝ่าฝืนอยู่"* ซึ่งเป็นมาตรการในทางอาญา และในมาตรา 98 ที่บัญญัติเกี่ยวกับมาตรการในทางแพ่งว่า

"มาตรการลงโทษทางแพ่ง ได้แก่

(1) ค่าปรับทางแพ่ง

(2) ชดใช้เงินในจำนวนที่เท่ากับผลประโยชน์ที่ได้รับหรือพึงได้รับจากการกระทำความผิดตามที่บัญญัติไว้ในมาตรา 96

(3) ห้ามเข้าซื้อขายสินทรัพย์ดิจิทัลในศูนย์ซื้อขายสินทรัพย์ดิจิทัลหรือเข้าผูกพันตามสัญญาซื้อขายล่วงหน้าที่เกี่ยวข้องกับสินทรัพย์ดิจิทัลภายในระยะเวลาที่กำหนดซึ่งต้องไม่เกินห้าปี

(4) ห้ามเป็นกรรมการหรือผู้บริหารของผู้เสนอขายโทเคนดิจิทัลหรือผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลภายในระยะเวลาที่กำหนดซึ่งต้องไม่เกินสิบปี

(5) ชดใช้ค่าใช้จ่ายของสำนักงาน ก.ล.ต. เนื่องจากการตรวจสอบการกระทำความผิดนั้นคืนให้แก่สำนักงาน ก.ล.ต.

จากการศึกษาสาระสำคัญและมาตรการต่างๆที่บัญญัติไว้ใน พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ทำให้สามารถวิเคราะห์ได้ว่า กฎหมายดังกล่าวมุ่งที่จะควบคุมกำกับดูแลเฉพาะการประกอบธุรกิจสินทรัพย์ดิจิทัลเท่านั้น **ยังมิได้มีเจตนารมณ์ที่ชัดเจนที่จะป้องกันการนำบิทคอยน์หรือสกุลเงินเข้ารหัสที่ถือเป็นสินทรัพย์ดิจิทัลไปใช้ในการก่ออาชญากรรมแต่อย่างใด** เห็นได้จากการที่กฎหมายกำหนดให้มีการขออนุญาตและใช้มาตรการการรู้จักลูกค้าเฉพาะกับผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสที่ใช้งานหรือมีการซื้อขายแลกเปลี่ยนผ่านผู้ประกอบธุรกิจสินทรัพย์

ดิจิทัลเท่านั้น และถึงแม้จะมีการกำหนดหลักเกณฑ์เกี่ยวกับการป้องกันการฟอกเงินก็ตาม แต่ปรากฏว่าไม่ได้มีการกำหนดมาตรการในทางปฏิบัติที่ชัดเจนแต่อย่างใด ตลอดจนการกำหนดให้พฤติกรรมต่างๆเป็นความผิดตามกฎมหมายนั้น ก็ไม่มีการบัญญัติให้การนำบิทคอยน์และสกุลเงินเข้ารหัสไปใช้ในการก่ออาชญากรรมเป็นความผิดตามกฎหมายนี้ ทั้งยังไม่มีการกำหนดบทลงโทษในกรณีดังกล่าว ทั้งนี้หากเกิดกรณีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นเครื่องมือในการกระทำผิดรูปแบบต่างๆแล้ว ก็จำเป็นที่เจ้าหน้าที่ของรัฐจะต้องนำหลักกฎหมายที่เกี่ยวข้องอย่าง พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ และประมวลกฎหมายวิธีพิจารณาความอาญามาปรับใช้ดังจะได้กล่าวต่อไป

3.4.3 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

แม้การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดนั้น จำเป็นจะต้องกระทำบนระบบคอมพิวเตอร์ เนื่องจากบิทคอยน์และสกุลเงินเข้ารหัสต่างๆอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ แต่อย่างไรก็ตามมิได้หมายความว่าการกระทำความผิดในลักษณะนี้จะถือเป็นความผิดตามกฎหมายนี้ทุกกรณี เนื่องจากเมื่อศึกษาถึงตัวบทบัญญัติของกฎหมายแล้วจะพบว่า ใน พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 หมวด 1 ความผิดเกี่ยวกับคอมพิวเตอร์นั้น มุ่งเน้นไปที่การกำหนดให้การกระทำความผิดในลักษณะของการพยายามลักลอบเข้าถึงคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่นหรือที่ตนไม่ได้มีสิทธิ์เข้าถึง การดักรับข้อมูล การนำเข้าข้อมูลอันเป็นเท็จ หรือข้อมูลที่อาจเกิดความเสียหายและเป็นภัยต่อความมั่นคงเป็นสำคัญ **ยังคงไม่ครอบคลุมถึงการกระทำความผิดตามกฎหมายที่มีโทษทางอาญาอื่นๆผ่านการใช้คอมพิวเตอร์หรือระบบคอมพิวเตอร์ด้วย** โดยใน พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.2550 นี้มีข้อกฎหมายที่สามารถนำมาปรับใช้กับการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นเครื่องมือในการกระทำผิดได้ในกรณีของ การใช้โปรแกรมเรียกค่าไถ่ (Ransomware) เนื่องจากการที่คนร้ายใช้โปรแกรมลักลอบเข้าไปยึดระบบคอมพิวเตอร์ของเหยื่อ เพื่อเรียกร้องให้จ่ายค่าไถ่เป็นบิทคอยน์นั้น เข้าองค์ประกอบความผิดในมาตรา 10 ที่บัญญัติไว้ว่า *“ผู้ใดกระทำด้วยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษจำคุกไม่เกินห้าปี และปรับไม่เกินหนึ่งแสนบาท หรือทั้งจำทั้งปรับ”*

ต่อมาใน พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่ 2) พ.ศ.2560 จึงได้มีการบัญญัติให้พนักงานเจ้าหน้าที่มีอำนาจสืบสวนรวบรวมพยานหลักฐานต่างๆในกรณีที่มีการกระทำความผิดทางอาญาในกฎหมายอื่น โดยอาศัยอำนาจและวิธีการตามกฎหมายนี้ โดยมีข้อบัญญัติแก้ไขใน มาตรา 18 ความว่า

“เพื่อประโยชน์ในการสืบสวนและสอบสวนของพนักงานสอบสวนตามประมวลกฎหมายวิธีพิจารณาความอาญา ในบรรดาความผิดอาญาต่อกฎหมายอื่นซึ่งได้ใช้ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ หรืออุปกรณ์ที่ใช้เก็บข้อมูลคอมพิวเตอร์เป็นองค์ประกอบหรือเป็นส่วนหนึ่งในการกระทำความผิด หรือมีข้อมูลคอมพิวเตอร์ที่เกี่ยวข้องกับการกระทำความผิดอาญาตามกฎหมายอื่น พนักงานสอบสวน อาจร้องขอให้พนักงานเจ้าหน้าที่ตามวรรคหนึ่งดำเนินการตามวรรคหนึ่งก็ได้ หรือหากปรากฏข้อเท็จจริง ดังกล่าวต่อพนักงานเจ้าหน้าที่เนื่องจากการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานเจ้าหน้าที่ รีบรวบรวมข้อเท็จจริงและหลักฐานแล้วแจ้งไปยังเจ้าหน้าที่ที่เกี่ยวข้องเพื่อดำเนินการต่อไป”

ผลจากกฎหมายมาตรานี้ จึงทำให้เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องกับการสืบสวนสอบสวนในคดีที่เกี่ยวกับการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิด สามารถร้องขอให้พนักงานเจ้าหน้าที่ใช้อำนาจตามกฎหมายในการเก็บรวบรวมพยานหลักฐานต่างๆที่เกี่ยวข้องได้

นอกจากนี้ในประเด็นเรื่อง**การเข้าถึงข้อมูลเพื่อเก็บรวบรวมพยานหลักฐาน** ที่เกี่ยวข้องกับการกระทำความผิดนั้นแม้ในมาตรา 18 จะบัญญัติให้สามารถกระทำได้ แต่จะต้องได้รับอนุญาตจากศาลก่อนตามที่บัญญัติในมาตรา 19 ว่า

“การใช้อำนาจของพนักงานเจ้าหน้าที่ตามมาตรา 18 (8) และ (7) (6) (5) (4) ให้พนักงานเจ้าหน้าที่ยื่นคำร้องต่อศาลที่มีเขตอำนาจเพื่อมีคำสั่งอนุญาตให้พนักงานเจ้าหน้าที่ดำเนินการตามคำร้อง ทั้งนี้ คำร้องต้องระบุเหตุอันควรเชื่อได้ว่าบุคคลใดกระทำหรือกำลังจะกระทำการอย่างหนึ่ง อย่างใดอันเป็นความผิด เหตุที่ต้องใช้อำนาจ ลักษณะของการกระทำความผิด รายละเอียดเกี่ยวกับอุปกรณ์ ที่ใช้ในการกระทำความผิดและผู้กระทำความผิด เท่าที่สามารถจะระบุได้ ประกอบคำร้องด้วย ในการพิจารณา คำร้องให้ศาลพิจารณาคำร้องดังกล่าวโดยเร็ว”

จึงอาจกล่าวได้ว่า พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ทั้ง 2 ฉบับมีความเกี่ยวข้องเชื่อมโยงกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ทั้งในลักษณะที่กำหนดให้การกระทำความผิดผ่านระบบคอมพิวเตอร์ที่ชัดแจ้งอย่างการใช้โปรแกรมเรียกค่าไถ่ (Ransomware) เพื่อข่มขู่

ให้เหยื่อชำระค่าไถ่เป็นบิทคอยน์เป็นความผิดเกี่ยวกับคอมพิวเตอร์ตามกฎหมายนี้ ทั้งยังครอบคลุมถึงการให้อำนาจพนักงานเจ้าหน้าที่ในการเก็บรวบรวมพยานหลักฐานในกรณีของการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมผ่านระบบคอมพิวเตอร์รูปแบบอื่นๆ แต่ทั้งนี้ในการเข้าถึงข้อมูลอิเล็กทรอกนิกส์ต่างๆจะต้องได้รับอนุญาตจากศาล ซึ่งในประเด็นเรื่องการเข้าถึงข้อมูลอันเป็นพยานหลักฐานนี้มีความแตกต่างกันกับหลักการของประมวลวิธีพิจารณาความอาญาดังจะได้กล่าวต่อไป

3.4.4 ประมวลกฎหมายวิธีพิจารณาความอาญา

ประมวลกฎหมายวิธีพิจารณาความอาญาถือเป็นกฎหมายวิธีสบัญญัติที่เป็นเครื่องมือสำคัญของกระบวนการยุติธรรม เนื่องจากเป็นกฎหมายที่บัญญัติถึงขั้นตอนและวิธีการในการปฏิบัติหน้าที่ของเจ้าหน้าที่ในกระบวนการยุติธรรมขั้นตอนต่างๆ โดยในส่วนที่เกี่ยวข้องกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสนั้น นอกจากจะเป็นการอาศัยอำนาจตามกฎหมายนี้ในการสืบสวน จับ ค้น สอบสวน และการดำเนินการตามขั้นตอนอื่นๆที่เกี่ยวข้องแล้ว ยังมีประเด็นสำคัญที่ต้องพิจารณาคือการแสวงหาและการรวบรวมพยานหลักฐานที่ในประมวลกฎหมายวิธีพิจารณาความอาญาได้บัญญัติไว้ในลักษณะ 2 การสอบสวน หมวด 1 การสอบสวนสามัญ มาตรา 132 (2) ดังนี้

มาตรา 132 “เพื่อประโยชน์แห่งการรวบรวมหลักฐาน ให้พนักงานสอบสวนมีอำนาจ ดังต่อไปนี้

...(2) ค้นเพื่อพบสิ่งของ ซึ่งมีไว้เป็นความผิด หรือได้มาโดยการกระทำผิด หรือได้ใช้หรือสงสัยว่าได้ใช้ในการกระทำผิด หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ แต่ต้องปฏิบัติตามบทบัญญัติแห่งประมวลกฎหมายนี้ว่าด้วยค้น”

ด้วยบทบัญญัตตามมาตราดังกล่าว จึงทำให้สามารถตีความไปในทางหนึ่งได้ว่า ในกรณีของการเกิดอาชญากรรมเกี่ยวกับสกุลเงินเข้ารหัส พนักงานสอบสวนมีอำนาจในการค้นเพื่อพบข้อมูลอิเล็กทรอนิกส์ซึ่งมีไว้เป็นความผิด หรือได้มาโดยกระทำผิด หรือได้ใช้ในการกระทำความผิดซึ่งจะใช้เป็นพยานหลักฐานได้โดยอาศัยอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญาดังกล่าว ซึ่งผู้ศึกษาวิเคราะห์ว่าเป็นการตีความทางกฎหมายแบบกว้างขวาง ซึ่งหากพิจารณาตามหลักการของกฎหมายนี้แล้ว จะพบว่ามีความขัดแย้งกันกับวิธีการในการรวบรวมพยานหลักฐานต่างๆตามที่บัญญัติใน พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่วางหลักไว้ว่าพนักงานเจ้าหน้าที่จะได้รับอนุญาตจากศาลซึ่งหลักการทางกฎหมายที่แตกต่างกัน อาจนำไปสู่การตีความและการบังคับใช้

กฎหมายที่อาจเกิดความผิดพลาดหรือบกพร่องได้ ดังนั้น จึงจำเป็นจะต้องศึกษาถึงประเด็นปัญหาดังกล่าวต่อไป

จากการศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสทั้งในต่างประเทศและในประเทศไทยตามที่ได้กล่าวมานี้ พบว่าในประเด็นของแนวนโยบายนั้นมีเพียงประเทศจีนประเทศเดียวที่มีแนวนโยบายในการไม่ยอมรับสกุลเงินเข้ารหัสและมีการประกาศห้ามไม่ให้มีการใช้งานและดำเนินการใดๆที่เกี่ยวกับสกุลเงินเข้ารหัสภายในประเทศจีนโดยเด็ดขาด สำหรับประเทศอื่นๆ เช่น ญี่ปุ่น สหรัฐอเมริกา สหพันธรัฐรัสเซีย สวิตเซอร์แลนด์ รวมทั้งในประเทศไทยนั้นมีแนวนโยบายต่อสกุลเงินเข้ารหัสไปในทิศทางเดียวกันคือ มีการยอมรับว่าสกุลเงินเข้ารหัสเป็นสินทรัพย์ที่มีมูลค่าประเภทหนึ่งที่สามารถนำมาใช้ในการแลกเปลี่ยนสินค้าและบริการ นำไปใช้ในการแลกเปลี่ยนกับเงินตราจริง และสามารถนำไปใช้ในภาคการลงทุนได้ **แต่ยังไม่มีประเทศใดรับรองให้สกุลเงินเข้ารหัสเป็นสิ่งที่สามารถนำมาชำระหนี้กันได้ตามกฎหมาย** และในขณะเดียวกันแต่ละประเทศก็ได้มีการออกกฎหมายและมาตรการต่างๆมากำกับและควบคุมดูแลการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เช่น มาตรการทางภาษี มาตรการในการป้องกันการนำสกุลเงินเข้ารหัสไปใช้ในการฟอกเงิน เป็นต้น

สำหรับในประเทศไทยนั้นพบว่ามีการออกกฎหมายเฉพาะอย่าง พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 มาบังคับใช้โดยมีสาระสำคัญในการควบคุมกำกับดูแลการประกอบธุรกิจโดยมิได้มีมาตรการหรือการวางแนวทางที่เกี่ยวกับการป้องกันปราบปรามการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญกรรมแต่อย่างใด โดยในปัจจุบันหากเกิดกรณีของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสขึ้น ก็จำเป็นจะต้องอาศัยกฎหมายที่เกี่ยวข้องอย่าง พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ประมวลกฎหมายอาญาและประมวลกฎหมายวิธีพิจารณาความอาญามาปรับใช้ จึงทำให้อาจเกิดปัญหาในด้านการตีความหรือการอาศัยอำนาจตามกฎหมายมาใช้เทียบเคียงในการปฏิบัติหน้าที่ได้

3.5 แนวทางการปฏิบัติของหน่วยงานของรัฐที่มีหน้าที่เกี่ยวข้องในการปองกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในปัจจุบัน

3.5.1 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.)

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) เป็นหน่วยงานตำรวจในสังกัด กองบัญชาการตำรวจสอบสวนกลาง (บช.ก.) สำนักงานตำรวจแห่งชาติ เป็นหน่วยงานที่จัดตั้งขึ้น เมื่อวันที่ 7 กันยายน 2552 ตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ.2552, กฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่นในสำนักงานตำรวจแห่งชาติ พ.ศ.2552 และ ระเบียบสำนักงานตำรวจแห่งชาติว่าด้วยการกำหนดอำนาจหน้าที่ของส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ.2552 **มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับเทคโนโลยี สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญาและตามกฎหมายอื่นที่เกี่ยวกับระบบคอมพิวเตอร์** มีหน่วยงานภายในสังกัด 4 ส่วน ประกอบด้วย (กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี [บก.ปอท.], ม.ป.ป.)

1) กองกำกับการ 1: การกระทำผิดที่มุ่งต่อระบบคอมพิวเตอร์เป็นเป้าหมาย

2) กองกำกับการ 2: การใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด

3) กองกำกับการ 3: การนำเข้าเผยแพร่ข้อมูลคอมพิวเตอร์ สู่ระบบคอมพิวเตอร์ที่เป็นความผิด

4) กลุ่มงานสนับสนุนคดีเทคโนโลยี: ปฏิบัติการโต้ตอบในเชิงรุกโดยฉับพลันทางอินเทอร์เน็ต และสนับสนุนคดีเทคโนโลยี

แนวทางการปฏิบัติของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

เมื่อพิจารณาจากอำนาจหน้าที่ความรับผิดชอบแล้ว จะเห็นได้ว่าอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสมีลักษณะเป็นอาชญากรรมที่เกี่ยวกับเทคโนโลยีและอยู่ในความรับผิดชอบของกองบังคับ

การปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) เช่น **ในกรณีของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรงอย่างการนำบิทคอยน์ไปใช้ในการซื้อขายแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย จะต้องมีการใช้คอมพิวเตอร์เป็นเครื่องมือในการกระทำผิด** ดังนั้น ผู้วิจัยจึงได้ศึกษารวบรวมข้อมูลถึงแนวทางการปฏิบัติของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส โดยพันตำรวจตรีอิสรพงศ์ ทิพย์อาภากุล สารวัตรกองกำกับการ 3 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี ได้ให้ข้อมูลว่า **หน่วยงานไม่ได้มีการกำหนดแนวทางการปฏิบัติสำหรับคดีที่เกี่ยวกับสกุลเงินเข้ารหัสไว้เป็นการเฉพาะแต่อย่างใด แต่จะใช้ขั้นตอนการปฏิบัติงานตามปกติ ซึ่งเป็นไปตามบทบัญญัติของประมวลกฎหมายวิธีพิจารณาความอาญาและกฎหมายอื่นๆที่เกี่ยวข้อง เพื่อรองรับและจัดการกับคดีดังกล่าว** โดยมีขั้นตอนการปฏิบัติดังนี้ (อิสรพงศ์ ทิพย์อาภากุล, การสื่อสารส่วนบุคคล, 11 สิงหาคม 2562)

1) กรณีการป้องกันเหตุ หน่วยงานจะทำการประชาสัมพันธ์ผ่านสื่อทุกแขนงถึงพฤติการณ์หรือรูปแบบการกระทำความผิดของคนร้าย เพื่อให้ประชาชนทั่วไปทราบข้อมูลและสามารถป้องกันตนเองไม่ให้ตกเป็นเหยื่อได้

2) กรณีภายหลังเกิดเหตุ หรือกรณีที่มีการกระทำความผิดที่เป็นอาชญากรรมทางเทคโนโลยีเกิดขึ้น หน่วยงานจะดำเนินการสอบสวนปากคำผู้เสียหายเพื่อให้ทราบรายละเอียดเบื้องต้น จากนั้นจะทำการสืบสวนสอบสวนและเก็บรวบรวมพยานหลักฐานทางอิเล็กทรอนิกส์โดยผู้เชี่ยวชาญและเครื่องมือพิเศษ เพื่อเป็นการเก็บร่องรอยหลักฐานการกระทำความผิดในระบบคอมพิวเตอร์ จากนั้นจะใช้ทักษะและความชำนาญพิเศษในการวิเคราะห์พยานหลักฐานทางดิจิทัล เพื่อสืบสวนจนพบตัวผู้กระทำผิด จากนั้นจึงทำการสืบสวนและจับกุมตัวผู้กระทำผิดมาดำเนินคดีตามกฎหมาย

จากข้อมูลดังกล่าวจึงสามารถสรุปได้ว่า ในปัจจุบันกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ยังไม่มีการกำหนดแนวทางการปฏิบัติหน้าที่ที่เกี่ยวข้องกับอาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือไว้เป็นการเฉพาะ

3.5.2 กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.)

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) เดิมเคยใช้ชื่อว่า กองทะเบียนคนต่างด้าวและภาษีอากร, กองบังคับการสืบสวนสอบสวนคดีเศรษฐกิจ และ กองบังคับการปราบปรามอาชญากรรมทางเศรษฐกิจและเทคโนโลยี จนต่อมาเมื่อวันที่ 7 กันยายน 2552 สำนักงานตำรวจแห่งชาติได้มีการแบ่งส่วนราชการใหม่ ตามพระราชกฤษฎีกาแบ่งส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ.2552, กฎกระทรวงแบ่งส่วนราชการเป็นกองบังคับการหรือส่วนราชการอย่างอื่นในสำนักงานตำรวจแห่งชาติ พ.ศ.2552 และ ระเบียบสำนักงานตำรวจแห่งชาติว่าด้วยการกำหนดอำนาจหน้าที่ของส่วนราชการสำนักงานตำรวจแห่งชาติ พ.ศ.2552 และได้มีการจัดตั้งกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) ขึ้น เป็นหน่วยงานตำรวจในสังกัดกองบัญชาการตำรวจสอบสวนกลาง (บช.ก.) สำนักงานตำรวจแห่งชาติ **มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับภาษี ทรัพย์สินทางปัญญา และการเงินการธนาคาร สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และตามกฎหมายอื่นที่เกี่ยวข้อง** โดยมีการแบ่งโครงสร้างภายในตามหน้าที่ความรับผิดชอบดังนี้

1) กองกำกับการ 1 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับภาษีทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมาย อื่นที่เกี่ยวข้องกับงานภาษีทุกประเภทและความผิดที่เกี่ยวเนื่อง ในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือ สนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

2) กองกำกับการ 2 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปราม อาชญากรรมที่เกี่ยวกับภาษีทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมาย อื่นที่เกี่ยวข้องกับงานภาษีทุกประเภทและความผิดที่เกี่ยวเนื่องทั่วราชอาณาจักร ยกเว้นในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

3) กองกำกับการ 3 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปราม อาชญากรรมที่เกี่ยวกับการละเมิดทรัพย์สินทางปัญญา สืบสวน

สอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวข้องกับการละเมิดทรัพย์สินทางปัญญาและความผิดที่เกี่ยวเนื่อง ในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

4) กองกำกับการ 4 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับการละเมิดทรัพย์สินทางปัญญาทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวข้องกับการละเมิดทรัพย์สินทางปัญญาทุกประเภทและความผิดที่เกี่ยวเนื่องทั่วราชอาณาจักร ยกเว้นในเขตพื้นที่กรุงเทพมหานคร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

5) กองกำกับการ 5 มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับรักษาความสงบเรียบร้อย ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับการเงินการธนาคารทุกประเภท สืบสวนสอบสวนปฏิบัติงานตามประมวลกฎหมายวิธีพิจารณาความอาญา และกฎหมายอื่นที่เกี่ยวข้องกับการงานการธนาคารทุกประเภทและความผิดที่เกี่ยวเนื่องทั่วราชอาณาจักร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

6) กลุ่มงานสอบสวน มีอำนาจหน้าที่และความรับผิดชอบเกี่ยวกับการปฏิบัติตามประมวลกฎหมายวิธีพิจารณาความอาญา สืบสวนสอบสวนการกระทำผิดที่มีโทษทางอาญาเกี่ยวกับอาชญากรรมทางเศรษฐกิจหรือการกระทำความผิดทางอาญาตามกฎหมายอื่นที่เกี่ยวเนื่องทั่วราชอาณาจักร รวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

7) ฝ่ายอำนวยการ รับผิดชอบงานอำนวยการ และงานธุรการรวมทั้งปฏิบัติงานร่วมกับหรือสนับสนุนการปฏิบัติงานของหน่วยงานอื่นที่เกี่ยวข้องหรือตามที่รับมอบหมาย

แนวทางการปฏิบัติของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

เมื่อพิจารณาจากอำนาจหน้าที่ความรับผิดชอบแล้ว จะเห็นได้ว่าอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสมีลักษณะเป็นอาชญากรรมที่เกี่ยวกับเศรษฐกิจและอยู่ในความรับผิดชอบของกองบังคับ

การปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) เช่น ในกรณีของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมทางอ้อมอย่างการหลอกลวงชักชวนให้ผู้อื่นนำเงินมาลงทุน โดยอ้างว่าจะนำไปลงทุนในการเก็งกำไรจากมูลค่าของบิทคอยน์ซึ่งถือเป็นสินทรัพย์ดิจิทัลประเภทหนึ่ง หรือ กรณีการหลอกลวงว่าจะนำเงินไปลงทุนในการขุดบิทคอยน์ เป็นต้น แต่จากการศึกษาค้นคว้าของผู้วิจัย ยังไม่ปรากฏข้อมูลที่เกี่ยวกับแนวทางการปฏิบัติของกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางศรษฐกิจ (บก.ปอศ.) ที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสแต่อย่างใด จึงวิเคราะห์ได้ว่าในปัจจุบัน**กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) ยังไม่มีการกำหนดแนวทางการปฏิบัติหน้าที่ที่เกี่ยวข้องกับอาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือไว้เป็นการเฉพาะ**

3.5.3 กรมสอบสวนคดีพิเศษ

กรมสอบสวนคดีพิเศษ (Department of Special Investigation หรือ DSI) เป็นหน่วยงานในสังกัดกระทรวงยุติธรรม ก่อตั้งขึ้นเมื่อวันที่ 3 ตุลาคม 2545 ตามพระราชบัญญัติปรับปรุงกระทรวง ทบวง กรม พ.ศ.2545 สืบเนื่องจากสถานการณ์ของโลกมีการเปลี่ยนแปลงอย่างรวดเร็วในทุกๆด้าน จนส่งผลทำให้รูปแบบอาชญากรรมเปลี่ยนแปลงไป จากอาชญากรรมดั้งเดิมกลายเป็นอาชญากรรมที่ก่อให้เกิดความเสียหายทางเศรษฐกิจที่มีมูลค่ามหาศาล ส่งผลกระทบต่อประชาชนเป็นจำนวนมาก และผู้กระทำผิดมีการใช้เทคโนโลยีระดับสูงและอาศัยช่องว่างของกฎหมายปิดบังความผิดของตน อีกทั้งยังมีกลุ่มผู้มีอิทธิพลและเครือข่ายองค์กรอาชญากรรมเข้ามาเกี่ยวข้องจากทั้งภายในและภายนอกประเทศ ทำให้ยากต่อการสืบสวนสอบสวนดำเนินคดีด้วยวิธีการตามปกติ **กรมสอบสวนคดีพิเศษมีหน้าที่รับผิดชอบในการป้องกันปราบปราม สืบสวนและสอบสวนคดีความผิดทางอาญาที่ต้องดำเนินการสืบสวนสอบสวนโดยใช้วิธีการพิเศษตามกฎหมายว่าด้วยการสอบสวนคดีพิเศษ** (กรมสอบสวนคดีพิเศษ, ม.ป.ป.) ทั้งนี้ คดีที่ถือเป็นคดีพิเศษจะมีลักษณะตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 มาตรา 21 ข้อ (1) ดังนี้

“ (1) คดีความผิดทางอาญาตามกฎหมายที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัตินี้ และที่กำหนดในกฎกระทรวงโดยการเสนอแนะของ กคพ. โดยคดีความผิดทางอาญาตามกฎหมายดังกล่าวจะต้องมีลักษณะอย่างหนึ่งอย่างใดดังต่อไปนี้

(ก) คดีความผิดทางอาญาที่มีความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษ

(ข) คดีความผิดทางอาญาที่มีหรืออาจมีผลกระทบอย่างรุนแรงต่อความสงบเรียบร้อยและศีลธรรมอันดีของประชาชน ความมั่นคงของประเทศ ความสัมพันธ์ระหว่างประเทศหรือระบบเศรษฐกิจหรือการคลังของประเทศ

(ค) คดีความผิดทางอาญาที่มีลักษณะเป็นการกระทำความผิดข้ามชาติที่สำคัญ หรือเป็นการกระทำขององค์กรอาชญากรรม หรือ

(ง) คดีความผิดทางอาญาที่มีผู้ทรงอิทธิพลที่สำคัญเป็นตัวการ ผู้ใช้หรือผู้สนับสนุน

ทั้งนี้ ตามรายละเอียดของลักษณะของการกระทำความผิดที่ กคพ. กำหนด ....”

ตามข้อ (1) ใน มาตรา 21 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 คดีความผิดทางอาญาตามกฎหมายที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัติดังกล่าว แก้ไขเพิ่มเติมตามประกาศ กคพ. (ฉบับที่7) พ.ศ.2562 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ ตามมาตรา 21 วรรคหนึ่ง (1) แห่งพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ได้แก่ความผิดดังต่อไปนี้

1) คดีความผิดตามกฎหมายว่าด้วยการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชน

2) คดีความผิดตามกฎหมายว่าด้วยการควบคุมการแลกเปลี่ยนเงิน

3) คดีความผิดตามกฎหมายว่าด้วยความผิดเกี่ยวกับการเสนอราคาต่อหน่วยงานของรัฐ

4) คดีความผิดตามกฎหมายว่าด้วยเครื่องหมายการค้า

5) คดีความผิดตามกฎหมายว่าด้วยบริษัทมหาชนจำกัด

6) คดีความผิดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน

7) คดีความผิดตามกฎหมายว่าด้วยลิขสิทธิ์

8) คดีความผิดตามกฎหมายว่าด้วยสิทธิบัตร

9) คดีความผิดตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

10) คดีความผิดตามประมวลรัษฎากร

11) คดีความผิดตามกฎหมายว่าด้วยศุลกากร

12) คดีความผิดตามกฎหมายว่าด้วยภาษีสรรพสามิต

13) คดีความผิดตามกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

14) คดีความผิดตามกฎหมายว่าด้วยการประกอบธุรกิจของคนต่างด้าว

15) คดีความผิดตามกฎหมายว่าด้วยการป้องกันและปราบปรามการค้ามนุษย์

16) คดีความผิดตามกฎหมายว่าด้วยแร่

17) คดีความผิดตามกฎหมายว่าด้วยธุรกิจสถาบันการเงิน

18) คดีความผิดตามกฎหมายว่าด้วยวัตถุอันตราย

19) คดีความผิดตามกฎหมายว่าด้วยการสงวนและคุ้มครองสัตว์ป่า

20) คดีความผิดตามกฎหมายว่าด้วยป่าไม้

21) คดีความผิดตามกฎหมายว่าด้วยป่าสงวนแห่งชาติ

22) คดีความผิดตามกฎหมายว่าด้วยอุทยานแห่งชาติ

23) คดีความผิดตามประมวลกฎหมายที่ดิน

ทั้งนี้ในแต่ละคดีความผิด ก็จะมีการกำหนดหลักเกณฑ์ที่จะเป็นคดีพิเศษไว้อีกส่วนหนึ่ง

อาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสกับความเป็นคดีพิเศษ

ก่อนที่จะกล่าวถึงแนวทางการปฏิบัติในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ของกรมสอบสวนคดีพิเศษนั้น จำเป็นจะต้องพิจารณาว่า**อาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสถือเป็นคดีพิเศษหรือไม่** โดยเมื่อพิจารณาตามพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 มาตรา 21 และความผิดทางอาญาที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัติดังกล่าว ประกอบกับประกาศ กคพ. (ฉบับที่7) พ.ศ.2562 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษแล้วสามารถพิจารณาได้ดังนี้

1) กรณีการใช้สกุลเงินเข้ารหัสเป็นเครื่องมือในการก่ออาชญากรรมโดยตรงบางรูปแบบอาจยังไม่ชัดเจนว่าจะเป็นคดีพิเศษหรือไม่ เช่นในกรณีของการนำบิทคอยน์ไปใช้ในการซื้อขายแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย เช่น ยาเสพติดหรืออาวุธปืนเถื่อน เป็นต้น กรณีเช่นนี้ยังไม่เป็นคดีพิเศษ เนื่องจากไม่ใช่การกระทำความผิดตามคดีที่กำหนดไว้ในบัญชีท้ายพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547 แม้จะมีการใช้บิทคอยน์เป็นเครื่องมือทำให้เกิดความซับซ้อน จำเป็นต้องใช้วิธีการสืบสวนสอบสวนและรวบรวมพยานหลักฐานเป็นพิเศษก็ตาม **ดังนั้น หากจะถือว่าการกระทำผิดลักษณะดังกล่าวเป็นคดีพิเศษจะต้องผ่านมติคณะกรรมการคดีพิเศษ (คกพ.) ด้วยคะแนนเสียงไม่น้อยกว่าสองในสามของคณะกรรมการทั้งหมด ตามที่ระบุใน ข้อ (2) มาตรา 21 พระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ.2547**

2) กรณีการใช้สกุลเงินเข้ารหัสเป็นเครื่องมือในการก่ออาชญากรรมโดยตรงในรูปแบบของการฟอกเงิน เช่น การนำผลประโยชน์ที่ได้จากการกระทำความผิดที่เป็นความผิดมูลฐานไปแลกเปลี่ยนหรือนำไปซื้อบิทคอยน์เพื่อเป็นการปกปิดแหล่งที่มาของเงินดังกล่าว แม้การกระทำลักษณะนี้จะเข้าข่ายเป็นความผิดตามประกาศ กคพ.(ฉบับที่ 7) พ.ศ.2562 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษก็ตาม แต่การกระทำความผิดในลักษณะดังกล่าวนี้ **จะเป็นคดีพิเศษก็ต่อเมื่อการฟอกเงินด้วยบิทคอยน์ดังกล่าวมีความผิดมูลฐานที่เป็นคดีพิเศษที่อยู่ในอำนาจของพนักงานสอบสวนคดีพิเศษ หรือเป็นคดีที่มีมูลค่าความเสียหายตั้งแต่หนึ่งร้อยล้านบาทขึ้นไป** ดังที่กำหนดไว้ในประกาศ กคพ.(ฉบับที่ 7) พ.ศ.2562 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ

3) กรณีการใช้สกุลเงินเข้ารหัสเป็นเครื่องมือในการก่ออาชญากรรมทางอ้อม เช่น การชักชวนให้ผู้อื่นนำเงินมาร่วมลงทุน โดยหลอกลวงว่าจะนำเงินดังกล่าวไปลงทุนในการเก็งกำไรในมูลค่าของบิทคอยน์หรือการลงทุนในการทำเหมืองหรือการขุดบิทคอยน์ แต่แท้จริงแล้วเป็นการกระทำผิดในลักษณะแชร์ลูกโซ่ที่เป็นการฉ้อโกงประชาชน แม้กรณีดังกล่าวจะมีลักษณะเข้าข่ายเป็นความผิดตามประกาศ กคพ.(ฉบับที่ 7) พ.ศ.2562 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ ในลำดับที่ (1) คดีความผิดตามกฎหมายว่าด้วยการกู้ยืมเงินที่เป็นการฉ้อโกงประชาชนก็ตาม แต่การกระทำความผิดในลักษณะดังกล่าวนี้**จะเป็นคดีพิเศษก็ต่อเมื่อการฉ้อโกงประชาชนดังกล่าว มีหรือมีมูลน่าเชื่อว่ามีจำนวนผู้เสียหายตั้งแต่สามร้อยคนขึ้นไป หรือมีจำนวนเงินที่กู้ยืมตั้งแต่หนึ่งร้อยล้านบาทขึ้นไป** ดังที่กำหนดไว้ในประกาศ กคพ.(ฉบับที่ 7) พ.ศ.2562 เรื่อง กำหนดรายละเอียดของลักษณะของการกระทำความผิดที่เป็นคดีพิเศษ

จากข้อพิจารณาที่กล่าวมานี้ทำให้สามารถสรุปได้ว่า การจะพิจารณาว่าอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสรูปแบบต่างๆที่เกิดขึ้นเป็นคดีพิเศษหรือไม่นั้น จำเป็นจะต้องพิจารณาเป็นรายคดี รายเหตุการณ์ว่าการกระทำผิดดังกล่าวที่เกิดขึ้น มีลักษณะเป็นคดีพิเศษที่อยู่ในความรับผิดชอบของกรมสอบสวนคดีพิเศษหรือไม่ ทั้งนี้ยังมีข้อสังเกตุที่น่าสนใจอีกหนึ่งประการคือ **ยังไม่มีการกำหนดคดีความผิดตามกฎหมายว่าด้วยสินทรัพย์ดิจิทัลให้เป็นหมวดความผิดที่เป็นคดีพิเศษอีกด้วย**

แนวทางการปฏิบัติของกรมสอบสวนคดีพิเศษ ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

จากการศึกษาค้นคว้าของผู้วิจัยยังไม่ปรากฏข้อมูลที่เกี่ยวกับแนวทางการปฏิบัติของกรมสอบสวนคดีพิเศษที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสแต่อย่างใด จึงวิเคราะห์ได้ว่าในปัจจุบัน**กรมสอบสวนคดีพิเศษ ยังไม่มีการกำหนดแนวทางการปฏิบัติหน้าที่ที่เกี่ยวข้องกับอาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือไว้เป็นการเฉพาะ** โดยแนวทางในการปฏิบัติในการสืบสวนสอบสวนคดีพิเศษตามปกติได้กำหนดไว้ในพระราชบัญญัติการสอบสวนคดีพิเศษ พ.ศ. 2547 ในมาตราต่างๆ เช่น

*“**มาตรา 24** เพื่อประโยชน์ในการปฏิบัติหน้าที่ตามพระราชบัญญัตินี้ ให้พนักงานสอบสวนคดีพิเศษมีอำนาจดังต่อไปนี้ด้วย*

(1) เข้าไปในเคหสถาน หรือสถานที่ใดๆ เพื่อตรวจค้น เมื่อมีเหตุสงสัยตามสมควรว่ามีบุคคลที่มีเหตุสงสัยว่ากระทำความผิดที่เป็นคดีพิเศษหลบซ่อนอยู่ หรือมีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้ ประกอบกับมีเหตุอันควรเชื่อว่าเนื่องจากการเนิ่นช้ากว่าจะเอาหมายค้นมาได้บุคคลนั้นจะหลบหนีไป หรือทรัพย์สินนั้นจะถูกโยกย้าย ซุกซ่อน ทำลาย หรือทำให้เปลี่ยนสภาพไปจากเดิม

(2) ค้นบุคคล หรือยานพาหนะที่มีเหตุสงสัยตามสมควรว่ามีทรัพย์สินซึ่งมีไว้เป็นความผิดหรือได้มาโดยการกระทำความผิด หรือได้ใช้หรือจะใช้ในการกระทำความผิดที่เป็นคดีพิเศษ หรือซึ่งอาจใช้เป็นพยานหลักฐานได้

(3) มีหนังสือสอบถามหรือเรียกให้สถาบันการเงิน ส่วนราชการ องค์การ หรือหน่วยงานของรัฐ หรือรัฐวิสาหกิจ ส่งเจ้าหน้าที่ที่เกี่ยวข้องมาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือหรือส่งบัญชีเอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(4) มีหนังสือสอบถาม หรือเรียกบุคคลใดๆ มาเพื่อให้ถ้อยคำ ส่งคำชี้แจงเป็นหนังสือหรือส่งบัญชีเอกสาร หรือหลักฐานใดๆ มาเพื่อตรวจสอบ หรือเพื่อประกอบการพิจารณา

(5) ยึด หรืออายัดทรัพย์สินที่ค้นพบ หรือที่ส่งมาดังกล่าวไว้ใน (1) (2) (3) และ (4)...”

*"**มาตรา 25** ในกรณีที่มีเหตุอันควรเชื่อได้ว่า เอกสารหรือข้อมูลข่าวสารอื่นใดซึ่งส่งทางไปรษณีย์ โทรเลข โทรศัพท์ โทรสาร คอมพิวเตอร์ เครื่องมือ หรืออุปกรณ์ในการสื่อสาร สื่ออิเล็กทรอนิกส์ หรือสื่อทางเทคโนโลยีสารสนเทศใด ถูกใช้หรืออาจถูกใช้ เพื่อประโยชน์ในการกระทำความผิดที่เป็นคดีพิเศษพนักงานสอบสวนคดีพิเศษซึ่งได้รับอนุมัติจากอธิบดีเป็นหนังสือ จะยื่นคำขอฝ่ายเดียวต่ออธิบดีผู้พิพากษาศาลอาญา เพื่อมีคำสั่งอนุญาตให้พนักงานสอบสวนคดีพิเศษได้มาซึ่งข้อมูลข่าวสารดังกล่าวก็ได้..."*

*"**มาตรา 30** ในการสืบสวนและสอบสวนคดีพิเศษคดีใดมีเหตุจำเป็นต้องใช้ความรู้ความเชี่ยวชาญเฉพาะด้านเป็นพิเศษ อธิบดีอาจแต่งตั้งบุคคลซึ่งมีความรู้ความเชี่ยวชาญในด้านนั้นเป็นที่ปรึกษาคดีพิเศษได้..."*

จากข้อกฎหมายในมาตราต่างๆที่ยกตัวอย่างมานี้ สามารถวิเคราะห์ได้ว่า ในระหว่างที่ยังไม่มีการออกข้อบังคับหรือการกำหนดแนวทางปฏิบัติเป็นการเฉพาะ หากเกิดคดีอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสที่เข้าข่ายหรือมีลักษณะเป็นคดีพิเศษขึ้น กรมสอบสวนคดีพิเศษก็จะดำเนินการตามแนวทางที่กำหนดในกฎหมาย เช่น อาศัยอำนาจตามมาตรา 24 ในการปฏิบัติหน้าที่เพื่อรวบรวมพยานหลักฐานต่างๆที่เกี่ยวข้อง, อาศัยอำนาจตามมาตรา 25 ในการยื่นร้องต่อศาลเพื่อให้ได้มาซึ่งอุปกรณ์อิเล็กทรอนิกส์ที่เกี่ยวข้องกับสกุลเงินเข้ารหัสที่คนร้ายใช้กระทำความผิด และอาศัยอำนาจตามมาตรา 30 แต่งตั้งบุคคลซึ่งมีความรู้ความเชี่ยวชาญในเรื่องสกุลเงินเข้ารหัสเป็นที่ปรึกษาคดีพิเศษได้ เป็นต้น

3.5.4 สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.)

สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) เป็นหน่วยงานของรัฐที่ขึ้นตรงต่อนายกรัฐมนตรี จัดตั้งขึ้นตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 มีอำนาจหน้าที่ในการ**กำหนดหลักเกณฑ์และศึกษาหามาตรการต่างๆในการป้องกันและปราบปรามการฟอกเงิน ดูแลให้มีการปฏิบัติตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และทำหน้าที่ในการตรวจสอบวิเคราะห์ข้อมูลทางการเงินต่างๆที่อาจมีความเกี่ยวข้องกับการฟอกเงิน รวมทั้งดำเนินการต่างๆกับทรัพย์สินที่เกี่ยวข้องกับการกระทำความผิดฟอกเงิน** มีหน่วยงานภายใน 15 หน่วยงาน ประกอบด้วย (สำนักงานป้องกันและปราบปรามการฟอกเงิน[ปปง.], ม.ป.ป.)

1) สำนักงานเลขานุการกรม

2) กองสื่อสารองค์กร

3) กองกำกับและตรวจสอบ

4) กองกฎหมาย

5) กองข่าวกรองทางการเงิน

6) กองคดี 1

7) กองคดี 2

8) กองคดี 3

9) กองคดี 4

10) กองความร่วมมือระหว่างประเทศ

11) กองนโยบายและยุทธศาสตร์

12) กองบริหารจัดการทรัพย์สิน

13) ศูนย์เทคโนโลยีสารสนเทศ

14) กลุ่มตรวจสอบภายใน

15) กลุ่มพัฒนาระบบบริหาร

แนวทางการปฏิบัติของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

เมื่อพิจารณาจากอำนาจหน้าที่ความรับผิดชอบแล้วจะเห็นได้ว่า อาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสที่อยู่ในความรับผิดชอบของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) คือ **กรณีที่มีการฟอกเงินด้วยสกุลเงินเข้ารหัส** เช่น เมื่อมีผู้กระทำผิดนำเงินผลประโยชน์ที่ได้จากการกระทำความผิดต่างๆ มาแลกเปลี่ยนเป็นบิทคอยน์ ดังนั้น ผู้วิจัยจึงได้ศึกษารวบรวมข้อมูลถึงแนวทางการปฏิบัติของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ที่เกี่ยวกับการป้องกันปราบปรามการใช้สกุลเงินเข้ารหัสเป็นเครื่องมือในการฟอกเงิน ปรากฏว่าถึงแม้จะยังไม่มีการออกเป็นระเบียบ ข้อกำหนด หรือ มาตรการการดำเนินการไว้เป็นการเฉพาะในกรณีของสกุลเงินเข้ารหัสก็ตาม แต่ก็ปรากฏข้อมูลแนวทางในการดำเนินการจากรายงานต่างๆ เช่น เมื่อวันที่ 30 มกราคม 2561 (มติชนออนไลน์, 2561) พล.ต.ต.รมย์สิทธิ์ วีริยาสรร รักษาราชการแทน เลขาธิการสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) กล่าวถึงกรณีที่มิจฉาชีพมีการพัฒนารูปแบบในการใช้สกุลเงินเข้ารหัส

เช่น บิทคอยน์ ริปเปิ้ล และเงินสกุลเข้ารหัสสกุลอื่นๆเป็นเครื่องมือในการฟอกเงิน ถึงแม้ว่าสกุลเงินเข้ารหัสจะไม่ใช่เงินจริงก็ตาม แต่ก็ถือเป็นทรัพย์สินที่มีมูลค่า ซึ่งหากมิจฉาชีพนำเงินที่ได้จากการกระทำความผิด หรือนำเงินที่ได้จากการหลอกลวงผู้เสียหายไปซื้อขายหรือไปแลกเปลี่ยนเป็นบิทคอยน์ ก็เท่ากับเป็นการเปลี่ยนสภาพทรัพย์สินเพื่อซุกซ่อนหรือปกปิดแหล่งที่มาจึงเข้าองค์ประกอบความผิดฐานฟอกเงิน **ซึ่ง ปปง.สามารถตรวจสอบและดำเนินการยึดอายัดทรัพย์สินรวมทั้งบิทคอยน์ดังกล่าวได้**

จากสถานการณ์ดังกล่าวทำให้ ปปง. มีการหารือและวางมาตรการในการจัดระบบกำกับดูแลทางการเงิน เพื่อให้สามารถรับมือกับมิจฉาชีพได้อย่างรวดเร็วและสอดคล้องกับการเปลี่ยนแปลงทางเทคโนโลยี โดยมีการดำเนินการเชิงรุกใน**การศึกษามาตรการในกำกับดูแลผู้ให้บริการในการแลกเปลี่ยนสกุลเงินเข้ารหัส (Cryptocurrency Exchanger)** ซึ่งผู้ให้บริการเหล่านี้ มีความเสี่ยงในการถูกใช้เป็นเครื่องมือในการฟอกเงินได้ อีกทั้งยังมีการ**พิจารณาเพื่อเสนอแก้ไขกฎหมายที่เกี่ยวข้อง** เช่น การกำหนดให้ผู้ให้บริการแลกเปลี่ยนสกุลเงินเข้ารหัส ต้องเป็นผู้มีหน้าที่รายงานตามกฎหมายของ ปปง. กำหนดให้ประเมินความเสี่ยงในเรื่องการฟอกเงิน กำหนดให้พิสูจน์ทราบข้อเท็จจริงเกี่ยวกับลูกค้าที่มาแลกเปลี่ยนเงินกับสกุลเงินเข้ารหัส และจะต้องเก็บรักษาเอกสารหลักฐานเกี่ยวกับการทำธุรกรรมซื้อขายแลกเปลี่ยนและข้อมูลเกี่ยวกับลูกค้าทั้งหมด เป็นต้น

นอกจากนี้ยังได้**มีการประชาสัมพันธ์ แจ้งเตือนให้ประชาชนระมัดระวังในการลงทุนต่างๆ** อย่าหลงเชื่อผู้ชักชวนให้ลงทุนกับธุรกิจที่มีลักษณะใช้เงินลงทุนน้อยแต่ได้ผลตอบแทนสูง เพราะส่วนมากจะเป็นรูปแบบในการหลอกลวงของมิจฉาชีพให้ผู้ตกเป็นเหยื่อได้รับผลตอบแทนเป็นจำนวนมากในช่วงแรกที่เริ่มลงทุน แต่เมื่อเวลาผ่านไปจะมีการหยุดจ่ายผลตอบแทนและปิดกิจการและช่องทางการติดต่อสื่อสารแล้วหลบหนีไป ซึ่งอาจก่อให้เกิดความสูญเสียเป็นจำนวนมาก เป็นต้น

จากรายงานดังกล่าวทำให้สามารสรุปแนวทางการปฏิบัติของสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ในการป้องกันการนำสกุลเงินเข้ารหัสไปใช้ในการฟอกเงินได้ ดังนี้

1) ประชาสัมพันธ์ให้ประชาชนรับทราบ ถึงรูปแบบการกระทำผิดของคนร้าย เพื่อให้ประชาชนรู้เท่าทันและไม่ตกเป็นเหยื่อของกลุ่มมิจฉาชีพ

2) เมื่อมีคดีที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือในการฟอกเงินเกิดขึ้น สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) จะเข้าทำการตรวจสอบและดำเนินการยึดอายัดทรัพย์สินที่เกี่ยวกับการกระทำผิดรวมทั้งบิทคอยน์และสกุลเงินเข้ารหัสอื่นๆด้วย

3) ศึกษามาตรการในกำกับดูแลผู้ให้บริการในการแลกเปลี่ยนสกุลเงินเข้ารหัส (Cryptocurrency Exchanger)

4) เสนอแก้ไขกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน โดยจะนำหลักการมาตรฐานสากลด้านการป้องกันปราบปรามการฟอกเงินมาปรับใช้กับสกุลเงินเข้ารหัส

จากการศึกษาค้นคว้ารวบรวมข้อมูลเกี่ยวกับแนวทางการปฏิบัติของหน วยงานของรัฐที่มีหน้าที่เกี่ยวข้องในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ได้แก่ กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) กรมสอบสวนคดีพิเศษ และ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) พบว่า **ยังไม่มีหน่วยงานใดกำหนดแนวทางการปฏิบัติสำหรับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสไว้เป็นการเฉพาะ** อย่างไรก็ตามผู้วิจัยมีความเห็นว่าด้วยอำนาจตามกฎหมายต่างๆที่เกี่ยวข้องตลอดจนแนวทางการปฏิบัติหน้าที่ตามปกติของหน่วยงานต่างๆข้างต้น มีความพร้อมที่จะรองรับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้ในระดับหนึ่ง แต่ขณะเดียวกันหากมีการพัฒนาหรือมีการกำหนดหลักการหรือขั้นตอนในการปฏิบัติไว้เป็นการเฉพาะ น่าจะทำให้การป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสมีประสิทธิภาพมากขึ้น

บทที่ 4
ผลการศึกษา

การศึกษาเรื่อง “แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์” มีวัตถุประสงค์เพื่อศึกษาลักษณะรูปแบบ สภาพปัญหาและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ และศึกษาแนวนโยบาย กฎหมาย และมาตรการต่าง ๆ ที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ เพื่อนำข้อมูลมาวิเคราะห์และเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือที่เหมาะสมกับบริบทของประเทศไทย โดยเป็นการศึกษาวิจัยเชิงคุณภาพ โดยการศึกษาวิจัยจากเอกสาร (Documentary Research) และการศึกษาวิจัยภาคสนามด้วยการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ให้ข้อมูลสำคัญ 4 กลุ่ม ได้แก่ กลุ่มที่ 1 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในเรื่องสกุลเงินเข้ารหัสทั้งในส่วนภาครัฐและภาคเอกชน กลุ่มที่ 2 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญทางด้านกฎหมายเกี่ยวกับสกุลเงินเข้ารหัส กลุ่มที่ 3 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญหรือผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส และ กลุ่มที่ 4 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการเสนอแนวทางในการป้องกันอาชญากรรม โดยผู้ศึกษาสามารถเรียบเรียงข้อมูลสำคัญที่ได้จากการศึกษาทั้งหมด ดังต่อไปนี้

4.1 ลักษณะและรูปแบบของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมในประเทศไทยในปัจจุบัน

จากการเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลสำคัญพบว่า ในปัจจุบันมีการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมในลักษณะและรูปแบบต่างๆ ทั้งที่**ปรากฏให้เห็นได้อย่างชัดเจน** กล่าวคือมีผู้เสียหายตกเป็นเหยื่อของการกระทำความผิดและได้รับความเสียหายในรูปแบบต่างๆและได้แจ้งความร้องทุกข์หรือได้แจ้งเรื่องดังกล่าวต่อหน่วยงานของรัฐที่เกี่ยวข้อง และ**การกระทำความผิดที่ยังไม่ปรากฏชัดเจน** ซึ่งเป็นการกระทำความผิดที่เจ้าหน้าที่หรือหน่วยงานของรัฐรับทราบจากข่าวกรองหรือข้อมูลข่าวสารต่างๆแต่ยังไม่ปรากฏว่ามีผู้ได้รับความเสียหายอย่างชัดเจนหรือยังไม่สามารถรวบรวมพยานหลักฐานที่ชัดเจนเพียงพอที่จะตรวจสอบติดตามหรือทำการสืบสวนจับกุมได้

โดย**การนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมที่ปรากฏขึ้นชัดเจน**ในประเทศไทยปัจจุบันมีลักษณะและรูปแบบต่างๆ ดังนี้

4.1.1 การฟอกเงินด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ

การกระทำความผิดในลักษณะนี้คนร้ายจะนำเอาเงินที่ได้จากการกระทำความผิดในลักษณะของการฉ้อโกง หลอกลวง หรือการกระทำความผิดที่เกี่ยวกับพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เช่น การกระทำความผิดที่มีลักษณะเป็นการ **“แสร้งรักออนไลน์ (Romance Scam)”** ที่กลุ่มมิจฉาชีพจะแสดงตัวเป็นคนต่างชาติทำการหลอกลวงให้เหยื่อซึ่งเป็นหญิงไทยหลงเชื่อว่ามีคนต่างชาติเข้ามาแสดงความรักและต้องการจะคบหาดูใจ แต่จะใช้กลวิธีหลอกล่อเพื่อให้เหยื่อตายใจจนหลงเชื่อแล้วโอนเงินไปให้คนร้าย หรือในกรณีของ**กลุ่มคนร้ายที่ใช้การโทรศัพท์มาหลอกลวงด้วยกลอุบายต่างๆ (Call Center)** เช่น หลอกว่าเหยื่อจะถูกดำเนินคดีตามกฎหมายเนื่องจากเป็นหนี้บัตรเครดิตเป็นจำนวนมาก เมื่อเหยื่อเกิดความสับสนและตกใจกลัวคนร้ายก็จะหลอกให้เหยื่อโอนเงินไปให้เป็นต้น รวมทั้งการกระทำความผิดเกี่ยวกับการเป็นขบวนการลักลอบค้ายาเสพติด โดยหลังจากที่กลุ่มคนร้ายเหล่านี้ได้รับเงินจากเหยื่อหรือจากการค้ายาเสพติดแล้ว **ก็จะนำเงินที่ได้มาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ โดยเจตนาที่จะซุกซ่อนหรือป้องกันไม่ให้เงินจำนวนนั้นถูกตรวจสอบเส้นทางการเงินจากเจ้าหน้าที่ของรัฐ** อันเป็นผลมาจากคุณลักษณะพิเศษของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่แม้จะมีการเปิดเผยเส้นทางการเงินอย่างสาธารณะ แต่ไม่มีการเปิดเผยหรือมีลักษณะของการปกปิดตัวตนของผู้ใช้งานที่แท้จริง

การกระทำความผิดในลักษณะนี้เป็นความผิดตามกฎหมายที่เกี่ยวกับการฟอกเงินในลักษณะของการปกปิดหรือปิดบังเส้นทางการเงินซึ่งในอดีตคนร้ายจะปิดบังเส้นทางการเงินด้วยการใช้วิธีการเปิดบัญชีที่ซับซ้อน แล้วนำเงินผลประโยชน์ที่ได้โอนไปมาระหว่างบัญชีหลากหลายบัญชีหรือมีการว่าจ้างผู้อื่นให้เปิดบัญชีแทนในลักษณะของการเป็นตัวแทนเชิดหรือนอมินีเพื่อสร้างความซับซ้อนให้กับเส้นทางการเงิน แต่หลังจากที่มีการสร้างสกุลเงินเข้ารหัสอย่างบิทคอยน์ซึ่งมีการทำงานอยู่บนระบบเครือข่ายคอมพิวเตอร์ออนไลน์ซึ่งไม่สามารถจับต้องได้ออกมาใช้งาน จึงส่งผลทำให้คนร้ายหันมาใช้สกุลเงินเข้ารหัสเป็นที่หลบซ่อนเงินที่ได้จากการกระทำความผิดเหล่านี้แทนการใช้วิธีการแบบดั้งเดิม

“ถ้าเป็น(คดี)บิทคอนย์โดยตรงเลยยังไม่มี จะมีเกี่ยวพันคือการกระทำผิดเกี่ยวกับการฉ้อโกง หลอกลวง หรือการทำผิด พ.ร.บ.คอมพิวเตอร์ฯ อย่างเช่น Romance Scam (แสร้งรักออนไลน์) ที่มีลักษณะของการหลอกให้โอนเงินเข้ามาในบัญชี แล้วผู้กระทำผิดก็จะโยกมาเป็นบิทคอยน์”

(C1, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

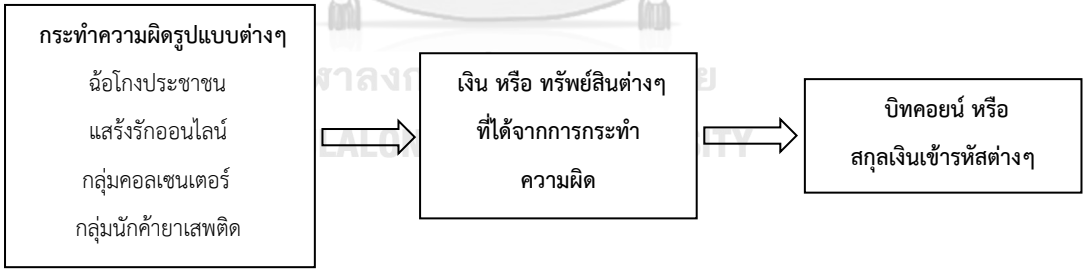
“มีเคสที่เกี่ยวกับการฟอกเงินคือ ถูกนำมาใช้คือทรัพย์ที่ได้จากการกระทำความผิดมาเก็บอยู่ในรูปแบบของคริปโทเคเรนซี ”

(C4, สัมภาษณ์, 9 กรกฎาคม 2563)

“คนร้ายใช้โดยมีวัตถุประสงค์เพื่อปกปิดผลประโยชน์ที่ได้มา โดยเท่าที่ทราบข้อมูลคือกลุ่มผู้ค้ายาเสพติดที่ได้ทรัพย์สินมาแล้วเอาไปเก็บไว้ในรูปแบบของพวกนี้ (บิทคอยน์และสกุลเงินเข้ารหัส)”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

โดยสามารถสรุปลักษณะและรูปแบบของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการฟอกเงินเพื่อหลบเลี่ยงการตรวจสอบเส้นทางการเงินได้ดังภาพต่อไปนี้



ภาพที่ 24 รูปแบบการนำบิทคอยน์ไปใช้ในการฟอกเงินด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ

(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2563)

4.1.2 การใช้โปรแกรมเรียกค่าไถ่ (Ransomware) เพื่อเข้าโจมตีเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ แล้วเรียกร้องให้มีการจ่ายค่าไถ่เป็นบิทคอยน์

การกระทำความผิดในลักษณะนี้คนร้ายจะใช้ความรู้ความเชี่ยวชาญในด้านคอมพิวเตอร์ในการสร้างหรือจัดหาโปรแกรมคอมพิวเตอร์ที่มีลักษณะเป็นไวรัสคอมพิวเตอร์ (Virus) แล้วจึงลักลอบนำโปรแกรมดังกล่าวเข้าไปปล่อยหรือทำให้แพร่ระบาดเข้าสู่เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์เป้าหมาย โดยเมื่อโปรแกรมเรียกค่าไถ่นี้สามารถเจาะระบบหรือเข้าสู่เครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์ได้แล้ว จะทำการยึดระบบการทำงานและนำข้อมูลทั้งหมดที่อยู่ภายในเครื่องของเหยื่อไปเข้ารหัสลับและทำการปิดกั้นข้อมูลไว้ ทำให้เหยื่อไม่สามารถเข้าถึงข้อมูลของตนเองได้ ส่งผลให้เกิดความเสียหาย หลังจากนั้น**คนร้ายจะทำการเรียกร้องให้เหยื่อซึ่งเป็นเจ้าของข้อมูลชำระค่าไถ่ในรูปแบบของบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ เพื่อแลกกับการปลดหรือทำลายโปรแกรมเรียกค่าไถ่ออกจากระบบ** โดยสาเหตุที่คนร้ายเรียกร้องให้มีการชำระค่าไถ่เป็นบิทคอยน์เนื่องจากไม่ต้องการให้เจ้าหน้าที่ของรัฐติดตามเส้นทางการเงินจากการติดตามเงินค่าไถ่ได้ ซึ่งเป็นผลมาจากลักษณะของบิทคอยน์ที่มีการปกปิดตัวตนของผู้ใช้งาน

“ที่พบมีการรับแจ้งคือลักษณะของการที่เหยื่อโดน Ransomware เข้ายึดระบบแล้วมีการส่ง Bitcoin Address เพื่อให้เจ้าของเครื่องคอมพิวเตอร์ หรือ บริษัทต่างๆ จ่ายเงินเป็นบิทคอยน์เพื่อให้ปลดล็อคให้ ไม่งั้นข้อมูลจะถูกทำลาย”

(A4, สัมภาษณ์, 10 กรกฎาคม 2563)

“เวลาที่เราโดนพวก Ransomware เจาะระบบเข้ามา คนร้ายจะให้คุณจ่ายเป็นบิทคอยน์นะเพราะว่ามันติดตามค่อนข้างยาก”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

4.1.3 การหลอกลวงให้ประชาชนนำเงินมาลงทุนเก็งกำไรในมูลค่าของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ

การกระทำความผิดในลักษณะนี้กลุ่มผู้กระทำผิดจะทำการโฆษณา ชักชวนให้เหยื่อนำเงินมาร่วมลงทุน โดยใช้กลอุบายหลอกลวงว่าจะเปิดระดมทุนเพื่อนำเงินไปลงทุนเก็งกำไรในมูลค่าของ

บิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ แล้วจะนำผลกำไรกลับมาจัดสรรคืนให้กับสมาชิกผู้เข้าร่วมลงทุน โดยกลุ่มผู้กระทำผิดมักจะมีการจูงใจให้เหยื่อหลงเชื่อด้วยการออกแผนการลงทุน (Package) ที่เป็นโฆษณาชวนเชื่อเพื่อแสดงให้เหยื่อเห็นว่าใช้เงินลงทุนน้อย มีความเสี่ยงน้อยแต่มีโอกาสได้รับผลตอบแทนสูง โดยแท้ที่จริงแล้ว**กลุ่มผู้กระทำผิดไม่ได้มีการนำเงินไปลงทุนตามที่กล่าวอ้างแต่อย่างใด**แต่มีลักษณะการกระทำความผิดอันเป็นการหลอกลวงหรือฉ้อโกงประชาชน ในลักษณะที่คล้ายกันกับแชร์ลูกโซ่ ที่เมื่อเหยื่อหลงเชื่อนำเงินมาให้แล้วในช่วงแรกเหยื่อจะได้รับผลตอบแทนตามแผนการลงทุนจริง โดยที่กลุ่มผู้กระทำผิดจะนำเงินของเหยื่อรายอื่นๆ มาหมุนเวียนเพื่อจ่ายเงินตอบแทนหลอกลวงให้กับเหยื่อรายอื่น เพื่อสร้างชื่อเสียงและความน่าเชื่อถือให้กับฉากหน้าการลงทุนของตน เมื่อผ่านไประยะหนึ่งกลุ่มผู้กระทำผิดก็จะปิดตัวลงและนำเงินที่ได้จากการกระทำความผิดหลบหนีไป

“มีส่วนหนึ่งที่ถูกหลอกลวงให้เข้าไปร่วมลงทุนโดยที่ตนเอง ไม่มีความรู้ ซึ่งอาจจะส่งผลกระทบต่อระบบการเงินของรัฐและเศรษฐกิจในภาพรวมของประเทศ”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

“หลอกให้มาลงทุนเกี่ยวกับคริปโทเคอเรนซี ซึ่งไม่มีอยู่จริง มีลักษณะคล้ายๆกับของแชร์ลูกโซ่ ”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

4.1.4 การหลอกลวงให้ประชาชนนำเงินมาลงทุนในการขุดบิทคอยน์

ผู้ให้ข้อมูลสำคัญได้กล่าวว่า ลักษณะของการได้มาซึ่งบิทคอยน์นั้นนอกจากจะได้มาจากการซื้อขายแลกเปลี่ยนกันระหว่างผู้ใช้งานแล้ว การจะถือครองหรือได้รับบิทคอยน์นั้นยังสามารถได้รับจากการขุดบิทคอยน์ (Mining) ซึ่งเป็นหนึ่งในกระบวนการหรือกลไกการทำงานของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ใช้ระบบบล็อคเชนเป็นระบบการทำงานพื้นฐาน ด้วยลักษณะดังกล่าวจึงทำให้เกิดการลงทุนชนิดหนึ่งคือ “การลงทุนในการขุดบิทคอยน์”ขึ้น ซึ่งเป็นการลงทุนด้วยการจัดหาเครื่องคอมพิวเตอร์ที่มีศักยภาพการคำนวณสูงพอที่จะสามารถแก้สมการทางคณิตศาสตร์ของระบบบิทคอยน์เพื่อให้ได้รับบิทคอยน์มาเป็นค่าตอบแทนตามที่ระบบกำหนด ซึ่งการลงทุนในลักษณะนี้มีการดำเนินการอยู่จริงซึ่งสามารถพบได้ทั้งในประเทศไทยและในต่างประเทศ

ในขณะเดียวกันได้มีกลุ่มผู้กระทำผิดอาศัยรูปแบบของการลงทุนในการขุดบิทคอยน์ในลักษณะนี้มาหลอกลวงให้เหยื่อหลงเชื่อว่าตนจะระดมเงินทุนเพื่อนำไปลงทุนในการขุดบิทคอยน์ แล้วเมื่อได้รับบิทคอยน์มาแล้วก็จะนำผลประโยชน์ที่ได้รับมาแจกจ่ายตามสิทธิ์การลงทุนของเหยื่อแต่ละราย แต่แท้จริงแล้วกลุ่มผู้กระทำผิดหรือคนร้าย **ไม่ได้มีการขุดบิทคอยน์แต่อย่างใด** แต่จะเป็นการกระทำผิดในลักษณะของแชร์ลูกโซ่ ที่จะมีลักษณะคล้ายกันกับการหลอกให้มาลงทุนในการเก็งกำไรในมูลค่าของบิทคอยน์คือเมื่อได้รับเงินจากเหยื่อแล้ว จะทำการจ่ายค่าตอบแทนให้กับเหยื่อบางส่วนเพื่อผลในการขยายตัวของจำนวนผู้ที่หลงเชื่อในทางอ้อม จากนั้นในท้ายที่สุดคนร้ายก็จะปิดตัวและหลบหนี

“ถ้าเคยได้ยินพวกกลุ่ม Crypto Mining Farm คือมันจะมีการกระทำผิดอีกรูปแบบหนึ่งที่หลอกว่าจะลงทุนกับการขุดพวกบิทคอยน์ ซึ่งมันจำเป็นต้องใช้ทรัพยากร เครื่องคอมพิวเตอร์สำหรับขุด ก็จะไปหลอกลวงชักชวนประชาชนให้นำเงินมาร่วมลงทุน แต่จริงๆคือไม่มีการขุดเลย เป็นการหลอกลวงทั้งสิ้น”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

4.1.5 การชักชวนให้นำสกุลเงินเข้ารหัสหรือคริปโทเคอเรนซีมาร่วมลงทุน ในลักษณะของการระดมทุน (Initial Coin Offering หรือ ICO) เถื่อน

การกระทำผิดในลักษณะนี้ กลุ่มผู้กระทำความผิดจะชักชวนให้ประชาชนนำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆมาร่วมลงทุนในกิจการอย่างใดอย่างหนึ่ง โดยประกาศว่าจะมีการจ่ายเงินปันผลตอบแทนตามผลประกอบการในลักษณะเดียวกันกับหุ้น ซึ่งการกระทำในลักษณะดังกล่าวจะมีลักษณะเป็นการประกอบธุรกิจเกี่ยวกับสินทรัพย์ดิจิทัลตาม พ.ร.ก.การประกอบสินทรัพย์ดิจิทัล พ.ศ. 2561 ที่จะต้องได้รับอนุญาตจากหน่วยงานของรัฐที่รับผิดชอบคือ คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) กลุ่มผู้กระทำผิดจึงมีการหลอกลวงว่า เป็นการระดมทุนเพื่อไปลงทุนในต่างประเทศเพื่อเป็นการหลีกเลี่ยงกฎหมายดังกล่าว และเมื่อได้รับสกุลเงินเข้ารหัสมาแล้วก็นำไปจ่ายเงินปันผลเป็นสกุลเงินเข้ารหัสให้กับเหยื่อรายต่างๆ จนทำให้เหยื่อหลงเชื่อว่ามีการลงทุนจริง ซึ่งเข้าข่ายการเป็นการฉ้อโกงประชาชนในอีกรูปแบบหนึ่ง ซึ่งเมื่อกลุ่มคนร้ายได้สกุลเงินเข้ารหัสไปแล้วก็จะปิดตัวลงและหลบหนีไป

“อีกลักษณะหนึ่งที่น่าสนใจคือ หลอกว่าจะมีการระดมทุนเป็นบิทคอยน์ไปลงทุนในต่างประเทศ คล้ายๆกับ ICO เถื่อน เพราะไม่งั้นจะต้องขึ้นทะเบียนกับทาง ก.ล.ต. เมื่อเหยื่อหลงเชื่อก็จะโอนบิทคอยน์ไปให้ แล้วพวกนี้ก็จะหลบหนีไป ”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

ลักษณะและรูปแบบของการกระทำผิดทั้ง 5 ลักษณะตามที่ได้กล่าวมานี้ เป็นการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมที่ปรากฏขึ้นชัดเจนในประเทศไทย ที่อยู่ในความรับผิดชอบของหน่วยงานของรัฐหรือเริ่มเกิดขึ้นอย่างแพร่หลาย

อย่างไรก็ตามนอกจากลักษณะและรูปแบบของการกระทำความผิดดังกล่าวแล้ว ยังปรากฏจากข้อมูลจากผู้ให้ข้อมูลสำคัญว่า ยังมี**การนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมที่ยังไม่ปรากฏขึ้นชัดเจนในประเทศไทย**ดังมีลักษณะและรูปแบบดังนี้

4.1.6 การนำบิทคอยน์ไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย

ผู้ให้ข้อมูลสำคัญกล่าวว่า ลักษณะของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดที่เกิดขึ้นอย่างแพร่หลายในต่างประเทศ โดยเฉพาะอย่างยิ่งประเทศที่มีการยอมรับในมูลค่าของบิทคอยน์อย่างกว้างขวางนั้น คือการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นสื่อกลางในการซื้อขายสินค้าและบริการที่ผิดกฎหมายต่างๆ เช่น การนำไปใช้เป็นสื่อกลางในการลักลอบซื้อขายอาวุธปืน ยาเสพติด การสื่อขายสื่อลามกอนาจาร การติดต่อเพื่อจ้างวานให้ผู้อื่นไปกระทำผิดกฎหมายเช่นการจ้างวานฆ่าผู้อื่น ซึ่งการกระทำผิดในลักษณะนี้**จะทำการติดต่อซื้อขายและจ้างวานกันเองโดยตรง ผ่านทางตลาดมืดออนไลน์ที่อยู่ในลักษณะของเว็บไซต์ที่เข้ารหัสที่สามารถเข้าถึงได้เฉพาะกลุ่ม (Darkweb/Darkmarket)** ซึ่งเป็นช่องทางการติดต่อเฉพาะที่ถูกสร้างขึ้นในระบบเครือข่ายคอมพิวเตอร์ ซึ่งคนร้ายซึ่งจะสามารถติดต่อสื่อสารถึงกันได้ผ่านระบบเครือข่ายอินเทอร์เน็ต และมีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้เป็นสื่อกลางในการแลกเปลี่ยนแทนการใช้สกุลเงินจริงเพื่อต้องการปกปิดตัวตนและป้องกันไม่ให้เจ้าหน้าที่ของรัฐสามารถติดตามเส้นทางการเงินได้

การกระทำความผิดในลักษณะนี้นั้นผู้ให้ข้อมูลสำคัญได้ให้ข้อมูลว่าจากการปฏิบัติหน้าที่และการรวบรวมข้อมูลข่าวสารต่างๆ ทำให้เริ่มรับทราบความเคลื่อนไหวว่าในประเทศไทยก็เริ่มปรากฏว่ามี

การกระทำความผิดในลักษณะนี้เช่นเดียวกัน แต่เนื่องจากยังไม่ปรากฏการกระทำผิดที่ชัดเจนและยังไม่เป็นที่แพร่หลาย รวมทั้งแหล่งตลาดมืดออนไลน์ที่มีการนำบิทคอยน์ไปใช้เป็นสื่อกลางในการกระทำผิดกันนั้นจะเป็นตลาดมืดที่ถูกสร้างขึ้นในต่างประเทศ จึงส่งผลทำให้การกระทำความผิดยังไม่ปรากฏชัดเจนขึ้นในประเทศไทย

“ก็ต้องยอมรับว่าเริ่มมีข่าวว่า มีการนำบิทคอยน์ไปใช้ในการซื้อขายพวกของผิดกฎหมายพวกนี้บ้างแล้ว ซึ่งส่วนมากที่เคยได้คุยกันจะเป็นพวกยาเสพติด แต่กลุ่มพวกนี้ยังเป็นส่วนน้อยมากๆ ต้องเป็นพวกที่สนใจพวกนี้จริงๆ ถึงจะรู้จักและส่วนมากพวกตลาดมืดแบบนี้ พวก Dark market นี่ ในเมืองไทยยังไม่มี ส่วนมากจะเป็นของต่างประเทศ”

(A4, สัมภาษณ์,10 กรกฎาคม 2563)

โดยสรุปแล้วจากการเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลสำคัญพบว่าปัจจุบันในประเทศไทยมีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมที่**ปรากฏขึ้นชัดเจน**ด้วยกัน 5 รูปแบบ ได้แก่

รูปแบบที่ 1 การฟอกเงินด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ

รูปแบบที่ 2 การใช้โปรแกรมเรียกค่าไถ่ (Ransomware) เพื่อเข้าโจมตีเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์แล้วเรียกร้องให้มีการจ่ายค่าไถ่เป็นบิทคอยน์

รูปแบบที่ 3 การหลอกลวงให้ประชาชนนำเงินมาลงทุนเก็งกำไรในมูลค่าของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ

รูปแบบที่ 4 การหลอกลวงให้ประชาชนนำเงินมาลงทุนในการขุดบิทคอยน์

รูปแบบที่ 5 การชักชวนให้นำสกุลเงินเข้ารหัสหรือคริปโทเคอเรนซีมาร่วมลงทุน ในลักษณะของการระดมทุน (Initial Coin Offering หรือ ICO) เถื่อน

นอกจากนี้**ข้อมูลจากผู้ให้ข้อมูลสำคัญยังบ่งชี้ว่า** ยังมีการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรม**ที่ยังไม่ปรากฏขึ้นชัดเจนในประเทศไทย** 1 รูปแบบ คือ รูปแบบที่ 6 การนำบิทคอยน์ไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย

ทั้งนี้ ผู้วิจัยได้นำข้อมูลที่ได้จากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญไปวิเคราะห์ประกอบกับข้อมูลที่ได้จากการศึกษาทบทวนวรรณกรรมพบว่า ลักษณะและรูปแบบของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมในประเทศไทยในปัจจุบันทั้ง 6 รูปแบบ เป็นลักษณะและรูปแบบที่ผู้วิจัยพบจากการทบทวนวรรณกรรมหรือกล่าวอีกนัยหนึ่งได้ว่า **ลักษณะและรูปแบบการนำบิทคอยน์มาใช้ในเป็นเครื่องมือในการก่ออาชญากรรมในประเทศไทยนั้น มีลักษณะเช่นเดียวกับลักษณะและรูปแบบการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมที่เกิดขึ้นทั่วโลก** โดยสามารถนำลักษณะและรูปแบบของการการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมในประเทศไทยทั้ง 6 รูปแบบ ไปแยกประเภทตามที่ผู้วิจัยได้แบ่งประเภทไว้ คือ **การนำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรง** ซึ่งเป็นรูปแบบของการกระทำความผิดที่การวิจัยครั้งนี้มุ่งที่จะศึกษาเนื่องจากมีลักษณะของการนำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไปใช้ประกอบการกระทำความผิดจริง ได้แก่ การกระทำความผิดในรูปแบบที่ 1 การฟอกเงินด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ และ การกระทำความผิดในรูปแบบที่ 6 การนำบิทคอยน์ไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย และการนำไปใช้กระทำความผิดอีกลักษณะหนึ่งคือ **การนำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไปใช้เป็นเครื่องมือในการก่ออาชญากรรมทางอ้อม** ได้แก่ การกระทำความผิดตามรูปแบบที่ 3 การหลอกลวงให้ประชาชนนำเงินมาลงทุนเก็งกำไรในมูลค่าของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ รูปแบบที่ 4 การหลอกลวงให้ประชาชนนำเงินมาลงทุนในการขุดบิทคอยน์และรูปแบบที่ 5 การชักชวนให้นำสกุลเงินเข้ารหัสหรือคริปโทเคอเรนซีมาร่วมลงทุน ในลักษณะของการระดมทุน (Initial Coin Offering หรือ ICO) เถื่อน ซึ่งการกระทำความผิดในลักษณะนี้ไม่อยู่ในขอบเขตของการศึกษาวิจัยเนื่องจากเมื่อพิจารณาถึงพฤติกรรมในการกระทำความผิดแล้วจะพบว่าไม่ได้มีการนำบิทคอยน์ไปใช้ในการกระทำความผิดอย่างแท้จริงแต่อย่างใด เพียงเป็นการนำชื่อ “บิทคอยน์” หรือชื่อของกิจกรรมการลงทุนที่เกี่ยวกับบิทคอยน์ ไปกล่าวอ้างเพื่อให้เหยื่อหลงเชื่อเท่านั้น หรืออาจกล่าวได้ว่าบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไม่ใช่สาระสำคัญหรือวัตถุในการกระทำความผิดแต่อย่างใด เพราะวัตถุที่นำมาใช้ในการหลอกลวงหรือฉ้อโกงประชาชนในลักษณะนี้ สามารถเปลี่ยนแปลงไปได้เสมอตามแต่ค่านิยมของคนในสังคมในแต่ละยุคสมัย เช่น เปลี่ยนจากการหลอกลวงให้มาลงทุนในบิทคอยน์ เป็น การหลอกลวงให้นำเงินมาลงทุนใน ราคาน้ำมัน ทองคำ การลงทุนด้วยการเปรียบต่างค่าเงินสกุลต่างๆ (Forex) รวมทั้ง ลักษณะของสินทรัพย์ที่อาจมีราคาหรืออาจถือเอาได้

ที่จะถูกพัฒนาขึ้นในอนาคต ก็สามารถนำมาใช้ในการหลอกลวงได้ เป็นต้น ทั้งนี้รูปแบบของการกระทำผิดที่ผู้วิจัยพบจากการศึกษาทบทวนวรรณกรรมและเอกสารทางวิชาการที่เกี่ยวข้องแต่**ไม่พบว่ามีการกระทำผิดในประเทศไทย คือ การระดมเงินทุนให้แก่กลุ่มผู้ก่อการร้ายผ่านบิทคอยน์**

จากการศึกษาในประเด็นของลักษณะและรูปแบบของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรม**สามารถสรุปได้ว่า** ในปัจจุบันมีการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมด้วยกันสองรูปแบบ คือ**การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรง** ได้แก่ การลักลอบซื้อขายสินค้าและบริการที่ผิดกฎหมายโดยการชำระค่าสินค้าและบริการเป็นบิทคอยน์ เช่น การลักลอบซื้อขายยาเสพติด การลักลอบซื้อขายอาวุธปืนเถื่อน การว่าจ้างให้ผู้อื่นไปกระทำความผิดในรูปแบบต่างๆ การใช้บิทคอยน์เพื่อซื้อขายสื่อลามกอนาจาร การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการเรียกค่าไถ่ทั้งการเรียกค่าไถ่แบบดั้งเดิมและการใช้โปรแกรมเรียกค่าไถ่ (Ransomware) การฟอกเงินผ่านบิทคอยน์ และการระดมเงินทุนของกลุ่มผู้ก่อการร้ายผ่านบิทคอยน์ และ **การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมทางอ้อม** ได้แก่ การหลอกลวงว่าจะมีการนำเงินไปใช้ในการลงทุนจากการเก็งกำไรในมูลค่าของบิทคอยน์ในรูปแบบและลักษณะต่างๆ และ การหลอกลวงว่าจะมีการนำเงินไปใช้ในการลงทุนในการขุดบิทคอยน์ โดยที่แท้จริงแล้วมิได้มีการนำเงินของเหยื่อไปลงทุนแต่อย่างใด แต่มีลักษณะของการกระทำความผิดที่เป็นการฉ้อโกงประชาชนในลักษณะของแชร์ลูกโซ่ เท่านั้น โดยสำหรับในประเทศไทยในปัจจุบันพบว่ามีการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมทั้งในลักษณะและรูปแบบโดยตรงและทางอ้อม โดยลักษณะและรูปแบบที่ปรากฏขึ้นชัดเจน ได้แก่ การฟอกเงินผ่านบิทคอยน์ การใช้โปรแกรมเรียกค่าไถ่ (Ransomware) แล้วเรียกร้องให้มีการจ่ายค่าไถ่เป็นบิทคอยน์ และการหลอกลวงให้ประชาชนนำเงินมาลงทุนเกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในรูปแบบต่างๆ ส่วนลักษณะและรูปแบบการกระทำผิดที่ยังไม่ปรากฏขึ้นชัดเจน คือ การลักลอบซื้อขายสินค้าและบริการที่ผิดกฎหมายโดยการชำระค่าสินค้าและบริการเป็นบิทคอยน์ และลักษณะและรูปแบบที่ยังไม่พบว่ามีการเกิดขึ้นในประเทศไทย คือ การระดมเงินทุนให้แก่กลุ่มผู้ก่อการร้ายผ่านบิทคอยน์

4.1.7 สถานการณ์และแนวโน้มของอาชญากรรมที่เกี่ยวกับบิทคอยน์ของประเทศไทย

เมื่อพิจารณาถึงการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรงในประเทศไทยซึ่งเป็นลักษณะและรูปแบบของการกระทำความผิดที่การวิจัยครั้ง

นี้สนใจที่จะศึกษาตามที่ได้กล่าวมาแล้วนั้น จะปรากฏให้เห็นได้ชัดเจนเพียงรูปแบบเดียวคือการฟอกเงินด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆก็ตาม แต่จากการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญพบว่ามีการเกิดขึ้นในปริมาณที่น้อย หรือในกรณีของการการนำบิทคอยน์ไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมายที่ยังไม่ปรากฏขึ้นชัดเจนทั้งในเรื่องของปริมาณและความร้ายแรงของการกระทำความผิด จึงทำให้มีผู้ให้ข้อมูลสำคัญวิเคราะห์ได้ว่าในปัจจุบันสถานการณ์การนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมโดยตรงนั้นอาจยังอยู่ในระดับต่ำหรืออาจจะยังอยู่ในช่วงการก่อตัวของปัญหา โดย**มีสาเหตุมาจากสถานการณ์การใช้งานบิทคอยน์ของประเทศไทยในปัจจุบันนั้นยังถือได้ว่าอยู่ในช่วงเริ่มต้น** พิจารณาได้จากจำนวนผู้ใช้งานที่ยังอยู่ในวงจำกัด ส่วนมากมักจะได้รับความนิยมเฉพาะกลุ่มนักลงทุนเก็งกำไรในมูลค่าของบิทคอยน์ หรือ เป็นกลุ่มผู้ขุดบิทคอยน์ (Miner) เท่านั้น อีกทั้งด้วยลักษณะในการกำหนดมูลค่าของบิทคอยน์ที่ไม่ได้มีการอ้างอิงกับทรัพย์หรือสินทรัพย์ใดๆ แต่จะขึ้นอยู่กับกลไกความต้องการซื้อขายของตลาด **ทำให้สังคมไทยยังไม่เกิดการยอมรับในมูลค่าของบิทคอยน์ในระดับที่สามารถใช้งานแทนเงินสดเพื่อซื้อขายสินค้าและบริการได้อย่างแพร่หลายทั่วไปอย่างในต่างประเทศ** ประกอบกับการจะถือครองบิทคอยน์ได้นั้น ผู้ที่จะครอบครองจำเป็นจะต้องมีทรัพย์สินหรือมีเงินทุนเป็นจำนวนมากจึงจะสามารถได้มาซึ่งบิทคอยน์ได้ จึงทำให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆยังไม่ได้รับความสนใจจนตกไปเป็นเครื่องมือของอาชญากรอย่างแพร่หลายในประเทศไทย

“มีครับ แต่ก็ยังถือเป็นส่วนน้อยมากๆ ใน 2-3 ปีที่ผ่านมา มีเคสที่เกี่ยวกับการฟอกเงินกับคริปโทเคอเรนซีอยู่เพียง 3-4 เคสเท่านั้น”

(C4, สัมภาษณ์, 9 กรกฎาคม 2563)

“บ้านเรา (ประเทศไทย) ยังไม่ถึงขั้นวิกฤติในเรื่องนี้เพราะคนยังใช้งานอยู่ข้างบน ยังไม่ถึงขนาดลงไปใช้งานใน Dark Web”

(C1, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“คนของเรา (ประเทศไทย) เพิ่งจะตื่นตัวและยังไม่เป็นที่นิยม ส่วนใหญ่คนที่เล่นพวกนี้ (บิทคอยน์) ต้องมีสินทรัพย์สูงจะเป็นกลุ่มเล็กๆ มันเลยยังไม่ค่อยบูม”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

นอกจากนี้ผู้ให้ข้อมูลสำคัญที่เป็นกลุ่มของผู้ทรงคุณวุฒิที่มีหน้าที่เกี่ยวข้องกับการบังคับใช้กฎหมายหรือมีหน้าที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสยังได้วิเคราะห์ถึง**แนวโน้มของสถานการณ์การใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นเครื่องมือในการก่ออาชญากรรมในอนาคตของประเทศไทย**ว่า มีแนวโน้มที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จะได้รับความนิยมและจะมีผู้ใช้งานมากขึ้นในอนาคตอันอาจเป็นผลมาจากกระแสนิยมของสังคมโลก หรือปัจจัยทางด้านการลงทุนประกอบกับผลของการออกกฎหมาย พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 รวมทั้งกระแสการพัฒนาระบบการเงินการธนาคารเข้าสู่การเป็น “สังคมไร้เงินสด” ส่งผลทำให้ประชาชนในประเทศให้ความสนใจและอาจส่งผลให้มีปริมาณการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเพิ่มมากขึ้นตามไปด้วย **ในขณะเดียวกันเมื่อมีจำนวนผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมากขึ้นก็จะส่งผลทำให้มีการนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรมหรือนำไปใช้ในกิจกรรมที่ผิดกฎหมายมากขึ้นตามไปด้วย** ประกอบกับผู้ให้ข้อมูลสำคัญยังได้พิจารณาถึงประเด็นปัญหาและสาเหตุสำคัญว่าตราบใดที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆยังมีคุณลักษณะของการปกปิดตัวตนผู้ใช้งานที่แท้จริงอยู่นั้น การถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิดจะมีปริมาณและความเข้มข้นมากขึ้น เพราะอาชญากรยังสามารถใช้ประโยชน์จากคุณลักษณะดังกล่าวทั้งในแง่ของการปกปิดตัวตน เพื่อสร้างโอกาสให้ตนเองหลุดรอดจากการตรวจสอบจับกุมจากเจ้าหน้าที่ของรัฐ รวมทั้งยังมีโอกาสที่จะนำทรัพย์สินที่ได้จากการกระทำความผิดไปซุกซ่อนและโอนย้ายได้โดยง่าย เนื่องจากเจ้าหน้าที่ของรัฐยังไม่สามารถตรวจสอบเส้นทางการเงินของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆได้โดยง่าย ซึ่งในประเด็นสภาพปัญหาและสาเหตุนี้จะได้กล่าวถึงต่อไป

“แนวโน้มหลังจาก ปี พ.ศ.2561 ที่มีการออกกฎหมาย พ.ร.ก.สินทรัพย์ดิจิทัลฯ จะทำให้อาชญากรรมพวกนี้เข้ามาเยอะขึ้นแน่นอน”

(C1, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“สมมติว่า วันนี้มีคนใช้บิทคอยน์ 100 ครั้ง ก็อาจจะมีคนนำไปใช้ก่ออาชญากรรม 1 ครั้ง ในอนาคตมันจะเพิ่มขึ้นเป็น 10 ครั้งแน่นอน และอาจจะไม่ใช่ 100 อาจจะถึงเป็น 10,000 ซึ่งมันจะถูกใช้ไปในทางที่ผิดมากขึ้นเมื่อเปอร์เซนต์การใช้งานสูงขึ้น”

(A5, สัมภาษณ์, 26 พฤศจิกายน 2562)

“ตราบใดที่ความไร้ตัวตน หรือ ความ Anonymous ของมัน(บิทคอยน์) คงอยู่ พวกคนร้ายจะใช้มันเป็นเครื่องมือมากขึ้นๆ อย่างแน่นอน เพราะเจ้าหน้าที่ของรัฐไม่สามารถทำอะไรได้เลย ผมเชื่อว่าในอนาคตมันจะมีปัญหามากขึ้นอย่างแน่นอน”

(A4, สัมภาษณ์, 10 กรกฎาคม 2563)

ขณะที่ผู้ให้ข้อมูลสำคัญอีกกลุ่มหนึ่ง ซึ่งเป็นกลุ่มที่เป็นหน่วยงานของรัฐที่มีหน้าที่เกี่ยวกับการกำกับดูแลและการพัฒนาเทคโนโลยีทางการเงินหรือมีแนวคิดเกี่ยวข้องกับการพัฒนาของระบบเศรษฐกิจในภาพรวมนั้นได้วิเคราะห์ว่าแม้ทั่วโลกรวมทั้งในประเทศไทยเองจะมีความพยายามที่จะสร้าง “สังคมไร้เงินสด” ที่ถือเป็นการพัฒนาระบบการเงินการธนาคารและการซื้อขายแลกเปลี่ยนสินค้าและบริการให้มีความทันสมัย สอดคล้องกับนวัตกรรมและเทคโนโลยีสมัยใหม่ก็ตาม แต่ก็**ยังไม่สามารถสรุปได้ว่ากระแสการพัฒนานี้จะส่งผลทำให้ประชาชนหันมาใช้งานบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆมากขึ้น** เนื่องจากเมื่อพิจารณาถึงข้อเท็จจริงแล้วจะ**พบว่าบิทคอยน์และสกุลเงินเข้ารหัสต่างๆยังขาดคุณสมบัติในการใช้เป็นสื่อกลางในการแลกเปลี่ยนที่น่าเชื่อถือ**โดยเฉพาะประเด็นในเรื่องของมูลค่าที่ไม่ได้ยึดโยงอยู่กับสถาบันการเงินหรือสินทรัพย์ใดๆ แต่ขึ้นอยู่กับการยอมรับของสังคมผู้ใช้งานเฉพาะกลุ่มเท่านั้น ประกอบกับ**ขั้นตอนการชำระ โอน-รับ บิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่จำเป็นจะต้องใช้ระยะเวลาในการตรวจสอบยืนยันธุรกรรมนานกว่าการใช้เงินสดที่สามารถเป็นสื่อกลางในการชำระเงินได้ในทันที** อีกทั้งในระบบการเงินการธนาคารที่ตอบสนองต่อแนวคิดสังคมไร้เงินสดยัง**มีทางเลือกการใช้งานที่สร้างความสะดวกให้กับผู้ใช้งานได้มากกว่าอย่างระบบพรอมต์เพย์ (Promptpay) หรือ แอพพลิเคชั่นธนาคารต่างๆ (Bank Application) ต่างๆ** เป็นต้น ด้วยเหตุผลต่างๆที่กล่าวมานี้ผู้ให้ข้อมูลสำคัญจึงเชื่อว่าการใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆในลักษณะที่จะเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการตามปกตินั้นยังไม่น่าจะเป็นที่แพร่หลายในอนาคต รวมทั้งลักษณะของการกระทำผิดที่ใช้บิทคอยน์เป็นเครื่องมือในลักษณะที่เป็นสื่อกลางในการแลกเปลี่ยนโดยตรงนั้นยังมีโอกาสน้อย

อย่างไรก็ตามยังมีผู้ให้ข้อมูลสำคัญกลุ่มนี้วิเคราะห์ไปในทิศทางเดียวกันว่าในประเทศไทยนั้น **แนวโน้มที่จะเกิดการกระทำความผิดในลักษณะที่มีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้เป็นเครื่องมือโดยตรงยังมีโอกาสน้อย** โดยผู้ให้ข้อมูลสำคัญได้อ้างอิงข้อมูลจากสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nation Office on Drugs and Crime [UNODC]) ที่ได้วิเคราะห์แนวโน้มการกระทำความผิดที่เกี่ยวกับการใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นเครื่องมือตามภูมิภาคต่างๆของโลก โดยจากข้อมูลพบว่าในภูมิภาคยุโรปและอเมริกานั้นจะมีลักษณะการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมายต่างๆในตลาดมืดออนไลน์ (Darkweb) โดยเฉพาะการลักลอบซื้อยาเสพติด รวมทั้งการใช้บิทคอยน์และสกุลเงินเข้ารหัสเป็นช่องทางในการสนับสนุนเงินทุนให้กับกลุ่มผู้ก่อการร้ายเป็นจำนวนมาก ขณะที่การกระทำความผิดในภูมิภาคเอเชียจะเป็นลักษณะของการหลอกลวง ฉ้อโกงต่างๆเท่านั้น ซึ่งหากวิเคราะห์ถึงแนวโน้นในอนาคตก็น่าจะมีลักษณะเป็นไปในทางเดียวกันกับปัจจุบัน โดยสาเหตุที่สำคัญประการหนึ่งคือประเทศไทยยังมีการยอมรับในมูลค่าและการใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆในฐานะของการเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการต่างๆที่ยังไม่แพร่หลาย อีกทั้งในช่องทางที่จะแลกเปลี่ยนบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆออกมาเป็นเงินและสินทรัพย์อื่นๆยังถูกกำหนดไว้ด้วย พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ที่ต้องดำเนินการผ่านตัวกลางที่เป็นผู้ประกอบธุรกิจที่ได้รับอนุญาต ดังนั้น จึงอาจกล่าวได้ว่าแนวโน้มของในการใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นเครื่องมือในการกระทำความผิดในประเทศไทยน่าจะเป็นไปในลักษณะของการหลอกหลวง ฉ้อโกงที่อาจมีปริมาณเพิ่มมากขึ้น

“ถ้ามองไปในอนาคต ต้องบอกว่าตัวคริปโทเคอเรนซีเอง มันไม่ได้เอื้อกับการเป็นสื่อกลางในการชำระเหมือนเงินทั่วไป ด้วยมูลค่าของมันที่ไม่แน่นอนประกอบกับการใช้ระยะเวลาในการชำระค่าสินค้าและบริการที่ไม่เกิดขึ้นในทันทีทันใดเหมือนเงิน อีกทั้ง เรายังมีช่องทางที่ไร้เงินสดได้อย่างพร้อมเพย์ หรือ แอพพลิเคชั่นของธนาคารต่างๆ ด้วยปัจจัยต่างๆก็เลยมองว่าคงไม่แพร่หลาย”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

“โอกาสที่จะเกิดการใช้งานโดยตรงจริงๆ มีโอกาสในระดับที่น้อย เหตุผลเพราะช่องทางที่จะนำคริปโทเคอเรนซีออกมาเป็นเงินหรือสินทรัพย์อื่นๆที่ใช้ในทางปกติ ส่วนหนึ่งมันยังถูกกรอบอยู่ด้วยตัวกลางผู้ประกอบธุรกิจที่จะต้องได้รับอนุญาต เพราะฉะนั้นการทำเงินพวกนี้ออกมาจะติด พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล”

(A3 ,สัมภาษณ์, 19 พฤษภาคม 2563)

จากข้อมูลความคิดเห็นดังกล่าวสามารถสรุปได้ว่ามีผู้ให้ข้อมูลสำคัญวิเคราะห์แนวโน้มสถานการณ์การใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆในการก่ออาชญากรรมในอนาคตของประเทศไทยแตกต่างกันออกไป โดยผู้ให้ข้อมูลสำคัญ**กลุ่มที่เป็นผู้ทรงคุณวุฒิที่เป็นผู้บังคับใช้กฎหมายหรือมีหน้าที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสจะมีแนวคิดว่าในอนาคตจะมีการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมเพิ่มมากขึ้น**อันเป็นผลมาจากกระแสการพัฒนาของภาคธุรกิจการเงินและความพยายามในการสร้างสังคมไร้เงินสด ที่จะส่งผลทำให้ประชาชนจะหันมาสนใจและใช้งานสกุลเงินเข้ารหัสเพิ่มมากขึ้น และ**เมื่อมีการใช้งานมากขึ้นบิทคอยน์และสกุลเงินเข้ารหัสต่างๆก็จะถูกนำไปใช้ในกิจกรรมที่ผิดกฎหมายเพิ่มมากขึ้นด้วย** ซึ่งแนวคิดนี้มีความสอดคล้องกันกับงานวิจัยของ **Aneta Vondráčková (2016)** ที่ได้ศึกษาเกี่ยวกับ **มาตรการในการกำกับดูแลสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสของสหภาพยุโรป (Regulation of Virtual Currency in the European Union)** ว่าปริมาณการใช้งานสกุลเงินเข้ารหัสที่มีจำนวนเพิ่มขึ้นอย่างรวดเร็ว จะทำให้เกิดความเสี่ยงที่จะมีการนำสกุลเงินเสมือนหรือสกุลเงินเข้ารหัสต่างๆ ไปใช้ในการก่ออาชญากรรมเพิ่มมากขึ้นตามไปด้วย

ขณะที่ผู้ให้ข้อมูลสำคัญกลุ่มที่เป็นผู้ทรงคุณวุฒิที่เกี่ยวกับสกุลเงินเข้ารหัส ที่มีหน้าที่ในการกำกับดูแลสกุลเงินเข้ารหัสในมิติของการพัฒนาเทคโนโลยีทางการเงินหรือการนำไปใช้ในการพัฒนาในภาคธุรกิจนั้นจะ**มีแนวคิดที่แตกต่างไปว่า โอกาสที่จะมีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้ในการก่ออาชญากรรมโดยตรงนั้นมีน้อย** อันเนื่องมาจากปัจจัยสำคัญคือการที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆยังขาดความน่าเชื่อถือในการทำหน้าที่เป็นสื่อกลางจนยังไม่สามารถนำมาใช้ในชีวิตประจำวันได้อย่างแพร่หลาย ซึ่งแนวคิดดังกล่าวสอดคล้องกับงานวิจัยของ **J. R. Clark, M. Scott Niederjohn, and William C. Wood (2018)** ที่พบว่า บิทคอยน์ยังไม่สามารถทำหน้าที่เป็นเงินได้อย่างสมบูรณ์ ทั้งในแง่ของการเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ยังมีร้านค้า

และผู้ประกอบการต่างๆยอมรับในมูลค่าเป็นจำนวนน้อย อันเป็นผลมาจากการที่มูลค่าของบิทคอยน์ที่ไม่แน่นอน และไม่ได้ยึดโยงกับรัฐบาล ธนาคารกลางหรือสถาบันการเงินใดๆ ประกอบกับข้อมูลต่างๆที่ผู้ให้ข้อมูลสำคัญนำมาบ่งชี้ว่า แนวโน้มการก่ออาชญากรรมที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในภูมิภาคเอเชียจะเป็นไปในลักษณะของการใช้ในทางอ้อมมากกว่าการใช้โดยตรง หรือเป็นลักษณะของการหลอกลวงฉ้อโกงมากกว่าการนำบิทคอยน์มาใช้เป็นเครื่องมือในการกระทำความผิดจริง

จากการวิเคราะห์ข้อมูลที่ได้จากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญประกอบกับข้อมูลที่พบจากการศึกษางานวิจัยที่เกี่ยวข้องทำให้ผู้วิจัยสามารถสรุปผลการศึกษาในประเด็นด้านสถานการณ์และแนวโน้มของอาชญากรรมที่เกี่ยวกับบิทคอยน์ของประเทศไทยได้ว่า หากวิเคราะห์จากมุมมองในเชิงการป้องกันอาชญากรรมเป็นหลักแล้ว จะทำให้คาดคะเนได้ว่า**ในอนาคตจะมีการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมเพิ่มมากขึ้น**ทั้งในภาพรวมของสังคมโลกและในประเทศไทยเอง แต่ในขณะเดียวกันหากพิจารณาด้วยข้อมูลและข้อเท็จจริงเชิงลึกที่เกี่ยวข้องต่างๆ โดยเฉพาะในประเด็นเรื่องความน่าเชื่อถือในมูลค่าของบิทคอยน์ประกอบกันแล้ว ก็ยังสามารถกล่าวได้ว่า**การนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมอาจมีโอกาสที่จะไม่เกิดขึ้นอย่างแพร่หลายในประเทศไทยได้เช่นกัน** ทั้งนี้แนวคิดและมุมมองดังกล่าวนี้จะส่งผลต่อการให้ข้อเสนอแนะหรือการวางมาตรการในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ซึ่งจำเป็นจะต้องนำข้อมูลข้อเท็จจริงและมุมมองต่างๆ โดยเฉพาะประเด็นในเรื่องสภาพปัญหาและสาเหตุของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรม มาใช้ในการพิจารณาเพื่อให้เกิดการกำหนดมาตรการที่เหมาะสมและสร้างความสมดุลและสอดรับกับสถานการณ์ จนสามารถนำไปใช้ในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสที่เหมาะสมกับประเทศไทยได้ ซึ่งจะได้กล่าวถึงต่อไป

4.2 สภาพปัญหาและสาเหตุของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมในประเทศไทยในปัจจุบัน

จากลักษณะและรูปแบบของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมในประเทศไทยดังที่ได้กล่าวมาแล้ว ได้มีผู้ให้ข้อมูลสำคัญกล่าวถึงสภาพปัญหาและสาเหตุของการเกิดอาชญากรรมดังกล่าวในประเด็นต่างๆดังนี้

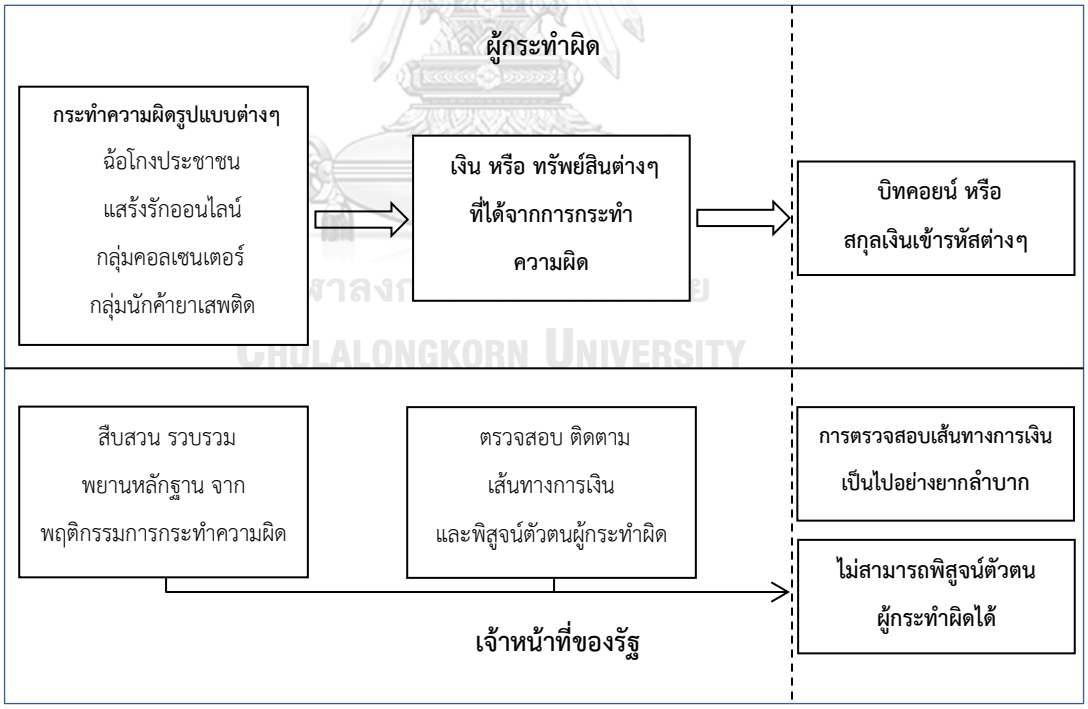
4.2.1 สภาพปัญหาและสาเหตุจาก “คุณลักษณะของบิทคอยน์”

“พอมีคริปโตเคอเรนซีเกิดขึ้นอย่างบิทคอยน์ คนร้ายก็เปลี่ยนเป็นซื้อบิทคอยน์ ทำให้ตามเงินยาก คือ โดนจับคดีอาญา แต่พอสืบทรัพย์ไม่สามารถสืบทรัพย์ได้ เพราะมันอยู่ในโลกดิจิทัลและไม่สามารถระบุตัวตนได้ การที่ไม่มีการลงทะเบียนเท่ากับปล่อยโอกาสให้คนที่ทำความผิดสามารถปกปิดตัวตนได้”

(C1, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

ในประเด็นเรื่องสภาพปัญหาและสาเหตุของการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรมจากลักษณะพิเศษของบิทคอยน์นี้มีผู้ให้ข้อมูลสำคัญได้ให้ความเห็นไว้แตกต่างกัน โดยผู้ทรงคุณวุฒิกลุ่มหนึ่งมีความเห็นว่าการที่บิทคอยน์ถูกนำมาใช้เป็นเครื่องมือในการก่ออาชญากรรมนั้นมีสาเหตุมาจาก**ลักษณะพิเศษของบิทคอยน์ที่เอื้อต่อการนำไปใช้เป็นเครื่องมือในการกระทำความผิด** ได้แก่ การอยู่ในรูปแบบของ**ข้อมูลอิเล็กทรอนิกส์ที่ไม่มีรูปร่าง ไม่สามารถจับต้องได้ มีระบบการทำงานและเก็บข้อมูลบนเครือข่ายคอมพิวเตอร์ที่ไม่มีฐานข้อมูลกลาง (Server) แต่ใช้ระบบการกระจายข้อมูลที่ให้ผู้ใช้งานสามารถซื้อขายแลกเปลี่ยนกันได้โดยตรง (Peer – to - Peer) โดยไม่จำเป็นต้องผ่านการตรวจสอบจากรัฐบาลหรือตัวกลางอย่างธนาคารหรือสถาบันการเงินต่างๆ** ด้วยลักษณะต่างๆดังกล่าวนี้จึงทำให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆสามารถถูกนำไปใช้งานได้ทั่วโลกโดยปราศจากการตรวจสอบที่มา ทั้งยังง่ายต่อการเป็นเครื่องมือในการเคลื่อนย้ายหรือปกปิดทรัพย์ ประกอบกับข้อมูลต่างๆที่เกี่ยวข้องยังถูกรักษาความปลอดภัยไว้อย่างแน่นหนา จึงทำให้การตรวจสอบข้อมูลต่างๆกระทำได้ยาก นอกจากนี้ลักษณะพิเศษที่สำคัญอีกประการหนึ่งของบิทคอยน์คือการที่**ผู้ใช้งานไม่จำเป็นต้องทำการยืนยันหรือแสดงตัวตนที่แท้จริง** ซึ่งเป็นลักษณะพิเศษที่ถูกออกแบบเพื่อสร้างความเป็นส่วนตัวให้กับผู้ใช้งาน และต้องการให้เกิดความคล่องตัวในการทำธุรกรรมมากที่สุด แต่อย่างไรก็ตามลักษณะพิเศษที่ไม่สามารถยืนยันตัวตนผู้ใช้งานที่แท้จริงได้นี้ เป็นช่องว่างสำคัญที่ทำให้กลุ่มอาชญากรอาศัยบิทคอยน์เป็นเครื่องมือในการกระทำความผิด เพราะ**ผู้กระทำผิดสามารถปกปิดตัวตนและนำบิทคอยน์ไปใช้ในการกระทำความผิดได้โดยไม่ถูกตรวจสอบตัวตนจากกลไกใดๆ และยังไม่ต้องกลัวว่าจะถูกสุ่มตรวจสอบจากเจ้าหน้าที่ของรัฐอีกด้วย**

โดยผลที่เกิดขึ้นจากการที่ผู้กระทำผิดอาศัยลักษณะพิเศษต่างๆของบิทคอยน์ไปใช้ในการกระทำความผิดนั้น ทำให้เกิดสภาพปัญหาที่เจ้าหน้าที่ของรัฐไม่สามารถติดตามหรือตรวจสอบเส้นทางการเงิน และประสบความยากลำบากในการสืบสวนหาตัวการผู้กระทำผิดที่แท้จริงเป็นอย่างมาก เช่น ในกรณีของการฟอกเงินด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆหากเป็นรูปแบบของการกระทำผิดแบบดั้งเดิมนั้น เมื่อเจ้าหน้าที่ทำการสืบสวนจับกุมตามมูลความผิดหลัก (ฉ้อโกง หลอกลวง หรือ การกระทำความผิดอื่นๆซึ่งเป็นต้นเหตุแห่งการได้เงินผลประโยชน์มาโดยมิชอบ) ก็จะสามารถสืบสวนสอบสวนเส้นทางการเงิน เพื่อพิสูจน์ทราบบัญชีที่คนร้ายใช้ซุกซ่อนเงินที่ได้จากการกระทำความผิดและจะสามารถทำการอายัดเงินดังกล่าวได้ในที่สุด แต่**หากเป็นกรณีที่คนร้ายใช้สกุลเงินเข้ารหัสอย่างบิทคอยน์ในการซุกซ่อนเงินผลประโยชน์ที่ได้จากการกระทำความผิดต่างๆ จะส่งผลทำให้โอกาสที่จะสามารถสืบสวนสอบสวนจนสามารถทราบตัวตนของผู้กระทำผิดและทำการอายัดบิทคอยน์หรือสกุลเงินเข้ารหัสได้เป็นไปอย่างยากลำบาก** โดยผู้วิจัยได้แสดงให้เห็นถึงสภาพปัญหาดังกล่าวได้จากภาพดังต่อไปนี้



ภาพที่ 25 สภาพปัญหาของการตรวจสอบติดตามเส้นทางการเงินและการพิสูจน์ตัวตนผู้กระทำผิดที่เกิดจากลักษณะพิเศษของบิทคอยน์

(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2563)

ขณะที่มีผู้ให้ข้อมูลสำคัญให้ความเห็นในมุมมองเปรียบเทียบกับ**การกระทำผิดด้วยการใช้เงินสดเป็นสื่อกลางในการกระทำผิดที่เกิดขึ้นในปัจจุบัน ก็มีลักษณะเช่นเดียวกับคุณลักษณะของบิทคอยน์หรือสกุลเงินเข้ารหัส** เช่น ในประเด็นปัญหาเรื่อง **ลักษณะของการซื้อขายแลกเปลี่ยนบิทคอยน์กันได้โดยตรง (Peer – to - Peer) โดยไม่ผ่านตัวกลางอย่างธนาคารหรือสถาบันทางการเงินต่างๆนั้น** ผู้ให้ข้อมูลสำคัญให้ความเห็นว่าเมื่อพิจารณาเทียบเคียงกับกรณีที่คนร้ายหรือผู้กระทำผิดใช้เงินสดในการซื้อขายแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมายระหว่างกันก็มีลักษณะเป็นการแลกเปลี่ยนกันโดยตรง (Peer – to - Peer) เช่นเดียวกัน และการที่คนร้ายใช้เงินสดในการกระทำความผิด ก็มีความยากลำบากในการตรวจสอบเส้นทางการเงินและการตรวจสอบตัวตนผู้กระทำความผิดไม่แตกต่างกัน นอกจากนี้อาจกล่าวได้ว่าบิทคอยน์ยังมีโอกาสที่จะทิ้งร่องรอยได้มากกว่าการใช้เงินสด เพราะมีการบันทึกข้อมูลการทำธุรกรรมทุกธุรกรรมแบบกระจายข้อมูล และยังมีการรักษาความปลอดภัยของข้อมูลนั้นด้วยการเข้ารหัสไว้ในระบบการเก็บข้อมูลด้วยเครือข่ายคอมพิวเตอร์ นอกจากนี้ยังมีผู้ให้ข้อมูลสำคัญชี้ให้เห็นถึง**ความแตกต่างระหว่างการใช้เงินสดและการใช้บิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆเป็นเครื่องมือในการกระทำความผิด**ว่า แม้การใช้เงินสดจะทำให้เกิดความยากลำบากในการตรวจสอบติดตามเส้นทางการเงินได้ไม่แตกต่างจากการใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆก็ตาม แต่การใช้เงินสดจะมีข้อจำกัดที่สำคัญในกรณีที่คนร้ายต้องการใช้เงินสดเป็นจำนวนมากในการกระทำความผิดและกรณีที่คนร้ายต้องการที่จะส่งมอบหรือเคลื่อนย้ายไปให้ผู้ร่วมกระทำความผิดที่อยู่ไกล เช่น การขนส่งเงินสดระหว่างประเทศที่อาจทำให้ตกเป็นเป้าหมายในการตรวจสอบจากเจ้าหน้าที่ของรัฐได้ **ขณะที่การใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นสื่อกลางในการกระทำความผิดจะปราศจากข้อจำกัดดังกล่าว เนื่องจากสามารถทำธุรกรรมระหว่างประเทศได้อย่างไม่จำกัดจำนวน** ด้วยสาเหตุดังกล่าวจึงทำให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นช่องทางสำคัญช่องทางหนึ่งที่อาชญากรนำไปใช้เป็นเครื่องมือในการกระทำความผิด

อีกกรณีหนึ่งที่ผู้ให้ข้อมูลสำคัญนำมาเทียบเคียงคือ ประเด็นปัญหา**เรื่องการปกปิดตัวตนผู้ใช้งานที่แท้จริง**ของบิทคอยน์ ซึ่งเมื่อเทียบเคียงกับกรณีของการเปิดบัญชีธนาคารที่ถูกกำหนดให้จะต้องมีการแสดงตนด้วยเอกสารทางราชการเพื่อยืนยันความเป็นเจ้าของบัญชีผู้ใช้งานนั้นๆ แต่ก็ปรากฏว่า คนร้ายก็ใช้วิธีการว่าจ้างให้ผู้อื่นซึ่งไม่เกี่ยวข้องกับการกระทำความผิดหลักมาเปิดบัญชีแทน ซึ่งส่งผลทำให้การตรวจสอบติดตามหรือการสืบสวนจนพบผู้กระทำผิดที่แท้จริงของเจ้าหน้าที่ของรัฐใน

กรณีเช่นนี้กับกรณีที่ผู้กระทำผิดใช้บิทคอยน์เป็นเครื่องมือในการกระทำผิด เกิดความยากลำบากไม่ต่างกัน

“ต้องมองว่า (บิทคอยน์)เป็นแค่เครื่องมือหนึ่ง เพราะถ้าบอกว่าเป็น Peer – to – Peer เงินสดก็เป็น Peer – to – Peer เหมือนกัน จริงๆถ้าเทียบกับการเอาเงินสดไปยื่นให้กันเราก็ตรวจสอบไม่ได้เหมือนกัน สำหรับบิทคอยน์ถ้าเป็นคนที่รู้จริงๆก็สามารถทำได้ แม้แทบจะตรวจสอบไม่ได้ในทางปฏิบัติ แต่ในทางทฤษฎีมีความเป็นไปได้”

(A5, สัมภาษณ์, 26 พฤศจิกายน 2562)

“การใช้เงินสดไปทำผิดต่างๆก็ติดตามไม่ได้เหมือนกัน แต่การใช้เงินสดมีข้อเสียคือ ถ้าต้องใช้จำนวนมากๆ กับถ้าต้องจ่ายให้กับคนที่อยู่ไกลๆ เงินสดจะไม่ตอบโจทย์ตรงนี้ แต่ถ้าเป็นคริปโทเคอเรนซีจะไม่เจอปัญหาสองข้อนี้ ดังนั้น พวกอาชญากรที่มีความไฮเทคจะหันมาใช้เป็นช่องทางหนึ่งแน่นอน”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

“มันก็จะเหมือนกับการรับเปิดบัญชีให้กัน ซึ่งมันก็ยังตรวจสอบไม่ได้ว่าใครเป็นตัวการที่เป็นผู้กระทำผิดที่แท้จริง”

(B1, สัมภาษณ์, 28 พฤศจิกายน 2562)

นอกจากลักษณะของบิทคอยน์ในเรื่องของการปกปิดตัวตนผู้ใช้งานที่แท้จริงและระบบการใช้งานที่ถูกออกแบบมาให้มีการใช้งานแบบไม่ต้องผ่านตัวกลาง (Peer – to – Peer) ที่เอื้อต่อการนำไปใช้ในการก่ออาชญากรรมแล้ว ยังมีผู้ให้ข้อมูลสำคัญได้กล่าวถึงลักษณะพิเศษอีกประการหนึ่งที่จูงใจให้เกิดการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมคือ**ลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์และมีการทำงานบนระบบเครือข่ายคอมพิวเตอร์ ทำให้การใช้งานในการกระทำความผิดนั้นสามารถกระทำได้จากทุกหนแห่งทั่วโลก ไม่มีพรหมแดนหรือไม่อยู่ภายใต้เขตแดนของรัฐในทางกายภาพ**อีกต่อไป ซึ่งผลของลักษณะดังกล่าวทำให้เจ้าหน้าที่ที่มีหน้าที่ในการบังคับใช้กฎหมายประสบปัญหาอันเนื่องมาจากข้อจำกัดของการใช้กฎหมายของแต่ละประเทศ ที่จำเป็นจะต้องพิจารณาถึงเขตอำนาจตามเขตแดน

ของรัฐ โดยผู้ให้ข้อมูลสำคัญได้ยกตัวอย่างในกรณีหากเกิดการนำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ ไปใช้ในการกระทำความผิด ซึ่งไม่สามารถระบุได้แน่ชัดว่าขณะกำลังกระทำความผิดนั้น อาชญากรกระทำในประเทศไทยหรือต่างประเทศ กรณีเช่นนี้จะทำให้เกิดความไม่ชัดเจนว่าจะสามารถนำกฎหมายไปบังคับใช้ได้หรือไม่ หรือในกรณีที่ข้อมูลหรือพยานหลักฐานสำคัญที่เกี่ยวกับอาชญากรรมที่ใช้บิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆเป็นเครื่องมือนั้นอยู่ในต่างประเทศ ก็จะทำให้เจ้าหน้าที่ของรัฐจะต้องประสานงานและขอความร่วมมือไปยังหน่วยงานในต่างประเทศซึ่งมีขั้นตอนและพิธีการต่างๆ จำนวนมาก จนอาจจะส่งผลกระทบต่อการรวบรวมข้อมูลและพยานหลักฐานต่างๆ และยังส่งผลทำให้รัฐไม่สามารถป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างทันท่วงที

ส่วนประเด็นที่สำคัญอีกประการหนึ่งที่มีผู้ให้ข้อมูลสำคัญได้วิเคราะห์ถึงสาเหตุที่บิทคอยน์ได้รับความนิยมในการใช้งานตามปกติรวมถึงการถูกนำไปใช้ในการก่ออาชญากรรมมากกว่าสกุลเงินเข้ารหัสสกุลอื่นเนื่องมาจากการที่บิทคอยน์ถูกสร้างเป็นสกุลเงินเข้ารหัสขึ้นเป็นสกุลแรกและยังเป็นสกุลเงินเข้ารหัสสกุลแรกที่นำระบบบล็อคเชน (Blockchain) มาใช้ ทำให้เกิดความน่าเชื่อถือและเกิดกระบวนการสร้างภาพลักษณ์ (Branding) จนทำให้คนทั่วไปหรืออาชญากรเมื่อต้องการใช้งานสกุลเงินเข้ารหัสก็มักจะนึกถึงบิทคอยน์เป็นสกุลแรก ทั้งจากปริมาณผู้ใช้งานและส่วนแบ่งการตลาดที่มากที่สุดด้วยปัจจัยต่างๆเหล่านี้ จึงทำให้บิทคอยน์ถูกนำมาใช้งานในการก่ออาชญากรรมมากกว่าสกุลเงินเข้ารหัสสกุลอื่น

“สภาพปัญหาของมัน ต้องยอมรับว่าสกุลเงินเข้ารหัสพวกนี้มันอยู่ในโลกเสมือนจริง ที่ไม่มีพรหมแดน ไม่สามารถระบุให้ชัดเจนว่ามีการใช้งานอยู่ในขอบเขตของประเทศใด หรือถ้าหากทราบว่าเป็นเรื่องระหว่างประเทศ ก็ยังมีประเด็นอีกว่าจะขอความร่วมมือจากต่างประเทศอย่างไร”

(A2, สัมภาษณ์, 19 พฤษภาคม 2563)

“มันเป็นตัวแรก ทำให้แง่ของการ Branding จึงทำให้เกิดความเชื่อ คล้ายๆกับทำไมเราเรียกบะหมี่กึ่งสำเร็จรูปว่า มาม่า เพราะมันเป็นตัวแรกที่สำเร็จและน่าเชื่อถือ ตัวมันมีมูลค่าสูงสุด มีคนใช้งานมากที่สุด ย่อมเปิดโอกาสให้คนร้ายนำไปใช้ได้ง่าย และยังมีระบบ Decentralized ที่โอกาสที่จะถูกควบคุมระบบโดยใครคนใดคนหนึ่งจะเป็นไปไม่ได้”

(A5, สัมภาษณ์, 26 พฤศจิกายน 2562)

จากข้อมูลที่ได้จากผู้ให้ข้อมูลสำคัญที่กล่าวมานี้สามารถสรุปได้ว่าลักษณะพิเศษของบิทคอยน์ที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ที่ไม่มีรูปร่าง ไม่สามารถจับต้องได้ มีระบบการทำงานและเก็บข้อมูลบนเครือข่ายคอมพิวเตอร์ที่ไม่มีฐานข้อมูลกลาง (Server) แต่ใช้ระบบการกระจายข้อมูลที่ให้ผู้ใช้งานสามารถซื้อขายแลกเปลี่ยนกันได้โดยตรง (Peer – to - Peer) โดยไม่จำเป็นต้องผ่านการตรวจสอบจากรัฐบาลหรือตัวกลางอย่างธนาคารหรือสถาบันการเงินต่างๆ ทั้งยังสามารถใช้งานได้จากทุกหนแห่งทั่วโลก ไม่อยู่ภายใต้ข้อจำกัดของพรมแดนหรือไม่อยู่ภายใต้เขตแดนของรัฐ (Borderless) โดยเฉพาะอย่างยิ่งการที่ผู้ใช้งานไม่จำเป็นต้องทำการยืนยันหรือแสดงตัวตนที่แท้จริง (Anonymity) เป็นสาเหตุสำคัญที่ทำให้บิทคอยน์ถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรมต่างๆ เนื่องจากทำให้เกิดสภาพปัญหาสำคัญคือ เจ้าหน้าที่ของรัฐยังไม่สามารถตรวจสอบติดตามเส้นทางการเงินได้โดยง่าย อีกทั้งยังไม่สามารถตรวจสอบยืนยันหรือพิสูจน์ตัวตนผู้กระทำผิดที่แท้จริงได้อีกด้วย ซึ่งข้อมูลดังกล่าวสอดคล้องกันกับงานวิจัยของ **J. R. Clark, M. Scott Niederjohn, and William C. Wood (2018), Sean Foley, Jonathan R. Karlsen and Talis J. Putnins (2018)** และ **Adam Turner and Angela Samantha Maitland Irwin (2018)** ที่กล่าวถึงสาเหตุสำคัญของการที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆถูกนำไปใช้ในการก่ออาชญากรรมตรงกันคือ ลักษณะพิเศษต่างๆของบิทคอยน์โดยเฉพาะอย่างยิ่งลักษณะของการไร้ตัวตน หรือ การไม่สามารถระบุตัวตนของผู้ใช้งานที่แท้จริงได้ (Anonymity) ดังนั้น จากการศึกษาจึงทำให้ผู้วิจัยวิเคราะห์และสรุปผลการศึกษาในประเด็นนี้ได้ว่าสภาพปัญหาและสาเหตุที่ทำให้เกิดการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมที่สำคัญประการหนึ่งคือลักษณะพิเศษต่างๆของบิทคอยน์เองที่เอื้อต่อการถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรม

4.2.2 สภาพปัญหาและสาเหตุจาก “กฎหมาย”

1) สถานภาพทางกฎหมายของบิทคอยน์

ประเด็นปัญหาในเรื่องสถานภาพทางกฎหมายของบิทคอยน์นั้น สืบเนื่องมาจากการที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เป็นสิ่งที่ถูกประดิษฐ์คิดค้นขึ้นใหม่ซึ่งมีลักษณะแตกต่างไปจากสื่อกลางในการแลกเปลี่ยนสินค้าและบริการชนิดเดิม ทำให้เกิด**สภาวะที่กฎหมายที่มีใช้อยู่ในปัจจุบันไม่สามารถนำมาปรับใช้ได้อย่างครอบคลุมและทำให้เกิดความคลุมเครือในการตีความสถานภาพทางกฎหมายของบิทคอยน์** ทำให้เกิดการขาดประสิทธิภาพในการกำกับดูแลในทางปฏิบัติซึ่งประเด็น

ปัญหานี้มีความสำคัญเป็นอย่างมาก เพราะหากรัฐไม่ได้มีการกำหนดสถานภาพของบิทคอยน์และสกุลเงินเข้ารหัสให้ชัดเจนและครบถ้วนแล้ว จะส่งผลต่อการบังคับใช้กฎหมายในทุกระดับตั้งแต่ในระดับเจ้าหน้าที่ผู้ปฏิบัติงานที่ไม่ทราบว่าจะต้องใช้อำนาจตามกฎหมายใดเพื่อมาใช้บังคับ ไปจนถึงในระดับการพิจารณาคดีที่จะเกิดปัญหาในเรื่องของการตีความตามกฎหมายที่มีอยู่ เป็นต้น

โดยในประเด็นปัญหาดังกล่าวนี้ ได้มีผู้ให้ข้อมูลสำคัญกล่าวถึงสถานภาพของบิทคอยน์ว่าในประเด็นต่างๆ ได้แก่ **ประเด็นของความเป็นทรัพย์สิน** จากเริ่มแรกที่บิทคอยน์เริ่มเข้ามาแพร่หลายในประเทศไทยนั้นไม่ได้มีกฎหมายเฉพาะใดๆมารองรับสถานะ แม้จะมีความคล้ายกับการเป็นเงินเนื่องจากใช้ในการแลกเปลี่ยนสินค้าและบริการต่างๆได้แต่ก็ยัง**ไม่ครบหลักเกณฑ์การเป็นเงินตราตามบทบัญญัติใน พ.ร.บ.เงินตรา พ.ศ. 2501** แต่อย่างใด จนต่อมาหลังจากที่ได้มีการออกกฎหมาย พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 **บัญญัติให้สกุลเงินเข้ารหัส (คริปโทเคอเรนซี) ถือเป็นสินทรัพย์ประเภทสินทรัพย์ดิจิทัล** ดังนั้น ในทางกฎหมายแล้วจึงทำให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆถือเป็นสินทรัพย์ชนิดหนึ่งที่มีราคาและอาจถือเอาได้ตามกฎหมาย ดังนั้น จากผลของกฎหมายดังกล่าวจึงทำให้สถานภาพของ**บิทคอยน์และสกุลเงินเข้ารหัสต่างๆถือเป็นทรัพย์สินประเภทหนึ่งตามประมวลกฎหมายแพ่ง แม้จะไม่ถือเป็นเงินตราก็ตาม** ดังนั้นเมื่อถือเป็นทรัพย์สินประเภทหนึ่งแล้ว การนำกฎหมายทางแพ่งมาปรับใช้ก็สามารถกระทำได้ เช่น หากมีข้อพิพาทกันเรื่องการซื้อขายแลกเปลี่ยนต่างๆ ก็จะนำหลักกฎหมายที่เกี่ยวกับนิติกรรมและสัญญามาปรับใช้ เป็นต้น

ส่วน**ประเด็นของความเป็นทรัพย์ในทางอาญา**นั้น ก็จำเป็นจะต้องพิจารณาเช่นกันโดยความเป็นทรัพย์ในทางอาญานั้นจะเกี่ยวข้องในประเด็นที่หากเกิดข้อพิพาทในทางอาญาอย่างกรณีการลักบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆขึ้นหรือมีการฉ้อโกงกัน จะถือเป็นการลักทรัพย์ตามกฎหมายอาญาหรือไม่นั้น ได้มีผู้ให้ข้อมูลสำคัญให้ความเห็นว่าประมวลกฎหมายอาญาไม่ได้ให้คำนิยามของคำว่า “ทรัพย์” ไว้แต่อย่างใด ในการตีความว่าวัตถุชนิดใดเป็นทรัพย์หรือไม่นั้น จะต้องอาศัยบทบัญญัติตามประมวลกฎหมายแพ่งและพาณิชย์ ในมาตรา 137 ที่บัญญัติไว้ว่า “ทรัพย์ หมายความว่า วัตถุมีรูปร่าง” ดังนั้นเมื่อพิจารณาในเบื้องต้นก็จะพบว่า ด้วยลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ไม่มีรูปร่าง ไม่สามารถจับต้องได้ ก็จะไม่เป็น “ทรัพย์” ทั้งในทางแพ่งและทางอาญา ประกอบกับ**คำพิพากษาศาลฎีกาที่ 5161/47** ซึ่งเป็นคดีที่มีการฟ้องร้องกันเกี่ยวกับการกระทำที่ลูกจ้างลักลอบใช้อุปกรณ์เก็บข้อมูล (Floppy Disk) ทำการคัดลอกข้อมูลของนายจ้างไป ซึ่งในกรณีพิพาทนี้ศาลได้ตีความว่าข้อมูลคอมพิวเตอร์ ไม่ใช่วัตถุที่มีรูปร่าง แม้จะมีการแสดงออกมาผ่านอุปกรณ์

คอมพิวเตอร์หรือหน้าจอคอมพิวเตอร์แต่ก็ไม่ใช่รูปร่างที่แท้จริงของข้อมูล ดังนั้น ข้อมูลคอมพิวเตอร์จึงไม่ถือเป็นทรัพย์ เมื่อไม่ถือเป็นทรัพย์ก็ไม่เข้าองค์ประกอบความผิดเรื่องลักทรัพย์ จากการเทียบเคียงหลักการและคำพิพากษาศาลฎีกาดังกล่าวจึงสามารถสรุปได้ว่า **บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ไม่ถือเป็นทรัพย์ในทางอาญา**

“เดิมบิทคอยน์ไม่มีอะไรมารองรับก็จริง แต่ต่อมามี พ.ร.ก.สินทรัพย์ดิจิทัล มายอมรับว่าเป็นสินทรัพย์ดิจิทัล ซึ่งมีมูลค่าในตัวเอง ทีนี้ถามว่าเมื่อเป็นสินทรัพย์ดิจิทัลแล้วก็ถือเป็นทรัพย์สินอย่างหนึ่ง แม้จะไม่ได้เป็นเงินตราแต่ก็ถือเป็นทรัพย์สิน และถามว่าคำว่า “ทรัพย์” ในทางกฎหมายอาญา จะตีความรวมถึงทรัพย์สินด้วยหรือไม่ ความเห็นผมว่าไม่ใช่ เพราะคำว่า “ทรัพย์”ในอาญาไม่ได้ให้นิยามไว้ ก็ต้องไปตีความตามกฎหมายแพ่งว่าทรัพย์จะต้องเป็นวัตถุที่มีรูปร่าง ดังนั้น บิทคอยน์จึงไม่น่าใช่ทรัพย์ในทางอาญา”

(B1, สัมภาษณ์, 28 พฤศจิกายน 2562)

“ศาลมองว่า ข้อมูลคอมพิวเตอร์มันไม่ใช่ทรัพย์เพราะมันไม่ใช่วัตถุที่มีรูปร่าง ศาลตีความว่าภาพที่เราเห็นที่หน้าจอเนี่ยไม่ใช่รูปร่างที่แท้จริงของข้อมูล ดังนั้นข้อมูลพวกนี้จึงไม่มีลักษณะเป็นทรัพย์ เมื่อไม่เป็นทรัพย์ ก็ไม่ผิดข้อหาลักทรัพย์”

(B2, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

อย่างไรก็ตามตามความเห็นของผู้ให้ข้อมูลสำคัญซึ่งเป็นผู้ทรงคุณวุฒิทางด้านกฎหมายยังได้ให้ความเห็นไว้ว่า แม้ในปัจจุบันบิทคอยน์และสกุลเงินเข้ารหัสจะไม่ถือเป็นทรัพย์ตามประมวลกฎหมายอาญาก็ตาม แต่เมื่อเกิดการกระทำผิดทางอาญาที่เกี่ยวกับบิทคอยน์หรือสกุลเงินเข้ารหัสก็ยังสามารถนำกฎหมายอาญาและกฎหมายที่มีโทษทางอาญามาปรับใช้ได้ เช่น ความผิดเกี่ยวกับเอกสาร หรือแม้กระทั่งหากเกิดลักษณะของการกระทำผิดบางลักษณะ เช่น หากเกิดกรณีการลักขโมยบิทคอยน์และสกุลเงินเข้ารหัสต่างๆขึ้นจริง ก็ยังสามารถนำ **พ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาปรับใช้ได้** หรือหากมีการนำบิทคอยน์ไปใช้ในการฟอกเงิน ก็สามารถใช้**กฎหมายที่เกี่ยวกับการฟอกเงิน**มาปรับใช้ได้ และหากในอนาคตมีการเปลี่ยนแปลงแนวทางการตีความหรือมีคำพิพากษาศาลฎีกาที่กำหนดให้ถือว่าบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นทรัพย์

ในทางกฎหมายอาญาด้วย หากมีการกระทำในลักษณะการลักลอบเข้าระบบเพื่อขโมยบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ ก็จะการเป็นการกระทำผิดกรรมเดียวผิดกฎหมายหลายบท ซึ่งทำให้สามารถลงโทษผู้กระทำผิดได้ทั้งในทางกฎหมายอาญาและโทษตามพ.ร.บ.ว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

“ไม่ใช่ไม่เข้าข้อกฎหมายทางอาญา แค่ไม่เป็นทรัพย์ก็ไม่ผิดฐานลักทรัพย์เท่านั้นเอง แต่ยังมีกฎหมายที่เอามาปรับใช้ได้ เช่น มันมีสถานะเป็นข้อมูลคอมพิวเตอร์ ก็เอา พ.ร.บ.คอมพิวเตอร์มาปรับใช้ความผิดทางอาญาในเรื่องของเอกสาร หรือในเรื่องของการฟอกเงินก็นำมาบังคับได้ ”

(B2, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

2) พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ไม่สามารถใช้เป็นเครื่องมือในการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมได้

ผู้ให้ข้อมูลสำคัญได้กล่าวถึงสภาพปัญหาและสาเหตุที่สำคัญอีกประการหนึ่งคือกฎหมายซึ่งเป็นเครื่องมือหลักของรัฐที่ใช้ในการกำกับดูแลสกุลเงินเข้ารหัสอย่าง พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ที่ยังมีข้อบกพร่องบางประการส่งผลให้ยังไม่สามารถทำหน้าที่เป็นเครื่องมือในการป้องกันอาชญากรรมที่มีประสิทธิภาพได้ ผู้ให้ข้อมูลสำคัญพบกล่าวถึงประเด็นปัญหานี้ว่าเจตนารมณ์ของกฎหมายฉบับนี้สามารถแบ่งออกได้เป็นสองประเด็นหลัก คือ**ประเด็นที่หนึ่งเพื่อกำหนดคำนิยามของสินทรัพย์ดิจิทัล**และรับรองสถานะการเป็นทรัพย์สินในรูปแบบของสินทรัพย์ดิจิทัลของสกุลเงินเข้ารหัสต่างๆรวมถึงบิทคอยน์ที่ถือเป็นสกุลเงินเข้ารหัส (Cryptocurrency) สกุลหนึ่ง และนอกจากรับรองสถานะการเป็นสินทรัพย์ดิจิทัลของสกุลเงินเข้ารหัสแล้ว ยังรับรองสถานะของโทเคนดิจิทัล (Digital Token) ให้เป็นสินทรัพย์ดิจิทัลอีกประเภทหนึ่งที่ใช้เป็นเครื่องมือในการระดมทุนในลักษณะของการซื้อขายเหรียญโทเคนดิจิทัล (Initial Coin Offering หรือ ICO) แทนการซื้อหุ้นหรือผลิตภัณฑ์เพื่อการลงทุนอื่นๆ

เจตนารมณ์**ประเด็นที่สอง**คือ **มุ่งที่จะคุ้มครองนักลงทุน สร้างความเป็นธรรมและโปร่งใสให้กับกระบวนการลงทุน และป้องกันการนำสินทรัพย์ดิจิทัลไปใช้ในการก่ออาชญากรรมหรือนำไปใช้สร้างความเสียหายให้แก่ระบบเศรษฐกิจหรือความเสียหายอื่นๆต่อสังคมโดยรวมผ่านการควบคุมกำกับดูแลตัวกลางที่เป็นผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลประเภทต่างๆ** ได้แก่

ผู้ประกอบธุรกิจเป็นศูนย์ซื้อขายสินทรัพย์ดิจิทัล นายหน้าซื้อขายสินทรัพย์ดิจิทัล ผู้ค้าสินทรัพย์ดิจิทัล ให้อยู่ในความควบคุมดูแลของรัฐ ผ่านหน่วยงานที่รับผิดชอบคือ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) โดยมีมาตรการในการกำกับดูแลที่สำคัญคือ **การใช้ระบบการออกใบอนุญาต** โดยสำนักงาน ก.ล.ต.จะเป็นหน่วยงานที่ทำหน้าที่กำหนดเงื่อนไขและหลักเกณฑ์ต่างๆ เพื่อให้ผู้ที่ต้องการประกอบธุรกิจดังกล่าวมาขอรับการอนุญาตประกอบกิจการ ทั้งนี้ภายหลังจากที่ได้รับอนุญาตแล้วยังจะต้องประกอบธุรกิจให้เป็นไปตามที่กฎหมายกำหนดโดยมาตรการบังคับที่สำคัญประการหนึ่งคือ **การกำหนดให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจะต้องมีมาตรการการรู้จักลูกค้าและการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า** ซึ่งมาตรการดังกล่าวถือเป็นมาตรการสากลในเรื่องความปลอดภัยทางการเงินที่นิยมเรียกว่า KYC หรือ Know Your Customer นอกจากนี้กฎหมายนี้ยังได้มีการกำหนดให้ผู้ที่ได้รับอนุญาตให้ประกอบธุรกิจสินทรัพย์ดิจิทัลจะต้องปฏิบัติตามมาตรการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้ายหรือการฟอกเงิน รวมทั้งยังถือว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลถือเป็นสถาบันการเงินตามกฎหมายที่เกี่ยวกับการป้องกันปราบปรามการฟอกเงินอีกด้วย

“พ.ร.ก.ตัวนี้ จะกำหนดนิยามของสินทรัพย์ดิจิทัลครอบคลุมทั้ง คริปโทเคอเรนซี และโทเคนดิจิทัล เมื่ออยู่ภายใต้กรอบของ พ.ร.ก.ตัวนี้แล้ว ผลจาก พ.ร.ก.ตัวนี้คือ กำหนดให้ผู้ประกอบธุรกิจเป็นสถาบันการเงินตามกฎหมายฟอกเงิน เหตุผลหลักในส่วนนี้ก็คือเราต้องการที่จะกำกับตัวกลางที่เกี่ยวกับการซื้อขายแลกเปลี่ยน การเป็นDealer Broker คุณจะต้องทำ KYC ลูกค้า จะต้องตรวจสอบที่มาที่ไป อันนี้เป็นวัตถุประสงค์หลักของ พ.ร.ก.”

(A2, สัมภาษณ์, 19 พฤษภาคม 2563)

อย่างไรก็ตาม แม้ใน พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 จะมีการวางมาตรการต่างๆ ที่ถือเป็นการแสดงเจตนารมณ์ที่ชัดเจนว่านอกจากต้องการกำกับดูแลการประกอบธุรกิจแล้วยังต้องการที่จะป้องกันไม่ให้มีการนำสกุลเงินเข้ารหัสไปใช้ในทางที่ผิดกฎหมายหรือนำไปใช้ก่ออาชญากรรมต่างๆด้วย ดังที่ปรากฏออกมาตามมาตรการต่างๆที่ได้กล่าวไปแล้ว แต่ยังได้มีผู้ให้ข้อมูลสำคัญชี้ให้เห็นถึงสภาพปัญหาว่า**มาตรการต่างๆที่กฎหมายกำหนดไม่สามารถนำมาใช้ในการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆได้** เนื่องจากเมื่อพิจารณาในเชิงลึกจะพบว่า

มาตรการต่างๆที่**กฎหมายนี้วางหลักเกณฑ์ไว้นั้น ใช้บังคับเฉพาะกับตัวกลางที่เป็นผู้ได้รับอนุญาตให้ประกอบธุรกิจสินทรัพย์ดิจิทัลเท่านั้น แต่ไม่ได้มีการวางหลักเกณฑ์เกี่ยวกับการตรวจสอบผู้ใช้งานในระดับปัจเจกบุคคลแต่อย่างใด** กล่าวคือกฎหมายจะเข้าไปกำกับเฉพาะตัวกลางที่ประกอบธุรกิจเท่านั้น ไม่รวมถึงการใช้งานของบุคคลทั่วไปที่ใช้งานกันเองแต่อย่างใด

โดยสาเหตุที่ พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 มุ่งที่จะควบคุมเฉพาะผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลนั้น ได้มีผู้ให้ข้อมูลสำคัญซึ่งเป็นผู้ทรงคุณวุฒิทางด้านกฎหมายให้ความเห็นไว้ว่า ด้วยเหตุผลที่ในปัจจุบันรัฐยังมองว่าตัวสินทรัพย์ดิจิทัลไม่ได้มีความผิดในตนเอง ทั้งยังเป็นเทคโนโลยีที่อาจนำมาซึ่งการพัฒนาด้านเศรษฐกิจในรูปแบบต่างๆ ดังนั้น กฎหมายจึงยังไม่ได้เข้าไปควบคุมถึงในระดับการใช้งานทั่วไปเนื่องจากจะเป็นการริดรอนสิทธิเสรีภาพของประชาชน แต่เพื่อเป็นการควบคุมการประกอบธุรกิจดังกล่าว ไม่ให้เกิดความเสียหายอันอาจจะกระทบต่อระบบบเศรษฐกิจหรือความสงบสุขในภาพรวมของประเทศ จึงยังจำเป็นจะต้องมีกลไกควบคุมกำกับดูแลตัวกลางที่แสดงตัวเป็นผู้ประกอบธุรกิจต่างๆ

“พ.ร.ก.ตัวนี้ เราจะกำกับเฉพาะตัวกลางที่ประกอบธุรกิจ แต่ถ้าเป็นตัวบุคคลที่ใช้งานกันเองผ่าน Wallet ของตนเอง ไปซื้อของกันเองโดยไม่ผ่านผู้ประกอบธุรกิจ ถ้าเป็นลักษณะนี้ พ.ร.ก. นี้จะไม่ได้กำกับ”

(A2, สัมภาษณ์, 19 พฤษภาคม 2563)

“กฎหมายปัจจุบันควบคุมเพียงแค่การประกอบธุรกิจ ยังไม่ได้ครอบคลุมการใช้งานทั่วไป”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

“เนื่องจากข้อจำกัดที่ว่าเราไปริดรอนเสรีภาพไม่ได้ เราก็เลยกำหนดให้เฉพาะคนที่จะเป็นผู้ให้บริการแลกเปลี่ยนในการทำธุรกิจพวกนี้ แต่ถ้าเป็นชาวบ้านมีบิทคอยน์อยู่แล้วต้องการจะซื้อมาขายไป กฎหมายไม่ได้เข้าไปควบคุม”

(B2, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

ผู้ให้ข้อมูลสำคัญได้กล่าวถึงประเด็นปัญหาที่เป็นผลจากการที่กฎหมายหนึ่งเดียวของรัฐที่เกี่ยวข้องกับการกำกับดูแลสกุลเงินเข้ารหัสโดยตรงมิได้มีมาตรการควบคุมการใช้งานในระดับปัจเจกบุคคลว่า เมื่อกลไกของรัฐไม่มีกระบวนการที่จะเข้าไปควบคุมกำกับดูแลการใช้งานทั่วไปก็เท่ากับว่ารัฐเปิดโอกาสให้ผู้ที่ใช้งานสกุลเงินเข้ารหัสต่างๆที่ไม่ได้ใช้บริการผ่านตัวกลางหรือผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล สามารถที่จะใช้งานหรือทำธุรกรรมต่างๆเกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆได้เอง ซึ่งหมายความรวมถึง**การเป็นช่องโหว่ทางกฎหมายที่เปิดทางให้ผู้กระทำผิดสามารถนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำผิดกฎหมายหรือใช้ในกิจกรรมที่ผิดกฎหมายได้อย่างอิสระโดยไม่ถูกตรวจสอบจากรัฐ** แม้รัฐจะมีข้อมูลที่ได้จากการขึ้นทะเบียนผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลและข้อมูลที่ได้จากมาตรการการรู้จักลูกค้า (KYC) ก็ตาม แต่ก็เป็นข้อมูลเฉพาะผู้ที่แสดงตัวว่าเป็นผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลและผู้ใช้งานสกุลเงินเข้ารหัสผ่านผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลเท่านั้น ส่งผลให้เกิดสภาพปัญหาเกี่ยวกับการป้องกันการนำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมต่างๆ เนื่องจาก**รัฐไม่มีทั้งกลไกป้องกันและไม่มีข้อมูลต่างๆของผู้ใช้งานที่ไม่ได้แสดงตนอีกด้วย** จนอาจส่งผลทำให้กฎหมายเป็นตัวสนับสนุนให้เกิดการรวมตัวกันของอาชญากรที่นำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้งานอยู่ภายนอกระบบของรัฐในทางอ้อม

นอกจากนี้ผู้ให้ข้อมูลสำคัญซึ่งเป็นผู้ทรงคุณวุฒิจากหน่วยงานที่ใช้อำนาจตามกฎหมายนี้กำกับดูแลการประกอบธุรกิจสินทรัพย์ดิจิทัลโดยตรงกล่าวว่า พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 ยังติด**ข้อจำกัดในกรณีที่หากข้อมูลที่เป็นข้อมูลสำคัญของผู้ใช้งาน ถูกจัดเก็บอยู่บนระบบเครือข่ายคอมพิวเตอร์หรือถูกจัดเก็บอยู่บนเทคโนโลยีการเก็บข้อมูลบนฐานข้อมูลสาธารณะออนไลน์ (Cloud Storage) หรือฐานข้อมูลอื่นๆที่อยู่ในต่างประเทศแล้ว จะส่งผลทำให้กฎหมายนี้ไม่สามารถใช้บังคับได้** เช่น เมื่อหน่วยงานที่มีหน้าที่กำกับดูแลต้องการที่จะตรวจสอบข้อมูลต่างๆเหล่านี้ที่ถูกจัดเก็บอยู่ในระบบจัดเก็บต่างประเทศ ก็จะส่งผลทำให้เจ้าหน้าที่ของรัฐไม่สามารถตรวจสอบได้ เนื่องจากกฎหมายดังกล่าวให้สิทธิการดำเนินการตรวจสอบได้เฉพาะข้อมูลที่มีการบันทึกอยู่ภายในประเทศ

“ถึงใน พ.ร.ก.สินทรัพย์ดิจิทัลฯ กำหนดไว้ว่า คนที่ทำธุรกิจเกี่ยวกับสินทรัพย์ดิจิทัลทั้งหมด จะต้องทำ KYC แต่ในหลักปฏิบัติจริงมันไม่เป็นแบบนั้น เพราะคนที่ใช้งานกันเอง ไม่ได้เป็นลักษณะของผู้ประกอบธุรกิจ ก็ยังใช้งานแบบ Private กันอยู่ดี”

(A5, สัมภาษณ์, 26 พฤศจิกายน 2562)

“ถามว่าเมื่อไม่ให้เขาโผล่ขึ้นมาบนดินและก็ไม่มีระบบตรวจสอบ เขาก็อยู่ใต้ดินและในทางกลับกันก็เหมือนส่งเสริมให้พวกอาชญากรเข้าไปรวมกลุ่มกันอยู่ใต้ดิน แล้วเราจะเอากฎหมายบนดินไปบังคับสิ่งที่อยู่ใต้ดินมันเป็นไปได้ยาก”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

“เคสที่มีลักษณะเกี่ยวข้องกับต่างประเทศ เช่น ข้อมูลที่ถูกเก็บอยู่ในคลาวด์ของเมืองนอก ลักษณะนี้ตัวกฎหมายเอื้อมไปไม่ถึง ”

(A2, สัมภาษณ์, 19 พฤษภาคม 2563)

จากข้อมูลที่ผู้ให้ข้อมูลได้กล่าวถึงสภาพปัญหาที่ พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ในประเด็นต่างๆ สามารถสรุปได้ว่ามีสาเหตุสำคัญมาจาก**การที่กฎหมายนี้ไม่มีมาตรการการตรวจสอบยืนยันตัวตนและไม่มีมาตรการการเก็บข้อมูลเกี่ยวกับผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในระดับปัจเจกบุคคลหรือผู้ใช้งานที่ไม่ได้มีการใช้งานผ่านตัวกลางหรือผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล** ทำให้เกิดเป็นช่องว่างทางกฎหมายที่เปิดโอกาสให้ผู้กระทำผิดหรืออาชญากรนำสกุลเงินเข้ารหัสไปใช้เป็นเครื่องมือในการกระทำผิดกฎหมายได้โดยไม่มีกลไกใดมาควบคุมหรือกำกับดูแล ทั้งยังไม่ถูกบังคับด้วยกฎหมายให้ต้องแสดงตนหรือแสดงข้อมูลอื่นใด ซึ่งประเด็นปัญหานี้จะส่งผลให้เกิดความยากลำบากและส่งผลให้เกิดสภาพปัญหาต่อเจ้าหน้าที่ผู้ปฏิบัติงานซึ่งจะได้กล่าวถึงต่อไป นอกจากนี้กฎหมายดังกล่าวยัง**มีข้อจำกัดเกี่ยวกับการเข้าถึงข้อมูลที่อยู่ในต่างประเทศ** ทำให้ยังเกิดปัญหาที่ไม่สามารถเข้าถึงข้อมูลที่สามารถพิสูจน์การกระทำความผิดต่างๆที่อยู่ในต่างประเทศได้ ด้วยสภาพปัญหาต่างๆนี้จึงอาจกล่าวได้ว่า พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ยังไม่สามารถนำมาใช้เป็นกลไกของรัฐในการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสไปใช้ในการก่ออาชญากรรมได้จริง

3) ประเด็นปัญหาเรื่องการตีความกฎหมายเพื่อเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

สภาพปัญหาที่สำคัญอีกประการหนึ่ง ที่ส่งผลถึงกระบวนการเก็บรวบรวมพยานหลักฐานในคดีที่เกี่ยวกับบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ คือ **การตีความกฎหมายที่แตกต่างกันของเจ้าหน้าที่ในกระบวนการยุติธรรมจนทำให้เกิดข้อถกเถียงและความสับสนในทางปฏิบัติ** โดยผู้ให้ข้อมูลสำคัญได้กล่าวถึงประเด็นปัญหานี้ว่า ด้วยสภาพของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ไม่ได้อยู่ในรูปแบบของวัตถุสิ่งของที่มีรูปร่างและเป็นพยานหลักฐานที่จับต้องได้ทั่วไป จึงทำให้เกิดการตีความที่หลากหลายประกอบกับการที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นนวัตกรรมใหม่ที่ถูกสร้างขึ้นด้วยวิศวกรรมคอมพิวเตอร์ที่มีความซับซ้อนทำให้เกิด**ความเข้าใจเกี่ยวกับหลักการพื้นฐานและข้อเท็จจริงเกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสที่แตกต่างกัน**ของเจ้าหน้าที่ในกระบวนการยุติธรรมแต่ละคน เช่น เจ้าหน้าที่ในกระบวนการยุติธรรมที่มีความสนใจในเรื่องบิทคอยน์และสกุลเงินเข้ารหัสอาจมีความรู้ความเข้าใจในหลักการพื้นฐานเจ้าหน้าที่บางกลุ่มอาจทราบแต่เพียงว่าเป็นเครื่องมือชนิดหนึ่งที่คล้ายกับสกุลเงินจริงหรือเข้าใจว่าเป็นเครื่องมือที่ใช้ในภาคการลงทุนเท่านั้น ในขณะที่เจ้าหน้าที่อีกหลายส่วนที่ยังไม่ทราบหรือไม่เข้าใจว่าบิทคอยน์และสกุลเงินเข้ารหัสต่างๆคืออะไรหรือใช้งานอย่างไร เป็นต้น ซึ่งประเด็นปัญหานี้ส่วนหนึ่งเกิดจากตัวเจ้าหน้าที่ผู้บังคับใช้กฎหมายซึ่งจะได้กล่าวถึงในโอกาสต่อไป

เมื่อความเข้าใจในข้อเท็จจริงซึ่งเป็นหลักการพื้นฐานของบิทคอยน์และสกุลเงินเข้ารหัสแตกต่างกัน ย่อมส่งผลทำให้เกิด **ความเห็นที่ขัดแย้งกันในการตีความและการนำกฎหมายที่มีอยู่มาปรับใช้ในการเก็บพยานหลักฐาน**ในคดีที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ โดยผู้ให้ข้อมูลสำคัญได้ให้ข้อมูลว่านักกฎหมายและบุคลากรในกระบวนการยุติธรรมกลุ่มหนึ่งมีความเห็นว่า เมื่อข้อมูลและพยานหลักฐานต่างๆอยู่ในอุปกรณ์อิเล็กทรอนิกส์ซึ่งใช้ในการกระทำความผิด เช่น เครื่องคอมพิวเตอร์ หรือโทรศัพท์สมาร์ทโฟน ถ้าได้มีการตรวจยึดอุปกรณ์ดังกล่าวมาโดยชอบด้วยกฎหมายแล้วการจะเข้าถึงข้อมูลต่างๆในอุปกรณ์ของกลางนั้นๆก็สามารถกระทำได้ ซึ่งเป็นไปตามหลักการที่บัญญัติไว้ในประมวลกฎหมายวิธีพิจารณาความอาญา ในขณะที่นักกฎหมายและบุคลากรในกระบวนการยุติธรรมอีกกลุ่มหนึ่งกลับมีความเห็นแย้งว่า การจะเข้าถึงข้อมูลอิเล็กทรอนิกส์ต่างๆนั้นไม่ใช่ลักษณะเป็นการดำเนินการตามหลักการทั่วไป เนื่องจากข้อมูลลักษณะนี้ได้รับการคุ้มครองโดยสภาพและยังมีลักษณะเป็นข้อมูลส่วนบุคคล ดังนั้น การจะเข้าถึงข้อมูลดังกล่าวจึงไม่อาจนำหลัก

กฎหมายธรรมดามาใช้ในลักษณะเดียวกันกับการตรวจยึดทรัพย์ของกลางอื่นๆได้ ดังนั้น การจะเข้าถึงข้อมูลดังกล่าวจะต้องได้รับอนุญาตจากศาล ซึ่งเป็นไปตามบทบัญญัติใน พ.ร.บ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์

ประเด็นปัญหาที่เกิดขึ้นตามมาจากความเห็นทางด้านการตีความกฎหมายที่แตกต่างกันนี้ คือเจ้าหน้าที่ผู้ปฏิบัติงานเกิดความสับสนและเกิดความไม่แน่ใจในการปฏิบัติ เช่น พนักงานสอบสวนอาจเกิดความไม่แน่ใจว่าตนมีอำนาจเข้าถึงข้อมูลในอุปกรณ์อิเล็กทรอนิกส์ที่ตรวจยึดมาหรือไม่ หรือหากต้องการเข้าถึงข้อมูลที่เป็นพยานหลักฐานสำคัญในคดีที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จะต้องปฏิบัติตามหลักกฎหมายใด หรือหากตัดสินใจดำเนินการอย่างใดอย่างหนึ่งไปแล้วจะมีผลกระทบหรือเกิดปัญหาในชั้นพิจารณาคดีอันเนื่องมาจากการที่พนักงานอัยการ หรือผู้พิพากษามีลักษณะการตีความที่แตกต่างกับพนักงานสอบสวนหรือไม่ อย่างไร

จากประเด็นปัญหาในเรื่องนี้ผู้วิจัยได้ศึกษาค้นคว้าเพิ่มเติมเพื่อต้องการที่จะเทียบเคียงแนวทางการปฏิบัติในการเข้าถึงและเก็บรวบรวมพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์โดยจากการศึกษาข้อกฎหมายของสหรัฐอเมริกาที่เกี่ยวข้องพบว่า สหรัฐอเมริกามีกฎหมายบัญญัติแนวทางที่ชัดเจนเกี่ยวกับการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ต่างๆ เช่น กฎหมายการดักฟังหรือดักรับข้อมูล (The Wiretap Act) โดยเจ้าหน้าที่ของรัฐจะต้องได้รับอนุญาตจากศาลก่อนจึงจะสามารถดำเนินการเก็บพยานหลักฐานได้ โดยกฎหมายดังกล่าวนี้ได้รับอิทธิพลมาจากการแก้ไขรัฐธรรมนูญ ฉบับที่ 4 ของสหรัฐอเมริกา (The Fourth Amendment) ที่ได้วางหลักเกี่ยวกับการป้องกันการละเมิดสิทธิมนุษยชนที่จะต้องได้รับความปลอดภัยในร่างกาย เคหสถาน เอกสารหรือทรัพย์สินของตนจากการถูกตรวจค้นหรือถูกตรวจยึดโดยเจ้าหน้าที่ของรัฐที่ไม่มีอำนาจหรือเป็นการกระโดยมิชอบ ดังนั้นหากเทียบเคียงกับกรณีของประเทศไทยแล้วก็จะมีลักษณะคล้ายกันกับการใช้อำนาจของเจ้าหน้าที่ตาม พ.ร.บ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ซึ่งจะต้องได้รับอนุญาตจากศาลเช่นเดียวกัน

“ทั้งตำรวจ อัยการ ศาล ยังมองไม่ตรงกันในเรื่องพยานหลักฐานที่เป็นข้อมูลคอมพิวเตอร์ เพราะข้อเท็จจริงที่แต่ละคนรับรู้มามันไม่เหมือนกัน และกฎหมายที่มีอยู่เราก็ยังไม่แน่ใจว่าจะตีความปรับใช้กับมันอย่างไร นักกฎหมายกลุ่มหนึ่งบอกทำได้ อีกกลุ่มหนึ่งบอกทำไม่ได้ ต้องยอมรับว่า ณ ตอนนี้ความเห็นทางกฎหมายยังไม่สอดคล้องกัน ทำให้เกิดคำถามว่าสุดท้ายแล้วเรามีอำนาจเข้าถึงข้อมูลพวกนี้หรือไม่”

(B2, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“ปัญหาตัวนี้คือมันเป็นเรื่องที่เกิดในระบบคอมพิวเตอร์ ซึ่งทำให้เรามีอำนาจอยู่สองทาง ทั้งจาก พ.ร.บ.คอมฯ และ ป.วิ.อาญา (ประมวลกฎหมายวิธีพิจารณาความอาญา) ทำให้เกิดปัญหาในการตีความว่า หากต้องการยึดเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้อง จะต้องใช้อำนาจตามกฎหมายใด เพราะมีขั้นตอนแตกต่างกัน หากใช้ พ.ร.บ.คอมฯ ต้องขอหมายจากศาล แต่ถ้าตีความตามกฎหมาย ป.วิ อาญาแล้ว สามารถยึดได้เลย ทำให้เกิดความสับสนของผู้ปฏิบัติ”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

4) ประเด็นปัญหาทางกฎหมายเกี่ยวกับการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ

ประเด็นปัญหาที่สำคัญอีกประเด็นหนึ่งที่ผู้ให้ข้อมูลสำคัญกล่าวถึงคือประเด็นปัญหาในเรื่องการยึดอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เนื่องด้วยสภาพของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ที่ไม่มีรูปร่างและไม่สามารถจับต้องได้เหมือนในกรณีของเงินสด ทองคำ หรือทรัพย์สินอื่นๆที่มีรูปร่างและสามารถถือเอาได้ ดังนั้นในการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆผู้ใช้งานจะต้องดำเนินการสร้างคำสั่งในการโอน – รับบิทคอยน์ผ่านกระเป๋าเงินอิเล็กทรอกนิกส์ (E – Wallet) ที่อยู่ในรูปแบบของโปรแกรมคอมพิวเตอร์ที่สามารถนำไปใช้ในงานได้จากหลากหลายอุปกรณ์ เช่น ใช้งานจากเครื่องคอมพิวเตอร์หรือโทรศัพท์สมาร์ทโฟน โดยที่การเข้าไปใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ผ่านกระเป๋าเงินอิเล็กทรอกนิกส์ (E – Wallet) นั้น จำเป็นจะต้องใช้ข้อมูลสองชุดคือ เลขที่บัญชีของบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ (Public Key) ประกอบกับรหัสผ่านในการเข้าบัญชี (Private Key) ซึ่งข้อมูลทั้งสองชุดนี้มีลักษณะที่เชื่อมโยงถึงกันผ่านการเข้ารหัสของข้อมูลที่มีลักษณะพิเศษคือ ไม่สามารถถูกโจมตีหรือถูกเข้าไปสุ่มทดสอบค่าของรหัสผ่านเพื่อให้สามารถลักลอบ

เข้าไปใช้งานในบัญชีของผู้อื่นได้ ซึ่งเป็นการออกแบบโดยระบบที่ทำให้การใช้งานสกุลเงินเข้ารหัสต่างๆมีความปลอดภัยสูง จากหลักการและข้อเท็จจริงดังกล่าวทำให้การจะสามารถยึดและอายัดบิทคอยน์ได้นั้น จำเป็นต้องอาศัยองค์ประกอบ 2 ประการ คือ 1) จำเป็นจะต้องใช้กระเป๋าเงินอิเล็กทรอนิกส์ (E – Wallet) ในการรับและเก็บรักษาบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ถูกยึดหรืออายัด และ 2) จำเป็นจะต้องใช้เลขที่บัญชีและรหัสผ่านของบัญชีบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เพื่อสร้างคำสั่งโอนเงินจากกระเป๋าเงินอิเล็กทรอนิกส์ของผู้กระทำผิดมายังกระเป๋าเงินอิเล็กทรอกนิกส์ของเจ้าหน้าที่ของรัฐ

ผู้ให้ข้อมูลสำคัญกลุ่มที่เป็นบุคลากรในกระบวนการยุติธรรม ได้กล่าวถึงประเด็นปัญหาที่เกิดขึ้นว่า ใน**ปัจจุบันยังไม่มีการบัญญัติกฎหมายเกี่ยวกับการสร้างกระเป๋าเงินอิเล็กทรอกนิกส์ของรัฐ (E – Wallet) ทำให้เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องยังขาดเครื่องมือที่จำเป็นในการบังคับใช้กฎหมายในเรื่องของการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ** จนส่งผลทำให้เจ้าหน้าที่ในกระบวนการยุติธรรมที่มีหน้าที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสยังเกิดความสับสนและยังขาดความรู้ถึงขั้นตอนและวิธีการที่จะยึดและอายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ โดยผู้ให้ข้อมูลสำคัญได้ยกตัวอย่างกรณีที่ผู้กระทำผิดรับสารภาพและยินยอมที่จะให้เจ้าหน้าที่ของรัฐทำการยึดและอายัดบิทคอยน์หรือสกุลเงินเข้ารหัสที่ตนครอบครองอยู่ก็จะทำให้เกิดปัญหาต่อมาว่าจะใช้วิธีใดยึดและอายัดบิทคอยน์ดังกล่าว และจะนำบิทคอยน์หรือสกุลเงินเข้ารหัสดังกล่าวไปเก็บรักษาไว้ที่ใด

ประเด็นปัญหาดังกล่าวจะส่งผลกระทบโดยตรงต่อหน่วยงานที่มีหน้าที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงินเนื่องจากตามอำนาจหน้าที่แล้วจำเป็นจะต้องมีการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำความผิด ซึ่งผู้ให้ข้อมูลสำคัญจากหน่วยงานดังกล่าวได้อธิบายถึงสภาพปัญหาที่เกิดขึ้นว่าในปัจจุบัน**ไม่มีกฎหมายกำหนดให้มีการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ของรัฐ (E - Wallet) ทำให้หน่วยงานไม่มีกระเป๋าเงินอิเล็กทรอนิกส์ที่ถูกรับรองโดยกฎหมาย** แต่เนื่องจากในการดำเนินการตามอำนาจหน้าที่นั้นจำเป็นจะต้องมีการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสที่ใช้ในการกระทำความผิด เจ้าหน้าที่ที่เกี่ยวข้องจึงใช้วิธีการแก้ปัญหาด้วยการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ขึ้นเองเพื่อใช้งานไปพลางก่อน ซึ่งการดำเนินการในลักษณะนี้เจ้าหน้าที่ผู้ปฏิบัติงานจำจะต้องแบกรับความเสี่ยงต่างๆที่จะเกิดขึ้น หากเกิดกรณีที่บิทคอยน์หรือสกุล

เงินเข้ารหัสต่างๆที่ถูกยึดหรืออายัดไว้สูญหายหรือได้รับความเสียหายจนไม่สามารถเข้าถึงได้ ซึ่งถือเป็นสภาพปัญหาที่ส่งผลกระทบต่อการปฏิบัติหน้าที่ตามกฎหมาย

“สมมติว่ายึดได้จริง ผู้ต้องหายอมบอกรหัส แล้วจะนำไปเก็บไว้ที่ไหนก็เป็นปัญหาเพราะมันไม่ใช่เงินที่หยิบจับได้ ยึดมาวันนี้ ยังไม่รู้จะไปไว้ที่ไหนเลย”

(C1, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“เรื่อง การยึดอายัด หรือ วอลเลทของรัฐ ยังไม่มีเลยครับ ปัจจุบันก็ใช้ ป.วิ.อาญา ใช้หลักทั่วไปว่าเจ้าพนักงานมีอำนาจยึดไว้จนกว่าคดีจะสิ้นสุด แต่ปัญหาคือจะยึดจะอายัดอย่างไร”

(B2, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“โดยระเบียบ กฎหมายยังไม่มีครับ แต่วิธีปฏิบัติเรารู้ว่าต้องทำยังไง เราเลยทำ wallet กลางขึ้นมาเอง เวลาที่เราเจอก็จะทำการโอนมาไว้ใน wallet กลางนี้ก่อน”

(C4, สัมภาษณ์, 9 กรกฎาคม 2563)

นอกจากประเด็นปัญหาเรื่องที่ยังไม่มีกฎหมายกำหนดให้มีการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ของรัฐแล้ว ผู้ให้ข้อมูลสำคัญยังกล่าวถึงสภาพปัญหาที่เกิดขึ้นในการปฏิบัติงานจริงคือในทางปฏิบัติแล้วจะสามารถยึดและอายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆได้ใน 2 กรณี คือ

1) กรณีที่ผู้กระทำผิดยินยอมบอกเลขที่บัญชีบิทคอยน์และรหัสผ่านให้เจ้าหน้าที่เข้าถึงกระเป๋าเงินอิเล็กทรอนิกส์ของผู้กระทำความผิด แล้วทำการโอนบิทคอยนหรือสกุลเงินเข้ารหัสต่างๆไปยังกระเป๋าเงินอิเล็กทรอนิกส์กลางที่สร้างไว้ ซึ่งกรณีนี้ผู้ให้ข้อมูลสำคัญให้ความเห็นว่ามีเป็นไปได้ยากที่ผู้กระทำผิดจะยอมบอกข้อมูลสำคัญดังกล่าวให้เจ้าหน้าที่ทราบ ซึ่งในทางกลับกัน **แม้เจ้าหน้าที่สามารถพิสูจน์หรือตรวจพบได้ว่ามีบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆอยู่ในความครอบครองของผู้กระทำความผิด แต่หากไม่ทราบข้อมูลสำคัญคือรหัสผ่านเพื่อเข้าสู่กระเป๋าเงินอิเล็กทรอนิกส์ของผู้กระทำผิดก็จะไม่สามารถเข้าไปทำการยึดหรืออายัดได้** ซึ่งในปัจจุบันแม้จะอาศัยอำนาจตามกฎหมายใดก็ตามก็ไม่สามารถทราบรหัสผ่านดังกล่าวได้หากตัวผู้กระทำผิดไม่เปิดเผยออกมาด้วยตนเอง หรือแม้กฎหมายจะอนุญาตให้ใช้วิธีการทางเทคนิคเพื่อเจาะระบบเข้าถึงข้อมูลดังกล่าว ก็ไม่

สามารถกระทำได้จริงเนื่องจากกลไกความน่าเชื่อถือของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆถูกป้องกันไว้อย่างแน่นหนา

2) อีกกรณีหนึ่งที่สามารถทำการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสที่ใช้ในการกระทำความผิดได้ คือ กรณีที่ผู้กระทำความผิดมีการสมัครใช้งานหรือใช้บริการกระเป๋าเงินอิเล็กทรอนิกส์ผ่านผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่เป็นตัวกลางในการดำเนินการที่ได้รับอนุญาตจากคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ตามหลักเกณฑ์ที่กำหนดใน พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 เนื่องด้วยผู้ประกอบการเป็นตัวกลางในลักษณะนี้จะถือเป็นสถานประกอบการที่อยู่ภายใต้ข้องบังคับของกฎหมายที่เกี่ยวกับการป้องกันและปราบปรามการฟอกเงินหน่วยงานจึงสามารถใช้อำนาจตามกฎหมายบังคับให้ผู้ประกอบการที่ดูแลกระเป๋าเงินอิเล็กทรอนิกส์ของผู้กระทำความผิด โอนบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำความผิดเข้ามาทำการยึดและอายัดไว้ในกระเป๋าเงินอิเล็กทรอนิกส์กลาง ซึ่งในทางกลับกัน**หากเป็นกรณีที่ผู้กระทำผิดใช้กระเป๋าเงินอิเล็กทรอนิกส์ที่ใช้งานด้วยตนเองโดยไม่ผ่านตัวกลางอย่างผู้ประกอบธุรกิจที่ขึ้นทะเบียนไว้ หรือ กรณีที่ผู้กระทำผิดทำการโอนบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆออกไปยังบัญชีกระเป๋าเงินอิเล็กทรอนิกส์อื่นๆที่ไม่ได้อยู่ในการดูแลของตัวกลางแล้วก็จะไม่สามารถทำการอายัดได้** ซึ่งสาเหตุส่วนหนึ่งเกิดจากข้อบังคับของกฎหมาย พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ที่กำหนดให้มีการลงทะเบียนตรวจสอบยืนยันเฉพาะผู้ที่ประกอบธุรกิจในลักษณะของการเป็นตัวกลางเท่านั้น

สภาพปัญหาในเรื่องของการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำความผิดที่กล่าวมานี้ ส่งผลทำให้การดำเนินการตามขั้นตอนในกระบวนการยุติธรรมเกิดช่องว่างหรือบกพร่อง ทั้งยังส่งผลให้ระบบกฎหมายยังไม่สามารถทำหน้าที่ในการข่มขู่ยับยั้งผู้กระทำผิดได้ เพราะหากกระบวนการในการยึดและอายัดไม่สามารถนำไปปฏิบัติได้จริงแล้ว จะทำให้ผลประโยชน์ที่ผู้กระทำผิดได้มานั้นยังอยู่ในความครอบครองของผู้กระทำผิดโดยปราศจากการลงโทษที่เหมาะสมหรือผู้กระทำผิดไม่ได้รับผลร้ายตามที่สมควรได้รับจากการกระทำความผิด จนอาจทำให้เกิดการกระทำผิดซ้ำและก่อให้เกิดความเสียหายต่อสังคมโดยรวมมากขึ้น ซึ่งจำเป็นอย่างยิ่งที่จะต้องหาแนวทางการป้องกันและแก้ไขปัญหานี้ต่อไป

“ถ้าเราไม่รู้(รหัส) ก็จะทำอะไรไม่ได้เลย เพราะโดยปกติเขาจะไม่บอกอยู่แล้วครับ ต่อให้เราฟรีซ (แจ้งอายัด)เป็นลายลักษณ์อักษร ก็ไม่มีผลในทางปฏิบัติ หนทางเดียวคือ ทำอย่างไรก็ได้ต้องทำให้เขายอมเปิด Wallet แล้วโอนเข้ามาใน Wallet กลางให้ได้ และปัจจุบันก็ยังไม่มีใครสามารถ Hack หรือเจาะเข้าไปใน Wallet ได้ โดยวิธีการยึดเงินที่เป็นคริปโทเคอเรนซี เราก็จะทำหนังสือไปถึงผู้บริการที่ประกอบธุรกิจสินทรัพย์ดิจิทัล แต่ทีนี้จะสามารถยึดได้เฉพาะทรัพย์ที่อยู่ใน wallet ที่ผูกไว้กับผู้ค้าสินทรัพย์ดิจิทัล ตัวที่เขาโอนออกไปยัง wallet ต่างๆ รวมทั้ง wallet ที่ไม่ได้ผูกไว้กับผู้ค้าสินทรัพย์ดิจิทัล อันนั้นตามไม่ได้ ”

(C4, สัมภาษณ์, 9 กรกฎาคม 2563)

จากการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญในประเด็นที่เกี่ยวกับสภาพปัญหาและสาเหตุของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสจากประเด็นปัญหาทางด้านกฎหมาย สามารถสรุปได้ว่าผู้ให้ข้อมูลสำคัญได้กล่าวถึงประเด็นปัญหาต่างๆดังนี้

1) สถานภาพทางกฎหมายของบิทคอยน์ ที่ยังไม่ชัดเจนส่งผลทำให้เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องยังเกิดความสับสนในการบังคับใช้กฎหมาย โดยเฉพาะในประเด็นด้านการเป็นทรัพย์ในทางอาญา รวมทั้งการกระทำความผิดที่มีโทษทางอาญาที่เกี่ยวกับบิทคอยน์ อันเป็นผลมาจากการที่กฎหมายมิได้มีการกำหนดสถานะในทางอาญาของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ชัดเจนซึ่งประเด็นปัญหานี้**มีความสอดคล้องกับที่ข้อมูลที่ผู้วิจัยพบจากการศึกษาทบทวนวรรณกรรม**ในเรื่องสถานภาพของบิทคอยน์ในแง่มุมของกฎหมายและอาชญากรรมว่า ในทางกฎหมายอาญาหรือกฎหมายที่มีโทษทางอาญายังไม่ได้มีการกำหนดหรือให้คำนิยามหรือมีบทเฉพาะกาลที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไว้โดยเฉพาะ ซึ่งส่งผลทำให้เกิดปัญหาในการนำกฎหมายมาบังคับใช้ตามที่ได้กล่าวมาแล้ว

2) พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ไม่สามารถใช้เป็นเครื่องมือในการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมได้ เนื่องจากกฎหมายนี้ไม่ได้มีเจตนาโดยตรงที่จะป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรม แต่มุ่งไปที่การควบคุมกำกับดูแลการประกอบธุรกิจสินทรัพย์ดิจิทัล จึงทำให้มาตรการและกลไกต่างๆในกฎหมายนี้ยังไม่สามารถนำไปใช้เป็นเครื่องมือในการป้องกันการนำบิทคอยน์และ

สกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมได้ โดยในประเด็นปัญหานี้จะมีความ**สอดคล้องกันกับผลการศึกษาของ สิรวิศ ศรีวิลาส (2561)** ที่ได้นำเสนอว่า แม้กฎหมายนี้จะมีการกำหนดแนวทางการประกอบธุรกิจสินทรัพย์ดิจิทัลและการเสนอขายโทเคนดิจิทัลให้แก่ประชาชนและมีการกำหนดมาตรการต่างๆก็ตาม แต่ก็ปรากฏว่ากฎหมายมุ่งควบคุมกำกับดูแลเฉพาะการประกอบธุรกิจเท่านั้น ไม่ครอบคลุมถึงกรณีที่ประชาชนถือครองหรือซื้อขายแลกเปลี่ยนกันเองโดยตรง ซึ่งถือเป็นช่องว่างทางกฎหมายที่สำคัญหรืออาจกล่าวได้ว่ากลไกของรัฐยังไม่สามารถทำหน้าที่ในการป้องกันอาชญากรรมประเภทนี้ได้อย่างสมบูรณ์ ทั้งนี้จากการศึกษาเจตนารมณ์ในการตรากฎหมายดังกล่าวของตัวผู้วิจัยเองก็พบว่ากฎหมายนี้มุ่งคุ้มครองให้เกิดการประกอบธุรกิจสินทรัพย์ดิจิทัลที่โปร่งใสเป็นประเด็นหลักซึ่งสอดคล้องกันกับข้อมูลที่กล่าวมานี้ด้วย

3) ประเด็นปัญหาเรื่องการตีความกฎหมายเพื่อเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่ไม่ตรงกันของเจ้าหน้าที่ในกระบวนการยุติธรรมนั้นส่งผลทำให้เจ้าหน้าที่ที่เกี่ยวข้องเกิดความสับสนจนอาจทำให้ไม่กล้าที่จะบังคับใช้กฎหมาย กล่าวคือในปัจจุบันยังเป็นที่ถกเถียงกันว่า การเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์นั้นจะต้องอาศัยอำนาจตามประมวลกฎหมายวิธีพิจารณาความอาญา หรือ พ.ร.บ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ เนื่องจากหลักการและแนวทางในการปฏิบัติมีความแตกต่างกัน ซึ่งประเด็นปัญหาที่ผู้ให้ข้อมูลสำคัญกล่าวถึงนี้**สอดคล้องกันกับที่ผู้วิจัยได้ศึกษาค้นคว้าเกี่ยวกับกฎหมายที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย** และพบว่าหลักการที่กำหนดในประมวลกฎหมายวิธีพิจารณาความอาญาและ พ.ร.บ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์มีความแตกต่างกัน โดยหากใช้หลักการตีความตามประมวลกฎหมายวิธีพิจารณาความอาญาแล้วหากเจ้าหน้าที่ที่เกี่ยวข้องได้ยึดอายัดเครื่องคอมพิวเตอร์หรืออุปกรณ์ที่เกี่ยวข้องมาถูกต้องก็ย่อมสามารถเข้าถึงข้อมูลอันอาจเป็นพยานหลักฐานในอุปกรณ์ดังกล่าวได้ แต่ในทางกลับกันหากเป็นการตีความตาม พ.ร.บ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว เจ้าหน้าที่ที่เกี่ยวข้องจะต้องทำการขออนุญาตจากศาลเพื่อเข้าถึงข้อมูลอิเล็กทรอนิกส์ก่อนจึงจะดำเนินการเข้าถึงข้อมูลภายในอุปกรณ์ต้องสงสัยได้ ซึ่งจากผลการศึกษาทั้งจากการเก็บข้อมูลและการทบทวนวรรณกรรมตรงกันว่าในปัจจุบันยังไม่มีการกำหนดชัดเจนจากรัฐว่า เจ้าหน้าที่ที่เกี่ยวข้องจะต้องใช้อำนาจตามกฎหมายใดเพื่อให้สามารถปฏิบัติหน้าที่ได้อย่างถูกต้องชอบธรรม

4) ประเด็นปัญหาทางกฎหมายเกี่ยวกับการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ โดยผู้ให้ข้อมูลสำคัญได้กล่าวถึงประเด็นปัญหานี้ว่าในปัจจุบันประเทศไทยยังขาดกฎหมายที่บัญญัติเกี่ยวกับการยึดและอายัด บิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำความผิด ทำให้ในปัจจุบันประเทศไทยยังไม่มีกฎหมายที่บัญญัติเกี่ยวกับการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ (E – Wallet) และยังขาดกฎหมายที่วางหลักเกี่ยวกับแนวทางหรือวิธีปฏิบัติที่ชัดเจนในการยึดและอายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่ถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิด **ในขณะที่หากพิจารณาข้อมูลที่ได้จากการทบทวนวรรณกรรมแล้วจะพบว่า**ในต่างประเทศอย่างประเทศญี่ปุ่นที่ได้มีการกำหนดมาตรการในการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆและได้มีการนำมาตรการดังกล่าวไปบังคับใช้ในการยึดอายัดบิทคอยน์ในคดีล้มละลายของบริษัท Mt.Gox โดยใช้การยึดรหัสผ่านส่วนตัว (Private Key) แล้วโอนบิทคอยน์เข้าไปยังบัญชี บิทคอยน์ที่ถูกควบคุมโดยรัฐ เช่นเดียวกันกับประเทศสหรัฐอเมริกาที่มีมาตรการในการยึดและอายัดในลักษณะนี้เช่นเดียวกัน แต่หากเป็นกรณีของประเทศสหรัฐอเมริกานั้น บิทคอยน์และสกุลเงินเข้ารหัสที่ถูกยึดอายัดจะถูกโอนไปยังบัญชีบิทคอยน์ที่ควบคุมดูแลโดยองค์กรศาล อีกทั้งจากการทบทวนวรรณกรรมในเรื่องเกี่ยวกับแนวทางการปฏิบัติของหน่วยงานของรัฐที่มีหน้าที่เกี่ยวข้องในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส โดยเฉพาะสำนักงานป้องกันและปราบปรามการฟอกเงินก็ไม่ได้มีการระบุถึงขั้นตอนและวิธีการต่างๆที่เกี่ยวกับการยึดหรืออายัดที่ชัดเจนและเป็นรูปธรรมแต่อย่างใด ทำให้ผู้วิจัยวิเคราะห์ได้ว่าประเทศไทยยังขาดการกำหนดมาตรการทางกฎหมายและหลักปฏิบัติที่ชัดเจนเกี่ยวกับการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จึงทำให้ศักยภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสยังไม่ทัดเทียมประเทศที่มีความพร้อมตามที่ได้กล่าวมาแล้ว

จากผลการศึกษาทั้งจากการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญและจากการศึกษาค้นคว้าทบทวนวรรณกรรมทำให้สามารถสรุปได้ว่าประเด็นปัญหาทางด้านกฎหมายถือเป็นสภาพปัญหาและสาเหตุสำคัญประการหนึ่งที่ทำให้เกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสขึ้น ดังนั้นหากต้องการจะแสวงหาแนวทางในการป้องกันอาชญากรรมประเภทนี้ ก็จำเป็นจะต้องศึกษาและพัฒนาแก้ไขปรับปรุงกฎหมายที่เกี่ยวข้องในประเด็นต่างๆด้วย

4.2.3 สภาพปัญหาและสาเหตุจาก "การบังคับใช้กฎหมาย"

1) การขาดองค์ความรู้เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆของผู้บังคับใช้กฎหมาย

ผู้ให้ข้อมูลสำคัญได้กล่าวถึงสภาพปัญหาในประเด็นนี้ว่า บิทคอยน์และสกุลเงินเข้ารหัสต่างๆยังถือเป็นเรื่องใหม่สำหรับกระบวนการยุติธรรม อีกทั้งยังเป็นเรื่องเฉพาะที่จำเป็นจะต้องอาศัยความรู้ความชำนาญเฉพาะด้าน เพราะบิทคอยน์และสกุลเงินเข้ารหัสต่างๆนั้นอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ที่ใช้ระบบการทำงานบล็อคเชน (Blockchain) ที่มีความซับซ้อนซึ่งจะต้องใช้ความรู้ความเข้าใจในระบบวิศวกรรมคอมพิวเตอร์ชั้นสูง จึงส่งผลทำให้**เจ้าหน้าที่ในกระบวนการยุติธรรมโดยเฉพาะอย่างยิ่งเจ้าหน้าที่ในหน่วยงานที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่จะต้องทำการสืบสวน รวบรวมพยานหลักฐานต่างๆที่เกี่ยวข้องยังขาดองค์ความรู้เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสในเชิงลึก** แม้ในปัจจุบันจะมีฝึกอบรมและมีการพัฒนาบุคลากรในกระบวนการยุติธรรมแล้วก็ตาม และนอกจากปัญหาการขาดองค์ความรู้เชิงลึกหรือในเชิงระบบจนทำให้เกิดเป็นสภาพปัญหาขึ้นกับเจ้าหน้าที่ผู้ปฏิบัติหน้าที่ในการสืบสวนรวบรวมพยานหลักฐานแล้ว ในส่วนของ**พนักงานสอบสวน หรือพนักงานอัยการและผู้พิพากษาซึ่งมีหน้าที่นำข้อกฎหมายมาปรับใช้กับการกระทำความผิดที่เกิดขึ้น ก็ประสบปัญหาอันเนื่องมาจากการขาดความเข้าใจในข้อเท็จจริงหรือหลักการพื้นฐานของบิทคอยน์และสกุลเงินเข้ารหัส** เช่น ยังคงมีความเข้าใจที่ไม่ตรงกันว่าแท้จริงแล้ว บิทคอยน์และสกุลเงินเข้ารหัสต่างๆคืออะไร มีหลักการหรือระบบการทำงานอย่างไร เป็นต้น ส่งผลทำให้เกิดความสงสัยหรือมีความไม่ชัดเจนว่าจะนำข้อกฎหมายที่มีอยู่มาปรับใช้กับข้อเท็จจริงอย่างไร ซึ่งประเด็นปัญหานี้อาจทำให้เกิดเป็นช่องว่างทางกฎหมาย หรือกล่าวอีกนัยหนึ่งได้ว่าการขาดองค์ความรู้ดังกล่าวนี้อาจส่งผลทำให้ผู้กระทำผิดหลุดรอดไปจากกระบวนการยุติธรรมอันเกิดจากความไม่เข้าใจในวัตถุที่กระทำผิดซึ่งเป็นสิ่งใหม่อย่างบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ

ผลจากการขาดองค์ความรู้ของเจ้าหน้าที่ผู้บังคับใช้กฎหมายนี้อาจส่งผลทำให้**เจ้าหน้าที่ในกระบวนการยุติธรรมเกิดความกลัวที่จะดำเนินการต่างๆเกี่ยวกับบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ** เช่น ในกรณีของความไม่ชัดเจนในการตีความทางกฎหมายเกี่ยวกับการเก็บพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอกนิกส์ที่ได้กล่าวมาแล้ว ทำให้เจ้าหน้าที่ที่เกี่ยวข้องอย่างเจ้าหน้าที่ที่มีหน้าที่สืบสวนสอบสวนรวบรวมพยานหลักฐาน อย่างเจ้าหน้าที่ฝ่ายสืบสวนและพนักงานสอบสวนยังมี

ความไม่แน่ใจว่าขอบเขตของการดำเนินการทำได้มากน้องเพียงใด จึงอาจเกิดความกังวลต่อไปได้ว่าหากกระทำการใดๆไปแล้ว เมื่อส่งสำนวนการสอบสวนหรือส่งพยานหลักฐานไปสู่ชั้นพิจารณาคดีแล้วหากพนักงานอัยการหรือผู้พิพากษามีความเห็นแย้งว่าการได้มาซึ่งพยานหลักฐานดังกล่าวเป็นการกระทำโดยมิชอบ ก็อาจสร้างความเดือดร้อนให้กับเจ้าหน้าที่ตำรวจและพนักงานสอบสวนได้ หรือในกรณีที่เจ้าหน้าที่ไม่กล้าที่จะดำเนินการอย่างหนึ่งอย่างใดกับบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ อันเนื่องมาจากเกิดความกลัวว่าหากกระทำการใดๆไปแล้วเกิดความเสียหายขึ้นกับบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ เช่น เกิดการสูญหาย ถูกลักลอบถ่ายโอนไป หรือ ทำให้บัญชีผู้ใช้งานเสียหายจนไม่สามารถเข้าถึงบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่เป็นของกลางในคดีได้ จะทำให้เกิดความเสียหายแก่ทางราชการส่งผลให้ตนจะต้องเป็นผู้รับผิดชอบ ดังนั้นผลจากการขาดองค์ความรู้ต่างๆที่เกี่ยวข้องบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ อาจนำไปสู่การละเว้นการปฏิบัติหน้าที่ของเจ้าหน้าที่ที่เกี่ยวข้องอันเนื่องมาจากความกลัว ซึ่งจะส่งผลทำให้ผู้กระทำผิดไม่ถูกลงโทษและส่งผลโดยตรงต่อประสิทธิภาพการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

มัน (บิทคอยน์)เป็นเรื่องใหม่และคนที่บังคับใช้กฎหมายยังไม่คุ้นชิน รู้สึกว่ามันอันตรายและยังไม่รู้ว่าจะจัดการกับมันยังไง ”

(A5, สัมภาษณ์, 26 พฤศจิกายน 2562)

“ในเรื่องขององค์ความรู้นั้นมีในระดับหนึ่ง มี(เจ้าหน้าที่)หลายคนไปเข้าคอร์สอบรมทั้งในและต่างประเทศ แต่ไม่ได้แตกฉาน เพียงแต่รู้ไว้ประกอบในการวิเคราะห์การกระทำความผิดต่างๆ ”

(C1, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“ปัญหาของนักกฎหมาย ปัญหาของกลุ่มผู้บังคับใช้กฎหมาย ตั้งแต่ตำรวจ อัยการ ศาล คือเทคโนโลยีพวกนี้เป็นของใหม่ พอเราไม่รู้ข้อเท็จจริงที่เป็นหลักการพื้นฐานของมัน เราก็เลยไม่รู้จะปรับกับข้อกฎหมายยังไง เจ้าหน้าที่เราก็เลยไม่กล้าที่จะไปจัดการกับพวกนี้ ไม่รู้ว่าทำไปแล้วจะพลาดพลั้งทำหลักฐานเสียหายหรือไม่ และกลัวว่าความรับผิดจะมาตกกับตนเอง อีกทั้งยังไม่แน่ใจว่ามีอำนาจเข้าถึงได้หรือไม่ จะผิด 157 หรือไม่ เมื่อไม่มีความรู้ ก็เกิดความกลัว”

(B2, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

2) การขาดวิธีปฏิบัติและเครื่องมือที่สามารถใช้ในการตรวจสอบติดตามการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมได้อย่างมีประสิทธิภาพ

ผู้ให้ข้อมูลสำคัญกล่าวถึงสภาพปัญหาในประเด็นนี้ว่าเป็นปัญหาที่เกิดขึ้นต่อเนื่องมาจากการขาดความรู้ความเข้าใจเกี่ยวกับระบบการทำงานของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในเชิงลึกประกอบกับลักษณะพิเศษของบิทคอยน์ที่ปกปิดตัวตนของผู้ใช้งานที่แท้จริง ส่งผลทำให้เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมเกี่ยวกับสกุลเงินเข้ารหัส **ยังไม่มีวิธีการในการสืบสวนตรวจสอบติดตามการกระทำความผิดที่เป็นรูปแบบเฉพาะ ที่จะสามารถพิสูจน์ยืนยันตัวบุคคลผู้กระทำความผิดจากข้อมูลการใช้งานบิทคอยน์หรือสกุลเงินเข้ารหัสโดยตรงได้** กล่าวคือ แม้จะมีข้อมูลการใช้งานบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่ถูกนำไปใช้ในการกระทำความผิดก็ตาม แต่เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องก็ยังไม่สามารถกำหนดแนวทางหรือวิธีการที่จะนำไปสู่การพิสูจน์ตัวตนของเจ้าของบัญชีผู้ใช้งานซึ่งเป็นผู้กระทำความผิดที่แท้จริงได้

โดยผู้ให้ข้อมูลสำคัญให้ข้อมูลว่าในการปฏิบัติหน้าที่ในปัจจุบันทำได้เพียงการนำวิธีการแบบดั้งเดิมที่ใช้ในการสืบสวนตรวจสอบการกระทำความผิดทั่วไปคือการพยายามตรวจสอบติดตามเส้นทางการเงิน โดยอาศัยข้อเท็จจริงที่สังคมไทยยังไม่ยอมรับในมูลค่าของบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ และยังไม่สามารถนำมาใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการในชีวิตประจำวันได้ตามปกติเหมือนเงินสกุลจริง ดังนั้นคนร้ายหรือผู้กระทำความผิดยังจำเป็นจะต้องมีการแลกเปลี่ยนบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆมาเป็นเงินสกุลจริงผ่านช่องทางใดช่องทางหนึ่งซึ่งเจ้าหน้าที่ก็จะอาศัยข้อมูลดังกล่าวประกอบในการสืบสวนติดตามผู้กระทำความผิด หรืออาจกล่าวได้ว่าช่องทางนี้ยังคงเป็นเพียงช่องทางเดียวที่เจ้าหน้าที่ของรัฐมีโอกาสที่จะตรวจสอบยืนยันตัวตนผู้กระทำผิดได้ อย่างไรก็ตามวิธีการดังกล่าวยังถือเป็นการทำงานเชิงรับเพราะต้องรอให้คนร้ายเปิดช่องโอกาสทั้งยังเป็นวิธีการที่ไม่สามารถนำไปใช้งานได้อย่างยั่งยืน เพราะยังติดข้อจำกัดอีกหลายประการ เช่น กรณีที่คนร้ายนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปเปลี่ยนเป็นเงินสกุลต่างประเทศ หรือกรณีที่หากสังคมไทยมีการใช้งานบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่แพร่หลายมากขึ้น วิธีการดังกล่าวจึงอาจไม่สามารถใช้ได้ในอนาคต

นอกจากสภาพปัญหาในประเด็นของการขาดวิธีการในการสืบสวนตรวจสอบติดตามการกระทำความผิด ที่จะสามารถพิสูจน์ยืนยันตัวผู้กระทำความผิดได้แล้ว ผู้ให้ข้อมูลสำคัญยังกล่าวถึงสภาพปัญหาที่เกิดจากการที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆอยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

ที่แม้จะมีการเปิดเผยข้อมูลเส้นทางการเงินอย่างสาธารณะก็ตาม แต่ข้อมูลดังกล่าวมีความเชื่อมโยงเกี่ยวข้องกับผู้ใช้งานเป็นจำนวนมาก ทั้งยังเป็นระบบเปิดที่มีผู้ใช้งานสามารถใช้งานโดยตรงต่อกัน (Peer – to - Peer) ได้อย่างอิสระ จึงทำให้มีข้อมูลเส้นทางการเงินต่างๆปรากฏเป็นจำนวนมากและมีความซับซ้อนกว่าเส้นทางการเงินสกุลจริงเป็นอย่างมาก ส่งผลทำให้การวิเคราะห์ตรวจสอบเส้นทางการเงินของสกุลเงินเข้ารหัสเป็นไปอย่างยากลำบาก และปัจจุบันเจ้าหน้าที่ของรัฐที่มีหน้าที่ตรวจสอบติดตามและวิเคราะห์เส้นทางการเงินของสกุลเงินเข้ารหัสที่เกี่ยวข้องกับการกระทำความผิดยัง**ขาดเครื่องมือหรืออุปกรณ์พิเศษที่จะนำมาช่วยในการวิเคราะห์เส้นทางการเงินหรือวิเคราะห์พฤติกรรมการกระทำความผิดที่ทันสมัยและมีประสิทธิภาพ** โดยจำเป็นจะต้องปรับอุปกรณ์ที่มีอยู่เดิมมาประยุกต์ใช้ซึ่งไม่เพียงพอที่จะสามารถตรวจสอบติดตามการกระทำความผิดได้อย่างทันท่วงที ซึ่งส่งผลทำให้การป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสของรัฐยังตามหลังผู้กระทำผิดอยู่เสมอ

“สุดท้ายเราต้องใช้วิธีการ Track (ตรวจสอบติดตาม) ไปเรื่อยๆ เพราะทั้งความรู้ความสามารถเครื่องไม้เครื่องมือ Solution (วิธีการ) ต่างๆที่มาช่วยแก้ไขปัญหาตรงนี้ ต้องบอกว่ายังไม่มีทุกวันนี้เราอ่านได้แค่ประมาณนึง ตีความอะไรมากไม่ได้มาก ส่วนในเรื่องอุปกรณ์ เครื่องไม้เครื่องมือเรียกว่ายังไม่มีจะดีกว่า ”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

“ตอนนี้ยังใช้วิธีการเหมือนการสืบทรัพย์ปกติอยู่ เพราะฉะนั้นถ้าเป็นเคสที่ไปเกี่ยวกับคริปโทเคอเรนซีแล้วยากมากที่จะสืบสวนทราบว่าเป็นใคร แม้เราจะสามารถติดตามเส้นทางการเงินได้ แต่เราไม่รู้ว่าใครเป็นเจ้าของบัญชี กลไกเดียวที่สามารถช่วยได้คือตราบใดที่คริปโทเคอเรนซีไม่สามารถมาใช้จ่ายในชีวิตประจำวันได้ มันจะต้องมีการแลกหรือเปลี่ยนกลับมาเป็นเงินสกุลหลัก สมมติว่าเขาเปลี่ยนกลับมาเราก็มีโอกาส แต่สมมติว่าเขาไม่เอาออกมาก็ยากมากๆ แม้จะติดตามทางอินเทอร์เน็ต ตามทางไอพีแอดเดรส ก็ควานหาไม่เจอ ส่วนเรื่องอุปกรณ์ที่เราใช้ เราก็ปรับอุปกรณ์ที่เราเคยใช้ก่อนหน้านี้มาปรับใช้เอา ก็เป็นเครื่องมือปกติ เราก็ประสบความสำเร็จบ้าง เป็นส่วนน้อย ไม่ทุกเคส”

(C4, สัมภาษณ์, 9 กรกฎาคม 2563)

3) ขาดการบูรณาการร่วมกันทั้งจากหน่วยงานของรัฐและภาคเอกชนที่เกี่ยวข้อง

สภาพปัญหาของผู้บังคับใช้กฎหมายอีกประเด็นหนึ่งที่มีผู้ให้ข้อมูลสำคัญให้ความเห็นไว้คือประเด็นปัญหาเรื่องการประสานงานและการบูรณาการร่วมกันระหว่างหน่วยงานของรัฐ โดยตามปกติแล้วหน่วยงานของรัฐต่างๆจะมีอำนาจและหน้าที่และความเชี่ยวชาญเฉพาะด้านแตกต่างกันไป เช่น สำนักงานตำรวจแห่งชาติมีหน้าที่ในการรักษาความสงบเรียบร้อยและป้องปันปราบปรามอาชญากรรมทุกประเภท สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) จะเป็นหน่วยงานที่มีความเชี่ยวชาญเกี่ยวกับการปราบปรามการกระทำความผิดที่เกี่ยวกับการฟอกเงิน ขณะที่ธนาคารแห่งประเทศไทยกำกับดูแลในเรื่องที่เกี่ยวกับเงินและเทคโนโลยีทางการเงิน สำนักงานกำกับหลักและตลาดหลักทรัพย์ (ก.ล.ต.) ก็จะมีความเชี่ยวชาญเกี่ยวกับการกำกับดูแลหลักทรัพย์และผลิตภัณฑ์ที่เกี่ยวกับการลงทุนต่างๆ เป็นต้น ซึ่งในแต่ละหน่วยงานก็จะดำเนินงานที่อยู่ในความรับผิดชอบเพื่อให้บรรลุวัตถุประสงค์และภารกิจของหน่วยงานต่างๆ

แต่เมื่ออาชญากรรมและปัญหาต่างๆเปลี่ยนไป โดยเฉพาะอย่างยิ่งในกรณีของ**อาชญากรรมที่มีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นเครื่องมือในการกระทำความผิดนั้น มีลักษณะของการกระทำผิดที่มีความซับซ้อน มีลักษณะและรูปแบบที่มีความเกี่ยวข้องกับศาสตร์หลายแขนง** เช่น เป็นเรื่องที่เกี่ยวกับเทคโนโลยีคอมพิวเตอร์ซึ่งจะต้องอาศัยผู้เชี่ยวชาญที่มีองค์ความรู้เกี่ยวกับเทคโนโลยีสารสนเทศ รวมทั้งยังเป็นเรื่องที่เกี่ยวข้องกับการโอนย้ายหรือเปลี่ยนแปลงสภาพของทรัพย์สิน หรือเกี่ยวข้องกับการฟอกเงิน ซึ่งจำเป็นต้องอาศัยผู้เชี่ยวชาญที่มีความชำนาญในการติดตามเส้นทางการเงิน รวมทั้งยังเกี่ยวเนื่องกับเรื่องของการติดต่อประสานงานหน่วยงานต่างประเทศและการพิจารณาตีความกฎหมายที่เกี่ยวข้อง ดังนั้นจึงสามารถกล่าวได้ว่า **การป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จึงไม่สามารถดำเนินการภายใต้หน่วยงานของรัฐหน่วยงานใดหน่วยงานหนึ่งได้** โดยผู้ให้ข้อมูลยังได้ชี้ให้เห็นสภาพปัญหาว่าในปัจจุบันนี้หน่วยงานของรัฐต่างๆ **ยังไม่มีการประสานงานหรือการทำงานร่วมกันอย่างเป็นรูปธรรม ทำให้การป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสรวมทั้งอาชญากรรมสมัยใหม่ประเภทอื่นๆยังขาดประสิทธิภาพ** อันเกิดองค์ความรู้ที่มีไม่ครบถ้วนและอำนาจหน้าที่รับผิดชอบที่ไม่ครอบคลุมประเด็นปัญหาที่เกิดขึ้น ตัวอย่างเช่น กรณีที่ผู้ให้ข้อมูลสำคัญที่เป็นผู้ทรงคุณวุฒิในหน่วยงานเกี่ยวกับการพัฒนาธุรกรรมอิเล็กทรอนิกส์ และมีหน้าที่เกี่ยวกับรักษาความมั่นคงปลอดภัยทางไซเบอร์เล่าถึงเกี่ยวกับกรณีที่ได้รับแจ้งจากเหยื่อว่าถูกโปรแกรมเรียกค่าไถ่

ออนไลน์โจมตีเข้าสู่ระบบคอมพิวเตอร์ แต่สิ่งที่เจ้าหน้าที่ในหน่วยงานทำได้ตามขอบเขตอำนาจหน้าที่คือการช่วยเหลือเยียวยาและพยายามยับยั้งความเสียหายที่จะเกิดขึ้นได้เท่านั้น ไม่สามารถทำการสืบสวนจับกุมตัวผู้กระทำผิดซึ่งเป็นหน้าที่โดยตรงของสำนักงานตำรวจแห่งชาติได้ เป็นต้น

“ปัญหาเรื่องการประสานงาน เช่น ผมรับแจ้งเรื่อง Ransomware ผมทำได้เพียง ช่วยเหลือเยียวยาไม่ให้ข้อมูลเสียหาย แต่ผมไม่มีอำนาจจะเข้าไปสืบสวนจับกุมคนร้าย ต้องประสานหรือแจ้งให้ผู้เสียหายไปแจ้งความอีกครั้งหนึ่ง”

(A4, สัมภาษณ์, 10 กรกฎาคม 2563)

“เราก็อาศัยอำนาจตาม พ.ร.บ.คอมพิวเตอร์ที่เรามี แต่ถ้าต้องสืบสวนในทางเทคนิคเชิงลึก เราไม่ได้เชี่ยวชาญถึงขั้นนั้น ยิ่งถ้าเป็นเรื่องเกี่ยวกับการเงินการธนาคาร ก็ต้องเป็นหน่วยงานอื่นเพราะไม่ใช่หน้างานของเราโดยตรง”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

4) ปัญหาในด้านการประสานงานในเรื่องข้อมูลกับหน่วยงานที่เกี่ยวข้องในต่างประเทศ

ผู้ให้ข้อมูลสำคัญได้ให้ความเห็นถึงประเด็นปัญหาที่สำคัญอีกประการหนึ่งซึ่งเป็นผลมาจากคุณลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์และมีการใช้งานผ่านระบบเครือข่ายคอมพิวเตอร์ ทำให้ผู้ใช้งานรวมทั้งอาชญากรสามารถนำบิทคอยน์และสกุลเงินเข้ารหัสไปใช้เป็นเครื่องมือในการก่ออาชญากรรมได้จากทุกหนแห่งทั่วโลกโดยไม่ถูกจำกัดด้วยเขตแดนของรัฐ ซึ่งคุณลักษณะนี้ได้เกิดเป็นสภาพปัญหาให้แก่เจ้าหน้าที่ของรัฐในประเด็นต่างๆ เช่น กรณีที่ตรวจพบว่ามีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้ในการกระทำความผิดจากต่างประเทศ หรือ ในกรณีที่ตรวจสอบพบว่าผู้กระทำผิดมีการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆผ่านผู้ให้บริการอินเทอร์เน็ต หรือผู้ให้บริการเกี่ยวกับการใช้งานบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆในต่างประเทศ ซึ่งกรณีเช่นนี้เจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องจำเป็นจะต้องทำการติดต่อประสานงานไปยังหน่วยงานต่างประเทศ เพื่อขอความร่วมมือให้ทำการตรวจสอบและส่งข้อมูลที่เกี่ยวข้องกลับมายังประเทศไทย แต่เนื่องจาก**กระบวนการประสานงานดังกล่าวจำเป็นจะต้องมีการ**

ติดต่อประสานงานผ่านหลายหน่วยงานและขั้นตอนที่จำเป็นต้องดำเนินการเป็นจำนวนมาก จนทำให้เกิดความล่าช้าและอาจส่งผลเสียหายต่อการสืบสวนติดตามผู้กระทำความผิด เช่น ข้อมูลซึ่งเป็นพยานหลักฐานสำคัญอาจถูกลบหรือทำลายได้ ก่อนที่ความร่วมมือระหว่างประเทศจะมาถึง ซึ่งสภาพปัญหาดังกล่าวนี้ทำให้เสียโอกาสที่จะนำตัวผู้กระทำผิดมารับการลงโทษในกระบวนการยุติธรรม อันจะส่งผลให้ผู้กระทำผิดลอยนวลและไม่เกรงกลัวต่อกฎหมาย จนอาจทำให้เกิดการกระทำผิดซ้ำหรือเกิดพฤติกรรมเลียนแบบ ซึ่งส่งผลต่อเนื่องไปถึงประสิทธิภาพของการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

“เราไม่สามารถเอาคำว่าเขตประเทศมาชี้วัดว่ามันเกิดในประเทศไหน เส้นแบ่งเหล่านี้ทุกวันนี้สำหรับอาขญากรมันไม่มีแล้ว ตรงไหนที่มีอินเทอร์เน็ตก็กระทำผิดได้หมด พอมันอยู่ในโลกอินเทอร์เน็ตแล้วความร่วมมือระหว่างประเทศเรามีจำกัด ประเด็นนี้แหล่ะที่เป็นปัญหาที่ท้าทาย”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

“ด้วยความที่มันไม่มีขอบเขตจำกัด ข้อมูลส่วนใหญ่ โดยเฉพาะข้อมูลของผู้ใช้งานจะอยู่กับผู้ให้บริการและหน่วยงานของรัฐทั่วโลก ซึ่งผมคิดว่าปัจจุบันการติดต่อประสานงานกับต่างประเทศของเรา ยังช้ามากๆ พูดง่ายๆว่ายังไปไม่ทันคนร้ายหรืออาชญากรรมต่างๆที่มันค่อนข้างเร็ว โดยเฉพาะเรื่องของคริปโทเคอเรนซีที่มันไปเร็วมากๆ”

(A5, สัมภาษณ์, 10 กรกฎาคม 2563)

“ปัจจุบันต้องยอมรับว่า การสร้างความร่วมมือระหว่างประเทศของเราทั้งในเรื่องการสืบสวนสอบสวน การส่งต่อพยานหลักฐานต่างๆ ยังคงต้องพัฒนาอีกมาก”

(D1, สัมภาษณ์ , 7 กรกฎาคม 2563)

จากการเก็บข้อมูลสามารถสรุปได้ว่าผู้ให้ข้อมูลสำคัญได้กล่าวถึงสภาพปัญหาและสาเหตุของการเกิดอาชญากรรมที่ใช้บิทคอยน์เป็นเครื่องมือในด้านการบังคับใช้กฎหมาย ในประเด็นต่างๆดังนี้

1) การขาดองค์ความรู้เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆของผู้บังคับใช้กฎหมายโดยผู้ให้ข้อมูลสำคัญซึ่งเป็นบุคลากรในหน่วยงานของรัฐที่เกี่ยวข้อง ซึ่งมีประสบการณ์ตรง

และประสบกับปัญหาดังกล่าวด้วยตนเอง ได้ชี้ให้เห็นถึงสภาพปัญหาสำคัญที่เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องกับการปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสและเจ้าหน้าที่ในกระบวนการยุติธรรมส่วนต่างๆยังขาดองค์ความรู้เกี่ยวกับบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆทำให้การบังคับใช้กฎหมายยังไม่เกิดผล

2) การขาดวิธีปฏิบัติและเครื่องมือที่สามารถใช้ในการตรวจสอบติดตามการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมได้อย่างมีประสิทธิภาพ โดยผู้ให้ข้อมูลซึ่งเป็นผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสโดยตรงได้กล่าวถึงสภาพปัญหานี้จากประสบการณ์ตรงว่า ในปัจจุบันยังไม่มีการกำหนดวิธีการปฏิบัติและยังไม่มีเครื่องมือพิเศษที่จะใช้ในการตรวจสอบติดตามการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมได้อย่างมีประสิทธิภาพ ซึ่งข้อมูลนี้**สอดคล้องกันกับที่ผู้วิจัยได้ทบทวนวรรณกรรม**ในประเด็นที่เกี่ยวกับแนวทางการปฏิบัติของหน่วยงานของรัฐที่มีหน้าที่เกี่ยวข้องในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสโดยปรากฏว่าในปัจจุบันหน่วยงานของรัฐที่เกี่ยวข้องยังไม่มีการกำหนดวิธีการปฏิบัติงานที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นการเฉพาะแต่อย่างใด โดยในการปฏิบัติงานที่ผ่านมาก็ได้อาศัยนำองค์ความรู้และเครื่องมือดั้งเดิมต่างๆมาประยุกต์ใช้ ซึ่งยังไม่เพียงพอที่จะสามารถป้องกันปราบปรามอาชญากรรมดังกล่าวได้

3) ขาดการบูรณาการร่วมกันทั้งจากหน่วยงานของรัฐและภาคเอกชนที่เกี่ยวข้อง โดยผู้ให้ข้อมูลสำคัญได้นำเสนอปัญหานี้ในประเด็นที่ในปัจจุบันหน่วยงานต่างๆของประเทศไทยทั้งภาครัฐและภาคเอกชนยังขาดการประสานงานหรือการทำงานร่วมกันอย่างเป็นรูปธรรม ทำให้การป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสยังขาดประสิทธิภาพ ซึ่งในประเด็นปัญหานี้**ผู้วิจัยได้นำข้อมูลที่ได้จากการทบทวนวรรณกรรมมาวิเคราะห์ประกอบก็จะพบว่า** ในการก่ออาชญากรรมที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมีลักษณะและรูปแบบการกระทำความผิดหลากหลายรูปแบบตามที่ได้กล่าวมาแล้ว ทั้งยังมีลักษณะคาบเกี่ยวกับการเป็นทั้งอาชญากรรมรูปแบบดั้งเดิมประกอบกับการเป็นอาชญากรรมคอมพิวเตอร์ อาชญากรรมทางเศรษฐกิจ และอาชญากรรมข้ามชาติ ดังนั้น จึงจำเป็นอย่างยิ่งจะต้องอาศัยความร่วมมือกันระหว่างหน่วยงานต่างๆที่เกี่ยวข้อง ซึ่งปรากฏว่าในปัจจุบันทั้งจากข้อมูลจากผู้ให้ข้อมูลสำคัญที่ได้ให้ข้อมูลเป็นไปในแนวทางเดียวกันประกอบกับจากประสบการณ์การทำงานของผู้วิจัยในฐานะเจ้าหน้าที่ในกระบวนการยุติธรรมเอง ทำให้สามารถสรุปตรงกันว่าปัญหาด้านการขาดการประสานงานกันระหว่างหน่วยงานของรัฐและภาคเอกชนเป็น

ประเด็นปัญหาสำคัญอีกประการหนึ่งที่ส่งผลต่อประสิทธิภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

4) ปัญหาในด้านการประสานงานในเรื่องข้อมูลกับหน่วยงานที่เกี่ยวข้องในต่างประเทศ โดยนอกจากปัญหาในด้านการประสานงานกันระหว่างหน่วยงานของรัฐเองและการประสานงานระหว่างหน่วยงานของรัฐและภาคเอกชนภายในประเทศแล้ว ผู้ให้ข้อมูลสำคัญทุกท่านยังได้ให้ข้อมูลไปในทิศทางตรงกัน โดยได้ชี้ให้เห็นถึงสภาพปัญหาที่การบังคับใช้กฎหมายในปัจจุบันยังขาดการประสานงานหน่วยงานที่เกี่ยวข้องในต่างประเทศอย่างเป็นรูปธรรมหรือมีการประสานงานหลายขั้นตอนจนทำให้เกิดความล่าช้า จนอาจส่งผลต่อการเก็บรวบรวมพยานหลักฐานและส่งผลต่อเนื่องไปถึงประสิทธิภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส โดยประเด็นปัญหานี้มีความสอดคล้องกันกับประสบการณ์การทำงานในกระบวนการยุติธรรมของผู้วิจัย จึงสามารถสรุปได้ว่าการขาดประสานงานกับหน่วยงานทีเกี่ยวข้องในต่างประเทศ เป็นปัจจัยหลักอีกประการหนึ่งที่ทำให้ผู้กระทำผิดหลุดรอดจากกระบวนการยุติธรรมหรือกล่าวอีกนัยหนึ่งว่า ประเด็นปัญหานี้เป็นสภาพปัญหาและสาเหตุที่ทำให้เกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสด้วย

ทั้งนี้จากการนำข้อมูลที่ได้จากการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญมาวิเคราะห์ร่วมกับข้อมูลหรือข้อเท็จจริงที่พบจากการทบทวนวรรณกรรมประกอบกับประสบการณ์การทำงานในฐานะเจ้าหน้าที่ในกระบวนการยุติธรรมของผู้วิจัย ทำให้สามารถสรุปได้ว่าปัญหาในด้านการบังคับใช้กฎหมายในประเด็นต่างๆที่กล่าวมานี้ ถือเป็นปัจจัยหนึ่งที่ทำให้เกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสขึ้นในประเทศไทย

4.3 แนวนโยบาย กฎหมาย และมาตรการที่เกี่ยวข้องกับสกุลเงินเข้ารหัสในต่างประเทศและประเทศไทย

เพื่อให้เกิดความเข้าใจถึงทิศทางของแนวนโยบาย กฎหมาย ตลอดจนมาตรการต่างๆที่เกี่ยวกับการกำกับดูแลบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ของประเทศที่มีกลไกการจัดเกี่ยวกับสกุลเงินเข้ารหัสที่ชัดเจน และมีอิทธิพลต่อสถานการณ์การใช้งานสกุลเงินเข้ารหัสของโลก จึงได้ทำการศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวข้องของประเทศต่างๆ ดังนี้

4.3.1 แนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศจีน

ประเทศจีน เป็นประเทศหนึ่งที่มีความตื่นตัวและตระหนักรู้ในการเกิดขึ้นของนวัตกรรมทางการเงินนี้ ทั้งการประเมินสถานการณ์และวิเคราะห์สภาพปัญหา ตลอดจนยังทำการศึกษาและวิจัยเพื่อหาทางป้องกันมิให้ประเทศและสังคมภายในประเทศจีนถูกสั่นคลอนโดยสกุลเงินเข้ารหัสทั้งยังมีความพยายามที่จะนำเทคโนโลยีสมัยใหม่มาใช้พัฒนาสกุลเงินดิจิทัลแห่งชาติอีกด้วย โดยอาจกล่าวได้ว่าทิศทางของแนวนโยบายประเทศจีนมีแนวนโยบายที่สวนทางกันระหว่างการยอมรับสกุลเงินเข้ารหัสต่างๆกับการสร้างสกุลเงินดิจิทัลของตนเอง กล่าวคือ **ประเทศจีนมีแนวทางที่ชัดเจนที่ไม่ยอมรับในสกุลเงินเข้ารหัสทุกสกุล** เนื่องจากมีมุมมองว่าสกุลเงินเข้ารหัสต่างๆไม่มีความน่าเชื่อถือ เป็นเครื่องมือที่จะถูกนำไปใช้ในการฟอกเงิน และการก่อการร้าย รวมทั้งยังมีโอกาสสูงที่จะถูกนำไปใช้ในการก่ออาชญากรรม รวมทั้งอาจส่งผลให้เกิดการหลอกลวงฉ้อโกงประชาชน จนอาจส่งผลกระทบให้เกิดความเสียหายของระบบเศรษฐกิจในภาพรวม ดังนั้นประเทศจีนจึงมีแนวนโยบายในทิศทางของการปฏิเสธและการห้ามใช้งานในประเทศโดยเด็ดขาด โดยแนวนโยบายดังกล่าวสะท้อนให้เห็นได้จากมาตรการต่างๆที่รัฐบาลประเทศจีนดำเนินการดังนี้ (พรชัย ชุนหจินดา, 2561) (Investing.com , 2020)

- พ.ศ. 2552 หรือ ค.ศ. 2009 ซึ่งเป็นไปที่มีการเปิดตัวบิทคอยน์เป็นครั้งแรก รัฐบาลจีนได้ออกมาประกาศ**ห้ามใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆในการซื้อขายแลกเปลี่ยนสินค้าและบริการในประเทศจีนโดยเด็ดขาด**

- พ.ศ. 2556 หรือ ค.ศ.2013 ทางรัฐบาลของประเทศจีนสั่งการห้ามธนาคาร สถาบันทางการเงิน รวมทั้งผู้ให้บริการเกี่ยวกับธุรกิจสินทรัพย์ดิจิทัล โดยเฉพาะอย่างยิ่งผู้ให้บริการธุรกิจประเภทรับแลกเปลี่ยน (Exchange) สกุลเงินเข้ารหัสกับเงินหยวน ไม่ให้มีการเข้าไปยุ่งเกี่ยวหรือสนับสนุนการใช้งานสกุลเงินเข้ารหัสโดยเด็ดขาด เนื่องจากในขณะนั้นมีการเข้ามาลงทุนในประเทศจีนเป็นจำนวนมาก

- พ.ศ. 2557 หรือ ค.ศ.2014 รัฐบาลประเทศจีนประกาศไม่อนุญาตให้มีการทำการระดมทุนผ่านการใช้โทเคนดิจิทัลหรือสกุลเงินเข้ารหัส (Initial Coin Offering หรือ ICO) โดยได้ให้เหตุผลว่าการระดมทุนในรูปแบบดังกล่าว **เป็นสิ่งหลอกลวงและผิดกฎหมาย** ส่งผลทำให้เกิดการปิดตัวลงของเว็บไซต์ที่ทำหน้าที่เป็นตัวแทนหรือนายหน้าในการระดมทุนแบบ ICO รวมทั้งพวกกลุ่มนายหน้ารับแลกเปลี่ยนสกุลเงินเข้ารหัสสกุลต่างๆ

จากมาตรการต่างๆที่ประเทศจีนประกาศออกมาตั้งแต่ ปี พ.ศ.2552 – 2557 หรือ ค.ศ.2009 - 2014 นั้น แสดงให้เห็นได้อย่างชัดเจนว่า**ประเทศจีนมีแนวนโยบายที่จะปฏิเสธสกุลเงินเข้ารหัสและการประกอบธุรกิจต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสโดยสิ้นเชิง** โดยผู้ให้ข้อมูลได้กล่าวถึงประเด็นนี้ว่ารัฐบาลประเทศจีนมองว่าบิทคอยน์และสกุลเงินเข้ารหัสจะนำมาซึ่งปัญหาอาชญากรรมและอาจกระทบต่อความสงบเรียบร้อยและกระทบต่อระบบเศรษฐกิจของประเทศจีน

“พวกบิทคอยน์หรือสกุลเงินดิจิทัลเหล่านี้ สร้างความกังวลให้ประเทศจีนมาก เพราะมองว่ามันไม่น่าเชื่อถือ ไม่มั่นใจว่าจะถูกนำไปใช้ยังไง และก่อให้เกิดผลเสียต่อประเทศหรือกระทบต่อความมั่นคงหรือไม่”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

แม้ประเทศจีนจะมีทิศทางที่ชัดเจนในการไม่ยอมรับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆก็ตาม แต่ขณะเดียวกันรัฐบาลประเทศจีนก็มองเห็นความสำคัญที่จะจำเป็นจะต้องนำเอาเทคโนโลยีต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสโดยเฉพาะอย่างยิ่งเทคโนโลยีบล็อคเชนมาประยุกต์ใช้จนทำให้เกิดแนวคิดในการสร้าง**สกุลเงินดิจิทัลแห่งชาติของประเทศจีนเอง**ขึ้นในปี พ.ศ. 2557 ซึ่งแนวคิดในการสร้างสกุลเงินดิจิทัลนี้ ได้มีผู้ให้ข้อมูลกล่าวว่าเกิดจากแรงผลักดันจากสภาพปัญหาต่างๆภายในประเทศจีน ได้แก่

1) สถานการณ์การใช้เงินสกุลหยวนในรูปแบบของธนบัตรหรือเหรียญไปใช้ในการก่ออาชญากรรม ที่รัฐบาลจีนเริ่มตระหนักว่าเงินสกุลจริงที่อยู่ในรูปแบบของธนบัตรถูกนำไปใช้ในกิจกรรมที่ผิดกฎหมายซึ่งกระทบต่อความมั่นคงของประเทศเป็นอย่างมาก ประเทศจีนจึงเริ่มแนวคิดและเกิดความพยายามที่จะสร้างระบบการจ่ายเงินแบบอิเล็กทรอนิกส์ขึ้น (Electronic Payment System หรือ E-payment)

2) หลังจากกระแสการพัฒนาระบบการจ่ายเงินแบบอิเล็กทรอนิกส์เกิดขึ้น ปรากฏว่าภาคเอกชนได้ทำการพัฒนาระบบการจ่ายเงินแบบอิเล็กทรอนิกส์ได้อย่างก้าวหน้า จนทำให้มีประชาชนชาวจีนใช้งานในการทำธุรกรรมต่างๆผ่านแอพลิเคชั่นที่ถูกผลิตโดยภาคเอกชนเป็นจำนวนมาก เช่น การใช้โปรแกรมวีแชทในการรับ – โอนเงิน (Wechat) และ การใช้จ่ายในการซื้อขายสินค้าและบริการต่างๆผ่านระบบอิเล็กทรอนิกส์ผ่านโปรแกรมอาลีเพย์ (Alipay) เป็นต้น รัฐบาลจีนจึงเริ่มตระหนักว่าภาคเอกชนได้เข้ามาควบคุมระบบการเงินอิเล็กทรอนิกส์ของประเทศไปแล้วกว่า 80 – 90

เปอร์เซนต์ ซึ่งรัฐบาลจีนมีความกังวลในสถานการณ์ดังกล่าวและต้องการที่จะเข้าไปควบคุมการดำเนินการในลักษณะนี้เพื่อให้สามารถรักษาความมั่นคงทางการเงินของรัฐได้

“เขาไม่ต้องการให้เงินของเขา(ประเทศจีน) อยู่ในรูปแบบของกระดาษ เพราะกระดาษมันเข้าไปในกิจกรรมที่ผิดกฎหมายเยอะ ในขณะที่สังคมเขาเริ่มเป็นสังคมไร้เงินสดโดยที่ภาคเอกชนอย่าง Alipay Wechat เข้ามาควบคุมการโอนเงินในประเทศไปแล้วกว่า 80-90 เปอร์เซนต์ เขาก็เริ่มไม่สบายใจ และอยากให้ภาครัฐทำเองมากกว่า”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

จากแนวคิดและสภาพปัญหาดังกล่าวรัฐบาลประเทศจีนจึงได้มีการขับเคลื่อนการพัฒนาสกุลเงินดิจิทัลแห่งชาติขึ้นโดยได้สั่งการให้ธนาคารกลางแห่งประเทศจีน (PBoC) เป็นผู้รับผิดชอบในการเริ่มทำการศึกษาและพัฒนาสกุลเงินเข้ารหัสของประเทศจีนเองขึ้น (สยามบล็อคเชน, 2561) ด้วยการดำเนินการดังกล่าวของประเทศจีนที่เริ่มหันมาสนใจศึกษาเกี่ยวกับสกุลเงินดิจิทัล**ทำให้ทั่วโลกตั้งข้อสงสัยว่า ประเทศจีนจะเปลี่ยนแปลงทิศทางของแนวนโยบายเกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสจากการปฏิเสธเป็นการยอมรับให้มีการใช้งานหรือไม่**

อย่างไรก็ตามเหตุการณ์สำคัญที่เป็นปัจจัยเร่งการพัฒนาสกุลเงินดิจิทัลแห่งชาติของประเทศจีน คือ **การประกาศสร้างสกุลเงินดิจิทัลลิบรา (Libra) ของนายมาร์ค ซักเกอร์เบิร์ก ผู้บริหารและผู้ก่อตั้งแอพลิเคชั่นที่มีคนใช้งานทั่วโลกอย่างเฟซบุ๊ค (Facebook) ในปี พ.ศ.2561 หรือ ค.ศ. 2019** ซึ่งเป็นแนวคิดที่จะทำการสร้างและพัฒนาสกุลเงินดิจิทัลที่เปิดเสรีให้ผู้ใช้งานแอพลิเคชั่นเฟสบุ๊คใช้งานเป็นสื่อกลางในการแลกเปลี่ยนแทนสกุลเงินจริงทุกสกุล โดยการพัฒนาสกุลเงินลิบราดังกล่าวมีการพัฒนาร่วมกันกับสถาบันการเงินชั้นนำของโลกอีก 28 สถาบัน โดยที่สกุลเงินลิบรานี้จะมีลักษณะเป็นสกุลเงินที่มีการค้ำประกันโดยเงินจริง (Stable Coin) ซึ่งในขั้นต้นของการพัฒนาจะใช้เงินดอลลาร์สหรัฐ (U.S. Dollar) เป็นฐานค้ำมูลค่า (จิรายุส ทรัพย์ศรีโภคา, 2562) ซึ่งภายหลังจากที่มีการประกาศแนวคิดเกี่ยวกับการสร้างสกุลเงินลิบราขึ้น ทำให้ประเทศจีนตระหนักได้ว่าการเกิดขึ้นของสกุลเงินลิบรา จะส่งผลกระทบต่อค่าเงินหยวนทั้งยังทำให้เงินสกุลดอลลาร์สหรัฐกลายเป็นมหาอำนาจทางการเงินของโลกทำให้ประเทศจีนเร่งพัฒนาสกุลเงินดิจิทัลแห่งชาติอย่างจริงจังมากขึ้น

จนกระทั่งในเดือนพฤษภาคม พ.ศ.2563 ประเทศจีนได้ทำการศึกษาพัฒนาจนสามารถทำการประกาศเปิดตัวและทดลองใช้งานสกุลเงินดิจิทัลแห่งชาติภายใต้ชื่อ**“หยวนดิจิทัล”** ซึ่งเป็นสกุลเงินดิจิทัลที่ออกโดยรัฐบาลของประเทศจีนเองและมีการค้ำประกันมูลค่าด้วยเงินสกุลหยวน ในอัตราแลกเปลี่ยน 1:1 และมีการควบคุมการดำเนินการแบบรวมศูนย์ซึ่งแตกต่างจากบิทคอยน์และสกุลเงินเข้ารหัสอื่นๆ โดยรัฐบาลจีนได้ทำการทดลองใช้หยวนดิจิทัลใน 4 เมืองสำคัญของประเทศจีน ได้แก่ เซินเจิ้น ซูโจว เฉิงตู และเขตเมืองใหม่สงอัน โดยการประกาศเปิดตัวและการทดลองใช้งานสกุลเงินหยวนดิจิทัลนี้ นอกจากจะถือเป็นการแสดงออกถึงความสำเร็จในการพัฒนาเทคโนโลยีทางการเงินของประเทศจีนแล้ว ยังถือเป็น**การแสดงออกถึงทิศทางของแนวนโยบายที่จะต้องการปิดกั้นการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ** เนื่องจากลักษณะสำคัญของหยวนดิจิทัล 3 ประการดังนี้ (มาณพ เสงี่ยมบุตร, 2563)

1) มีกฎหมายรองรับเงินหยวนดิจิทัล และไม่ถือว่าเงินหยวนดิจิทัลนี้เป็นเงินสกุลใหม่เพียงแต่เป็นเงินสกุลหยวน (สกุลเงินหลักของประเทศจีน) ที่เปลี่ยนรูปแบบจากเงินกระดาษหรือธนบัตรไปสู่รูปแบบเงินดิจิทัลที่รัฐบาลรองรับ

2) เงินดิจิทัลไม่ได้ใช้ระบบบล็อคเชนเป็นระบบพื้นฐาน แต่ใช้ระบบการรวมศูนย์ (Centralized) ที่มีการจัดเก็บข้อมูลอยู่ที่ธนาคารกลาง ซึ่งแนวคิดลักษณะนี้มีความตรงกันข้ามกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ใช้ระบบการกระจายข้อมูลอย่างสิ้นเชิง

3) มีระบบดอกเบี้ย ซึ่งจะถูกนำมาใช้กับเงินหยวนดิจิทัลภายหลังจากการทดลอง ซึ่งแสดงให้เห็นว่ารัฐบาลจีนโดยธนาคารกลางจะยังสามารถกำหนดนโยบายทางการเงิน หรือควบคุมสภาพเศรษฐกิจของประเทศได้ ซึ่งการมีระบบดอกเบี้ยนี้จะสวนทางกับแนวทางของสกุลเงินเข้ารหัสอย่างชัดเจน

จากข้อมูลดังกล่าว สามารถสรุปได้ว่า**ประเทศจีนมีทิศทางของแนวนโยบายที่ชัดเจนที่ไม่สนับสนุนจะให้มีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้งานในประเทศ** โดยได้แสดงออกให้เห็นด้วยมาตรการในการห้ามใช้งานที่เด็ดขาดตลอดจนการสร้างสกุลเงินหยวนดิจิทัลขึ้นมาใช้งานที่ทำให้เห็นได้ชัดเจนว่า ประเทศจีนไม่จำเป็นต้องพึ่งพาหรือสนใจในสกุลเงินเข้ารหัสต่างๆอีกต่อไป

เนื่องจากนโยบายที่ชัดเจนของประเทศจีนในการห้ามการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในทุกรูปแบบทั้งในการใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการต่างๆ การประกอบธุรกิจแลกเปลี่ยนซื้อขายหรือการเก็งกำไร รวมทั้งการระดมทุนผ่านสกุลเงินเข้ารหัส (ICO) จึง

ทำให้จากการค้นคว้าและทบทวนเอกสารทางวิชาการและสื่อต่างๆแล้วผู้วิจัยยัง**ไม่พบหลักฐานหรือเอกสารที่เชื่อถือได้ว่าประเทศจีนมีการออกกฎหมายเฉพาะเกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ** โดยในการกำหนดมาตรการต่างๆของประเทศจีนจะดำเนินการในลักษณะของการออกประกาศหรือ การประชุมร่วมกันระหว่างหน่วยงานที่เกี่ยวข้องเท่านั้น

ทั้งนี้จากแนวนโยบายและข้อเท็จจริงดังกล่าว สามารถสรุปได้ว่า **บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ไมมีสถานะเป็นเงินหรือไม่สามารถนำไปใช้ชำระหนี้ตามกฎหมายกันได้ในประเทศจีน (Non Legal Tender) ทั้งยังไม่ปรากฏข้อมูลเกี่ยวกับกฎหมายที่เกี่ยวกับการยึดหรืออายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆแต่อย่างใด**

4.3.2 แนวนโยบาย กฎหมายและมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศสหรัฐอเมริกา

สหรัฐอเมริกาเป็นประเทศที่มีนโยบายเกี่ยวกับสกุลเงินเข้ารหัสที่เป็นไปในทางบวกหรือมีทิศทางที่จะยอมรับและเปิดเสรีในการใช้งาน **อันเนื่องมาจากแนวคิดในด้านเสรีประชาธิปไตยที่เข้มแข็งประกอบกับปัญหาวิกฤติการณ์ทางเศรษฐกิจในสหรัฐอเมริกา** ที่เป็นส่วนทำให้ประชาชนในสหรัฐอเมริกาหันมาสนใจบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ โดยเฉพาะ “วิกฤติซับไพรม์” (Sub-Prime Mortgage) หรือที่ถูกเรียกอีกชื่อหนึ่งว่า “วิกฤติแฮมเบอร์เกอร์” (Hamburger Crisis) ที่เกิดขึ้นในปี ค.ศ 2007–2008 ที่เกิดจากการบริหารสินเชื่อที่ผิดพลาดประกอบกับการควบคุมกำกับดูแลสถาบันการเงินการลงทุนที่ไม่รัดกุมพอ กล่าวคือ ธนาคารต่างๆมีการอนุมัติเงินกู้บุคคลทั่วไปเป็นจำนวนมาก จากการเกิดกระแสว่าบ้านและอสังหาริมทรัพย์ต่างๆจะมีราคาสูงขึ้น จนทำให้เกิดปรากฏการณ์ที่มีการกู้ส่วนบุคคลเพิ่มมากขึ้นจนผิดปกติ และส่งผลให้เกิดปัญหาหนี้เสีย เมื่อเกิดหนี้เสียทำให้ธนาคารต้องยึดบ้านและอสังหาริมทรัพย์เหล่านั้น และส่งผลทำให้เกิดการขาดทุนทั้งระบบจนทำให้เกิดปัญหาการขาดสภาพคล่องทางการเงินขึ้นที่รุนแรงขึ้น จะเห็นได้จากการที่บริษัทใหญ่หลายบริษัทในสหรัฐอเมริกาต้องล้มละลายปิดกิจการ และเกิดวิกฤตเศรษฐกิจลุกลามกระทบไปทั่วโลกนับว่ารุนแรงที่สุดนับตั้งแต่ทศวรรษที่ 1930 **ส่งผลให้อำนาจและความน่าเชื่อถือของสหรัฐอเมริกาและกลุ่มประเทศตะวันตกลดลง โดยเฉพาะชื่อเสียงของสหรัฐอเมริกาในฐานะผู้นำโลกลดลงด้วย** โดยจากเหตุการณ์ดังกล่าวทำให้ธนาคารและสถาบันการเงิน ได้รับความเสียหายไปกว่า 4.35 แสนล้านดอลลาร์สหรัฐ (มหาวิทยาลัยสุโขทัยธรรมาธิราช, 2556)

เหตุการณ์ดังกล่าวนี้มิได้ส่งผลกระทบต่อความน่าเชื่อถือในประเด็นของภาพลักษณ์ระหว่างประเทศเท่านั้น **แต่ยังทำให้อเมริกันชนเกิดความไม่เชื่อถือต่อระบบการเงินของประเทศ โดยเฉพาะอย่างยิ่งเกิดความไม่พอใจและไม่ไว้ใจธนาคารและสถาบันการเงินต่างๆด้วย** (Pasupol Bunsaen, 2018) ซึ่งในช่วงระยะเวลาเดียวกันกับที่เกิดวิกฤติซับไพรม์นั้น ได้มีการกล่าวถึง**แนวคิดของบิทคอยน์** ที่มากระตุ้นให้ประชาชนชาวอเมริกันที่กำลังสิ้นศรัทธากับสถาบันการเงินต่างๆเกิดความสนใจเป็นอย่างมาก เพราะแนวคิดในการสร้างบิทคอยน์ให้เป็นสกุลเงินดิจิทัลนั้น มีระบบการทำงานที่ไม่ต้องพึ่งพิงตัวกลางอย่างสถาบันการเงินหรือธนาคารต่างๆอีกต่อไป แต่เปิดเสรีให้ผู้ใช้งานสามารถใช้งานกันได้เองโดยตรง (Peer – to - Peer) ผ่านแนวคิดการกระจายข้อมูล ที่นำเสนอโดยนักพัฒนาที่ใช้นามแฝงว่าซาโตชิ นากาโมโตะ **ซึ่งกระแสของบิทคอยน์ที่เกิดขึ้นในช่วงเวลาแห่งวิกฤตศรัทธาดังกล่าว จะเป็นปัจจัยสำคัญที่ทำให้ประชาชนหันมาสนใจในบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จนส่งให้มีการใช้งานอย่างแพร่หลายมาจนถึงปัจจุบัน อันมีผลทำให้ทิศทางนโยบายของสหรัฐอเมริกาเป็นไปในทิศทางที่ยอมรับให้มีการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ**

ผลจากแนวคิดและแนวนโยบายดังกล่าวทำให้สหรัฐอเมริกาได้บัญญัติกฎหมายรองรับสกุลเงินเข้ารหัสให้อยู่ในรูปของ**ตัวแทนของมูลค่าที่อยู่ในรูปแบบดิจิทัล (Digital Representation of Value)** ที่สามารถนำไปใช้ในการซื้อขายแลกเปลี่ยนสินค้าและบริการในโลกดิจิทัล แต่ทั้งนี้ **สกุลเงินเข้ารหัสยังไม่ถูกรับรองให้เป็นสกุลเงินจริง (Fiat Currency) และยังไม่สามารถนำไปชำระหนี้กันตามกฎหมายในสหรัฐอเมริกาได้ (Legal Tender)** โดยหน่วยงานที่กำกับดูแลเกี่ยวกับการเงินกล่าวถึงสาเหตุดังกล่าวว่าเนื่องจากสกุลเงินเข้ารหัสไม่ได้มีการออกหรือรับรองจากรัฐบาล ทั้งยังไม่เป็นฯไปตามหลักเกณฑ์ดั้งเดิมที่กำหนดไว้ (Financial Action Task Force [FATF], 2015)

หลังจากที่สหรัฐอเมริกาออกมารับรองให้บิทคอยน์และสกุลเงินเข้ารหัสเป็นสื่อกลางในทางดิจิทัลแล้ว จึงเริ่มนำมาตรการการกำกับดูแลต่างๆมาใช้บังคับเพื่อป้องกันการถูกนำไปใช้ในการก่ออาชญากรรม การฟอกเงิน และป้องกันสิ่งที่รัฐบาลสหรัฐอเมริกามีความกังวลสูงคือประเด็นในเรื่องของการสนับสนุนเงินทุนให้กับกลุ่มผู้ก่อการร้ายจึงทำให้ในปี ค.ศ. 2013 รัฐบาลจึงได้มีการกำหนดให้ผู้ประกอบธุรกิจต่างๆที่มีลักษณะเป็นการบริการด้านการเงินเกี่ยวกับสกุลเงินเข้ารหัสต้องถูกควบคุมด้วยกฎหมายต่อต้านการฟอกเงิน **ส่งผลทำให้ผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสทุกประเภทจะต้องทำการลงทะเบียนยืนยันตัวต่อก่อนการใช้งาน**

ต่อมาในปี ค.ศ. 2014 สหรัฐอเมริกาได้ผ่านกฎหมายต้นแบบเกี่ยวกับการกำกับดูแลผู้ประกอบธุรกิจที่เกี่ยวข้องกับเงินเสมือน หรือ US Uniform Regulation of Virtual-Currency Businesses ACT โดยกฎหมายนี้ได้กำหนดให้กิจกรรมดังต่อไปนี้ ถือเป็นการประกอบธุรกิจที่เกี่ยวข้องกับเงินเสมือน (Virtual-Currency Business Activity) ได้แก่ (ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561)

1) การแลกเปลี่ยน การโอน หรือการจัดเก็บเงินเสมือน

2) การมีส่วนร่วมในการจัดการเงินเสมือน ไม่ว่าโดยทางตรงหรือโดยผ่านข้อตกลงกับผู้ให้บริการเงินเสมือน

3) การแลกเปลี่ยนมูลค่าทางดิจิทัล (Digital Representations of Value) ภายในเกมออนไลน์หรือเกมแพลตฟอร์มอื่นๆ เช่น เพื่อใช้เป็นเงินเสมือนหรือการชำระหนี้ตามกฎหมาย

การออกกฎหมายดังกล่าวนี้ จึง**อาจกล่าวได้ว่าสหรัฐอเมริกามีการยอมรับการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆอย่างเต็มรูปแบบ เพียงแต่ยังไม่มีสถานะเป็นเงินและไม่สามารถชำระหนี้ได้ตามกฎหมายเท่านั้น** ทั้งนี้ในประเด็นเรื่องการยึดและอายัด สหรัฐอเมริกาใช้การยึดรหัสผ่านส่วนตัว (Private Key) ของลูกหนี้ โดยจะมีการควบคุมให้เฉพาะบุคคลที่เกี่ยวข้องกับกระบวนการบังคับคดีเท่านั้นที่จะสามารถเข้าถึงรหัสผ่านส่วนตัว (Private Key) ดังกล่าว จากนั้นเจ้าพนักงานบังคับคดีจะใช้รหัสผ่านส่วนตัวของเจ้าหนี้เพื่อโอนสกุลเงินเข้ารหัสเข้าไปที่บัญชีของศาล

4.3.3 แนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

สำหรับประเทศไทยนั้น ถือเป็นประเทศหนึ่งในโลกที่มีการออกกฎหมายรับรองบิทคอยน์และสกุลเงินเข้ารหัสต่างๆให้มีสถานะเป็นสินทรัพย์ดิจิทัล โดยทิศทางของนโยบายที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในประเทศไทยนั้น เริ่มปรากฏให้เห็นในปี พ.ศ.2557 ที่ธนาคารแห่งประเทศไทยได้มีประกาศฉบับที่ 8/2557 ลงวันที่ 18 มีนาคม 2557 เรื่องข้อมูลเกี่ยวกับ Bitcoin และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่นๆที่ลักษณะใกล้เคียงกัน โดยเนื้อหาในประกาศฉบับดังกล่าวมีเนื้อหาสำคัญในการ**แจ้งเตือนประชาชนถึงความเสี่ยงในการครอบครองสกุลเงินเข้ารหัสที่มีมูลค่าเปลี่ยนแปลงได้อย่างรวดเร็ว และอาจได้รับความเสียหายจากการปิดตัวไปอย่างกะทันหันของบริษัทตัวกลางที่ทำหน้าที่ในการแลกเปลี่ยนสกุลเงินเข้ารหัส**เหล่านี้ นอกจากนั้นยังมีการระบุว่า

บิทคอยน์และสกุลเงินเข้ารหัสต่างๆไม่ถือเป็นเงินที่ชำระหนี้ได้ตามกฎหมาย รวมทั้งยังระบุว่าผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆจะไม่ได้รับการคุ้มครองใดๆจากกฎหมาย หากเกิดกรณีที่ถูดหลอกลวง หรือเกิดปัญหาในการใช้งาน ดังนั้น การที่ธนาคารแห่งประเทศไทยซึ่งถือเป็นหน่วยงานของรัฐที่มีบทบาทสำคัญในการพิจารณากำหนดนโยบายทางการเงินออกประกาศแจ้งเตือนประชาชนในลักษณะนี้ ทำให้สามารถวิเคราะห์ได้ว่าในช่วงระยะแรกที่เริ่มมีประชาชนใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในประเทศไทยนั้น **ภาครัฐมีนโยบายที่ในลักษณะการดูท่าที ไม่ได้ห้ามใช้อย่างเด็ดขาด แต่ไม่รับรองให้เป็นเงินที่ชำระหนี้ได้ตามกฎหมายและไม่รับรองความปลอดภัย** ซึ่งแสดงให้เห็นถึงความไม่แน่ใจและการขาดองค์ความรู้ที่ชัดเจนเกี่ยวกับนวัตกรรมใหม่นี้ แต่ในขณะเดียวกันภาครัฐก็สามารถพยากรณ์ได้ในเบื้องต้นว่า ด้วยความที่บิทคอยน์และสกุลเงินเข้ารหัสเป็นสิ่งใหม่ที่อาจจะมีการดำเนินการในลักษณะของแชร์ลูกโซ่ที่เป็นการหลอกลวงจึงมีความพยายามที่จะแจ้งเตือนเพื่อไม่ให้เกิดความเสียหายต่อประชาชน

ทิศทางของแนวนโยบายเกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทยได้ปรากฏขึ้นอีกครั้งในปี พ.ศ.2561 เมื่อธนาคารแห่งประเทศไทยได้มีการแจ้งไปยังธนาคารพาณิชย์และสถาบันการเงินทุกแห่งในประเทศ **เรื่อง ขอความร่วมมือสถาบันการเงินไม่ให้ทำธุรกรรมที่เกี่ยวข้องกับคริปโตเคอเรนซี (Cryptocurrency)** โดยมีใจความสำคัญว่า ธนาคารแห่งประเทศไทยเล็งเห็นประเด็นปัญหาที่อาจเกิดขึ้นจากการทำธุรกรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส **โดยเฉพาะประเด็นที่ไม่สามารถระบุตัวตนผู้ออกได้อย่างชัดเจน ไม่มีสินทรัพย์ค้ำประกันตามมูลค่าหรือไม่มีทรัพย์สินอ้างอิง** โดยได้ขอความร่วมมือสถาบันการเงินต่างๆไม่ให้ทำธุรกรรมหรือมีส่วนร่วมในการสนับสนุนการทำธุรกรรมเกี่ยวกับสกุลเงินเข้ารหัสทุกประเภท (ธนาคารแห่งประเทศไทย, 2561) ดังนั้น หากวิเคราะห์จากประกาศของธนาคารแห่งประเทศไทยในปี พ.ศ. 2557 และการขอความร่วมมือไปยังธนาคารพาณิชย์และสถาบันการเงินต่างๆในปี พ.ศ. 2561 จะเห็นได้ว่า**ทิศทางของแนวนโยบายของรัฐจะเอนเอียงไปทางการห้ามหรือการปฏิเสธการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ แต่ไม่มีกฎหมายใดๆที่บัญญัติห้ามใช้งานภายในประเทศที่ชัดเจนแต่อย่างใดและในขณะเดียวกันการใช้งานก็ไม่มีกฎหมายใดๆรับรองและรักษาสิทธิประโยชน์ให้เช่นกัน**

ในปีเดียวกัน **ทิศทางของนโยบายเกี่ยวกับสกุลเงินเข้ารหัสของประเทศไทยก็เปลี่ยนไปอย่างสิ้นเชิง** จากเดิมที่ภาครัฐออกมาแจ้งเตือนและขอความร่วมมือไม่ให้มีการใช้สนับสนุนการใช้งานนั้นถูกเปลี่ยนไปด้วยการที่ประเทศไทยได้ออกกฎหมายที่ถือเป็นการกำกับดูแลบิทคอยน์และสกุลเงิน

เข้ารหัสเป็นการเฉพาะคือ พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 โดยมีสาเหตุของการออกกฎหมายดังกล่าวระบุในหมายเหตุท้ายกฎหมายปรากฏดังนี้

“เหตุผลในการประกาศใช้พระราชกำหนดฉบับนี้ คือ โดยที่ในปัจจุบันได้มีการนำคริปโทเคอร์เรนซีและโทเคนดิจิทัลมาใช้เป็นเครื่องมือในการระดมทุนผ่านการเสนอขายโทเคนดิจิทัลต่อประชาชน เป็นสื่อกลางในการแลกเปลี่ยน รวมถึงนำมาซื้อขายหรือแลกเปลี่ยนในศูนย์ซื้อขายคริปโทเคอร์เรนซีและโทเคนดิจิทัล ***แต่ยังไม่มีกฎหมายที่กำกับหรือควบคุมการดำเนินการดังกล่าวในประเทศไทย*** *ซึ่งทำให้มีการประกอบธุรกิจหรือการดำเนินกิจกรรมทางเศรษฐกิจที่อาจส่งผลกระทบต่อเสถียรภาพทางการเงิน ระบบเศรษฐกิจของประเทศและเกิดผลกระทบต่อประชาชนในวงกว้าง ดังนั้น* ***เพื่อกำหนดให้มีการกำกับและควบคุมการประกอบธุรกิจและการดำเนินกิจกรรมเกี่ยวกับสินทรัพย์ดิจิทัล*** *และ****เพื่อรองรับการนำเทคโนโลยีมาทำให้เกิดการพัฒนาทางเศรษฐกิจและสังคมอย่างยั่งยืน*** *อันจะเป็นการสนับสนุนและอำนวยความสะดวกให้ผู้ประกอบธุรกิจที่มีศักยภาพมีเครื่องมือในการระดมทุนที่หลากหลาย รวมทั้งประชาชนและผู้ที่เกี่ยวข้องมีข้อมูลที่ชัดเจนเพียงพอเพื่อใช้ในการตัดสินใจ เกิดความโปร่งใสในการดำเนินการ และป้องกันมิให้มีการนำสินทรัพย์ดิจิทัลที่ไม่มีแหล่งที่มาที่ชัดเจนไปใช้ประโยชน์หรือกระทำการใดในลักษณะที่เป็นการหลอกลวงประชาชนหรือที่เกี่ยวข้องกับการประกอบอาชญากรรม และโดยที่เป็นกรณีฉุกเฉินที่มีความจำเป็นรีบด่วนอันมิอาจจะหลีกเลี่ยงได้เพื่อประโยชน์ในอันที่จะรักษาความมั่นคงในทางเศรษฐกิจของประเทศ จึงจำเป็นต้องตราพระราชกำหนดนี้”*

โดยที่ พ.ร.ก.การประกอบธุรกิจสอนทรัพย์ดิจิทัล พ.ศ.2561 นี้ มีการบัญญัติรับรองและมีการบัญญัติมาตรการสำคัญ ดังนี้

1) บัญญัติรับรองให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ รวมโทเคนดิจิทัลที่ใช้สำหรับการระดมทุน มีสถานะเป็น**สินทรัพย์ดิจิทัล**

2) บัญญัติ**รับรองการประกอบธุรกิจสินทรัพย์ดิจิทัล** ทั้งในลักษณะของการศูนย์ซื้อขายสินทรัพย์ดิจิทัล นายหน้าซื้อขายสินทรัพย์ดิจิทัล ผู้ค้าสินทรัพย์ดิจิทัล และการระดมผ่านโทเคนดิจิทัล (Initial Coin Offering หรือ ICO)

3) กำหนดมาตรการให้กับผู้ที่ต้องการจะประกอบธุรกิจสินทรัพย์ดิจิทัล จะต้องทำ**การยื่นขอรับการอนุญาตจาก สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.)**

4) กำหนดมาตรการที่ให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลจะต้องดำเนินการตามมาตรการรู้จักลูกค้าของตนเอง (Know Your Customer หรือ KYC) ซึ่งหมายถึงการจะต้องทราบรายละเอียดของข้อมูลลูกค้าที่มาใช้บริการ

5) กฎหมายนี้ยังได้กำหนดให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ถือเป็นสถานประกอบการตามกฎหมายเกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน ซึ่งมีหน้าที่จะต้องรายงานให้หน่วยงานของรัฐทราบเมื่อเกิดกรณีที่เป็นไปตามหลักเกณฑ์ที่กำหนด เช่น เมื่อพบการทำธุรกรรมหรือการซื้อขายสกุลเงินเข้ารหัสที่มีความผิดปกติ หรือเป็นพิรุธต้องสงสัยเป็นต้น

6) มีหลักเกณฑ์การคุ้มครองนักลงทุนและมีการควบคุมการระดมทุนให้มีความเป็นธรรมสูงสุด โดยมีหลักการในการคุ้มครองคล้ายกันกับหลักทรัพย์ต่างๆ

7) เป็นกฎหมายที่บัญญัติบทลงโทษในทางอาญาและทางแพ่ง

ผลของการออกกฎหมายดังกล่าวทำให้ประเทศไทย เป็นประเทศที่มีการออกกฎหมายเฉพาะมาบังคับใช้ในการควบคุมกำกับดูแลการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ โดยได้มีผู้ให้ข้อมูลสำคัญกล่าวถึงที่มาของกฎหมายนี้ว่า เกิดจากแนวคิดสำคัญที่รัฐเห็นประโยชน์จากการรับรองให้เกิดการประกอบธุรกิจสินทรัพย์ดิจิทัลในรูปแบบต่างๆว่าจะส่งผลดีกับภาคเศรษฐกิจและการพัฒนาทางด้านเทคโนโลยีทางการเงิน แต่ในขณะเดียวกันก็ยังเล็งเห็นถึงความเสี่ยงที่จะเกิดขึ้นจากการกระทำที่ผิดกฎหมาย การฟอกเงิน การสนับสนุนเงินให้แก่ผู้ก่อการร้ายและการนำไปใช้ในการก่ออาชญากรรมรูปแบบต่างๆ จึงทำให้มีการกำหนดมาตรการต่างๆไว้โดยเฉพาะมาตรการในการรู้จักลูกค้าของตนเองที่เกิดมาจากแนวคิดสำคัญว่า **ปัจจุบันการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆยังจำเป็นต้องมีการแลกเปลี่ยนกลับมาเป็นเงินสกุลจริง (Cash Out)** เนื่องจากแม้ประเทศไทยจะมีการรับรองสถานะของสกุลเงินเข้ารหัสแล้ว แต่ด้วยเหตุที่มูลค่าของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไม่ได้ถูกค้ำประกันหรือยึดโยงอยู่กับทรัพย์สินใดๆ เช่น ทองคำ เงินดอลลาร์สหรัฐ แต่อย่างใด จึงส่งผลทำให้สังคมไทยยังไม่เชื่อมั่นในมูลค่าของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จนทำให้ยังไม่สามารถนำไปใช้ในการซื้อขายสินค้าอุปโภคบริโภคตามปกติได้ ดังนั้น**การออกมาตรการต่างๆจึงมุ่งที่จะตรวจสอบผู้ที่มีเจตนาจะนำสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดไปที่ขั้นตอนของการแลกเปลี่ยนกลับเป็นเงินบาท** ซึ่งถือเป็นกลไกหนึ่งที่จะช่วยในเรื่องของการตรวจสอบยืนยันตัวตนผู้กระทำความผิด

“การที่ออก พ.ร.ก.นี้ สาเหตุหนึ่งคือเราไม่อยากปล่อย เพราะต้องอย่าลืมว่าการเข้าสู่โลกพวกนี้ได้ต้องใช้เงินในโลกจริงก่อน ต้องใช้เงินบาท ต้องผ่าน Gateway ต้องผ่านตัวกลางอย่าง Cryptocurrency Exchange พวกนี้จะเป็นตัวคอยสกัดกั้น ตราบใดคนที่ใช้งานยังต้องกลับเข้าโลกความจริง ยังต้อง Cash Out มันก็จะเป็นช่องทางที่เราจะพอตามตัวได้ ดมกลิ่นได้ในระดับหนึ่ง”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

จึงอาจกล่าวได้ว่า ณ ปัจจุบัน**แนวนโยบายของประเทศไทยยอมรับสถานะของสกุลเงินเข้ารหัส ยอมรับให้มีการใช้งานและยอมรับให้มีการประกอบธุรกิจสินทรัพย์ดิจิทัล** แต่อย่างไรก็ตามกฎหมายนี้ยังคงมีข้อบกพร่องหรือจุดอ่อนบางประการในมุมมองของผู้บังคับใช้กฎหมายตามที่ได้กล่าวมาแล้ว ทั้งนี้ ในระบบกฎหมายไทยยังคงไม่มีการบัญญัติในเรื่องของการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นการเฉพาะรวมทั้งยังไม่มีการบัญญัติในเรื่องการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ของรัฐ (E-Wallet) ตามที่ได้กล่าวมาแล้ว

จากการศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสของประเทศจีน สหรัฐอเมริกา ซึ่งถือเป็นคู่แข่งขันในทางการพัฒนาระบบเศรษฐกิจและการแย่งชิงความเป็นหนึ่งในฐานะประเทศมหาอำนาจด้านเทคโนโลยีการเงินของโลก ทำให้ทราบถึงที่มาที่ไปของทิศทางของแนวนโยบายต่างๆ รวมทั้งการกลับมาพิจารณาข้อมูลที่เกี่ยวข้องของประเทศไทยเอง ทำให้**สรุปและเปรียบเทียบแนวนโยบาย กฎหมายและมาตรการต่างๆ** ได้ดังต่อไปนี้

	ความเป็นเงิน (Legal Tender)	การมีกฎหมายเฉพาะ	ระบบการอนุญาตให้ประกอบธุรกิจ	การใช้ซื้อขายสินค้าปกติประจำวัน	มีกฎหมาย/มาตรการ การยึดและอายัด
ประเทศจีน	X	N/A	X	X	N/A
สหรัฐอเมริกา	X	/	/	/	/
ประเทศไทย	X	/	/	X	X

ตารางที่ 1 เปรียบเทียบแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสของประเทศจีน สหรัฐอเมริกา และประเทศไทย
(ผู้วิจัย: กิจชัยยะ สุรารักษ์ , 2563)

ตามตารางดังกล่าวสามารถสรุปให้เห็นได้ว่าประเทศจีนไม่ปรากฏหลักฐานว่าได้มีการออกกฎหมายเฉพาะมาบังคับใช้กับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆแต่อย่างใด แต่มีการกำหนดมาตรการห้ามใช้งานบิทคอยน์และสกุลเงินเข้ารหัสในทุกรูปแบบแต่ยังไม่ปรากฏเอกสารหลักที่เกี่ยวกับการยึดหรืออายัด ในขณะที่สหรัฐอเมริกาและประเทศไทยมีการออกกฎหมายเฉพาะขึ้นมากำกับดูแลบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ รวมทั้งมีมาตรการในการให้ผู้ที่จะประกอบธุรกิจเกี่ยวกับสกุลเงินเข้ารหัสจะต้องทำการขออนุญาตจากหน่วยงานของรัฐ ส่วนในสหรัฐอเมริกานั้นมีการนำบิทคอย์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการซื้อขายแลกเปลี่ยนสินค้าและบริการและมีกฎหมายหรือมาตรการการยึดอายัดสกุลเงินเข้ารหัสต่างๆที่ชัดเจนซึ่งในประเทศไทยยังไม่มีแต่อย่างใด ทั้งนี้สิ่งที่เหมือนกันทั้งสามประเทศคือ ยังไม่มีประเทศใดให้การยอมรับให้สามารถนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้เป็นวัตถุที่สามารถชำระหนี้กันได้ตามกฎหมาย (Legal Tender) แต่อย่างใด

4.4 แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

จากการศึกษาเกี่ยวกับสภาพปัญหา สาเหตุ ลักษณะและรูปแบบของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ ประกอบการศึกษาวิเคราะห์ถึงแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวข้องในปัจจุบันที่ได้กล่าวมาแล้ว จะได้กล่าวถึงข้อมูลที่ผู้ให้ข้อมูลสำคัญซึ่งเป็นผู้ทรงคุณวุฒิในด้านต่างๆเสนอแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย ดังนี้

4.4.1 การกำหนดมาตรการบังคับให้มีการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งาน

ตามที่ผู้ให้ข้อมูลสำคัญได้กล่าวถึงสาเหตุสำคัญที่ทำให้อาชญากรนำบิทคอยน์ไปใช้การก่ออาชญากรรม คือ **ลักษณะของบิทคอยน์ที่ไม่เปิดเผยตัวตนผู้ใช้งานที่แท้จริง** ซึ่งลักษณะดังกล่าวได้สร้างปัญหาให้กับกระบวนการยุติธรรมในประเด็นของความยากลำบากในการสืบสวนเพื่อพิสูจน์ตัวผู้กระทำผิดที่แท้จริงเป็นอย่างมาก จนทำให้เกิดเป็นช่องว่างในการบังคับใช้กฎหมายส่งผลให้ผู้กระทำผิดลอยนวลและไม่ถูกจับกุมดำเนินคดี อันจะส่งผลให้เกิดการกระทำผิดซ้ำโดยที่กระบวนการยุติธรรมไม่สามารถหยุดยั้งการกระทำความผิดในลักษณะนี้ได้ ดังนั้นเพื่อเป็นการแก้ไขในประเด็นปัญหาดังกล่าวจึงได้มี**ผู้ให้ข้อมูลสำคัญให้ความเห็นว่าประเทศไทยควรมีการออกหรือแก้ไขกฎหมายโดยกำหนดให้มีแนวทางหรือมาตรการบังคับให้ผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆจะต้องทำการยืนยันตัวตนกับหน่วยงานของรัฐก่อนจึงจะสามารถใช้งานได้** โดยผู้ให้ข้อมูลสำคัญได้เสนอถึง

รูปแบบและวิธีการในการยืนยันตัวดังกล่าวนี้ ที่อาจกระทำได้ในลักษณะเดียวกันกับการยืนยันตัวตนเพื่อเปิดบัญชีธนาคารหรือการลงทะเบียนซิมการ์ดก่อนใช้งานเบอร์โทรศัพท์ โดยผู้ใช้งานจะต้องทำการลงทะเบียนเปิดเผยข้อมูลต่อเจ้าหน้าที่ของรัฐเพื่อยืนยันตัวตนว่า **เลขบัญชีบิทคอยน์ (Bitcoin Address /Public Key) ใดบ้างที่ตนเป็นผู้ใช้งาน และนำข้อมูลเลขที่บัญชีดังกล่าวบันทึกไว้กับข้อมูลส่วนบุคคลอย่างเลขประจำตัวประชาชน** และนำไปบันทึกไว้ในระบบฐานข้อมูลที่มีการรักษาความปลอดภัย โดยรัฐจะต้องมอบหมายให้หน่วยงานที่เกี่ยวข้องรับผิดชอบในการเก็บข้อมูลผู้ใช้งานที่ได้รับการยืนยันตัวตนไว้เพื่อประโยชน์ในการตรวจสอบยืนยันกรณีที่พบพฤติกรรมการใช้งานที่ต้องสงสัยหรือการพบการกระทำความผิดต่างๆ ซึ่งประเด็นปัญหาสำคัญประการหนึ่งที่อาจเกิดขึ้นคู่ขนานกับการบังคับใช้มาตรการการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ คือ การที่กลุ่มผู้ใช้บิทคอยน์และสกุลเงินเข้ารหัสเป็นเครื่องมือในการกระทำความผิด ย่อมจะต้องแสวงหาวิธีการที่จะหลบเลี่ยงมาตรการดังกล่าวนี้ ดังนั้น แม้จะถูกบังคับให้ยืนยันตัวตนแต่ผู้กระทำผิดก็อาจมีการจ้างให้ตัวแทนไปทำการยืนยันตัวตนแทน หรืออาจเกิดการกระทำความผิดในลักษณะของการหลอกลวงเพื่อให้บุคคลที่สามหลงเชื่อและรับจ้างมายืนยันตัวตนแทนในลักษณะเดียวกันกับการรับจ้างเปิดบัญชีธนาคาร ดังนั้น นอกจากจะกำหนดมาตรการการยืนยันตัวตนให้ชัดเจนแล้วยังจำเป็นจะต้อง**มีการกำหนดบทลงโทษที่เด็ดขาดและรุนแรงกรณีที่ตรวจพบการฝ่าฝืนหรือกรณีที่ปรากฏว่ามีการปลอมแปลงตัวตนผู้ใช้งาน หรือการกระทำความผิดในลักษณะของการลักลอบยืนยันตัวตนแทนผู้อื่นควบคู่กันไปด้วย เพื่อให้การดำเนินการตามมาตรการยืนยันตัวตนสามารถเก็บข้อมูลผู้ใช้งานที่แท้จริงได้อย่างมีประสิทธิภาพ**

นอกจากนี้ผู้ให้ข้อมูลสำคัญยังได้กล่าวว่าการกำหนดมาตรการในลักษณะนี้ย่อมจะต้องขัดต่อหลักสิทธิเสรีภาพของประชาชนบ้างบางประการ อีกทั้งยังอาจส่งผลกระทบต่อการพัฒนาหรือการขยายตัวทางเศรษฐกิจ เพราะเจตนารมณ์ที่แท้จริงของการสร้างบิทคอยน์และสกุลเงินเข้ารหัสต่างๆคือการพัฒนาเครื่องมือที่จะสร้างสภาพคล่องให้แก่ระบบเศรษฐกิจ แต่ทั้งนี้หากพิจารณาในมิติของการป้องกันอาชญากรรมและการรักษาความสงบเรียบร้อยของสังคมแล้ว ผู้ให้ข้อมูลสำคัญที่เป็นบุคลากรในกระบวนการยุติธรรมยังคงมีความเห็นว่า การกำหนดมาตรการดังกล่าวยังมีความจำเป็นและจะก่อให้เกิดผลประโยชน์ต่อส่วนรวมมากกว่าผลร้าย ตัวอย่างเช่น เมื่อพิจารณาเทียบเคียงกับกรณีในอดีตที่คนร้ายนำซิมการ์ดโทรศัพท์ที่สามารถซื้อขายได้ทั่วไปไปใช้ในการประกอบระเบิดแสวงเครื่อง ทำให้เจ้าหน้าที่ไม่สามารถติดตามตรวจสอบผู้กระทำผิดได้เพราะซิมการ์ดที่ใช้งานดังกล่าวไม่ได้

ผ่านการลงทะเบียนหรือยืนยันตัวตนผู้ใช้งาน แต่หลังจากที่รัฐได้มีการกำหนดมาตรการในการลงทะเบียนผู้ใช้งานซิมการ์ดโทรศัพท์แล้ว ทำให้การนำซิมการ์ดไปใช้ในการก่อวินาศกรรมลดน้อยลง

ทั้งนี้การกำหนดมาตรการบังคับให้มีการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆนี้ จะทำให้เกิดประโยชน์อย่างยิ่งต่อการสืบสวนสอบสวนเพื่อหาตัวผู้กระทำผิดที่แท้จริง โดยผู้ให้ข้อมูลสำคัญได้ให้ความเห็นในประเด็นนี้ว่า **หากสามารถบังคับใช้มาตรการนี้ได้จริง ก็จะทำให้เกิดการผลักดันให้การใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเข้าสู่กระแสหลัก (Mainstream) มากขึ้น** ซึ่งแตกต่างจากเดิมที่การใช้งานมีลักษณะคล้ายกับอยู่ใต้ดิน เพราะยังไม่มีกฎหมายหรือหน่วยงานใดตรวจสอบอย่างจริงจัง และเมื่อการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสเข้าสู่กระแสหลักมากขึ้นในที่สุดสภาพปัญหาของการปกปิดตัวตนก็จะเบาบางลง ในขณะที่เมื่อวิเคราะห์ไปในทางตรงกันข้ามว่าหากการผลักดันให้การใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเข้าสู่กระแสหลักด้วยมาตรการการยืนยันตัวตนนี้ ใช้ไม่ได้ผลกับกลุ่มผู้กระทำผิดหรืออาชญากรกล่าวคือผู้ที่ต้องการใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆกระทำความผิดก็อาจจะยังคงหลีกเลี่ยงและไม่แสดงตนตามมาตรการของรัฐก็ตาม แต่ผลจากการที่ผู้ใช้งานตามปกติตอบสนองต่อการลงทะเบียนของรัฐทำให้รัฐมีฐานข้อมูลที่สำคัญที่อาจใช้ในการเชื่อมโยงไปยังตัวผู้กระทำความผิดได้ เช่น หากไม่มีมาตรการการลงทะเบียนยืนยันตัวตนใดๆ เมื่ออาชญากรนำไปใช้งานในการจ่ายหรือโอนบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไปมาระหว่างกันเจ้าหน้าที่ของรัฐก็จะไม่สามารถตรวจสอบได้ แต่หากมีการลงทะเบียนตัวตนผู้ใช้งานไว้แล้วแม้ผู้กระทำผิดหลักจะหลบเลี่ยงไม่แสดงตัวตนตามมาตรการดังกล่าว แต่เจ้าหน้าที่ของรัฐก็ยังมีโอกาสในการติดตามตัวผู้กระทำผิดหลักมากขึ้น จากการติดตามกระแสการจ่ายหรือโอนบิทคอยน์และสกุลเงินเข้ารหัสต่างๆระหว่างกัน โดยหากบิทคอยน์หรือสกุลเงินเข้ารหัสที่ถูกตรวจสอบติดตามอยู่ถูกส่งผ่านไปยังบัญชีผู้ใช้งานที่ได้ลงทะเบียนไว้ ก็จะสามารถพบตัวตนบุคคลที่อาจมีความเกี่ยวข้องในการกระทำผิดได้ เป็นต้น

“เรายังไม่มีกฎหมายมาบังคับให้เขาต้องระบุตัวตน ให้เขาต้องเปิดเผย หรือ ต้องไม่ยอมให้คนอื่นใช้งาน ผมว่าปัจจุบันควรมี ซึ่งผมมองสิทธิส่วนบุคคลเป็นเรื่องรองนะครับ ถ้าการใช้สิทธิส่วนบุคคลมันไม่กระทบกับอาชญากรรม ไม่กระทบกับสังคมก็ไม่เป็นไร แต่ถ้าวันใดวันหนึ่งการใช้สิทธิส่วนบุคคลมันกลายเป็นช่องทางในการกระทำความผิด แล้วเป็นเรื่องสำคัญ เป็นเรื่องใหญ่ ก็จำเป็นต้องทำ ”

(B2, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“ในต่างประเทศได้ตระหนักในเรื่องนี้ (การยืนยันตัวตน) โดยมีการออกกฎหมายว่าต้องลงทะเบียนถ้าจะเล่นพวกนี้ จะได้ระบุตัวตนได้ว่าบัญชีนี้คือใคร ถ้าเพิ่มได้ต้องเพิ่มโทษของการปลอมบัญชีให้หนักกว่านี้ และถ้าคิดแบบสุดโต่งเลยคือทุกคนต้องลงทะเบียน มันอาจจะมีคำถามกลับในเรื่องสิทธิมนุษยชนหรือเรื่องสิทธิเสรีภาพแต่ถ้ามองในมิติเรื่องการป้องกันมันก็ต้องยอม เหมือนอย่างซิมการ์ดโทรศัพท์เมื่อก่อนที่ยังไม่ควบคุมการซื้อตามร้านสะดวกซื้อแล้วใช้ได้เลย ก็กลายเป็นเอาไปทำเป็นระเบิดแต่พอมาลงทะเบียนซิมโทรศัพท์ก็เกิดน้อยลง ”

(C1, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“มีการทำ KYC มันก็ดี แต่ต้องพิจารณาอีกว่า มันจะบังคับใช้ได้จริงขนาดไหน KYC ปลอมก็เยอะแยะ มีฐานข้อมูลมันเป็นเรื่องดี แต่ต้องมีมาตรการรองรับการปลอมแปลงด้วย ไม่งั้นจะทำให้ปัญหาซับซ้อนเพิ่มขึ้น ”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

“คนที่ทำถูกกฎหมาย เขาไม่มีปัญหากับการ KYC (ยืนยันตัวตนผู้ใช้งาน)หรอก แต่มันจะเป็นปัญหากับพวกอาชญากรที่ไม่ต้องการแสดงตน ต้องการหลบระบบ ที่ถึงแม้จะถูกบังคับให้แสดงตนเราก็อาจไม่ได้ข้อมูลตัวตนที่แท้จริง เพราะคนเหล่านี้ก็จะใช้นอมินีมายืนยันตัวตนแทนอยู่ดี ”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

“ในทางปฏิบัติมันจะติดตามไม่ได้เลยในกรณีที่เกิดว่าบัญชีนั้นๆ นำไปใช้งานแบบ Peer – to – Peer อย่างเดียวโดยตลอด แต่ถ้ามีมาตรการในการลงทะเบียน หรือ KYC (Know Your Customer หรือ วิธีการลงทะเบียนยืนยันตัวตน) แล้ว สมมติว่าถ้าเส้นทางการกระทำผิดผ่านคนใช้งานไป 5 คน แล้วหนึ่งในนั้น เป็นผู้ที่ KYC (ลงทะเบียนยืนยันตัวตน) ไว้ ตำรวจก็จะสามารถทราบตัวตนแล้วเข้าไปสืบสวนเส้นทางการเงินต่อได้ทันที”

(A5, สัมภาษณ์, 26 พฤศจิกายน 2562)

ในขณะที่ผู้ให้ข้อมูลสำคัญบางส่วน ยังมีความเห็นแตกต่างในประเด็นดังกล่าวว่า **การดำเนินนโยบายดังกล่าวจะต้องคำนึงถึงความสมดุลระหว่างการควบคุมอาชญากรรมกับ**

ประเด็นเรื่องสิทธิเสรีภาพและการพัฒนาระบบการเงินการธนาคารควบคู่กันไปด้วย โดยอาจจะต้องมีการเก็บข้อมูลและวิเคราะห์สภาพปัญหาที่เกิดขึ้นจริงในประเทศไทย แล้วจึงวางระดับความเข้มข้นของนโยบายให้สอดคล้องเหมาะสมกับสถานการณ์ เนื่องจากหากมีการกำหนดมาตรการที่มีความเคร่งครัดมากเกินกว่าระดับของปัญหาแล้วอาจส่งผลลัพธ์ไปในทิศทางตรงกันข้าม กล่าวคือ การเปิดเผยการถือครองในลักษณะนี้อาจส่งผลให้ประชาชนรู้สึกว่ากระทบต่อสิทธิเสรีภาพจนเกินไป หรือทำให้สังคมรู้สึกว่าเป็นการยุ่งยากที่จะต้องแสดงตัวตนให้รัฐตรวจสอบ ซึ่งขัดต่อสภาพโดยธรรมชาติของบิทคอยน์หรือสกุลเงินเข้ารหัส จนทำให้ผู้ใช้งานกลับตอบสนองต่อมาตรการดังกล่าวด้วยการหลบเลี่ยงและไม่แสดงตัวตนเพิ่มมากยิ่งขึ้นกว่าปกติก็เป็นได้ ทั้งนี้เพื่อประโยชน์ในการตรวจสอบยืนยันตัวบุคคลที่มีพฤติกรรมการใช้งานที่น่าสงสัย ผู้ให้ข้อมูลสำคัญกลุ่มนี้จึงเสนอแนวทางให้นำหลักการในการป้องกันและปราบปรามการฟอกเงินมาประยุกต์ใช้ในลักษณะที่กำหนดให้พฤติกรรมการใช้งานที่มีลักษณะต้องสงสัย จะต้องรายงานข้อมูลมายังหน่วยงานของรัฐ หรือ จะต้องให้หน่วยงานของรัฐเข้าทำการตรวจสอบได้ เช่น การกำหนดให้ผู้ที่ทำธุรกรรมเกี่ยวกับบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆเป็นจำนวนมากกว่า 1 ล้านบาท จะต้องรายงานให้หน่วยงานของรัฐที่รับผิดชอบทราบ เป็นต้น

“ถ้าให้เปิดเผยการถือครองเลยมันจะเป็นการจำกัดสิทธิมากเกินไป พอรู้สึกว่ามันยากคนก็จะยิ่งไม่ทำ มันไม่ค่อยตอบโจทย์เท่าไหร่ เพราะมันเหมือนกับว่ามันไม่เป็นธรรมชาติของสกุลเงินเข้ารหัส แต่ถ้าไปควบคุมรายใหญ่ มูลค่าเกินสองล้านขึ้นไป ต้องรายงานถ้าเป็นอย่างนั้นได้น่าสนใจ แต่ถ้าไปคุมรายย่อยด้วยมันก็ผิดหลักสภาพคล่อง”

(B1, สัมภาษณ์, 28 พฤศจิกายน 2562)

“ต้องสร้างความสมดุลระหว่างการควบคุมอาชญากรรมและเสถียรภาพของประเทศทั้งด้านการเงิน ทั้งด้านอาชญากรรม ถามว่าจำเป็นมั้ยผมว่าก็จำเป็น เพียงแต่ว่าจำเป็นในระดับไหน เช่น สมมติว่าผมจะใช้แค่ 100 บาท 500 บาท มาตรการอาจจะไม่จำเป็นต้องเข้ม แต่ถ้าใช้เยอะหรือมีพฤติกรรมแปลกๆ อาจจะต้องมาให้ข้อมูลเพิ่มเติม เหมือนหลักการของการฟอกเงินถ้าเกินสองล้านบาทต้องนำรายละเอียดมาแสดง”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

กล่าวโดยสรุปได้ว่าจากประเด็นปัญหาที่เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ไม่สามารถตรวจสอบติดตามหรือสืบสวนเพื่อพิสูจน์ตัวตนผู้ที่นำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดได้ เนื่องจากลักษณะพิเศษของบิทคอยน์ที่มีการปกปิดตัวตนของผู้ใช้งานนั้น **ผู้ให้ข้อมูลสำคัญกลุ่มหนึ่งจึงได้เสนอและสนับสนุนให้รัฐมีมาตรการในการตรวจสอบยืนยันตัวตนผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสด้วย**วิธีการในการลงทะเบียนข้อมูลส่วนบุคคลและข้อมูลที่เกี่ยวข้องกับการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เช่น เลขที่บัญชีบิทคอยน์ (Bitcoin Address /Public Key) โดยให้ข้อมูลดังกล่าวเก็บรักษาไว้กับหน่วยงานภาครัฐที่ได้รับมอบหมายหรือมีหน้าที่รับผิดชอบ เป็นต้น ซึ่งการดำเนินการตามแนวทางนี้จะทำให้เกิดผลในการจะสามารถบรรเทาปัญหาในเรื่องความไร้ตัวตนของผู้ใช้งานบิทคอยน์ (Anonymity) ได้ ซึ่งแนวคิดของผู้ให้ข้อมูลสำคัญดังกล่าวมีความสอดคล้องกันกับงานวิจัยของ **จุฑารัตน์ ชวดนุช (2557)** ที่เสนอข้อเสนอแนะสำคัญคือความจำเป็นอย่างยิ่งที่รัฐจะต้องกำหนดให้ผู้ใช้งานบิทคอยน์ ต้องมีการระบุชื่อนามสกุลจริงในการใช้งานเพื่อเป็นการเปิดเผยตัวตนของผู้ใช้งานเพื่อความสะดวกในการควบคุมโดยรัฐ ในขณะที่ผู้ให้ข้อมูลสำคัญกลุ่มหนึ่งมีความเห็นในทางตรงกันข้ามว่า หากรัฐกำหนดมาตรการบังคับให้ผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆทำการยืนยันตัวตนในการใช้งานอย่างเข้มข้นจนเกินไปนั้นก็อาจส่งผลกระทบต่อภาคเศรษฐกิจทั้งยังอาจเกิดประเด็นปัญหาในเรื่องของการริดรอนสิทธิเสรีภาพจนเกินกว่าเหตุ โดยผู้ให้ข้อมูลสำคัญกลุ่มนี้จึงได้เสนอให้มีการเก็บข้อมูลและวิเคราะห์สภาพปัญหาที่เกิดขึ้นจริงในประเทศไทย ณ ขณะนั้นที่มีการดำเนินขั้นตอนการกำหนดนโยบาย แล้วจึงวางระดับความเข้มข้นของนโยบายให้สอดคล้องเหมาะสมกับสถานการณ์ต่อไป

ทั้งนี้ในส่วนของวิธีการในการยืนยันตัวตนผู้ใช้งานนั้น **ผู้วิจัยมีมุมมองเพิ่มเติมที่สอดคล้องกันกับผู้ให้ข้อมูลสำคัญว่า** เพื่อให้มาตรการบังคับให้มีการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานนี้บังคับใช้ได้จริงและเป็นการ เพื่อป้องกันลักลอบการแสดงตนแทนกัน จึงสมควรอย่างยิ่งที่จะต้องมีการกำหนดขั้นตอนและวิธีการให้ผู้ใช้งานจะต้องแสดงตนตามมาตรการ ดังนี้

1) กำหนดให้มีการมาแสดงตัวเพื่อลงทะเบียนการใช้งานต่อหน้าพนักงานเจ้าหน้าที่ของรัฐที่ได้รับมอบหมาย พร้อมทั้งแสดงเอกสารประจำตัวเพื่อแสดงเจตจำนงค์เป็นผู้ใช้งานสกุลเงินเข้ารหัสในฐานะต่างๆ เช่น นักลงทุน ผู้ซื้อขาย ตัวแทนผู้ประกอบธุรกิจ เป็นต้น

2) เจ้าหน้าที่ของรัฐที่ได้รับมอบหมาย จะต้องดำเนินการเก็บข้อมูลผู้ที่ลงทะเบียนใช้งานสกุลเงินเข้ารหัสไว้เป็นฐานข้อมูลสำคัญ เพื่อใช้ในการตรวจสอบการใช้งานต่อไป

3) หากรัฐมีความจำเป็น เพื่อประโยชน์ในการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรม อาจกำหนดวิธีการพิเศษ เพิ่มเติมเพื่อเป็นมาตรการป้องปรามการกระทำความผิดเพิ่มเติมได้ เช่น หากสถานการณ์การใช้บิทคอยน์ไปก่ออาชญากรรมมีความรุนแรงขึ้น อาจกำหนดมาตรการเพิ่มเติมในการยืนยันตัวตนผู้ใช้งาน เช่น กำหนดให้การซื้อขาย การซื้อขาย แลกเปลี่ยน โอน-รับ จะต้องมีการยืนยันตัวตนทั้งต้นทางและปลายทาง ด้วยวิธีการต่างๆ เช่น การมากระทำต่อหน้าเจ้าหน้าที่ของรัฐ หรือ การยืนยันตัวตนผ่านอุปกรณ์อิเล็กทรอนิกส์ที่สามารถใช้ระบบการสื่อสารทางไกลแบบเห็นใบหน้า (VDO Call) เพื่อเป็นการยืนยันตัวบุคคลว่า ผู้ใดกระทำธุรกรรมที่เกี่ยวกับสกุลเงินเข้ารหัสกับผู้ใด เป็นต้น

อย่างไรก็ตาม การที่รัฐจะกำหนดความเข้มข้นในการบังคับใช้มาตรการการลงทะเบียนยืนยันตัวตนผู้ใช้งานในระดับใด หรือการที่รัฐจะพิจารณาว่าบุคคลใดบ้างที่มีหน้าที่ที่จะต้องลงทะเบียนยืนยันตัวตนตามมาตรการดังกล่าวนั้น ภาครัฐหรือผู้มีอำนาจจำเป็นจะต้องนำสถานการณ์และสภาพปัญหาที่เกี่ยวกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในขณะนั้นมาพิจารณาประกอบเพื่อให้เกิดความเหมาะสมสูงสุดและให้เกิดผลกระทบต่อการพัฒนาทางด้านเทคโนโลยีทางการเงินและภาคเศรษฐกิจอย่างสมเหตุสมผลด้วย ซึ่งจะได้กล่าวถึงต่อไป ทั้งนี้จากการศึกษาทบทวนวรรณกรรมและการเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลสำคัญทำให้ผู้วิจัยสามารถสรุปได้ว่า เพื่อประโยชน์ในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสแล้ว ประเทศไทยจำเป็นอย่างยิ่งที่จะต้องมี**มาตรการบังคับให้มีการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งาน** ที่สามารถดำเนินการได้จริง

4.4.2 การกำหนดวิธีปฏิบัติในการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่ชัดเจน

จากประเด็นปัญหาเรื่องการตีความกฎหมายเพื่อเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่แตกต่างกันของเจ้าหน้าที่ในกระบวนการยุติธรรมจนทำให้เกิดข้อถกเถียงและความสับสนในทางปฏิบัติ ส่งผลทำให้เจ้าหน้าที่ที่มีหน้าที่ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสเกิดความไม่มั่นใจในขั้นตอนและวิธีการที่ถูกต้องในการปฏิบัติงาน หรือเกิดความกังวลว่าตนจะกระทำการอันเป็นการขัดต่อหลักกฎหมายจนอาจทำให้

เจ้าหน้าที่ที่เกี่ยวข้องหลีกเลี่ยงหรือเลือกที่จะไม่เสี่ยงดำเนินการใดๆ เช่น ไม่กล้าเข้าถึงข้อมูลที่เป็นพยานหลักฐานสำคัญในเครื่องคอมพิวเตอร์ที่ตรวจยึดมาได้ เป็นต้น ซึ่งหากปัญหาดังกล่าวไม่ได้รับการแก้ไขก็อาจทำให้เกิดช่องว่างในการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้

เพื่อเป็นการแก้ไขปัญหาดังกล่าว จึงได้มีผู้ให้ข้อมูลสำคัญเสนอแนวทางการแก้ปัญหาดังกล่าวโดย **การสร้างข้อยุติร่วมกันของเจ้าหน้าที่ภาครัฐในการตีความกฎหมายเกี่ยวกับการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์** โดยมีวัตถุประสงค์เพื่อให้เจ้าหน้าที่ในกระบวนการยุติธรรมตั้งแต่ในชั้นตำรวจ อัยการ ศาล รวมทั้งหน่วยงานราชการอื่นๆที่เกี่ยวข้องมีความเข้าใจที่ตรงกันในรายละเอียดต่างๆ โดยอาจดำเนินการในรูปแบบของการประชุมใหญ่ของคณะกรรมการพิเศษอันได้แก่ ผู้พิพากษา พนักงานอัยการ เจ้าหน้าที่ตำรวจ และเจ้าหน้าที่หน่วยงานอื่นๆที่เกี่ยวข้อง เช่น กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน เป็นต้น เพื่อร่วมกันหาข้อยุติในเรื่องการตีความกฎหมายร่วมกันให้ชัดเจนว่า เมื่อเจ้าหน้าที่ที่มีหน้าที่เก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ต้องการจะเข้าถึงข้อมูลอันเป็นพยานหลักฐานสำคัญจะต้องทำอย่างไร จะต้องใช้หลักการตามกฎหมายประมวลวิธีพิจารณาความอาญา หรือ จะต้องใช้หลักการตามกฎหมาย พ.ร.บ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ หรือหากหลักกฎหมายที่มีอยู่ในปัจจุบันยังไม่ครอบคลุมจำเป็นจะต้องมีการพิจารณาแก้ไขเพิ่มเติมหรือออกกฎหมายใหม่หรือไม่ อย่างไร **หลังจากที่ได้ข้อยุติแล้วจะต้องมีการออกประกาศหรือคำสั่งแจ้งเวียนให้ทุกหน่วยงานที่เกี่ยวข้องทราบ รวมทั้งจัดให้มีการอบรม เผยแพร่ความรู้ ให้เจ้าหน้าที่ในกระบวนการยุติธรรมทุกภาคส่วนรับทราบและมีความเข้าใจที่ถูกต้องตรงกัน** เพื่อมิให้เกิดความเห็นขัดแย้งในทางการวิเคราะห์ตีความกฎหมายในขั้นตอนต่างๆของระบบกระบวนการยุติธรรมอีก

นอกจากนี้ ผู้ให้ข้อมูลสำคัญยังมีความเห็นว่าควรจะต้องจัดทำรายละเอียดข้อสรุปดังกล่าวให้อยู่ในรูปแบบของ**หนังสือ ตำรา หรือ คู่มือการปฏิบัติงานเกี่ยวกับการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบอิเล็กทรอนิกส์** เพื่อให้เกิดการพัฒนาองค์ความรู้อย่างต่อเนื่ององค์และเป็นการสร้างหลักปฏิบัติที่ชัดเจนให้แก่เจ้าหน้าที่ผู้ปฏิบัติงาน ซึ่งการหาข้อยุติในการตีความกฎหมายและการกำหนดขั้นตอนการปฏิบัติที่ชัดเจนนี้ จะทำให้เจ้าหน้าที่ผู้ปฏิบัติงานไม่เกิดความสับสน และยังส่งผลให้เจ้าหน้าที่มีองค์ความรู้และความมั่นใจที่จะแสวงหาหรือเก็บรวบรวมพยานหลักฐานต่างๆที่สามารถนำไปใช้ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ

“ถ้าเราสามารถตีความร่วมกันได้ว่า ตกลงมันทำได้มั้ย ถ้าทำไม่ได้แล้วควรจะทำยังไงต่อ จะต้องออกกฎหมายใหม่หรือจะทำยังไง เพราะฉะนั้นผมเห็นด้วยมากๆ เช่น ควรจะประชุมใหญ่ แล้วฟันธงเลยว่าจะต้องมีวิธีการกับเรื่องนี้ (การเข้าถึงข้อมูลอิเล็กทรอนิกส์) อย่างไร เอาให้ชัดเจน แล้วอาจทำเป็นคู่มือ เพราะสำคัญเลยคือ กระบวนการยุติธรรมเราจะต้องเข้าใจตรงกันก่อนว่าตกลงเราจะเอาแบบไหน”

(B2, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“ต้องมีการต่อยอดและพัฒนาองค์ความรู้อย่างต่อเนื่อง เรายังขาดเรื่องพวกนี้ ดังนั้น เมื่อเราสร้างองค์ความรู้ได้แล้วต้องรวบรวม ส่งต่อ แจกจ่าย เผยแพร่ เพื่อให้เกิดการกระจายความรู้เหล่านี้ออกไปให้ได้มากที่สุด”

(C2, สัมภาษณ์, 25 มีนาคม 2563)

กล่าวโดยสรุปว่า สืบเนื่องจากที่ผู้ให้ข้อมูลสำคัญซึ่งเป็นผู้ทรงคุณวุฒิทางด้านกฎหมายและเป็นบุคลากรในกระบวนการยุติธรรมได้ชี้ให้เห็นถึงปัญหาของการตีความกฎหมายเพื่อเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่แตกต่างกันของเจ้าหน้าที่ในกระบวนการยุติธรรมจนทำให้เกิดข้อถกเถียงและความสับสนในทางปฏิบัติ ผู้ให้ข้อมูลสำคัญจึงเสนอให้มีการแก้ปัญหาดังกล่าวโดยการดำเนินการดังนี้ คือ

1) การสร้างข้อยุติร่วมกันของเจ้าหน้าที่ภาครัฐในการตีความกฎหมายเกี่ยวกับการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์

2) หลังจากที่ได้ข้อยุติแล้วจะต้องมีการออกประกาศหรือคำสั่งแจ้งเวียนให้ทุกหน่วยงานที่เกี่ยวข้องทราบ รวมทั้งจัดให้มีการอบรม เผยแพร่ความรู้ ให้เจ้าหน้าที่ในกระบวนการยุติธรรมทุกภาคส่วนรับทราบและมีความเข้าใจที่ถูกต้องตรงกัน

3) จัดทำรายละเอียดข้อสรุปดังกล่าวให้อยู่ในรูปแบบของหนังสือ ตำรา หรือ คู่มือการปฏิบัติงานเกี่ยวกับการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบอิเล็กทรอนิกส์

โดยที่แนวทางการดำเนินการในลักษณะนี้ มีความสอดคล้องกันกับสภาพปัญหาที่ผู้วิจัยพบจากการศึกษาทบทวนวรรณกรรมในประเด็นที่เกี่ยวกับแนวทางการปฏิบัติงานของหน่วยงานของรัฐที่มีหน้าที่เกี่ยวข้องในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ที่หน่วยงานของรัฐที่เกี่ยวข้องยังมิได้มีการกำหนดหลักเกณฑ์และวิธีการปฏิบัติในเรื่องที่เกี่ยวกับการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบอิเล็กทรอนิกส์ไว้อย่างชัดเจน โดยมีลักษณะเป็นการดำเนินการไปตาม

แนวทางหรือวิธีปฏิบัติแบบดั้งเดิมซึ่งเป็นการปฏิบัติที่แตกต่างกันไปตามหน่วยงานต่างๆ จนทำให้เกิดเป็นสภาพปัญหาตามที่ได้กล่าวมาแล้ว ผู้วิจัยจึงเห็นว่าการดำเนินการตามแนวทางนี้ย่อมจะทำให้กระบวนการสืบสวนสอบสวนเก็บรวบรวมพยานหลักฐานมีประสิทธิภาพมากขึ้น อันจะส่งผลต่อการเพิ่มศักยภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอีกด้วย

4.4.3 การออกกฎหมายหรือปรับปรุงแก้ไขกฎหมาย เพื่อให้มีการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ (E - Wallet) ของรัฐ เพื่อใช้เป็นเครื่องมือหลักในการยึดหรืออายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำผิดกฎหมาย

ผู้ให้ข้อมูลสำคัญได้กล่าวถึงการกำหนดแนวทางหรือกระบวนการที่สำคัญอีกประการหนึ่ง ซึ่งจะส่งผลถึงการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรม คือ การสร้างกระเป๋าเงินอิเล็กทรอนิกส์ของรัฐขึ้น เพื่อใช้เป็นเครื่องมือในการเก็บรักษาบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำความผิดในกรณีที่สามารถยึดหรืออายัดมาจากผู้กระทำผิดได้ เนื่องจากบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไม่ได้อยู่ในรูปแบบของทรัพย์สินที่จับต้องได้ ซึ่งตามปกติแล้วบิทคอยน์และสกุลเงินเข้ารหัสต่างๆนั้นจะถูกเก็บรักษาอยู่ในกระเป๋าเงินอิเล็กทรอนิกส์ที่ถูกสร้างในรูปแบบต่างๆ แต่ปรากฏว่าในปัจจุบันประเทศไทยยังไม่มีการออกกฎหมายที่เกี่ยวข้องกับเรื่องดังกล่าว ดังนั้น เพื่อให้รัฐมีกระบวนการทางยุติธรรมที่ครบถ้วนจนถึงขั้นตอนการยึดและอายัดก็จำเป็นจะต้องมีการ**ออกหรือแก้ไขเพิ่มเติมกฎหมายหรือกฎระเบียบต่างๆ เพื่อให้มีการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ หรือ (E - Wallet) ของรัฐเพื่อรองรับการเก็บรักษาบิทคอยน์และสกุลเงินเข้ารหัสในฐานะของกลางที่ถูกยึดหรืออายัดโดยหน่วยงานของรัฐ** นอกจากนี้ยังจำเป็นจะต้องตรวจสอบปรับปรุงแก้ไข กฎหมาย ระเบียบ ตลอดจนคำสั่งของหน่วยงานของรัฐต่างๆที่เกี่ยวข้องกับการยึดหรืออายัดทรัพย์สินให้ครอบคลุมและรองรับการยึดและอายัดสกุลเงินเข้ารหัส เพื่อให้เจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องสามารถอาศัยอำนาจตามกฎหมายในการกระทำการต่างๆได้อย่างครบถ้วนสมบูรณ์ ทั้งเพื่อเป็นหลักประกันความปลอดภัยในทางกฎหมายให้แก่เจ้าหน้าที่ผู้ปฏิบัติงานอีกด้วย

นอกจากนี้ ผู้ให้ข้อมูลสำคัญยังให้ข้อเสนอแนะอีกว่า นอกจากการออกกฎหมายหรือการแก้ไขกฎหมายที่เกี่ยวข้องเพื่อให้เกิดการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet) ของรัฐ และการแก้ไขกฎหมาย ระเบียบ คำสั่งต่างๆ เพื่อให้สอดคล้องและรองรับกับการยึดและอายัดสกุลเงินเข้ารหัสที่ใช้ในการกระทำความผิดแล้ว **ยังจำเป็นจะต้องมีการกำหนดวิธีการและขั้นตอนในการยึดและ**

อายัดด้วยกระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet) ของรัฐที่ชัดเจน เพื่อให้เจ้าหน้าที่ผู้ปฏิบัติสามารถดำเนินการได้อย่างถูกต้อง อันเป็นการป้องกันไม่ให้เกิดความเสี่ยงที่จะทำให้สกุลเงินเข้ารหัสที่ถูกยึดหรืออายัดเสียหาย ถูกทำลาย สูญหาย หรือถูกโอนออกไปบังบัญชีใช้งานอื่นๆ อันอาจทำให้เกิดความเสียหายทั้งในแง่ของมูลค่าและการเป็นวัตถุพยานหรือของกลางที่สำคัญในคดี ทั้งนี้ยังจำเป็นจะต้องจัดให้มีการฝึกอบรมและขยายองค์ความรู้ดังกล่าวออกไปสู่เจ้าหน้าที่ในกระบวนการยุติธรรมเพื่อให้เกิดความรู้ความเข้าใจที่ตรงกัน ในเครื่องมือและกลไกใหม่ดังกล่าว

จากข้อเสนอแนะของผู้ให้ข้อมูลสำคัญซึ่งมีประสบการณ์การทำงานเกี่ยวกับการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆโดยตรงในประเด็นนี้นั้น ผู้วิจัยมีความเห็นว่า ควรมีการออกกฎหมายหรือปรับปรุงแก้ไขกฎหมาย เพื่อให้มีการสร้างกระเป๋าอิเล็กทรอนิกส์ (E - Wallet) ของรัฐเพื่อใช้เป็นเครื่องมือหลักในการยึดหรืออายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำผิดกฎหมายนั้น เป็นแนวทางที่จำเป็นที่ภาครัฐของไทยจะต้องดำเนินการ เนื่องจากเมื่อพิจารณาจากข้อมูลที่ได้จากการทบทวนวรรณกรรมจะพบว่าประเทศที่มีการเตรียมพร้อมรับมือกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้เป็นอย่างดีอย่างประเทศสหรัฐอเมริกาและประเทศญี่ปุ่น ได้มี การนำกระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet) ของรัฐมาใช้ในการบังคับคดีแล้ว ซึ่งส่งผลทำให้กระบวนการยุติธรรมสามารถทำหน้าที่ในการลงโทษและระงับยับยั้งผู้กระทำผิดได้อย่างสมบูรณ์ครบถ้วน ดังนั้นเพื่อให้หน่วยงานที่เกี่ยวข้องสามารถดำเนินการในการยึดอายัดได้อย่างมีประสิทธิภาพ มีกฎหมายรองรับ จึงจำเป็นอย่างยิ่งที่จะต้องดำเนินการตามข้อเสนอดังกล่าว

4.4.4 ส่งเสริมให้มีการศึกษาวิจัย เพื่อค้นหาวิธีการ เครื่องมือหรือกลไกการป้องกันอาชญากรรมรูปแบบใหม่ ที่สามารถป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ

จากสภาพปัญหาที่เจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ยังขาดองค์ความรู้และวิธีการเฉพาะที่จะใช้ในการตรวจสอบติดตามการกระทำความผิด ส่งผลให้ยังไม่สามารถพิสูจน์ยันยันตัวบุคคลผู้กระทำความผิดที่แท้จริงจากข้อมูลการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆโดยตรงได้ จึงได้มีผู้ให้ข้อมูลสำคัญเสนอแนะให้ภาครัฐมีการสนับสนุนและส่งเสริมให้หน่วยงานหรือสถาบันทางวิชาการต่างๆที่เป็นผู้เชี่ยวชาญหรือมีองค์ความรู้เกี่ยวกับการวิจัยในด้านเทคโนโลยีสารสนเทศหรือวิศวกรรมคอมพิวเตอร์หรือระบบคอมพิวเตอร์ขั้นสูง

ร่วมกัน**ทำการศึกษาวิจัยระบบการทำงานของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ตลอดจนร่วมกันทดลองหรือทดสอบวิธีการด้วยเครื่องมือหรือกลไกต่างๆ เพื่อให้สามารถสร้างเครื่องมือหรือกลไกที่จะสามารถตรวจสอบยืนยันตัวตนผู้กระทำความผิดที่แท้จริงได้**

โดยประเด็นดังกล่าวผู้ให้ข้อมูลสำคัญได้เล่าถึงความพยายามในการพัฒนาวิธีการในการตรวจสอบเส้นทางการเงินและความพยายามในการพิสูจน์ตัวตนของ สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ว่า ในปัจจุบันนี้สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ได้ตระหนักถึงสภาพปัญหาต่างๆที่เกิดจากการที่คนร้ายนำบิทคอยน์ไปใช้เป็นเครื่องมือในการฟอกเงิน จึงเกิดแนวคิดในการพยายามที่จะพัฒนาวิธีการใหม่ขึ้น เพื่อให้สามารถรู้เท่าทันและสามารถป้องกันและปราบปรามการฟอกเงินผ่านสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ จึงได้มีการดำเนินการทดลองภายในหน่วยงานโดยใช้ชื่อว่า **“ชุมชนบล็อคเชน” ซึ่งโครงการดังกล่าวเป็นการสร้างชุมชนของผู้ใช้งานสกุลเงินเข้ารหัสจำลองและสร้างสกุลเงินเข้ารหัสจำลองขึ้น** โดยมีผู้ลงทะเบียนใช้งานจำนวน 100 คน ซึ่งเป็นเจ้าหน้าที่ของหน่วยงาน โดยมีการแบ่งกันทำหน้าที่สมมติในชุมชนดังกล่าวทั้งการเป็นผู้ใช้งาน (User) และ ผู้กำกับดูแล (Regulator) ทั้งยังจำลองสถานการณ์ต่างๆให้ใกล้เคียงกับการใช้งานในโลกแห่งความจริงมากที่สุดเริ่มตั้งแต่การโอน – รับสกุลเงินเข้ารหัส ทั้งส่วนของการนำไปใช้ในการซื้อขายสินค้าและบริการต่างๆ การนำไปใช้แลกเปลี่ยนระหว่างสกุลเงินเข้ารหัสด้วยกัน การขุดสกุลเงินเข้ารหัส การประกอบธุรกิจในรูปแบบต่างๆ เพื่อให้เกิดเส้นทางการเงินของสกุลเงินเข้ารหัสที่มีความใกล้เคียงกับธรรมชาติหรือสภาพที่แท้จริง รวมทั้งยังได้กำหนดโจทย์ของสถานการณ์ทั้งกรณีที่มีผู้นำสกุลเงินเข้ารหัสไปใช้งานปกติและกรณีที่มีการนำไปใช้ในการกระทำความผิด จากนั้นจะให้เจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องในการวิเคราะห์และตรวจสอบพฤติกรรมทางการเงิน ทำการฝึกปฏิบัติจากสถานการณ์จำลองดังกล่าว โดยมุ่งเน้นไปที่การฝึกตรวจสอบติดตามเส้นทางการเงินที่มีพิรุธต้องสงสัยเพื่อหาช่องทางและวิธีการที่จะพิสูจน์ทราบถึงตัวตนของผู้ที่นำไปใช้กระทำความผิดในระบบจำลอง โดยวัตถุประสงค์ของโครงการดังกล่าวก็เพื่อให้เกิดการศึกษา วิเคราะห์ จากสถานการณ์และสภาพปัญหาอุปสรรคที่ใกล้เคียงกับความเป็นจริงมากที่สุด แล้วจึงนำข้อมูล สถิติและองค์ความรู้ที่ได้จากการทดลองซ้ำๆ มาถอดบทเรียนและสรุปเป็นหลักเกณฑ์และวิธีการใหม่ ที่จะสามารถนำไปสู่การตรวจสอบติดตามเส้นทางการเงินของสกุลเงินเข้ารหัสและการตรวจสอบยืนยันตัวตนของผู้ที่นำสกุลเงินเข้ารหัสไปใช้ในการกระทำความผิดได้อย่างมีประสิทธิภาพ

“ตอนนี้ผมตั้งชุมชนบล็อคเชนขึ้นมาแล้ว และสร้างคริปโทเคอเรนซีจำลองขึ้นมา และจำลองทุกส่วน ส่วนที่เป็นธุรกิจ ส่วนที่เป็นการขุดเหรียญ มีตลาดชุมชนที่ซื้อขายสินทรัพย์ดิจิทัล มีกิจกรรมต่างๆที่ทำแล้วเกิดการแจกจ่ายเหรียญออกไป ให้เกิดการซื้อขายในตลาดชุมชน โดยมีผู้เข้าร่วมชุมชนกว่า 10 คน มีทั้งที่เป็น User (ผู้ใช้งาน) มีทั้งที่เป็น Regulator (ผู้กำกับดูแล) โดยทุกคนที่จะเข้ามาในชุมชนต้องผ่านการ KYC พอเราสร้างให้เกิดความเคลื่อนไหวและมีเส้นทางการเงินเกิดขึ้นในระบบแล้ว เราก็ให้เจ้าหน้าที่สืบสวนเข้าไป Track Transection (ตรวจสอบติดตามเส้นทางธุรกรรมทางการเงิน) เพื่อพยายามพิสูจน์ทราบว่าคนเหล่านี้เป็นใคร เพื่อการเรียนรู้”

(C4, สัมภาษณ์, 9 กรกฎาคม 2563)

ทั้งนี้ผู้ให้ข้อมูลสำคัญยังกล่าวว่าโครงการดังกล่าวยังอยู่ในช่วงระยะเริ่มต้นของการศึกษาทดลอง ซึ่งคาดว่าจะต้องใช้เวลาในการทดลองดังกล่าวประมาณ 1-2 ปีขึ้นไป จึงจะสามารถสรุปเป็นหลักสูตรเกี่ยวกับการวิเคราะห์ธุรกรรมทางการเงินของสกุลเงินเข้ารหัสได้ โดยโครงการดังกล่าวมุ่งที่จะ**นำข้อมูลและองค์ความรู้ต่างๆที่ได้จากการดำเนินโครงการในระยะแรกนี้ให้พัฒนาไปสู่การสร้างเครื่องมือและกลไกสมัยใหม่ ที่จะสามารถทำให้การวิเคราะห์ธุรกรรมทางการเงินเป็นไปอย่างแม่นยำและสะดวกรวดเร็วขึ้น** เช่น การพัฒนาโปรแกรมปัญญาประดิษฐ์ (AI Platform) สำหรับการวิเคราะห์และตรวจจับเส้นทางการเงินของสกุลเงินเข้ารหัสที่มีพิรุธต้องสงสัย หรือ อาจพัฒนาไปถึงการวิเคราะห์ข้อมูลอื่นๆประกอบกันจนสามารถชี้ตัวผู้กระทำผิดที่ปกปิดตัวตนอยู่เบื้องหลังได้ในอนาคต อย่างไรก็ตามผู้ให้ข้อมูลสำคัญยังได้กล่าวว่า โครงการดังกล่าวเป็นการดำเนินการขึ้นเองภายในหน่วยงาน ดังนั้นหากรัฐให้การสนับสนุนให้มีการการศึกษาวิจัยในลักษณะนี้ จะทำให้มีโอกาสที่จะเกิดการพัฒนาหรือค้นพบวิธีการใหม่และอาจนำไปสู่การสร้างเครื่องมือหรือกลไกต่างๆที่สามารถนำไปใช้ในการติดตามตรวจสอบเส้นทางการเงินของสกุลเงินเข้ารหัส และนำไปใช้ในการตรวจพิสูจน์ยืนยันตัวบุคคลของผู้ใช้งานที่แท้จริงได้

นอกจากนี้จากสภาพปัญหาที่เจ้าหน้าที่ที่มีหน้าที่เกี่ยวข้องยังขาดเครื่องมือหรือกลไกพิเศษที่จะช่วยให้สามารถสืบสวนและตรวจสอบติดตามการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดได้ จึงได้มีผู้ให้ข้อมูลสำคัญเสนอแนวทางการแก้ไขปัญหาดังกล่าวว่าในปัจจุบันหน่วยงานต่างๆจะมีข้อมูลสำคัญที่อยู่ในความรับผิดชอบของหน่วยงานแตกต่างกันไปตามอำนาจหน้าที่รับผิดชอบ เช่น สำนักงานตำรวจแห่งชาติมีข้อมูลเกี่ยวกับทะเบียนประวัติอาชญากร

บุคคลเฝ้าระวัง หรือกลุ่มบุคคลที่มีประวัติเกี่ยวข้องกับอาชญากรรม สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) มีข้อมูลสำคัญเกี่ยวกับกลุ่มผู้กระทำความผิดที่มีลักษณะเกี่ยวกับการฟอกเงิน สำนักงานป้องกันและปราบปรามยาเสพติด (ป.ป.ส.) มีข้อมูลเกี่ยวกับกลุ่มขบวนการลักลอบค้ายาเสพติด กรมสอบสวนคดีพิเศษ (ดีเอสไอ) มีข้อมูลของกลุ่มผู้กระทำผิดเกี่ยวกับอาชญากรรมที่มีความรุนแรงที่เกี่ยวกับการฉ้อโกงประชาชน หรือเป็นไปในลักษณะของการเป็นอาชญากรรมเศรษฐกิจ สำนักงานอัยการและสำนักงานศาลยุติธรรมมีประวัติการลงโทษและผลของการดำเนินคดีหรือคำสั่งลงโทษของศาล กรมราชทัณฑ์มีประวัตินักโทษและบุคคลพ้นโทษ ในขณะที่สำนักงานกำกับดูแลหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ก็มีประวัติเกี่ยวกับกลุ่มบุคคลที่ประกอบธุรกิจเกี่ยวสินทรัพย์ดิจิทัลและการลงทุนต่างๆ เป็นต้น

ข้อมูลต่างๆที่กล่าวมานี้ ในปัจจุบันยังไม่ได้มีการแลกเปลี่ยนระหว่างกันอย่างเป็นรูปธรรม ส่งผลให้การป้องกันปราบปรามอาชญากรรมต่างๆ เกิดความบกพร่องจนทำให้ในบางกรณีอาชญากรสามารถหลุดรอดพ้นจากกระบวนการยุติธรรมไปอันเนื่องมาจากการพิจารณาดำเนินการต่างๆภายใต้ข้อมูลที่ไม่ครบถ้วน เช่น กรณีที่เจ้าหน้าที่ตำรวจสายตรวจเรียกตรวจบุคคลเนื่องจากพบว่ามีการใช้ยานพาหนะที่ไม่ติดแผ่นป้ายทะเบียน โดยที่ผู้ขับขี่รายนั้นแท้จริงแล้วเป็นผู้ค้ายาเสพติดรายใหญ่ แต่เนื่องจากเจ้าหน้าที่ตำรวจสายตรวจไม่มีข้อมูลหรือไม่สามารถเข้าถึงข้อมูลบุคคลที่เกี่ยวข้องกับขบวนการลักลอบค้ายาเสพติดได้ เมื่อตรวจค้นแล้วไม่พบสิ่งผิดกฎหมายจึงปล่อยตัวไป ซึ่งทำให้เสียโอกาสในการป้องกันปราบปรามอาชญากรรมไป หรือกรณีที่อาจเกิดขึ้นซึ่งมีความเกี่ยวข้องกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส เช่น เจ้าหน้าที่ของสำนักงานกำกับดูแลหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) อาจพิจารณาออกใบอนุญาตให้ผู้ประกอบการรายหนึ่งดำเนินธุรกิจเกี่ยวกับการเป็นตัวกลางในการซื้อขายแลกเปลี่ยนสินทรัพย์ดิจิทัล โดยที่ไม่ทราบข้อมูลว่าผู้ประกอบการรายนั้นมีความเกี่ยวข้องกับการกระผิดเกี่ยวกับอาชญากรรมเศรษฐกิจที่กรมสอบสวนคดีพิเศษติดตามสืบสวนอยู่ เป็นต้น

ดังนั้น ผู้ให้ข้อมูลสำคัญจึงเสนอให้มีการแลกเปลี่ยนข้อมูลซึ่งกันและกันระหว่างหน่วยงานเพื่อเป็นการลดปัญหาความบกพร่องของกระบวนการยุติธรรมและกระบวนการป้องกันปราบปรามอาชญากรรมต่างๆ โดยลักษณะของการแลกเปลี่ยนข้อมูลระหว่างกันนั้น เพื่อให้เกิดการจัดระเบียบและสามารถควบคุมความปลอดภัยให้กับข้อมูลดังกล่าวซึ่งเกี่ยวเนื่องกับข้อมูลส่วนบุคคลของประชาชนนั้น ควรจะต้องกระทำในรูปแบบของของ**การสร้างฐานข้อมูลภาครัฐที่เกี่ยวกับการ**

ป้องกันอาชญากรรม ซึ่งเป็นฐานข้อมูลขนาดใหญ่ (Big Data) ที่เก็บรวบรวมข้อมูลสำคัญที่สามารถนำไปวิเคราะห์และประเมินความเสี่ยงของบุคคลที่เกี่ยวข้องหรืออาจเกี่ยวข้องกับการก่ออาชญากรรมประเภทต่างๆ รวมทั้งอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้ ทั้งนี้ ในการจัดเก็บข้อมูลดังกล่าวจำเป็นจะต้องออกแบบระบบการรักษาความปลอดภัย ให้มีชั้นความลับและ**กำหนดสิทธิ์ให้ผู้เข้าถึงกลุ่มต่างๆเฉพาะกรณีที่เป็นประโยชน์ต่อรัฐเช่นการป้องกันปราบปรามอาชญากรรมเท่านั้น** โดยจะต้องมีระบบการตรวจสอบการเข้าถึงข้อมูลดังกล่าวอย่างเป็นรูปธรรมและต้องมีการกำหนดบทลงโทษกรณีที่มีการนำข้อมูลส่วนบุคคลของประชาชนไปใช้ในทางมิชอบ โดยแนวทางเกี่ยวกับการสร้างฐานข้อมูลดังกล่าวนี้จะทำให้รัฐมีเครื่องมือชนิดใหม่ที่ส่งผลให้เกิดการเพิ่มประสิทธิภาพในการบังคับใช้กฎหมายและการป้องกันอาชญากรรมต่างๆ ไม่เฉพาะกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสแต่ยังสามารถป้องกันอาชญากรรมสมัยใหม่ต่างๆที่จะเกิดขึ้นในอนาคตได้อีกมาก

“ตัวหน่วยงานแต่ละหน่วยงานจะต้องมีการแลกเปลี่ยนข้อมูลซึ่งกันและกัน จนอาจสร้างเป็นฐานข้อมูลขนาดใหญ่ ที่รวบรวมข้อมูลที่เกี่ยวข้องกับอาชญากรรมทั้งหมดไว้ และจะต้องออกแบบระบบให้สามารถแจ้งเตือนหน่วยงานที่เกี่ยวข้อง กรณีพบการกระทำที่เข้าข่ายความผิด เพื่อให้เกิดการเฝ้าระวังอย่างทันท่วงที”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

“ถ้าทำเป็นฐานข้อมูลภาครัฐแบบ Big Data หรือ Center Data ได้จะเป็นประโยชน์มาก เพราะข้อมูลต่างๆในปัจจุบันมันกระจัดกระจาย แต่ละหน่วยเห็นเฉพาะเสี้ยวของตนเอง ซึ่งคงไม่ทันการกับโลกยุคปัจจุบัน แต่ขณะเดียวกันต้องสร้างกลไกที่ปลอดภัย ต้องระบุผู้เกี่ยวข้องและการอนุมัติสิทธิการเข้าถึงให้ชัดเจน เพราะเป็นเรื่องของข้อมูลที่ละเอียดอ่อน รัฐต้องควบคุมการนำข้อมูลไปใช้ ถ้าทำได้จะเป็นประโยชน์ต่อภาครัฐอย่างมาก”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

อย่างไรก็ตามประเด็นข้อควรระวังเกี่ยวกับการดำเนินการตามแนวทางของการสร้างฐานข้อมูลภาครัฐขนาดใหญ่ที่ จำเป็นจะต้องมีการออกแบบระบบการทำงานที่มีความปลอดภัยสูง เพราะข้อมูลดังกล่าวเกี่ยวข้องกับความปลอดภัยของข้อมูลซึ่งถือเป็นข้อมูลส่วนบุคคล (Data Privacy)

ที่ได้มีผู้ให้ข้อมูลสำคัญกล่าวถึงนั้น ผู้วิจัยได้พิจารณาจากกฎหมายที่เกี่ยวข้องคือ พ.ร.บ.คุ้มครองข้อมูลส่วนบุคคล พ.ศ. 2562 ที่มีการวางหลักการสำคัญเกี่ยวกับการคุ้มครองข้อมูลส่วนบุคคลของประชาชน โดยมีหลักการสำคัญคือ

1) ข้อมูลส่วนบุคคล หมายถึง ข้อมูลที่เกี่ยวข้องกับบุคคลหรือข้อมูลที่สามารถระบุถึงตัวตนของบุคคลได้ เช่น ชื่อ นามสกุล เลขประจำตัวประชาชน เบอร์โทรศัพท์ ภาพถ่าย เป็นต้น

2) การที่ผู้ใดผู้หนึ่งจะทำการเก็บข้อมูลส่วนบุคคลของบุคคลใดจะต้องได้รับความยินยอมจากเจ้าของข้อมูล และการเก็บข้อมูลดังกล่าวจะต้องมีความปลอดภัยและไม่เกิดการรั่วไหล

3) ข้อมูลที่ผู้เก็บข้อมูลเก็บรักษาไว้จะต้องถูกตรวจสอบได้อย่างชัดแจ้งว่า ได้มาอย่างไร ถูกต้องตามหลักเกณฑ์ที่กฎหมายกำหนดหรือไม่ อย่างไร

โดยหากวิเคราะห์ตามหลักการของกฎหมายแล้วจะพบว่า กฎหมายดังกล่าวมุ่งที่จะคุ้มครองไม่ให้มีการนำข้อมูลส่วนบุคคของประชาชนไปใช้ในทางมิชอบ อย่างไรก็ตามในกฎหมายดังกล่าวได้มีบทบัญญัติซึ่งเป็นข้อยกเว้นให้ทำการเก็บและเข้าถึงข้อมูลส่วนบุคคลได้ในกรณีที่เอื้อประโยชน์ต่อสังคมโดยรวมดังที่บัญญัติในมาตรา 24 ว่า

“ห้ามมิให้ผู้ควบคุมข้อมูลส่วนบุคคลทำการเก็บรวบรวมข้อมูลส่วนบุคคลโดยไม่ได้รับความยินยอมจากเจ้าของข้อมูลส่วนบุคคล เว้นแต่...

(4) เป็นการจำเป็นเพื่อการปฏิบัติหน้าที่ในการดำเนินภารกิจเพื่อประโยชน์สาธารณะของผู้ควบคุมข้อมูลส่วนบุคคล หรือปฏิบัติหน้าที่ในการใช้อำนาจรัฐที่ได้มอบให้แก่ผู้ควบคุมข้อมูลส่วนบุคคล”

จากบทบัญญัติของกฎหมายดังนี้ ทำให้วิเคราะห์ได้ว่า หากเป็นการกระทำเพื่อประโยชน์ของรัฐ โดยเฉพาะอย่างยิ่งประโยชน์ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสจะมีลักษณะเข้าข้อยกเว้นตามบทบัญญัติดังกล่าว ทั้งนี้เพื่อให้การดำเนินการตามแนวทางการสร้างฐานข้อมูลเพื่อป้องกันอาชญากรรมนี้ สามารถดำเนินไปได้อย่างเป็นรูปธรรมอาจมีความจำเป็นจะต้องมีการออกกฎหมายควบคุม หรือการกำหนดข้อยกเว้นตามกฎหมายดังกล่าว รวมทั้งกฎหมายอื่นๆที่เกี่ยวข้องด้วย

ผลจากการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญในประเด็นด้านการส่งเสริมให้มีการศึกษาวิจัยเพื่อค้นหาวิธีการ เครื่องมือหรือกลไกการป้องกันอาชญากรรมรูปแบบใหม่ ที่สามารถป้องกัน

อาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพนี้ สรุปได้ว่าผู้ให้ข้อมูลสำคัญได้แนวทางสำคัญ 2 ประการที่จะช่วยเพิ่มศักยภาพให้กับการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส คือ

1) ทำการศึกษาวิจัยระบบการทำงานของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ตลอดจนร่วมกันทดลองหรือทดสอบวิธีการด้วยเครื่องมือหรือกลไกต่างๆ โดยผู้ให้ข้อมูลสำคัญได้ยกตัวอย่างกรณีการศึกษาระบบการทำงานของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆด้วยการสร้างชุมชนบล็อคเชนของสำนักงานป้องกันและปราบปรามการฟอกเงิน เพื่อเป็นการจำลองสถานการณ์การใช้งานสกุลเงินเข้ารหัสขึ้นมาเพื่อให้สามารถนำข้อมูลและองค์ความรู้ต่างๆที่ได้จากการดำเนินโครงการนี้ให้พัฒนาไปสู่การสร้างเครื่องมือและกลไกสมัยใหม่ ที่จะสามารถทำให้การวิเคราะห์ธุรกรรมทางการเงินเป็นไปอย่างแม่นยำและสะดวกรวดเร็วขึ้น ซึ่งข้อเสนอและตัวอย่างการดำเนินการตามโครงการนี้มีความสอดคล้องกับงานวิจัยของ **Sean Foley, Jonathan R. Karlsen and Talis J. Putnins (2018)** ซึ่งได้มีการศึกษาและนำเอาเทคโนโลยีทางคอมพิวเตอร์มาใช้ในการเก็บและสังเกตข้อมูลการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ และวิเคราะห์พฤติกรรมของผู้ใช้งานที่มีความเสี่ยงจะนำบิทคอยน์ไปใช้ในการกระทำความผิด ตลอดจนวิเคราะห์ ค้นหา และเปรียบเทียบข้อมูลการใช้งานโปรแกรมต่างๆ โดยเฉพาะโปรแกรมในโลกออนไลน์ (Social Media) เพื่อวิเคราะห์และค้นหาตัวผู้ใช้งานที่แท้จริง จากข้อมูลที่มีอยู่บนเครือข่ายคอมพิวเตอร์หรืออินเทอรเน็ต ดังนั้นผู้วิจัยจึงมีความเห็นว่า หากมีการศึกษาวิจัยและค้นคว้าด้วยการใช้ศาสตร์ในทางเทคโนโลยีคอมพิวเตอร์ร่วมกันกับกระบวนการยุติธรรมอย่างจริงจัง จะทำให้ประเทศไทยสามารถค้นพบวิธีการหรือเครื่องมือพิเศษต่างๆที่จะสามารถใช้ในการสืบสวนติดตามผู้กระทำความผิดที่นำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้เป็นเครื่องมือได้อย่างมีประสิทธิภาพ

2) การสร้างฐานข้อมูลภาครัฐที่เกี่ยวกับการป้องกันอาชญากรรม เป็นอีกแนวทางหนึ่งซึ่งผู้ให้ข้อมูลสำคัญได้เสนอขึ้นจากแนวคิดที่จำเป็นจะต้องนำข้อมูลสำคัญต่างๆที่อยู่ภายใต้ความดูแลของหน่วยงานภาครัฐแต่ละหน่วยงาน นำมาบูรณาการร่วมกันเป็นฐานข้อมูลภาครัฐขนาดใหญ่ เพื่อนำมาใช้ในการเป็นฐานข้อมูลสำคัญในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส รวมทั้งสามารถขยายผลให้สามารถใช้ในการป้องกันและปราบปรามอาชญากรรมได้ในทุกประเภท ซึ่งเมื่อพิจารณาข้อเสนอแนะจากผู้ให้ข้อมูลสำคัญกับข้อเท็จจริงที่ผู้วิจัยพบว่าข้อเท็จจริงที่พบจากการทบทวนวรรณกรรมและจากประสบการณ์การทำงานในกระบวนการยุติธรรมของตัวผู้วิจัยเองจะพบว่ามีความสอดคล้องกันในแนวคิดดังกล่าว เนื่องจากหน่วยงานภาครัฐต่างๆจะมีการเก็บข้อมูลสำคัญ

แตกต่างกันไปตามอำนาจหน้าที่รับผิดชอบของหน่วยงานนั้นๆ แต่ในปัจจุบันยังไม่มีการนำข้อมูลดังกล่าวมาใช้ร่วมกันหรือยังไม่มีการนำข้อมูลดังกล่าวมาใช้เพื่อประโยชน์ในภาพรวมของประเทศในเรื่องการป้องกันอาชญากรรมเท่าที่ควร ดังนั้น การสร้างฐานข้อมูลภาครัฐที่เกี่ยวกับการป้องกันอาชญากรรม จึงเป็นแนวทางสำคัญที่จะสามารถยกระดับการป้องกันอาชญากรรมทุกประเภท โดยเฉพาะอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้เป็นอย่างดี อย่างไรก็ตามการสร้างฐานข้อมูลดังกล่าวก็จำเป็นจะต้องจัดระบบการเก็บรักษาและการกำหนดชั้นความลับและผู้มีสิทธิ์เข้าถึงให้มีความปลอดภัยสูงสุด และรัฐจะต้องกำหนดมาตรการป้องกันเพื่อให้มีการนำข้อมูลดังกล่าวไปใช้เพื่อประโยชน์ในการป้องกันอาชญากรรมหรือประโยชน์ส่วนรวมของประเทศเท่านั้น

4.4.5 การสร้างความร่วมมือระหว่างหน่วยงานทั้งภาครัฐและภาคเอกชนในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

จากประเด็นปัญหาเรื่องการขาดการประสานงานหรือการบูรณาการในการทำงานร่วมกันระหว่างหน่วยงานภาครัฐรวมทั้งภาคเอกชนที่เกี่ยวข้องตามที่ได้กล่าวมาแล้วนั้น ได้มีผู้ให้ข้อมูลสำคัญเสนอแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ในประเด็นเรื่องความจำเป็นที่จะต้องมีการบูรณาการร่วมกันของหน่วยงานภาครัฐที่เกี่ยวข้อง โดยเกิดจากแนวคิดที่สำคัญที่ว่าหน่วยงานราชการแต่ละหน่วยจะมีความชำนาญหรือความเชี่ยวชาญเฉพาะด้านแตกต่างกันไปตามแต่หน้าที่รับผิดชอบของหน่วยนั้นๆ เช่น หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องอย่าง กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.) ก็จะมีความรู้ ความชำนาญในประเด็นที่เกี่ยวกับการเก็บพยานหลักฐานทางดิจิทัล แต่ก็ไม่มีความเชี่ยวชาญเกี่ยวกับงานด้านอื่นๆ เช่น หากมีกรณีของประเด็นปัญหาที่เกี่ยวเนื่องกับเรื่องภาษี ก็จำเป็นจะต้องอาศัยหน่วยงานที่เชี่ยวชาญเรื่องอาชญากรรมเศรษฐกิจอย่าง กองบังคับการปราบปรามการกระทำความผิดที่เกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.) ซึ่งมีความรู้ความชำนาญในเรื่องภาษีมากกว่าเข้ามาพิจารณา หรือในกรณีที่มีประเด็นปัญหาที่เกี่ยวกับการฟอกเงิน ก็จำเป็นจะต้องอาศัยความเชี่ยวชาญของหน่วยงานเฉพาะด้านอย่าง สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) เข้ามาดำเนินการเป็นต้น

จากแนวคิดดังกล่าวจะเห็นได้ว่าการมอบหมายให้หน่วยงานใดเพียงหน่วยงานเดียวรับผิดชอบการป้องกันอาชญากรรมสมัยใหม่ที่มีความซับซ้อนอย่างอาชญากรรมที่เกี่ยวกับสกุลเงิน

เข้ารหัส จะทำให้การดำเนินการไม่ครอบคลุมและจะส่งผลทำให้การป้องกันอาชญากรรมไม่เกิดประสิทธิภาพเท่าที่ควร ดังนั้นจึงจำเป็นอย่างยิ่งที่จะต้องมีการบูรณาการการทำงานร่วมกันระหว่างหน่วยงานภาครัฐ โดยรูปแบบของสร้างความร่วมมือระหว่างหน่วยงานภาครัฐนี้ ได้มีผู้ให้ข้อมูลสำคัญเสนอแนะไปในแนวทางต่างๆกัน ทั้งรูปแบบของการตั้งเป็น**คณะทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง** โดยมีลักษณะเป็นคณะทำงานเฉพาะกิจ กรณีเมื่อเกิดคดีสำคัญที่จำเป็นจะต้องอาศัยทักษะและความชำนาญเฉพาะด้านจากหลากหลายหน่วยงานมาดำเนินการร่วมกัน ไปจนถึงการนำบุคลากรของแต่ละหน่วยงานมาจัดตั้งเป็น **“ศูนย์ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสแห่งชาติ”** ที่มีลักษณะของการปฏิบัติหน้าที่ประจำเพื่อกำกับดูแลและแก้ไขปัญหาอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอย่างเป็นรูปธรรมและครบวงจร

“ต้องตั้งเป็นคณะทำงานเพราะหน่วยเราไม่ได้เป็นผู้เชี่ยวชาญโดยตรง เจ้าหน้าที่อาจจะไม่สันทัดเรื่องนี้เท่าใดนัก ก็จะต้องประสานหน่วยงานที่เกี่ยวข้องมาร่วมทำงาน ต้องบูรณาการคนที่ถนัดในด้านต่างๆ เพราะความรู้ความถนัดแต่ละคนมันไม่ครอบคลุม ต้องอาศัยผู้เชี่ยวชาญหลายด้าน หรืออาจตั้งเป็นศูนย์ป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับพวกนี้ (บิทคอยน์และสกุลเงินเข้ารหัส) ให้เป็นรูปธรรมไปเลย ”

(C1, สัมภาษณ์, 7 กุมภาพันธ์ 2563)

“เมื่อยังไม่มีหน่วยงานไหนรับผิดชอบโดยตรง เพราะเป็นเรื่องใหม่ ก็จำเป็นต้องอาศัยความร่วมมือกันของทุกหน่วยงานที่เกี่ยวข้อง ไม่ใช่แค่ตำรวจ ทหาร ดีเอสไอ (กรมสอบสวนคดีพิเศษ)เท่านั้น แต่ต้องไปถึงระดับกระทรวงดิจิทัลฯ ที่จะต้องเข้ามาช่วยสนับสนุนในฐานะผู้เชี่ยวชาญ หน่วยปฏิบัติอาจจะไม่จำเป็นต้องเชี่ยวชาญ แต่ต้องสามารถที่จะสื่อสารกับผู้เชี่ยวชาญได้ว่า ต้องการพยานหลักฐานอะไร”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

นอกจากนี้ผู้ให้ข้อมูลสำคัญยังเสนอแนะแนวทางที่จำเป็นอีกประการหนึ่งคือ**การสร้างความร่วมมือระหว่างภาครัฐและภาคเอกชนโดยเฉพาะกลุ่มผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล**ซึ่งถือเป็นภาคเอกชนที่ภาครัฐจำเป็นจะต้องดำเนินการให้เกิดการบูรณาการและการทำงานร่วมกันอย่างใกล้ชิด เนื่องด้วยสาเหตุสำคัญสองประการคือ **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่ทำหน้าที่เป็น**

ตัวกลางหรือผู้ให้บริการนั้นจะมีข้อมูลของลูกค้าตามมาตรการบังคับของกฎหมายซึ่งข้อมูลดังกล่าวนี้จะเป็นประโยชน์ต่อภาครัฐในเรื่องที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมไม่มากก็น้อย และความสำคัญอีกประการหนึ่งคือ **ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลนั้นถือเป็นผู้เชี่ยวชาญที่มีองค์ความรู้หรือมีความเข้าใจในเรื่องที่เกี่ยวกับสกุลเงินเข้ารหัสในเชิงลึก**และมีประสบการณ์เกี่ยวกับการสกุลเงินเข้ารหัสไปใช้งานในรูปแบบต่างๆ ดังนั้นหน่วยงานภาครัฐจึงจำเป็นอย่างยิ่งที่จะต้องอาศัยความเชี่ยวชาญของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลมาช่วยในการสืบสวนสอบสวนหรือการตรวจสอบติดตามเส้นทางธุรกรรมทางการเงินรวมทั้งการพิสูจน์ยืนยันตัวตนผู้กระทำความผิดด้วย โดยรูปแบบการให้ความร่วมมือหรือการบูรณาการการทำงานร่วมกันนั้นอาจอยู่ในรูปแบบของการให้ความร่วมมือทางด้านข้อมูล การเป็นพยานบุคคลในฐานะพยานผู้เชี่ยวชาญ หรือการให้ความเห็นหรือคำแนะนำในกระบวนการสืบสวน เป็นต้น

“ผมว่ากลุ่มผู้ประกอบการที่เป็นตัวกลาง หรือ Service Provider นี่สำคัญมากๆนะครับ เพราะกลุ่มบุคคลเหล่านี้มีข้อมูลเกี่ยวกับผู้ใช้งาน ซึ่งข้อมูลเหล่านี้จะเป็นประโยชน์อย่างมากในทางการสืบสวนหรือแกะรอยต่างๆ”

(A4, สัมภาษณ์, 10 กรกฎาคม 2563)

“ภาครัฐของเรายังขาดบุคลากรที่เชี่ยวชาญตรงด้านนี้ แต่อันนึงที่ผมว่าทำได้คือ กลุ่มบริษัทธุรกิจเหล่านี้ 5-6 บริษัท ต้องดึงธุรกิจเหล่านี้เข้ามาร่วม ผมว่าเขายินดีที่จะเข้ามา มาหากลไกร่วมกันถ้าเกิดเคสอะไรขึ้น เพราะคนเหล่านี้เก่ง ถ้าสามารถทำงานด้วยกันได้จะไปได้เร็ว”

(C4, สัมภาษณ์, 9 กรกฎาคม 2563)

จากข้อมูลข้างต้นสามารถสรุปได้ว่าผู้ให้ข้อมูลสำคัญได้เสนอถึงแนวทางในการสร้างความร่วมมือระหว่างหน่วยงานทั้งภาครัฐและภาคเอกชนในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ซึ่งประกอบด้วยการตั้งเป็น**คณะทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง** โดยมีลักษณะเป็นคณะทำงานเฉพาะกิจ หรือดำเนินการจัดตั้งเป็น **“ศูนย์ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสแห่งชาติ”** ที่เป็นหน่วยงานเฉพาะที่มีการระดมสรรพกำลังและเจ้าหน้าที่ของรัฐที่มีความรู้ ความเชี่ยวชาญเกี่ยวข้องมาปฏิบัติหน้าที่อยู่ในคณะทำงานหรือศูนย์ดังกล่าว รวมทั้ง

ผู้ให้ข้อมูลสำคัญยังเสนอแนะให้มี**การสร้างความร่วมมือระหว่างภาครัฐและภาคเอกชนโดยเฉพาะกลุ่มผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล** เนื่องจากภาครัฐจำเป็นจะต้องอาศัยความร่วมมือจากภาคเอกชนที่เป็นผู้เชี่ยวชาญและอยู่ในวงธุรกิจที่เกี่ยวกับสกุลเงินเข้ารหัส ซึ่งสามารถอาศัยความร่วมมือได้ในรูปแบบต่างๆ เช่น การให้ความร่วมมือทางด้านข้อมูลสำคัญ เบาะแสการกระทำความผิด หรือแม้กระทั่งการเป็นเข้าเป็ฯพยานผู้เชี่ยวชาญในการพิจารณาคดีตามที่ได้กล่าวมาแล้ว โดยแนวคิดทั้งสองประเด็นดังกล่าวจากผู้ให้ข้อมูลสำคัญสอดคล้องกันกับงานวิจัยของ **จุฑารัตน์ ชวดนุช (2557)** ที่กล่าวถึงข้อเสนอแนะที่เป็นไปในแนวทางเดียวกันว่า หน่วยงานที่เกี่ยวข้องจะต้องให้การสนับสนุนและให้ความร่วมมือในการให้ข้อมูลที่เป็นประโยชน์ในการตรวจสอบบุคคลหรือเส้นทางการเงินที่อาจเกี่ยวข้องกับการกระทำความผิดหากได้รับการร้องขอจากหน่วยงานของรัฐด้วยกัน ทั้งยังควรกำหนดให้มีการสร้างเครือข่ายต่างๆเพื่อเฝ้าระวังอีกด้วย ทั้งนี้ในมุมมองของตัวผู้วิจัยเองก็มีความเห็นที่สอดคล้องตรงกันกับผลการศึกษาดังกล่าว โดยหากต้องการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ก็จำเป็นอย่างยิ่งที่จะต้องสร้างความร่วมมือให้เกิดขึ้นตามที่ได้กล่าวมานี้

4.4.6 การสร้างความร่วมมือกับหน่วยงานในต่างประเทศที่เกี่ยวข้องอย่างเป็นรูปธรรม

จากที่ผู้ให้ข้อมูลสำคัญได้ชี้ให้เห็นถึงสภาพปัญหาและลักษณะของการกระทำความผิดที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆว่า เนื่องด้วยลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์และมีการทำงานบนระบบคอมพิวเตอร์ ทำให้การใช้งานในการกระทำความผิดนั้น สามารถกระทำได้จากทุกหนแห่งทั่วโลก และไม่อยู่ภายใต้ขอบเขตของเขตแดนระหว่างรัฐในทางกายภาพอีกต่อไป ในขณะที่การดำเนินการของหน่วยงานกระบวนการยุติธรรมทั่วโลกยังถูกกำหนดอำนาจหน้าที่ตามเขตแดนของรัฐ ซึ่งทำให้การดำเนินการในการป้องกันปราบปรามและสืบสวนจับกุมผู้กระทำผิดมีข้อจำกัดในเรื่องเขตอำนาจรับผิดชอบ แม้จะมีการจัดตั้งหน่วยงานเฉพาะที่มีอำนาจหน้าที่ที่สามารถดำเนินการระหว่างประเทศได้ แต่ในทางปฏิบัติจริงก็มีข้อจำกัดต่างๆ เช่น ความล่าช้าในการติดต่อประสานงานซึ่งอาจทำให้การส่งต่อหรือรับข้อมูลสำคัญที่จะนำมาใช้ในการติดตามตรวจสอบ สืบสวนหาตัวผู้กระทำผิดหรือนำมาใช้ประกอบการพิจารณาคดีถูกลบ ทำลาย หรือทำให้เสียหาย หรือไม่สามารถนำมาใช้ในกระบวนการป้องกันปราบปรามอาชญากรรมอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างทันท่วงที

เพื่อแก้ไขปัญหาดังกล่าวผู้ให้ข้อมูลสำคัญจึงได้เสนอแนะว่า **ประเทศไทยควรมีการสร้างความร่วมมือกับหน่วยงานในต่างประเทศในรูปแบบต่างๆ** เช่น การทำข้อตกลงความร่วมมือร่วมกัน (MOU) ในเรื่องของการตกลงแลกเปลี่ยนข้อมูลสำคัญระหว่างกันในกรณีที่จำเป็นที่จะต้องใช้ข้อมูลต่างๆที่คนร้ายทิ้งร่องรอย หรือกระทำความผิดจากในต่างประเทศมาใช้ประกอบการพิจารณาคดี หรือประกอบการสืบสวนเพื่อหาตัวผู้ร่วมกระทำความผิดทั้งในและนอกประเทศ เป็นต้น ซึ่งความร่วมมือในลักษณะนี้ถือเป็นปัจจัยสำคัญที่จะส่งผลต่อการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส รวมทั้งอาชญากรรมสมัยใหม่ที่เกิดขึ้นในสังคมเสมือนหรือบนระบบเครือข่ายคอมพิวเตอร์เป็นอย่างมาก เพราะหากขาดความร่วมมือระหว่างประเทศในลักษณะดังกล่าว จะทำให้พยานหลักฐานต่างๆซึ่งอยู่ในรูปแบบของข้อมูลดิจิทัลถูกลบล้างและทำลายไปก่อนที่เจ้าหน้าที่จะเข้าถึงได้ ทั้งนี้ผู้ให้ข้อมูลสำคัญยังได้เน้นว่า**การประสานความร่วมมือดังกล่าวจะต้องมีการปฏิบัติให้ได้ผลจริง ไม่เพียงแต่เป็นการสร้างความร่วมมือแต่เพียงในหลักการ** เช่น จะต้องมีการระบุตัวตนผู้ประสานงานหลัก (Contact Person) ซึ่งเป็นบุคคลหรือตำแหน่งประจำขึ้น เพื่อให้เกิดการมอบหมายหน้าที่ที่ชัดเจนในการประสานงานและเพื่อประโยชน์ในด้านความรวดเร็วในการติดต่อสื่อสาร

“เราจำเป็นต้องมีคอนเนคชั่นกับต่างประเทศ โดยเฉพาะการขอข้อมูลจำเป็นต่างๆ ถ้าเป็นการดำเนินการตามปกติต้องยอมรับว่าช้ามาก เพราะฉะนั้นสำคัญที่สุดเลยคือต้องสร้างความร่วมมือ ต้องมีการทำ MOU เพื่อตกลงกัน และต้องชัดเจน จริงจัง และรวดเร็ว และต้องมีการกำหนดตัว Contact point แต่ละหน่วยงานให้ชัดเจน เพื่อไม่ให้เกิดความสับสน”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

“เรื่องของกลไกภาครัฐในเรื่องของข้อมูลสำคัญมาก ไม่ใช่เฉพาะในประเทศซึ่งแค่ในประเทศก็ยากอยู่แล้วในการประสานงานกัน แต่พวกนี้มันข้ามประเทศ ข้ามเขตแดน ดังนั้นต้องพยายามเชื่อมต่อข้อมูลกับต่างประเทศให้ได้”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

จากข้อเสนอแนะต่างๆที่ผู้ให้ข้อมูลสำคัญได้กล่าวมานี้ สามารถสรุปได้ว่าประเทศไทยควรมีการสร้างความร่วมมือกับหน่วยงานในต่างประเทศในรูปแบบต่างๆ โดยในการดำเนินการนั้นจะต้อง

ให้ได้ผลจริง และไม่เพียงแต่เป็นการสร้างความร่วมมือแต่เพียงหลักการเท่านั้น ซึ่งในกรณีของแนวทางการแก้ปัญหานี้ ผู้วิจัยมีความเห็นและข้อเสนอแนะที่สอดคล้องกัน เพื่อให้การประสานงานระหว่างประเทศในเรื่องที่เกี่ยวกับการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ดังนี้

1) ควรมีการทำข้อตกลงระหว่างประเทศ เพื่อกำหนดตัวแทนบุคคลของหน่วยงานที่เกี่ยวข้องของแต่ละประเทศ และกำหนดวิธีการพิเศษที่ตัวแทนดังกล่าวจะสามารถติดต่อสื่อสารกันได้ด้วยความรวดเร็ว ไม่ผ่านพิธีการทางการฑูตหรือธรรมเนียมการปฏิบัติระหว่างประเทศ เพื่อให้สามารถระงับยับยั้งความเสียหาย หรือ เพื่อให้เท่าทันต่อการทำลายพยานหลักฐานที่เกี่ยวกับการกระทำความผิดเกี่ยวกับสกุลเงินเข้ารหัส

2) กำหนดขอบเขตและกรอบความร่วมมือที่ชัดเจน เพื่อให้แต่ละชาติสามารถประเมินขีดความสามารถในการขอความร่วมมือได้อย่างถูกต้อง และลดระยะเวลาในการดำเนินการประสานงาน เช่น

4.4.7 การสร้างสกุลเงินเข้ารหัสหรือสกุลเงินดิจิทัลแห่งชาติ

ได้มีผู้ให้ข้อมูลสำคัญ เสนอแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสด้วยการผลักดันให้ประเทศไทยควรมีการสร้างสกุลเงินเข้ารหัสของชาติขึ้น สาเหตุเพราะแนวคิดของการสร้างบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเกิดจากเจตนารมย์ที่ต้องการจะเป็นเอกเทศจากการควบคุมของรัฐ เห็นได้จากการแสดงออกที่ชัดเจนด้วยการออกแบบระบบการทำงานให้เป็นแบบการกระจายข้อมูล (Decentralization) ที่ไม่มีการควบคุมด้วยตัวกลางอย่างธนาคารหรือสถาบันการเงินใดๆ ดังนั้นการพยายามที่จะควบคุมกำกับดูแลบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ด้วยการกำหนดมาตรการต่างๆของรัฐจึงอาจไม่ได้ผลเท่าที่ควร แต่หากรัฐมีการสร้างสกุลเงินเข้ารหัสแห่งชาติขึ้นจะทำให้ประชาชนมีตัวเลือกที่จะเข้าสู่การเป็นสังคมไร้เงินสดที่ได้รับการรับรองโดยรัฐ และหากมีการออกแบบระบบการรักษาความปลอดภัยที่มั่นคง จนสามารถทำให้เกิดการยอมรับและมีการใช้งานได้อย่างแพร่หลายแล้ว ก็มีความเป็นไปได้ว่าจะส่งผลให้คนในประเทศหันมาใช้งานสกุลเงินเข้ารหัสแห่งชาติ มากกว่าบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ ทั้งยังอาจส่งผลต่อเนื่องให้ในกรณีที่จะเกิดการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ก่ออาชญากรรมลดลงอีกด้วย

ซึ่งข้อเสนอในการดำเนินการตามแนวทางนี้ ได้มีผู้ให้ข้อมูลสำคัญกล่าวถึงข้อเท็จจริงที่เกี่ยวข้องเกี่ยวกับสร้างสกุลเงินดิจิทัลของธนาคารแห่งประเทศไทย (Central Bank Digital Currency หรือ CBDC) **ว่าธนาคารแห่งประเทศไทยได้ทำการศึกษาและพัฒนาสกุลเงินดิจิทัล ชื่อ “อิน**

ทนนท์" มาตั้งแต่ปี พ.ศ. 2561 สกุลเงินดิจิทัลตัวนี้จะมีลักษณะและระบบการทำงานเบื้องหลังที่คล้ายกันกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ แต่แตกต่างกันตรงที่มีการรับรองมูลค่าโดยธนาคารแห่งประเทศไทยและยึดโยงมูลค่ากับเงินบาทไทย แนวคิดระยะแรกของการพัฒนานั้นมีเจตนาที่จะนำไปทดลองใช้ในลักษณะของการเป็นสื่อกลางในการแลกเปลี่ยนระดับธนาคารพาณิชย์ที่อาจจะยังถือได้ว่าสกุลเงินดิจิทัลดังกล่าวยังยึดโยงหรือถูกผูดขาดกับสถาบันทางการเงิน ต่อมาผู้พัฒนาได้เล็งเห็นถึงประโยน์สำคัญที่อาจนำไปใช้ทำให้เกิดการขยายตัวของภาคเศรษฐกิจอันเกิดจากความคล่องตัวของสกุลเงินดิจิทัล จึงมีแนวคิดที่จะมีการเปิดกว้างให้ภาคธุรกิจนำสกุลเงินดิจิทัลนี้ ไปใช้เป็นสื่อกลางแลกเปลี่ยนระหว่างกันเพื่อความคล่องตัวในทางธุรกิจต่อไป ทั้งนี้โครงการดังกล่าวยังอยู่ระหว่างการศึกษาพัฒนาและยังไม่มีข้อยุติว่าจะมีการสร้างและพัฒนาสกุลเงินดิจิทัลนี้จนสามารถนำออกมาใช้เป็นสื่อกลางในการชำระเงินในชีวิตประจำวันของประชาชนหรือไม่ เนื่องจากยังจะต้องทำการศึกษาถึงข้อมูลที่เกี่ยวข้องอีกเป็นจำนวนมาก เช่น จำเป็นจะต้องพิจารณาถึงความพร้อมของประชาชนว่ามีความสามารถในการเข้าถึงมากน้อยเพียงใด ในขณะเดียวกันก็จะต้องพิจารณาถึงประโยชน์อันอาจจะได้รับจากการที่ภาคธุรกิจนำสกุลเงินดิจิทัลนี้ไปพัฒนาและสร้างมูลค่าทางเศรษฐกิจได้มากกว่าเดิมโดยไม่ต้องพึ่งพิงตัวกลางอย่างสถาบันการเงินต่างๆประกอบกัน

ส่วนในประเด็นที่เกี่ยวข้องว่า การสร้างสกุลเงินดิจิทัลของชาติอย่างในกรณีของ "อินทนนท์" ของประเทศไทยนั้น จะมีผลต่อการป้องกันหรือลดการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมได้มากน้อยเพียงใดนั้น ผู้ให้ข้อมูลสำคัญเห็นว่าขึ้นอยู่กับ**แนวนโยบายหรือทิศทางในการออกแบบสกุลเงินดิจิทัลแห่งชาติ** โดยยกตัวอย่างกรณีใกล้เคียงกันในประเทศจีนที่มีการสร้างสกุลเงินดิจิทัลแห่งชาติคือ "ดิจิทัลหยวน" ซึ่งเกิดจากแนวคิดที่ฝ่ายบริหารของประเทศจีนมีความคิดว่าสื่อกลางในการแลกเปลี่ยนดั้งเดิมอย่างธนบัตรถูกนำไปใช้ในกิจกรรมที่ผิดกฎหมายเป็นจำนวนมาก เพราะเจ้าหน้าที่ของรัฐไม่สามารถตรวจสอบการใช้ธนบัตรได้อย่างครอบคลุม ประกอบกับในปัจจุบันประชาชนในประเทศจีนมีการใช้บริการธุรกรรมการเงินอิเล็กทรอนิกส์ผ่านภาคเอกชนอย่างอาลีเพย์ (Alipay) หรือในแอพพลิเคชั่นวีแชท (Wechat) เป็นจำนวนมาก ทำให้รัฐบาลของประเทศจีนเล็งเห็นถึงความเสี่ยงที่อาจเกิดขึ้นต่อความมั่นคงและเสถียรภาพทางเศรษฐกิจ จึงมีการผลักดันให้มีการสร้างสกุลเงินดิจิทัลแห่งชาติขึ้นโดยเจตนาที่ต้องการสร้างสังคมไร้เงินสดที่รัฐบาลสามารถควบคุมกำกับดูแลได้อย่างเต็มรูปแบบ โดยมีหลักการสำคัญคือให้ประชาชนชาวจีนสามารถใช้เงินดิจิทัลซื้อขายสินค้าอุปโภคบริโภคในชีวิตประจำวันได้อย่างเป็นปกติ

ทั้งยังได้รับการรับรองและดำเนินการโดยรัฐบาล ดังนั้น เมื่อประเทศจีนมีนโยบายที่ชัดเจนเกี่ยวกับการสร้างสกุลเงินดิจิทัลแห่งชาติขึ้น จึงมีนโยบายต่อต้านการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในประเทศจีน เพื่อเป็นการตัดช่องทางในการนำไปกระทำผิดกฎหมายและสร้างความเดือดร้อนให้สังคมในประเทศจีนอย่างเด็ดขาด

ส่วนในประเทศไทยเองนั้นในปัจจุบันแนวทางในการพัฒนาสกุลเงินดิจิทัลแห่งชาตินั้น ยังไม่ชัดเจนว่าจะเป็นในทิศทางใดเนื่องจากยังอยู่ในระหว่างขั้นตอนการศึกษาและพัฒนา แต่หากในอนาคตมีการพัฒนาจนสามารถนำมาใช้งานได้จริง ก็จำเป็นจะต้องพิจารณาว่าภาครัฐจะมีการวางกรอบนโยบายอย่างไร ตัวอย่างเช่น หากมีการนำสกุลเงินดิจิทัลอย่างอินทนนท์มาใช้งานได้ในลักษณะเดียวกันกับเงินบาทตามปกติและมีการจำกัดหรือห้ามการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในลักษณะเดียวกันกับประเทศจีนแล้ว ก็อาจส่งผลในทางการป้องกันการนำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมได้ไม่มากก็น้อย เป็นต้น

“บิทคอยน์ เพราะมันเป็นเอกเทศเพราะมันเกิดจากแนวคิดของเสรีชนที่ไม่ต้องการขึ้นกับรัฐบาล เราควรสนับสนุนให้มีคริปโทเคอเรนซีของชาติมากกว่าแทนที่จะไปมุ่งแต่จะควบคุมบิทคอยน์ ผลักดันให้คนใช้งานสกุลเงินเข้ารหัสของประเทศให้มากที่สุด”

(A5, สัมภาษณ์, 26 พฤศจิกายน 2562)

“ตัวอินทนนท์เป็นโครงการที่ทำขึ้นเพื่อทดสอบจำลอง ยังไม่ได้ใช้จริง ใช้เทคโนโลยีเดียวกันกับคริปโทเคอเรนซี แต่คนออกเป็นแบงก์ชาติ ที่ผ่านมาเราทำในระดับธนาคารพาณิชย์และกำลังจะขยายไปสู่ภาคธุรกิจ เพื่อให้เกิดความคล่องตัว เช่น ในเรื่องของการโอนเงินระหว่างกัน แต่ยังบอกไม่ได้ว่าจะนำมาใช้จริงหรือไม่ เพราะต้องดูอีกหลายเรื่องอย่างความพร้อมของประชาชน”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

จากข้อเสนอแนะของผู้ให้ข้อมูลสำคัญดังกล่าวที่เสนอให้มีการสร้างและผลักดันให้มีการใช้งานสกุลเงินเข้ารหัสหรือสกุลเงินดิจิทัลแห่งชาตินั้น ในมุมมองของผู้วิจัยเองมีความเห็นว่าแนวทางดังกล่าวอาจยังไม่สามารถกล่าวได้ว่าเป็นแนวทางหรือวิธีการในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้โดยตรง แต่อย่างไรก็ตามจากการศึกษาทบทวนวรรณกรรมและการศึกษางานวิจัย

ที่เกี่ยวข้องจะพบข้อเท็จจริงประการสำคัญที่สอดคล้องกันคือ ความเสี่ยงหนึ่งที่ทำให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ถูกใช้เป็นเครื่องมือในการกระทำความผิดคือ **การที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆไม่ถูกควบคุมและกำกับดูแลโดยรัฐ หรือสถาบันการเงินของรัฐ** ดังนั้น เพื่อเป็นการตอบสนองต่อสภาพเศรษฐกิจที่มีการขยายตัวและเพื่อไม่เป็นการตัดโอกาสในการพัฒนานวัตกรรมทางการเงินแล้ว ผู้วิจัยเห็นว่าการผลักดันให้มีการใช้งานสกุลเงินเข้ารหัสหรือสกุลเงินดิจิทัลแห่งชาตินั้นอาจมีส่วนช่วยในการลดปริมาณการเกิดของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้ ในกรณีที่ประชาชนหันมาสนใจใช้งานสกุลเงินเข้ารหัสหรือสกุลเงินดิจิทัลแห่งชาติ ที่ออกและควบคุมโดยรัฐเอง หรือกล่าวอีกนัยหนึ่งว่าแนวทางนี้สามารถดำเนินการในลักษณะเป็นมาตรการเสริมให้กับการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้

4.4.8 สร้างความรับรู้ให้แก่ประชาชนและสังคมโดยรวม ในเรื่องที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ และการถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรม

ผู้ให้ข้อมูลสำคัญได้เสนอแนวทางหนึ่ง ที่จะเป็นแนวทางสำคัญอันจะมีส่วนในการช่วยให้เกิดกระบวนการป้องกันตนเองของภาคประชาชน คือการสร้างความรับรู้ในเรื่องที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ และการตกเป็นเครื่องมือในการกระทำความผิดของคนร้ายหรือกลุ่มอาชญากร โดยผู้ให้ข้อมูลสำคัญเสนอแนะว่า ปัจจัยประกอบประการหนึ่งที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิดนั้น เนื่องจากเป็นเทคโนโลยีชนิดใหม่ที่เกิดจากนวัตกรรมทางคอมพิวเตอร์ที่มีความสลับซับซ้อน ทำให้ประชาชนทั่วไปที่อาจไม่ได้มีความสนใจในเรื่องเกี่ยวกับเทคโนโลยีทางการเงินยังขาดความรู้ ความเข้าใจ หรือไม่ทราบข้อเท็จจริงเกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จึงมีส่วนทำให้มีโอกาสที่จะตกเป็นเหยื่อจากการประกอบอาชญากรรม ดังนั้น จึงจำเป็นอย่างยิ่งที่ภาครัฐจะต้องมีการสร้างการรับรู้ในเรื่องดังกล่าวให้กับประชาชนในระดับต่างๆ ตั้งแต่ระดับการศึกษา เช่น การปรับปรุงหรือเพิ่มเนื้อหาบทเรียนที่เกี่ยวกับภัยอันตรายที่เกี่ยวกับบิทคอยน์หรือสกุลเงินเข้ารหัส รวมทั้งเทคโนโลยีและอาชญากรรมสมัยใหม่ต่างๆที่จะเกิดขึ้นในอนาคต ไปจนถึงการสร้างการรับรู้ในเรื่องที่เกี่ยวกับการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดในแง่ของบทลงโทษหรือผลร้ายที่จะได้รับหากถูกจับกุมดำเนินคดีตามกฎหมายผ่านช่องทางต่างๆ เช่น สื่อมวลชน เป็นต้น

ผลประโยชน์ที่จะเกิดขึ้นเมื่อมีการสร้างความรับรู้ในประเด็นที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ และการถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรมแล้วคือ ทำให้ประชาชนมีความรู้ ความเข้าใจในเทคโยโลยีสมัยใหม่นี้ในเบื้องต้น เพื่อให้สามารถป้องกันตนเองหรือไม่นำตนเองเข้าไปยุ่งเกี่ยวกับกระบวนการหรือการกระทำผิดกฎหมายที่เกี่ยวข้องกับสกุลเงินเข้ารหัส และเมื่อประชาชนในสังคมสามารถป้องกันตนเองได้แล้วย่อมส่งผลให้มีอัตราการเกิดของอาชญากรรมประเภทดังกล่าวนี้น้อยลง ทำให้รัฐสามารถนำทรัพยากรไปพัฒนาหรือหาวิธีการป้องกันในแนวทางอื่นๆได้อย่างมีประสิทธิภาพ นอกจากนี้การสร้างการรับรู้ยังก่อให้ผลในทางการข่มขู่ยับยั้ง เนื่องจากประชาชนและสังคมโดยรวมได้รับรู้รับทราบถึงมาตรการต่างๆที่รัฐจะดำเนินการต่อผู้กระทำผิด ทั้งประชาชนยังได้เห็นตัวอย่างของโทษที่ผู้กระทำความผิดจะได้รับอีกด้วย

“ผมมองว่า เป็นเรื่องของการให้การศึกษากับประชาชน อย่างที่บอกว่าวัตถุประสงค์ของการสร้างบิทคอยน์ เพื่อที่จะใช้สร้างสังคมไร้เงินสด แต่ถูกคนบางกลุ่มเอาไปใช้ในทางที่ผิด ”

(B1, สัมภาษณ์, 28 พฤศจิกายน 2562)

“ต้องให้ความรู้กับประชาชนด้วย เพื่อไม่ให้ตกเป็นเหยื่อ ไม่ให้ถูกหลอกลวง และต้องให้ประชาชนรับทราบว่า การเข้าไปกระทำความผิดนั้น จะได้รับโทษที่หนัก เพื่อเป็นการข่มขู่ยับยั้งไปในตัว”

(C3, สัมภาษณ์, 27 พฤษภาคม 2563)

“ต้องให้ความรู้การป้องกันให้กับประชาชนมากๆ เพราะถ้าเทคโนโลยีมันไปเร็วเกินไป แล้วคนตามไม่ทันจะตกเป็นเป้า เพราะฉะนั้นต้องทำให้ประชาชนมีความรู้ เมื่อประชาชนปกป้องตนเองได้ภาครัฐก็จะเบาไปด้วย”

(A1, สัมภาษณ์, 22 มิถุนายน 2563)

จากการศึกษาทั้งจากการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญประกอบกับการนำข้อมูลที่ได้จากการศึกษาทบทวนวรรณกรรมและงานวิจัยที่เกี่ยวข้อง ในประเด็นการเสนอแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส **สามารถสรุปได้ว่าประเทศไทยจำเป็นจะต้องแก้ปัญหาและพัฒนากลไกของรัฐต่างๆ 3 ประเด็นหลัก** ได้แก่

1) การกำหนดมาตรการในการยืนยันตัวตนผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เพื่อเป็นการป้องกันมิให้คนร้ายอาศัยลักษณะพิเศษต่างๆของบิทคอยน์และสกุลเงินเข้ารหัสไปใช้เป็นเครื่องมือในการก่ออาชญากรรมได้โดยง่าย

2) การพัฒนาแก้ไขปรับปรุงกฎหมาย โดยจำเป็นจะต้องพิจารณาให้ความชัดเจนกับสถานภาพของบิทคอยน์ในมิติต่างๆทางกฎหมาย แก้ไขปัญหาด้านการตีความกฎหมายที่เกี่ยวกับการเก็บพยานหลักฐานทางอิเล็กทรอนิกส์ที่ไม่ตรงกันให้เกิดความชัดเจนและกำหนดหลักปฏิบัติให้แก่เจ้าหน้าที่ผู้ปฏิบัตงาน รวมทั้งพิจารณาออกกฎหมายหรือออกบทบัญญัติเพิ่มเติมเกี่ยวกับการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet) และการรับรองการดำเนินการยึดอายัดสกุลเงินเข้ารหัส

3) การพัฒนาแก้ไขปรับปรุงการบังคับใช้กฎหมายให้มีความรู้เท่าทันเทคโนโลยีและนวัตกรรมสมัยใหม่อย่างบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ตลอดจนจำเป็นจะต้องแสวงหาและพัฒนาวิธีการ เครื่องมือหรือกลไกต่างๆที่จะสามารถนำมาใช้ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ รวมทั้งยังจะต้องสร้างความร่วมมือระหว่างหน่วยงานภาครัฐด้ยกันเองและขยายความร่วมมือดังกล่าวไปยังภาคเอกชน โดยเฉพาะผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลและรวมถึงการสร้างความร่วมมือระหว่างประเทศ

ทั้งนี้ เพื่อเป็นการเสริมมาตรการหลักต่างๆแล้ว ประเทศไทยยังจำเป็นจะต้องผลักดันให้มีการสร้างและใช้งานสกุลเงินเข้ารหัสหรือสกุลเงินดิจิทัลแห่งชาติ ทั้งยังจำเป็นจะต้องสร้างความตระหนักรู้ให้แก่ประชาชนและสังคมส่วนรวมเพื่อให้ทราบถึงสถานการณ์และสภาพปัญหาต่างๆของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส เพื่อให้เกิดกระบวนการป้องกันตนเอง

บทที่ 5
อภิปรายผล

จากการศึกษาทบทวนวรรณกรรมจากตำรา เอกสาร บทความวิชาการ งานวิจัย ตลอดจนสื่อต่างๆประกอบกับการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญ สามารถอภิปรายผลการศึกษาตามแนวคิดและทฤษฎี และงานวิจัยที่เกี่ยวข้อง ตามหัวข้อต่างๆดังนี้

5.1 ลักษณะและรูปแบบของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ

จากการเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลสำคัญประกอบกับการศึกษาค้นคว้าทางเอกสารวิชาการและงานวิจัยที่เกี่ยวข้อง สามารถแบ่งลักษณะและรูปแบบของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทยได้ออกเป็น 2 ประเภท ได้แก่ การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมโดยตรงและทางอ้อม โดยสามารถอภิปรายผลการศึกษาตามหัวข้อดังต่อไปนี้

5.1.1 การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมโดยตรง

ลักษณะและรูปแบบของการกระทำผิดในลักษณะนี้เป็นลักษณะและรูปแบบของการกระทำความผิดที่การวิจัยครั้งนี้มุ่งที่จะศึกษาเนื่องจากมีลักษณะของการนำบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไปใช้ประกอบการกระทำความผิดจริง โดยจากการศึกษาทบทวนวรรณกรรมและการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญพบว่า มีลักษณะและรูปแบบของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมโดยตรง ได้แก่

1) การใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นสื่อกลางในการซื้อขายสินค้าและบริการที่ผิดกฎหมายแทนเงินสกุลจริง ได้แก่ การลักลอบซื้อขายยาเสพติด การลักลอบซื้อขายอาวุธปืน การจ้างวานให้ผู้อื่นไปกระทำความผิด และการซื้อขายสื่อลามกอนาจาร

2) การเรียกค่าไถ่ ทั้งรูปแบบดั้งเดิมและการใช้โปรแกรมเรียกค่าไถ่ (Ransomware) แล้วมีการเรียกร้องให้ชำระค่าไถ่เป็นบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ

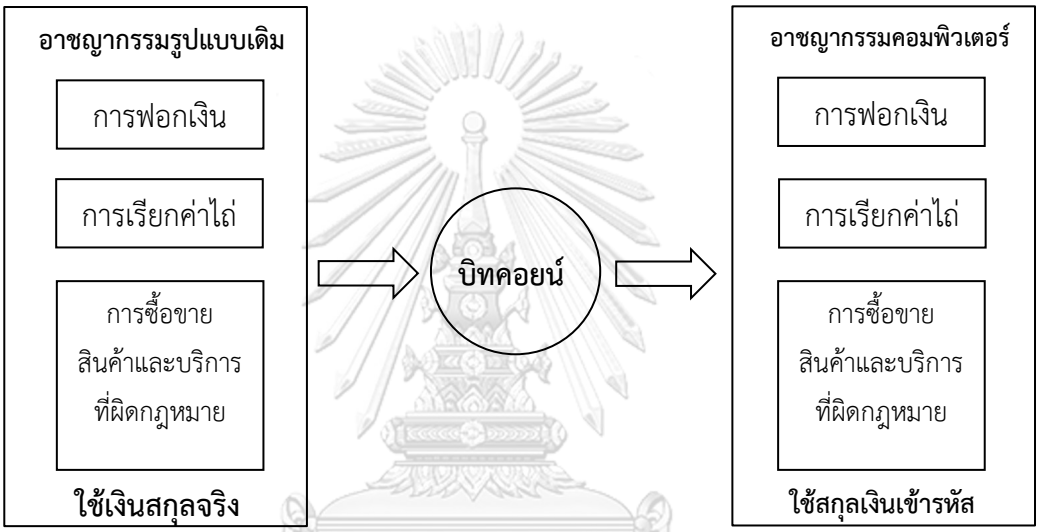
3) การสนับสนุนเงินทุนให้แก่กลุ่มผู้ก่อการร้ายผ่านบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ

4) การฟอกเงินผ่านบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ

ลักษณะและรูปแบบของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาขญากรรมโดยตรงตามที่กล่าวมานี้จำเป็นจะต้องมีการกระทำผ่านการใช้งานระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์เนื่องจากลักษณะของตัวบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ดังนั้นหากวิเคราะห์ตาม**แนวคิดเกี่ยวกับบทบาทหน้าที่ของเครื่องคอมพิวเตอร์ในการก่ออาชญากรรมคอมพิวเตอร์** (จตุชัย แพงจันทร์, 2547 อ้างถึงใน กองวิจัย สำนักงานยุทธศาสตร์ตำรวจ สำนักงานตำรวจแห่งชาติ, 2559) จะพบว่า**การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมโดยตรงมีลักษณะเป็นอาชญากรรมคอมพิวเตอร์ในลักษณะที่คอมพิวเตอร์เป็นเครื่องมือจำเป็นที่ต้องใช้ในการกระทำความผิด** เพราะหากไม่มีคอมพิวเตอร์หรือระบบคอมพิวเตอร์แล้วการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยตรงรูปแบบต่างๆจะไม่สามารถเกิดขึ้นได้

นอกจากนี้หากวิเคราะห์ตามประเภทและลักษณะของอาชญากรรมคอมพิวเตอร์ตามหลักเกณฑ์ของอนุสัญญาแห่งสภายุโรปว่าด้วยอาชญากรรมทางคอมพิวเตอร์ ค.ศ. 2001 จะพบว่า **กรณีการใช้โปรแกรมเรียกค่าไถ่ (Ransomware) เพื่อเข้าโจมตีเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์แล้วเรียกร้องให้มีการจ่ายค่าไถ่เป็นบิทคอยน์ถือเป็นอาชญากรรมคอมพิวเตอร์ในลักษณะของการลักลอบแทรกแซงระบบ (System interference) โดยไม่ได้รับอนุญาต** จนทำให้เกิดความเสียหายอย่างรุนแรงต่อระบบคอมพิวเตอร์ ตามมาตรา 5 (Article 5) ถือเป็นอาชญากรรมคอมพิวเตอร์ ประเภทที่ 1 การกระทำความผิดอันเป็นการกระทบต่อความลับ ความมั่นคงปลอดภัยและความสมบูรณ์ของข้อมูลและระบบคอมพิวเตอร์ (Offences against Confidentiality, Integrity and Availability of Computer Data and Systems) เพราะมีลักษณะการกระทำผิดที่มีเจตนาลักลอบเข้าไปควบคุมหรือจัดการระบบคอมพิวเตอร์โดยไม่ได้รับอนุญาตด้วยการใช้โปรแกรมเรียกค่าไถ่ เพื่อบีบบังคับให้ผู้เสียหายต้องจ่ายค่าไถ่เป็นบิทคอยน์เพื่อให้คนร้ายยอมคืนระบบคอมพิวเตอร์ให้ นอกจากนี้หากกรณีนี้เกิดขึ้นในประเทศไทยยังถือเป็นความผิดตาม พ.ร.บ.การกระทำความผิดเกี่ยวกับคอมพิวเตอร์ ในลักษณะของการกระทำโดยมิชอบเพื่อให้การทำงานระบบคอมพิวเตอร์ผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ ตามที่บัญญัติไว้ใน มาตรา 10 ของกฎหมายดังกล่าว ทั้งนี้เมื่ออาชญากรรมรูปแบบนี้มีลักษณะเป็นอาชญากรรมคอมพิวเตอร์แล้วรูปแบบของการป้องกันก็จะต้องมีลักษณะเป็นการป้องกันอาชญากรรมคอมพิวเตอร์ด้วย

อย่างไรก็ตามเมื่อวิเคราะห์จากอีกมุมมองหนึ่งจะเห็นว่าลักษณะและรูปแบบของการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยตรงนั้น มีรากฐานมาจากรูปแบบของอาชญากรรมตามปกติ ไม่ว่าจะเป็นการฟอกเงิน การเรียกค่าไถ่ หรือการใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการต่างๆ โดยอาชญากรได้มีการพัฒนาวิธีการในการกระทำความผิดให้มีความซับซ้อนและเพิ่มโอกาสที่จะกระทำความผิดสำเร็จได้มากขึ้นด้วยการศึกษาและนำเทคโนโลยีสมัยใหม่มาใช้จนทำให้เกิดเป็นอาชญากรรมรูปแบบใหม่ขึ้น โดยสามารถอธิบายให้เห็นภาพชัดเจนขึ้นได้จากภาพดังนี้



ภาพที่ 26 แนวคิดการพัฒนาของอาชญากรรมจากการนำบิทคอยน์ไปใช้แทนเงินสกุลจริง
(ผู้วิจัย: กิจชัยยะ สุรารักษ์ , 2563)

นอกจากการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมโดยตรงจะมีลักษณะเป็นอาชญากรรมคอมพิวเตอร์แล้ว ด้วยคุณลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ และสามารถใช้งานบนระบบเครือข่ายคอมพิวเตอร์ผ่านเครื่องคอมพิวเตอร์หรือโทรศัพท์มือถือสมาร์ทโฟนได้จากทุกหนแห่งทั่วโลก ทำให้มีการใช้งานที่ไร้พรมแดน (Borderless) ซึ่งส่งผลให้การก่ออาชญากรรมผ่านบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ สามารถกระทำได้ทั่วโลกเช่นกัน ดังนั้น หากพิจารณาจากลักษณะของอาชญากรรมข้ามชาติที่เป็นการกระทำความผิดที่ได้กระทำลงมากกว่าหนึ่งรัฐ การกระทำผิดที่ได้กระทำในรัฐหนึ่งแต่มีการเตรียมการวางแผนหรือควบคุมการกระทำความผิดจากอีกรัฐหนึ่ง หรือมีส่วนเกี่ยวข้องกับองค์กรอาชญากรรมที่มีพฤติกรรม

เกี่ยวข้องกับอาชญากรรมต่างๆมากกว่าหนึ่งรัฐ และการกระทำความผิดที่ได้ทำลงในรัฐหนึ่ง แต่ผลเสียหายหลักไปเกิดขึ้นในอีกรัฐหนึ่ง จะพบว่า การนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยตรงก็มีลักษณะและรูปแบบที่เป็น**อาชญากรรมข้ามชาติ** เช่น ในกรณีของการใช้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นสื่อกลางในการซื้อขายยาเสพติดและอาวุธเถื่อนที่มีการติดต่อซื้อขายกันข้ามประเทศ หรือในกรณีของการใช้โปรแกรมเรียกค่าไถ่ (Ransomware) ที่ผู้กระทำผิดมีการกระทำความผิดจากต่างประเทศ แต่ส่งโปรแกรมเรียกค่าไถ่นี้เข้ามาโจมตีระบบคอมพิวเตอร์ของเหยื่อที่อยู่ในประเทศไทย เป็นต้น และด้วยลักษณะของการเป็นอาชญากรรมข้ามชาติดังที่กล่าวมานี้ ในการกำหนดแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส จึงจำเป็นจะต้องคำนึงถึงมาตรการที่เกี่ยวกับการประสานงานในต่างประเทศด้วย

สำหรับสถานการณ์ในประเทศไทยนั้น ลักษณะและรูปแบบที่พบว่า**มีการกระทำความผิดเกิดขึ้นในประเทศไทยที่ปรากฏชัดเจน**คือ **การฟอกเงินด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆและการใช้โปรแกรมเรียกค่าไถ่ (Ransomware)** เพื่อเข้าโจมตีเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์แล้วเรียกร้องให้มีการจ่ายค่าไถ่เป็นบิทคอยน์ ส่วนลักษณะและรูปแบบของ**การกระทำความผิดที่ยังไม่ปรากฏชัดเจนในประเทศไทยคือการนำบิทคอยน์ไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมายต่างๆ** ส่วนลักษณะและรูปแบบที่ยังไม่พบการกระทำความผิดนั้นคือการสนับสนุนเงินทุนให้แก่กลุ่มผู้ก่อการร้าย อย่างไรก็ตามสถานการณ์ดังกล่าวอาจมีการเปลี่ยนแปลงไปในอนาคตขึ้นอยู่กับการแพร่หลายและแนวนโยบายของรัฐ

5.1.2 การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมทางอ้อม

ลักษณะและรูปแบบของการกระทำผิดในลักษณะนี้ที่เกิดขึ้นในประเทศไทย ได้แก่ การหลอกลวงให้ประชาชนนำเงินมาลงทุนเก็งกำไรในมูลค่าของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ การหลอกลวงให้ประชาชนนำเงินมาลงทุนในการขุดบิทคอยน์และ การชักชวนให้นำสกุลเงินเข้ารหัสหรือคริปโทเคอเรนซีมาร่วมลงทุน ในลักษณะของการระดมทุน (Initial Coin Offering หรือ ICO) เถื่อน ซึ่งการกระทำความผิดในลักษณะนี้ไม่อยู่ในขอบเขตของการศึกษาวิจัยเนื่องจากเมื่อพิจารณาถึงพฤติกรรมในการกระทำความผิดแล้วจะพบว่า **ไม่ได้มีการนำบิทคอยน์ไปใช้ในการกระทำความผิดอย่างแท้จริงแต่อย่างใด** เพียงเป็นการนำชื่อ “บิทคอยน์” หรือชื่อของกิจกรรมการลงทุนที่เกี่ยวกับ

บิทคอยน์ ไปกล่าวอ้างเพื่อให้เหยื่อหลงเชื่อเท่านั้น หรืออาจกล่าวได้ว่าบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไม่ใช่สาระสำคัญหรือวัตถุในการกระทำความผิดแต่อย่างใด เพราะวัตถุที่นำมาใช้ในการหลอกลวงหรือฉ้อโกงประชาชนในลักษณะนี้ สามารถเปลี่ยนแปลงไปได้เสมอตามแต่ค่านิยมของคนในสังคมในแต่ละยุคสมัย เช่น เปลี่ยนจากการหลอกลวงให้มาลงทุนในบิทคอยน์ เป็น การหลอกลวงให้นำเงินมาลงทุนใน ราคาน้ำมัน ทองคำ การลงทุนด้วยการเปรียบต่างค่าเงินสกุลต่างๆ (Forex) รวมทั้งลักษณะของสินทรัพย์ที่อาจมีราคาหรืออาจถือเอาได้ที่จะถูกพัฒนาขึ้นในอนาคต ก็สามารถนำมาใช้ในการหลอกลวงได้ เป็นต้น

นอกจากนี้หากพิจารณาตามนิยามของอาชญากรรมเศรษฐกิจที่มีความหมายว่า “การกระทำความผิดต่อกฎหมายซึ่งมีผลกระทบต่อเศรษฐกิจและความมั่นคง”แล้วจะพบว่าลักษณะและรูปแบบของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมทางอ้อมจะ**มีลักษณะเป็นอาชญากรรมเศรษฐกิจ**เนื่องจากการหลอกลวงชักชวนให้มาลงทุนในการเก็งกำไรในมูลค่าบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆ รวมทั้งการหลอกลวงให้มาลงทุนในการขุด หรือในการระดมทุนเถื่อนก็ตามแท้จริงแล้วมีลักษณะการกระทำความผิดเช่นเดียวกันกับ “แชร์ลูกโซ่” ซึ่งก่อให้เกิดความเสียหายกับประชาชนเป็นจำนวนมาก จนอาจกระทบต่อความมั่นคงทางเศรษฐกิจของประเทศได้ อย่างไรก็ตามการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมในทางอ้อมเช่นนี้ไม่ได้อยู่ในขอบเขตของการศึกษาครั้งนี้แต่อย่างใด

5.2 สภาพปัญหาและสาเหตุของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

จากการศึกษาทบทวนวรรณกรรมและเก็บรวบรวมข้อมูลจากผู้ให้ข้อมูลสำคัญซึ่งได้ให้แนวคิดเกี่ยวกับสภาพปัญหาและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือนั้น สามารถสรุปประเด็นปัญหาและสาเหตุออกเป็น 3 ประเด็นหลัก คือ

1) สภาพปัญหาและสาเหตุจาก “บิทคอยน์”

2) สภาพปัญหาและสาเหตุจาก “กฎหมาย”

3) สภาพปัญหาและสาเหตุจาก “การบังคับใช้กฎหมาย”

โดยผู้วิจัยสามารถวิเคราะห์และอภิปรายผลการศึกษาแยกตามหัวข้อได้ดังนี้

5.2.1 สภาพปัญหาและสาเหตุจาก “บิทคอยน์”

ทั้งข้อมูลจากการศึกษาทบทวนวรรณกรรมและข้อมูลจากผู้ให้ข้อมูลสำคัญต่างชี้ให้เห็นถึงประเด็นปัญหาที่เป็นปัจจัยสำคัญตรงกันว่า คุณลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่ไม่มีรูปร่าง ไม่สามารถจับต้องได้ มีระบบการทำงานและเก็บข้อมูลบนเครือข่ายคอมพิวเตอร์ที่ไม่มีฐานข้อมูลกลาง (Server) แต่ใช้ระบบการกระจายข้อมูลที่ให้ผู้ใช้งานสามารถซื้อขายแลกเปลี่ยนกันได้โดยตรง (Peer – to - Peer) โดยไม่จำเป็นต้องผ่านการตรวจสอบจากรัฐบาลหรือตัวกลางอย่างธนาคารหรือสถาบันการเงิน สามารถนำไปใช้งานได้จากทั่วทุกมุมโลกโดยไม่ติดข้อจำกัดเรื่องเขตแดนของรัฐ (Borderless) และคุณลักษณะพิเศษที่สำคัญคือการที่ผู้ใช้งานไม่จำเป็นต้องทำการยืนยันหรือแสดงตัวตนที่แท้จริง (Anonymity) (Satoshi Nakamoto, 2008) เป็นสาเหตุที่ทำให้บิทคอยน์ถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรม โดยหากพิจารณาตามหลัก**ทฤษฎีการคิดก่อนกระทำผิด (Rational Choice Theory)** ที่มีหลักการสำคัญว่าก่อนที่ผู้กระทำผิดจะตัดสินใจลงมือกระทำผิดนั้น จะได้มีการคิดไตร่ตรองเพื่อชั่งน้ำหนักระหว่างผลประโยชน์ที่ได้รับจากการกระทำความผิด เช่น โอกาสที่จะก่ออาชญากรรมสำเร็จและโอกาสที่จะสามารถหลบหนีหรือรอดพ้นจากการถูกจับกุมดำเนินคดี เปรียบเทียบกันกับผลร้ายที่จะได้รับจากการก่ออาชญากรรม เช่น อัตราโทษและความเสียหายด้านต่างๆ โดยหากผู้กระทำผิดเห็นว่าการก่ออาชญากรรมจะทำให้ตนได้ประโยชน์มากกว่าโทษก็จะตัดสินใจกระทำความผิด ซึ่งในกรณีของการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมโดยอาศัยลักษณะพิเศษต่างๆนั้นสามารถวิเคราะห์ได้ว่าผู้กระทำผิดน่าจะได้ทำการคิดไตร่ตรองอย่างมีเหตุผลและชั่งน้ำหนักก่อนแล้วว่าตนจะได้รับผลประโยชน์จากกระทำความผิดจากการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรม เนื่องจากคุณลักษณะต่างๆของบิทคอยน์ตามที่ได้กล่าวมาแล้วจะทำให้ผู้กระทำผิดอยู่ในสถานะของบุคคลนิรนาม (Anonymous) ซึ่งจะทำให้เจ้าหน้าที่ของรัฐเกิดความยากลำบากในการตรวจสอบติดตามเส้นทางธุรกรรมทางการเงิน ทั้งยังทำให้ไม่สามารถตรวจสอบยืนยันเพื่อพิสูจน์ตัวผู้ใช้งานที่แท้จริงได้ ซึ่งจะส่งผลทำให้ผู้กระทำผิดมีโอกาสที่จะรอดพ้นจากการถูกตรวจสอบจับกุมและการถูกดำเนินคดีตามกฎหมายสูง จึงทำให้ผู้กระทำผิดตัดสินใจนำบิทคอยน์ไปใช้ในการกระทำความผิด

ตัวอย่างเช่น อาชญากรได้ทำการคิดไตร่ตรองอย่างมีเหตุผลและชั่งน้ำหนักแล้วว่าการนำบิทคอยน์มาใช้ในการฟอกเงิน ด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนให้อยู่ในรูปแบบของบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ จะทำให้เจ้าหน้าที่ของรัฐไม่สามารถตรวจสอบ

ติดตามเส้นทางการเงินได้โดยง่ายและจะไม่สามารถตรวจสอบยืนยันเพื่อพิสูจน์หาตัวตนของผู้กระทำผิดที่แท้จริงได้อันเป็นผลมาจากคุณลักษณะพิเศษของบิทคอยน์ที่มีการปกปิดตัวตนผู้ใช้งานที่แท้จริง ซึ่งจะทำให้ผู้กระทำผิดได้ประโยชน์จากการกระทำความผิดและยังรอดพ้นจากการตรวจสอบจับกุมของเจ้าหน้าที่ของรัฐ ด้วยสาเหตุนี้อาชญากรจึงตัดสินใจใช้บิทคอยน์เป็นเครื่องมือในการป้องกันอาชญากรรม

5.2.2 สภาพปัญหาและสาเหตุจาก “กฎหมาย”

จากการศึกษาสภาพปัญหาและสาเหตุของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมในประเด็นที่เกี่ยวข้องกับกฎหมาย ทำให้พบว่ากฎหมายต่างๆที่เกี่ยวข้องยังไม่สามารถทำหน้าที่เป็นกลไกในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ และก่อให้เกิดสภาพปัญหาต่างๆทั้งในด้านการกำหนดสถานภาพความเป็นทรัพย์และทรัพย์สิน การตีความเพื่อเก็บพยานหลักฐานต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอกนิกส์ ตลอดจนยังขาดกฎหมายที่เกี่ยวข้องที่มีลักษณะเป็นกฎหมายวิธีสบัญญัติที่จะกำหนดขั้นตอนและวิธีการปฏิบัติที่ชัดเจนรวมทั้งให้อำนาจในการดำเนินการต่างๆให้แก่เจ้าหน้าที่ผู้ปฏิบัติงานโดยเฉพาะอย่างยิ่งในประเด็นเกี่ยวกับการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ อีกทั้งเมื่อศึกษาถึงกฎหมายที่กำกับดูแลเกี่ยวกับสกุลเงินเข้ารหัสโดยตรงอย่าง พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 พบว่าแม้กฎหมายนี้จะมีเจตนารมณ์ในการป้องกันไม่ให้มีการนำสกุลเงินเข้ารหัส ซึ่งถือเป็นสินทรัพย์ดิจิทัลประเภทหนึ่งไปใช้ในการก่ออาชญากรรมหรือนำไปใช้ในกิจกรรมที่ผิดกฎหมายก็ตาม แต่ปรากฏว่ากลไกและมาตรการต่างๆที่บัญญัติในกฎหมายยังเป็นไปเพื่อให้เอื้อต่อการเกิดการพัฒนาทางเศรษฐกิจและการเปิดรับให้เกิดการนำเทคโนโลยีทางการเงินมาใช้ภายใต้การกำกับดูแลของรัฐเป็นวัตถุประสงค์หลัก ซึ่งแสดงให้เห็นว่า**รัฐยังมีทิศทางหรือแนวนโยบายในการควบคุมกำกับดูแลสกุลเงินเข้ารหัสในลักษณะของการแบ่งรับแบ่งสู้ ส่งผลทำให้มาตรการทางกฎหมายยังไม่ชัดเจน ซึ่งยังส่งผลทำให้การป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในมิติของกฎหมายยังคงบกพร่องหรือมีช่องว่าง**

ผู้วิจัยวิเคราะห์สาเหตุสำคัญประเด็นหนึ่งที่รัฐไม่ได้มีแนวนโยบายทางกฎหมายที่ชัดเจนไปในทางใดทางหนึ่ง หรือกล่าวอีกนัยหนึ่งว่ารัฐยังไม่ได้มีแนวนโยบายในการควบคุมหรือไม่ยอมรับในสกุลเงินเข้ารหัสอย่างเด็ดขาดหรือไม่ได้มีแนวนโยบายที่เปิดกว้างให้ใช้งานกันได้อย่างอิสระ แต่เป็นแนวนโยบายที่มุ่งจะควบคุมกำกับดูแลในลักษณะของการตั้งรับ คือ **ความเป็นอาชญากรรมของ**

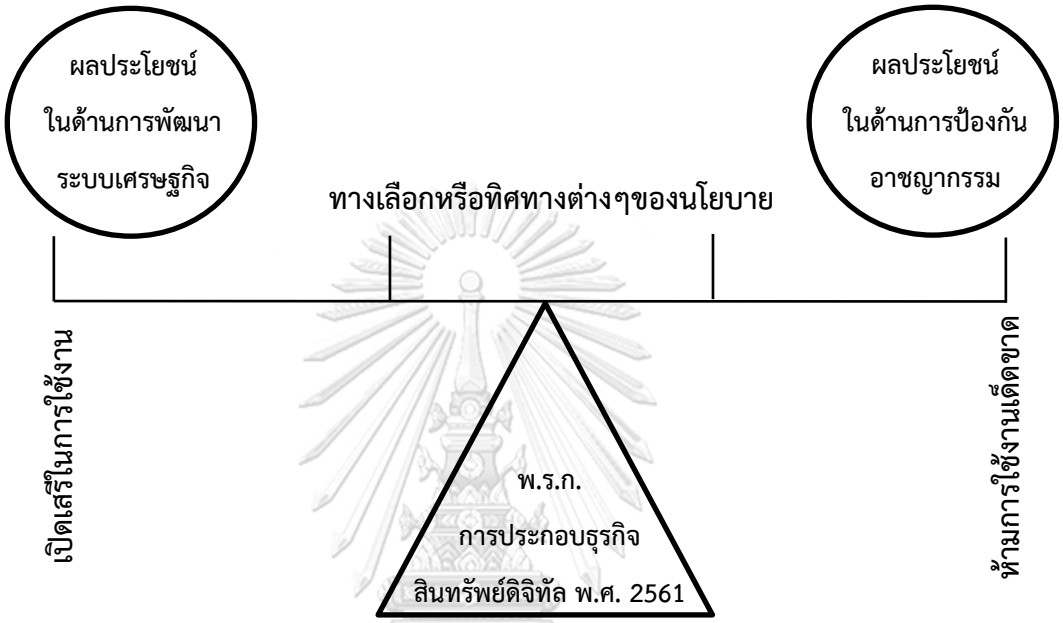
บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ กล่าวคือเมื่อพิจารณาถึงรายละเอียดและข้อเท็จจริงตั้งแต่แนวคิดที่นำมาสู่การสร้างบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ระบบการทำงาน รวมทั้งสภาพการใช้งานโดยทั่วไปแล้วจะพบว่า เจตนารมณ์ของการสร้างและใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เป็นไปเพื่อการสร้างความอิสระทางการเงินและการสร้างเทคโนโลยีทางการเงินสมัยใหม่ให้สอดคล้องกับยุคสมัยในปัจจุบัน เมื่อพิจารณาได้ดังนี้แล้วจะพบว่า**ตัวบิทคอยน์และสกุลเงินเข้ารหัสต่างๆนั้นมิได้มีความชั่วร้ายในตัวเองและการใช้งานและการถือครองบิทคอยน์และสกุลเงินเข้ารหัสต่างๆก็ไม่ได้มีลักษณะเป็นอาชญากรรมโดยสภาพ (Mala Inse)** หรือไม่ได้มีลักษณะเป็นการกระทำที่มีความผิดหรือมีความชั่วร้ายรุนแรงในตัวเองแต่อย่างใด แต่ในขณะเดียวกันด้วยลักษณะต่างๆของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆตามที่ได้กล่าวมาแล้วนั้นมีลักษณะบางประการที่เอื้อต่อการนำไปใช้ในการกระทำความผิด ดังนั้น **รัฐจึงจำเป็นต้องวางหลักการและมาตรการทางกฎหมายบางประการเพื่อกำหนดให้การกระทำบางอย่างที่ไม่ได้มีความชั่วร้ายในตัวเองเป็นความผิดตามกฎหมาย (Mala Prohibita)** เพื่อประโยชน์ในการป้องกันมิให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆถูกนำไปใช้ในการกระทำความผิด ตัวอย่างเช่น การประกอบธุรกิจสินทรัพย์ดิจิทัลที่โดยเนื้อหาสาระของกิจกรรมต่างๆที่เกิดขึ้นตามปกตินั้น เป็นไปเพื่อการซื้อขายแลกเปลี่ยนสินทรัพย์ดิจิทัลซึ่งมิใช่กิจกรรมที่ผิดกฎหมายหรือละเมิดต่อศีลธรรมอันดี แต่กฎหมายก็ยังกำหนดให้ผู้ประกอบการจะต้องขออนุญาตและได้รับอนุญาตจาก สำนักงาน ก.ล.ต. หากฝ่าฝืนประกอบการโดยไม่ได้รับอนุญาตจะเป็นความผิดตามกฎหมาย ซึ่งเป็นกลไกของรัฐที่กำหนดให้พฤติกรรมบางประการเป็นความผิดเพื่อประโยชน์ในการควบคุมกำกับดูแลการประกอบธุรกิจและป้องปรามการจะนำสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดไปพร้อมๆกัน

สาเหตุอีกประการหนึ่งที่ทำให้รัฐไม่สามารถกำหนดแนวนโยบายทางกฎหมายให้เน้นหนักไปในทิศทางใดทิศทางหนึ่งได้นั้น คือ**ความจำเป็นที่จะต้องสร้างสมดุลให้เกิดขึ้นระหว่างการพัฒนาระบบเศรษฐกิจในภาพรวมของประเทศกับการป้องกันอาชญากรรมเพื่อรักษาความสงบสุขในสังคม** เนื่องจากเจตนาอันเป็นที่มาของการสร้างบิทคอยน์และสกุลเงินเข้ารหัสต่างๆนั้น เป็นไปเพื่อการสร้างสื่อกลางในการแลกเปลี่ยนสินค้าและบริการรูปแบบใหม่ที่ทำให้ระบบการเงินการธนาคารมีความคล่องตัว แก้ไขปัญหาข้อจำกัดในเรื่องการทำธุรกรรมข้ามประเทศและลดระยะเวลาในการติดต่อทำธุรกรรม (Satoshi Nakamoto, 2008) จนอาจกล่าวได้ว่าหากพิจารณาในมุมมองของการพัฒนาเศรษฐกิจแล้ว บิทคอยน์และสกุลเงินเข้ารหัสอาจเป็นปัจจัยสำคัญที่จะทำให้เศรษฐกิจของประเทศเกิด

การขยายตัวไปในทิศทางที่ดีขึ้น ในขณะที่หากพิจารณาในมุมมองของการป้องกันอาชญากรรมแล้ว เทคโนโลยีสมัยใหม่ลักษณะนี้ย่อมจะนำมาซึ่งอาชญากรรมรูปแบบใหม่ที่มีความซับซ้อนและยากลำบากต่อการสืบสวนติดตามผู้กระทำผิดจนอาจทำให้เกิดความเสียหายและกระทบต่อความสงบสุขในสังคมได้ ซึ่งประเด็นในเรื่องความขัดแย้งดังกล่าวนี้จะเห็นได้จากการที่ผู้ให้ข้อมูลสำคัญที่เป็นกลุ่มของผู้เชี่ยวชาญเกี่ยวกับสกุลเงินเข้ารหัสทั้งในภาคเอกชน และหน่วยงานของรัฐที่เกี่ยวข้องกับการพัฒนาเทคโนโลยีทางการเงินและการลงทุนจะมีความเห็นว่าหากเข้าไปควบคุมหรือกำกับดูแลการใช้สกุลเงินเข้ารหัสต่างๆอย่างเข้มงวดจนเกินไป อาจส่งผลกระทบให้เกิดการหยุดชะงักหรือทำให้เกิดการชะลอการพัฒนาระบบเศรษฐกิจได้ ในขณะที่ผู้ทรงคุณวุฒิกลุ่มที่เป็นผู้บังคับใช้กฎหมายที่มีหน้าที่ในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสกลับเสนอแนวคิดว่าจำเป็นจะต้องป้องกันมิให้เกิดการนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรมอย่างเด็ดขาด

ลักษณะของความขัดแย้งในมุมมองของการรักษาผลประโยชน์ของประเทศดังกล่าวนี้ เมื่อนำ**แนวคิดเกี่ยวกับนโยบายสาธารณะในเรื่องตัวแบบนโยบายสาธารณะแบบกลุ่ม (Group Model)** ที่มีหลักการสำคัญว่าการกำหนดนโยบายสาธารณะของรัฐนั้นเป็นผลมาจากที่ ปัจเจกบุคคลได้รวมกลุ่มกันเพื่อสร้างและรักษาผลประโยชน์ของตนในมุมต่างๆ กลุ่มสังคมเหล่านี้จะทำหน้าที่เป็นตัวเชื่อมโยงระหว่างรัฐบาลและประชาชน โดยกลุ่มสังคมเหล่านี้จะมีบทบาทต่อกระบวนการการกำหนดนโยบายสาธารณะด้วยการชี้ให้รัฐบาลเห็นถึงสภาพปัญหาต่างๆ แนวทางการพัฒนาผลประโยชน์ของกลุ่ม และเสนอข้อเรียกร้องต่างๆเพื่อให้เกิดการกำหนดหรือเปลี่ยนแปลงนโยบายสาธารณะ ซึ่งกลุ่มในทางสังคมดังที่กล่าวมานี้จะมีเป็นจำนวนมาก ส่งผลให้เกิดการต่อสู้ระหว่างกลุ่มต่างๆเพื่อเข้าไปมีอิทธิพลในการกำหนดนโยบายสาธารณะหรือกล่าวอีกนัยหนึ่งว่า นโยบายสาธารณะเป็นผลจากการต่อสู้ของกลุ่มผลประโยชน์ต่างๆ ทำให้รัฐจำเป็นจะต้องเข้าไปจัดการความขัดแย้งนี้โดยการสร้างสมดุลให้เกิดขึ้นด้วยการประนีประนอมและจัดสรรผลประโยชน์ให้กับกลุ่มต่างๆในรูปแบบของการกำหนดนโยบายสาธารณะที่สร้างสมดุลระหว่างความขัดแย้งขึ้น (มยุรี อนุมานราชธน , 2556 , น.73) **โดยในกรณีของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส**นี้ กลุ่มทางสังคมที่มุ่งรักษาผลประโยชน์จนเกิดความขัดแย้งกันในทางความคิดคือ **กลุ่มหน่วยงานภาครัฐและภาคเอกชนที่มุ่งให้เกิดการพัฒนาทางด้านเศรษฐกิจและเทคโนโลยีทางการเงินกับกลุ่มของผู้บังคับใช้กฎหมายที่ต้องการจะป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส** ทำให้รัฐบาลจำเป็นจะต้องสร้างความสมดุลระหว่างผลประโยชน์ในด้านต่างๆ ผ่านการวิเคราะห์และประเมินสถานการณ์การใช้งานบิทคอยน์และสกุลเงิน

เข้ารหัสต่างๆทั้งในภาพรวมของสังคมโลกและสถานการณ์ภายในประเทศจนทำให้มีการบัญญัติ พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัลขึ้นบังคับใช้ในปี พ.ศ. 2561 ซึ่งสามารถวิเคราะห์ได้ตามแนวคิดตัวแบบนโยบายสาธารณะแบบกลุ่มตามภาพดังต่อไปนี้



ภาพที่ 27 การกำหนดนโยบายสาธารณะในการกำกับดูแลสกุลเงินเข้ารหัสตามแนวคิดตัวแบบนโยบายสาธารณะประเภทตัวแบบกลุ่ม (Group Model)
(ประยุกต์จาก Dye, 1984, p.27 อ้างถึงโดย มยุรี อนุมานราชธน, 2556, น.72)

จากภาพสามารถอธิบายได้ว่า ในปี พ.ศ. 2561 รัฐบาลได้ตระหนักถึงสถานการณ์ ณ ขณะนั้นที่เริ่มมีการนำสกุลเงินเข้ารหัสมาใช้เป็นเครื่องมือในการลงทุนและนำมาใช้ในการซื้อขายแลกเปลี่ยนและเริ่มมีการประกอบธุรกิจเกี่ยวกับสินทรัพย์ดิจิทัลขึ้น โดยที่ประเทศไทย ณ ขณะนั้นยังไม่มีกฎหมายรองรับหรือกำกับดูแล รัฐบาลจึงจำเป็นต้องออกกฎหมายเพื่อเป็นการกำกับควบคุมการประกอบธุรกิจและการดำเนินกิจกรรมเกี่ยวกับสินทรัพย์ดิจิทัล โดยรัฐบาลได้ประนีประนอมและจัดสรรผลประโยชน์ให้แก่กลุ่มสังคมทั้งสองกลุ่มแล้วโดยจะเห็นได้จากบทบัญญัติและมาตรการทางกฎหมายที่บัญญัติรับรองสถานะความเป็นสินทรัพย์ดิจิทัลและกำหนดหลักเกณฑ์เกี่ยวกับการประกอบธุรกิจสินทรัพย์ดิจิทัลที่ถูกกฎหมายขึ้นและในขณะเดียวกันก็ มีการบัญญัติบทบัญญัติที่เป็นมาตรการ

ป้องกันต่างๆ เช่น การบังคับใช้มาตรการรู้จักลูกค้า การให้ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลถือเป็นสถานประกอบการที่อยู่ภายใต้กฎหมายที่เกี่ยวกับการป้องกันปราบปรามการฟอกเงิน ซึ่งเท่ากับว่ากฎหมายดังกล่าวได้สะท้อนให้เห็นว่ารัฐบาลในขณะนั้นมีเจตนาที่จะให้เกิดการพัฒนาทางด้านเศรษฐกิจและการป้องกันอาชญากรรมในระดับที่สมดุลกัน และ**มาตรการทางกฎหมายที่จำเป็นจะต้องสร้างสมดุลให้เกิดขึ้นดังกล่าวนี้ จึงไม่สามารถที่จะใช้เป็นกลไกในการป้องกันอาชญากรรมได้อย่างครอบคลุมครบถ้วน เพราะหากกำหนดให้นโยบายหรือกฎหมายมุ่งไปที่การป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสเป็นประเด็นหลักแล้ว อาจจะกระทบกับการพัฒนาระบบเศรษฐกิจในภาพรวมของประเทศได้**

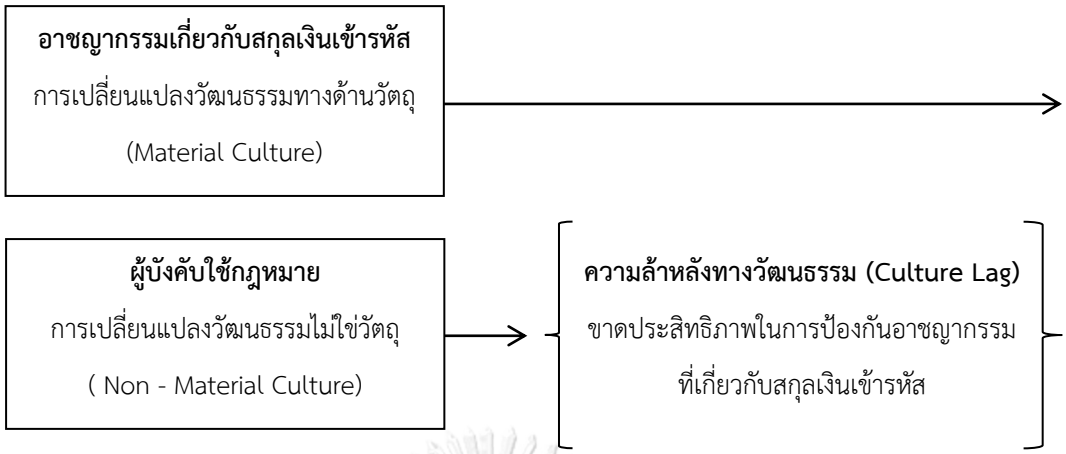
ด้วยเหตุผลสำคัญทั้งสองประการได้แก่ การพิจารณาถึงความเป็นอาชญากรรมของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆประกอบกับความจำเป็นที่จะต้องกำหนดกฎหมายที่เป็นนโยบายสาธารณะเพื่อให้เกิดผลในการสมดุลระหว่างการพัฒนาระบบเศรษฐกิจและการป้องกันอาชญากรรมไปในเวลาเดียวกัน จึงเป็นสาเหตุที่ทำให้กฎหมายที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสคือ พ.ร.บ.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 ยังมีข้อบกพร่องและยังไม่สามารถนำไปใช้ในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพเพียงพอดังที่ได้กล่าวไปแล้ว

อย่างไรก็ตามการกำหนดนโยบายสาธารณะตามตัวแบบกลุ่ม (Group Model) ที่ผู้วิจัยนำมาใช้วิเคราะห์นี้ สามารถนำไปใช้ในการปรับปรุงแก้ไขนโยบายสาธารณะที่มีให้เหมาะสมกับสถานการณ์ในอนาคต เนื่องจากทั้งการออกกฎหมาย พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 และการศึกษาวิจัยในครั้งนี้ เป็นการศึกษาวิจัยจากประเด็นปัญหาเดียวคือ **“บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ”** ซึ่งถือเป็นการศึกษาแบบภาคตัดขวางในขณะที่ความก้าวหน้าทางเทคโนโลยียังมีการพลวัตไปอย่างต่อเนื่องไม่ว่าจะเป็นเทคโนโลยีทางการเงินหรือนวัตกรรมด้านอื่นๆ ซึ่งอาจส่งผลให้ในอนาคตอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสมีการเปลี่ยนแปลงรูปแบบและระดับความรุนแรงไป ดังนั้นเมื่อสถานการณ์และสภาพปัญหามีการเปลี่ยนแปลงก็จำเป็นที่จะต้องวิเคราะห์และทบทวนเพื่อให้มีการกำหนดจุดสมดุลของนโยบายสาธารณะที่เหมาะสมดังจะได้กล่าวต่อไป

5.2.3 สภาพปัญหาและสาเหตุจาก “การบังคับใช้กฎหมาย”

จากการศึกษาสภาพปัญหาและสาเหตุของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมในประเด็นที่เกี่ยวข้องกับผู้บังคับใช้กฎหมายทำให้พบว่า เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องยังขาดองค์ความรู้ วิธีการ และเครื่องมือหรือกลไกต่างๆที่จะสามารถใช้ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสต่างๆได้อย่างมีประสิทธิภาพ ทั้งยังขาดการบูรณาการร่วมกันทั้งจากหน่วยงานภาครัฐ ภาคเอกชน และความร่วมมือจากต่างประเทศในมิติต่างๆ ส่งผลให้การป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสยังขาดประสิทธิภาพ ซึ่งผู้วิจัยวิเคราะห์ว่าปัญหาดังกล่าวเป็นไป**ตามทฤษฎีความล้าหลัง (Culture Lag Theory)** ซึ่งมีแนวคิดสำคัญคือ เมื่อเกิดการพัฒนาทางนวัตกรรมหรือเทคโนโลยีต่างๆขึ้นในสังคมของมนุษย์นั้น จะส่งผลให้เกิดการเปลี่ยนแปลงทางสังคมใน 2 ด้าน ได้แก่ การเปลี่ยนแปลงวัฒนธรรมทางด้านวัตถุ (Material Culture) หมายถึงการเปลี่ยนแปลงเกี่ยวกับการแต่งกาย เสื้อผ้า เครื่องประดับ การใช้ยานพาหนะ และการเปลี่ยนแปลงวัฒนธรรมที่ไม่ใช่วัตถุ (Non - Material Culture) หมายถึงการเปลี่ยนแปลงความเชื่อ ความคิดค่านิยม บรรทัดฐานทางสังคม กฎหมายและประเพณีต่างๆ ซึ่งการเปลี่ยนแปลงทางด้านวัตถุจะเกิดขึ้นได้รวดเร็วกว่าจนทำให้การเปลี่ยนแปลงวัฒนธรรมที่ไม่ใช่วัตถุพัฒนาเปลี่ยนแปลงไปตามไปไม่ทันจนทำให้เกิดช่องว่างและทำให้เกิดปัญหาต่างๆขึ้นในสังคมโดยเฉพาะปัญหาอาชญากรรม

จากสภาพปัญหาและสาเหตุจากผู้บังคับใช้กฎหมายตามที่กล่าวข้างต้นจึงสามารถวิเคราะห์และอธิบายตามหลักการของทฤษฎีความล้าหลังทางสังคม (Culture Lag Theory) ได้ว่า ภายหลังจากที่มีการประดิษฐ์คิดค้นบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ส่งผลทำให้มีการเผยแพร่นวัตกรรมดังกล่าวไปสู่สังคมต่างๆ จนทำให้**เกิดการเปลี่ยนแปลงวัฒนธรรมทางด้านวัตถุ (Material Culture)** ซึ่งในกรณีนี้คือ การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการรวมทั้งการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นเครื่องมือในการก่ออาชญากรรม ซึ่งการเปลี่ยนแปลงวัฒนธรรมทางด้านวัตถุนี้เกิดขึ้นอย่างรวดเร็ว ในขณะที่การเปลี่ยนแปลงวัฒนธรรมที่ไม่ใช่วัตถุ (Non - Material Culture) ซึ่งในกรณีนี้คือเจ้าหน้าที่ที่มีหน้าที่บังคับใช้กฎหมายรวมทั้งกลไกและมาตรการต่างๆของรัฐที่เกี่ยวข้อง **ไม่สามารถปรับตัวให้เท่าทันกับการอุบัติขึ้นของสกุลเงินเข้ารหัสและอาชญากรรมที่ใช้สกุลเงินเข้ารหัสเป็นเครื่องมือได้** จนทำให้เกิดเป็นช่องว่างทางสังคมคือการขาดประสิทธิภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส โดยสามารถสรุปแนวคิดดังกล่าวได้ตามภาพดังนี้



ภาพที่ 28 แนวคิดความล้าหลังทางวัฒนธรรม (Culture Lag) ที่ผู้บังคับใช้กฎหมายไม่สามารถปรับตัวให้ทันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้
(ผู้วิจัย: กิจชัยยะ สุรารักษ์ , 2563)

5.2.4 บทสรุปสาเหตุของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

จากการวิเคราะห์และอภิปรายสภาพปัญหาและสาเหตุของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรม ทำให้สามารถสรุปสาเหตุของการเกิดอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ ตามแนวคิดของทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) ที่มีหลักการสำคัญคือ อาชญากรรมจะเกิดขึ้นก็ต่อเมื่อมีองค์ประกอบเกิดขึ้นครบถ้วนทั้ง 3 องค์ประกอบได้แก่ มีผู้กระทำความผิดที่มีแรงจูงใจ (Motivated Offender) มีเป้าหมายที่เหมาะสม (Suitable Target) และ การขาดความสามารถในการป้องกันเป้าหมาย (Absense of a Capable Guardian) ได้ว่า อาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทยเกิดจากองค์ประกอบสำคัญสามประการคือ

1) ผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender)

ผู้กระทำผิดหรืออาชญากรที่มีความรู้ความเชี่ยวชาญทางเทคโนโลยีสมัยใหม่ได้เล็งเห็นถึงคุณลักษณะพิเศษของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่ไม่มีรูปร่าง ไม่สามารถจับต้องได้ มีระบบการทำงานและเก็บข้อมูลบนเครือข่ายคอมพิวเตอร์ที่ไม่มีฐานข้อมูลกลาง (Server) แต่ใช้ระบบการกระจายข้อมูลที่ให้ผู้ใช้งานสามารถซื้อ

ขายแลกเปลี่ยนกันได้โดยตรง (Peer – to - Peer) โดยไม่จำเป็นต้องผ่านการตรวจสอบจากรัฐบาล หรือตัวกลางอย่างธนาคารหรือสถาบันการเงิน สามารถนำไปใช้งานได้จากทั่วทุกมุมโลกโดยไม่ติดข้อจำกัดเรื่องเขตแดนของรัฐ (Borderless) และคุณลักษณะพิเศษที่สำคัญคือการที่ผู้ใช้งานไม่จำเป็นต้องทำการยืนยันหรือแสดงตัวตนที่แท้จริง **จนทำให้เกิดเป็นแรงจูงใจที่จะกระทำผิด เนื่องจากลักษณะพิเศษต่างๆตามที่กล่าวมานี้ ส่งผลทำให้เจ้าหน้าที่ของรัฐไม่สามารถตรวจสอบติดตามเส้นทางธุรกรรมทางการเงินของผู้กระทำผิด ตลอดจนยังไม่สามารถพิสูจน์ตัวตนของผู้กระทำผิดได้ จึงทำให้ผู้กระทำผิดตัดสินใจที่จะนำบิทคอยน์และสกุลเงินเข้ารหัสไปใช้ในการกระทำความผิด**

2) มีเป้าหมายที่เหมาะสม (Suitable Target)

เป้าหมายที่เหมาะสมในที่นี้ผู้วิจัยสามารถวิเคราะห์ได้หลายมุมมอง เช่น หากพิจารณาในมุมของเป้าหมายซึ่งเป็นสถานที่หรือสภาวะแวดล้อมที่เหมาะสม (Place) นั้นสามารถอธิบายได้ว่าการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมนั้น มีลักษณะเป็นอาชญากรรมคอมพิวเตอร์ตามที่ได้กล่าวมาแล้ว ดังนั้น **จึงจำเป็นจะต้องกระทำความผิดผ่านระบบคอมพิวเตอร์หรือเครือข่ายคอมพิวเตอร์** ประกอบกับคุณลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ที่สามารถใช้งานกันเองได้โดยตรง (Peer – to - Peer) โดยที่ไม่มีการเก็บข้อมูลไว้ที่ส่วนกลาง (Server) จึงส่งผลทำให้ระบบคอมพิวเตอร์มีลักษณะเป็นสังคมเสมือน (Virtual Society) ที่เหมาะแก่การก่ออาชญากรรมเนื่องจากมีโอกาสที่จะกระทำผิดสำเร็จสูงและมีโอกาสที่จะถูกตรวจสอบติดตามน้อย เนื่องจากข้อมูลต่างๆที่อยู่ในระบบคอมพิวเตอร์นี้มีความสลับซับซ้อน

นอกจากนี้หากวิเคราะห์ถึงเป้าหมายที่เหมาะสมในแง่ของสังคมศาสตร์แล้ว อาจกล่าวได้ว่าสภาพของสังคมไทยที่ยังมีระดับการตระหนักถึงปัญหาอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสต่างๆอยู่ในระดับต่ำเห็นได้จากนโยบายของรัฐและกฎหมายที่เกี่ยวข้อง ทำให้สังคมไทยถือเป็นเป้าหมายที่เหมาะสมในเชิงสังคม กล่าวคือหากในสังคมใดที่ประชาชนหรือคนในสังคมยังขาดความรู้ความเข้าใจ ตลอดจนยังไม่รับทราบถึงความเสี่ยงหรือผลร้ายที่อาจเกิดขึ้นจากการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรม ก็จะส่งผลให้สังคมนั้นตกเป็นเป้าหมายของอาชญากรหรือผู้กระทำผิดต่างๆ

3) การขาดความสามารถในการป้องกันเป้าหมาย (Absense of a Capable Guardian)

การขาดศักยภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ทั้งในเรื่องของกลไกการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสไปใช้ในทางที่ผิดกฎหมาย ปัญหาในเรื่องการตีความทางกฎหมาย การขาดการบัญญัติกฎหมายในเรื่องที่เกี่ยวข้องกับผู้ปฏิบัติงาน ตลอดจนการขาดศักยภาพของ “**ผู้บังคับใช้กฎหมาย**” ที่ยังขาดองค์ความรู้ วิธีการ และเครื่องมือหรือกลไกต่างๆที่จะป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสต่างๆได้อย่างมีประสิทธิภาพ ทั้งยังขาดการบูรณาการร่วมกันทั้งจากหน่วยงานภาครัฐ ภาคเอกชน และความร่วมมือจากต่างประเทศ อันเป็นผลมาจากการพัฒนาเปลี่ยนแปลงทางเทคโนโลยีอย่างก้าวกระโดดของการประดิษฐ์คิดค้นบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จนส่งผลทำให้กฎหมายและผู้บังคับใช้กฎหมายไม่สามารถทำหน้าที่ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างทันท่วงที **เมื่อกลไกในการป้องกันดังกล่าวขาดความสามารถในการป้องกันแล้วจึงเท่ากับเป็นการเปิดโอกาสให้คนร้ายหรือผู้กระทำผิดสามารถนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดได้สำเร็จ**

เมื่อองค์ประกอบทั้ง 3 ประการเกิดขึ้นในสังคมไทย กล่าวคือ มีผู้กระทำผิดที่มีแรงจูงใจจากบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ทำให้มีโอกาสกระทำผิดสำเร็จและมีโอกาสที่จะรอดพ้นจากกระบวนการยุติธรรมสูง ประกอบกับการมีเป้าหมายที่เหมาะสมทั้งจากการกระทำผิดที่เกิดขึ้นในระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ รวมทั้งสภาพสังคมไทยที่ยังมีระดับการตระหนักรู้ปัญหาอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในระดับต่ำ ในขณะที่กลไกที่ใช้ในการป้องกันเป้าหมายอย่างกฎหมายและผู้บังคับใช้กฎหมายยังขาดศักยภาพ ด้วยปัจจัยต่างๆที่กล่าวมานี้จึงทำให้เกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทยขึ้น ดังสามารถสรุปตามแนวคิดของทฤษฎีกิจวัตรประจำวันได้ตามภาพดังนี้

ภาพที่ 29 สาเหตุการเกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย
ตามแนวคิดทฤษฎีกิจวัตรประจำวัน
(ผู้วิจัย: กิจชัยยะ สุรารักษ์ , 2563)

5.3 แนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัส

จากการศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆ ที่เกี่ยวข้องกับสกุลเงินเข้ารหัสทั้งในต่างประเทศและในประเทศไทยทั้งจากการทบทวนวรรณกรรมและเอกสารที่เกี่ยวข้องรวมทั้งจากการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญทำให้วิเคราะห์ได้ว่า ประเทศต่างๆมีแนวนโยบายเกี่ยวกับการกำกับดูแลสกุลเงินเข้ารหัสในทิศทางที่แตกต่างกันขึ้นอยู่กับสถานการณ์ภายในประเทศ แนวความคิดในทางการเมือง สภาพเศรษฐกิจและบริบทของสภาพสังคมและวัฒนธรรม โดยสามารถแบ่งแนวทางการกำหนดนโยบายตามระดับความเข้มข้นของมาตรการในการควบคุมกำกับดูแลการใช้งานหรือการดำเนินการและการประกอบธุรกิจที่เกี่ยวข้องกับสกุลเงินเข้ารหัสต่างๆออกได้เป็น 3 แนวทาง ได้แก่ แนวนโยบายในลักษณะยอมรับ (ระดับความเข้มข้นต่ำ) แนวนโยบายในลักษณะกึ่งยอมรับกึ่งควบคุม (ระดับความเข้มข้นปานกลาง) และแนวนโยบายในลักษณะไม่ยอมรับ (ระดับความเข้มข้นสูง) โดยสามารถแสดงให้เห็นถึงความแตกต่างของแต่ละแนวนโยบายได้ ดังตารางต่อไปนี้

แนวนโยบายยอมรับ (ความเข้มข้นต่ำ)	**แนวนโยบายกึ่งยอมรับกึ่งควบคุม** (ความเข้มข้นปานกลาง)	**แนวนโยบายไม่ยอมรับ** (ความเข้มข้นสูง)
- มีกฎหมายรองรับสกุลเงินเข้ารหัส - เปิดเสรีในการใช้งานไม่ต้องมีระบบการยืนยันตัวตนผู้ใช้งานหรือมีในระดับต่ำ - สามารถนำไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการในชีวิตประจำวันปกติได้	- มีกฎหมายรองรับสกุลเงินเข้ารหัสและกำกับดูแลการใช้สกุลเงินเข้ารหัสโดยมีการกำหนดบทลงโทษ - มีระบบการขออนุญาตประกอบธุรกิจ - มีระบบการยืนยันตัวตนผู้ใช้งานในระดับปานกลางจนถึงระดับสูง - มีระบบป้องกันการฟอกเงินและการสนับสนุนเงินทุนให้กลุ่มผู้ก่อการร้าย	- ไม่มีการรองรับสกุลเงินเข้ารหัส - ห้ามการทำธุรกิจทุกประเภท - กำหนดบทลงโทษกรณีพบการลักลอบใช้งาน

ตารางที่ 2 แนวนโยบาย กฎหมาย และมาตรการที่เกี่ยวข้องกับสกุลเงินเข้ารหัส
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2563)

จากตารางดังกล่าวสามารถอภิปรายตามแต่ละแนวนโยบายได้ว่า

1) **แนวนโยบายในลักษณะยอมรับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ**

แนวนโยบายในลักษณะนี้จะมีระดับความเข้มข้นของมาตรการในการกำกับดูแลอยู่ในระดับต่ำ ซึ่งแสดงให้เห็นถึงแนวคิดหรือเจตนาของภาครัฐที่ต้องการจะให้เสรีภาพแก่ประชาชนในการใช้งานสกุลเงินเข้ารหัสต่างๆอันอาจเกิดจากปัจจัยประกอบต่างๆ เช่น สภาพสังคมที่มีความพร้อมและคุ้นชินกับเทคโนโลยีและนวัตกรรมสมัยใหม่ หรือความสามารถในการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการพัฒนาระบบเศรษฐกิจในภาพรวมของประเทศ จึงทำให้เกิดการรับรองและส่งเสริมให้ประชาชนใช้งาน โดยแนวนโยบายในลักษณะของการยอมรับนี้จะเป็นลักษณะของการที่รัฐออกกฎหมายหรือให้การรับรองทางกฎหมายให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆถือเป็นสินทรัพย์ประเภทหนึ่งที่อาจมีราคาและอาจถือเอาได้ และในการใช้งานนั้นรัฐจะไม่มีกลไกบังคับใดๆเป็นพิเศษในเรื่องเกี่ยวกับการยืนยันตัวตนผู้ใช้งาน หรือหากมีการนำมาตรการดังกล่าวมาใช้ก็จะกระทำเฉพาะเท่าที่จำเป็น เพื่อการรักษาความสงบเรียบร้อยของสังคมโดยรวมเท่านั้น นอกจากนี้ยังอาจเป็นในลักษณะที่ภาครัฐสนับสนุนส่งเสริมให้มีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในภาค

เศรษฐกิจทั้งในด้านการลงทุนและในภาคเศรษฐกิจครัวเรือนอย่างการนำมาใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการต่างๆในชีวิตประจำวันของประชาชน เป็นต้น

แนวนโยบายในลักษณะของการยอมรับนี้จะมีความเหมาะสมกับประเทศที่มีระดับการเกิดปัญหาอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอยู่ในระดับต่ำและมีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในภาคธุรกิจจนทำให้เกิดการขยายตัวทางเศรษฐกิจที่ดี หรือกล่าวอีกนัยหนึ่งว่าการเกิดขึ้นของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆส่งผลดีต่อภาพรวมในประเทศมากกว่าผลเสียที่จะได้รับ โดยจากการศึกษาพบว่ามีประเทศต่างๆที่มีการดำเนินนโยบายที่เกี่ยวข้องในลักษณะของการยอมรับนี้ ได้แก่ ประเทศสวิตเซอร์แลนด์โดยจะเห็นได้จากการที่มีการพัฒนาปรับปรุงกฎหมายต่างๆ เพื่อให้เกิดการพัฒนาทางเทคโลยีทางการเงิน โดยมีการสนับสนุนให้มีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการชำระค่าบริการต่างๆผ่านโทรศัพท์มือถือเป็นต้น (Jenny Gesley, 2018)

อย่างไรก็ตาม แม้จะมีแนวนโยบายในการยอมรับก็ตามแต่ในปัจจุบันยังไม่มีประเทศใดให้การรับรองให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นเงินหรือวัตถุที่ใช้ชำระหนี้กันได้ตามกฎหมาย (Legal Tender) แต่อย่างใด

2) **แนวนโยบายในลักษณะกึ่งยอมรับกึ่งควบคุมบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ**

เป็นลักษณะของการที่รัฐประเมินสถานการณ์ต่างๆแล้วว่า บิทคอยน์และสกุลเงินเข้ารหัสต่างๆจะเป็นโอกาสในด้านการนำมาใช้ในการพัฒนาทางด้านเศรษฐกิจได้ไม่มากก็น้อย จึงไม่ได้มีแนวนโยบายที่ปิดกั้นหรือห้ามการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆแต่อย่างใด ทั้งยังมีการรับรองสถานะตามกฎหมายเพื่อเปิดช่องให้ประชาชนสามารถใช้ในการประกอบธุรกิจและนำไปซื้อขายแลกเปลี่ยนในลักษณะของการเป็นสินทรัพย์ชนิดหนึ่ง แต่ในขณะเดียวกันรัฐเองก็ได้ประเมินความเสี่ยงในด้านต่างๆ ทั้งผลกระทบที่อาจเกิดต่อระบบเศรษฐกิจโดยรวมหากเกิดการประกอบธุรกิจที่มิชอบ หรือเกิดการลงทุนที่มีลักษณะไม่เป็นปกติ รวมทั้งปัญหาในด้านอื่นๆ เช่น การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการฟอกเงินหรือสนับสนุนเงินทุนให้แก่กลุ่มผู้ก่อการร้าย หรือการกระทำอื่นๆที่อาจส่งผลต่อความสงบเรียบร้อยของสังคม จึงทำให้ภาครัฐต้องมีมาตรการควบคุมอย่างใกล้ชิดเพื่อเป็นการป้องปรามมิให้เกิดลักษณะดังกล่าวได้ แนวนโยบายในรูปแบบนี้จึงมักจะมีการออกกฎหมายหรือการบัญญัติรับรองสถานภาพทางกฎหมายของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆขึ้นเพื่อประโยชน์ในทางเศรษฐกิจและประโยชน์ในทางการบังคับใช้กฎหมาย และยังมีการกำหนดมาตรการต่างๆ เช่น การขออนุญาตจากหน่วยงานภาครัฐเพื่อประกอบธุรกิจ การกำหนดมาตรการการ

ยืนยันตัวตนในระดับปานกลางถึงระดับสูง(ขึ้นอยู่กับการวิเคราะห์ความเสี่ยงที่จะมีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิดของแต่ละประเทศ) และการกำหนดมาตรการเกี่ยวกับการป้องกันการฟอกเงินและการสนับสนุนเงินทุนให้กลุ่มผู้ก่อการร้าย

ผู้วิจัยได้จัดให้ประเทศไทยอยู่ในกลุ่มที่มีแนวนโยบายเกี่ยวกับสกุลเงินเข้ารหัสอยู่ในรูปแบบของการกึ่งยอมรับกึ่งควบคุม เนื่องจากประเทศไทยมีการออกกฎหมาย พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ที่มีการรับรองสถานะให้บิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นสินทรัพย์ดิจิทัลประเภทหนึ่งและมีการออกหลักเกณฑ์ในการควบคุมกำกับดูแลการประกอบธุรกิจและการซื้อขายแลกเปลี่ยนสกุลเงินเข้ารหัส และมีมาตรการการยืนยันตัวตนผ่านมาตรการในการรู้จักลูกค้าของตนเอง (Know Your Customer – KYC) และมีการกำหนดบทบัญญัติเกี่ยวกับการฟอกเงินและให้ถือว่าผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลเป็นสถาบันการเงินตามกฎหมายว่าด้วยการป้องกันปราบปรามการฟอกเงินซึ่งระบุไว้ในกฎหมายดังกล่าว

3) **แนวนโยบายในลักษณะไม่ยอมรับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ**

เป็นรูปแบบของแนวนโยบายที่รัฐมีมุมมองต่อบิทคอยน์และสกุลเงินเข้ารหัสต่างๆว่าเป็นภัยคุกคามที่จะก่อให้เกิดปัญหาต่างๆภายในประเทศหากปล่อยให้มีการใช้งาน เช่น มีมุมมองว่าการลงทุนเก็งกำไรในบิทคอยน์และการระดมทุนต่างๆเป็นสิ่งหลอกลวงหรือเป็นแชร์ลูกโซ่ รวมทั้งมีมุมมองว่าบิทคอยน์และสกุลเงินเข้ารหัสจะถูกนำไปใช้เป็นเครื่องมือในการฟอกเงินและถูกนำไปใช้ในกิจกรรมที่ผิดกฎหมายต่างๆ หรือหากปล่อยให้มีการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสอย่างแพร่หลายแล้วหรืออาจส่งผลกระทบหรือก่อให้เกิดปัญหาในด้านเสถียรภาพทางเศรษฐกิจและความมั่นคงทางการเมืองได้ จึงทำให้รัฐมีการกำหนดแนวนโยบายในการห้ามการใช้งานในทุกรูปแบบ เพื่อเป็นการป้องกันปัญหาแบบเบ็ดเสร็จเด็ดขาด ดังนั้น แนวนโยบายในรูปแบบนี้จึงมีลักษณะเป็นการห้ามและกำหนดให้การใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นสิ่งผิดกฎหมาย และไม่อนุญาตให้มีการประกอบธุรกิจที่เกี่ยวกับสกุลเงินเข้ารหัสทุกประเภท

ประเทศที่มีแนวทางการกำหนดนโยบายเกี่ยวกับสกุลเงินเข้ารหัสในรูปแบบนี้คือประเทศจีน โดยตามที่ได้ศึกษามาแล้วพบว่า ประเทศจีนมีการสั่งห้ามการใช้งาน ห้ามการซื้อขายแลกเปลี่ยนและการประกอบธุรกิจทุกประเภทที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ทั้งยังมีการปราบปรามผู้ลักลอบกระทำผิดด้วย แต่ทั้งนี้เพื่อเป็นการปรับตัวเข้ากับกระแสการเปลี่ยนแปลงทางเทคโนโลยีและนวัตกรรมของโลก จีนจึงมีความพยายามที่จะสร้างสกุลเงินดิจิทัลขึ้นเป็นของตนเอง ซึ่งในปัจจุบัน

สามารถนำออกทดลองใช้ได้แล้วภายใต้ชื่อ “หยวนดิจิทัล” ซึ่งเป็นสกุลเงินดิจิทัลที่ออกและกำกับการดำเนินการต่างๆโดยรัฐบาล อันเป็นการตอกย้ำถึงแนวทางการปฏิเสธบิทคอยน์และสกุลเงินเข้ารหัสต่างๆอย่างชัดเจน

5.4 แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

จากการศึกษาทบทวนวรรณกรรมและจากการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญซึ่งเป็นผู้ทรงคุณวุฒิและผู้เชี่ยวชาญในด้านต่างๆ พบว่าแนวทางในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย สามารถแบ่งออกเป็น 4 ประเภท ได้แก่

1) แนวทางการป้องกันในมิติของการควบคุมการใช้งานบิทคอยน์ด้วยมาตรการบังคับให้มีการลงทะเบียนยืนยันตัวตนผู้ใช้งาน

2) แนวทางการป้องกันในด้านการพัฒนากฎหมาย

3) แนวทางการป้องกันด้านการพัฒนาการบังคับใช้กฎหมาย และ

4) แนวทางการป้องกันในด้านอื่นๆ

โดยสามารถอภิปรายผลการศึกษาตามหัวข้อต่างๆดังนี้

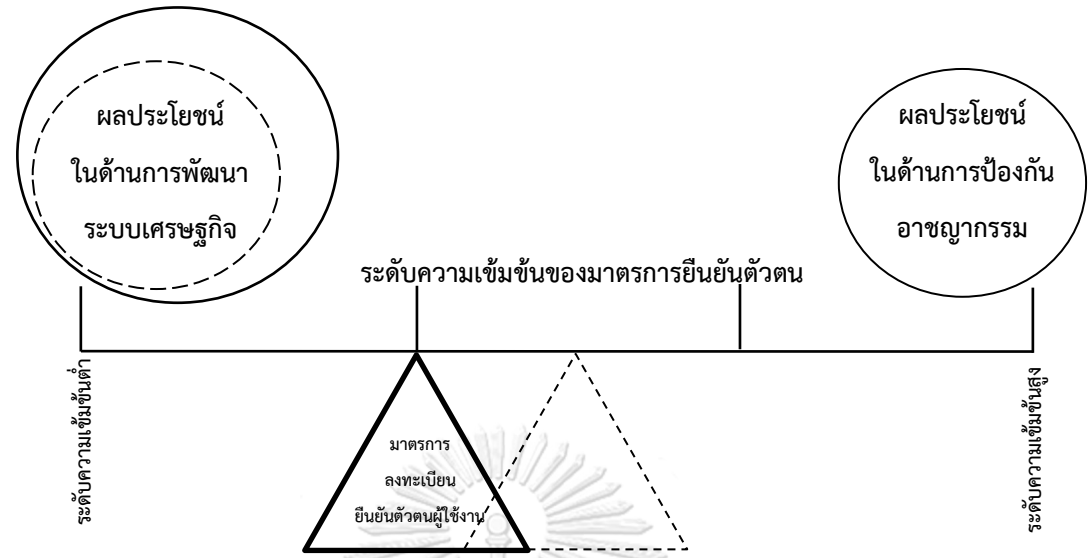
5.4.1 การกำหนดมาตรการบังคับให้มีการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งาน

มาตรการบังคับให้มีการยืนยันตัวตนนี้ เป็นแนวทางในการป้องกันอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัสแนวทางหนึ่งที่เกิดจากสภาพปัญหาและสาเหตุที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ที่มี**ลักษณะพิเศษคือการปกปิดตัวตนผู้ใช้งานที่แท้จริง**จนส่งผลทำให้เกิดเป็นสภาพปัญหาต่างๆ เช่น เจ้าหน้าที่ของรัฐที่มีหน้าที่เกียวข้องไม่สามารถตรวจสอบยืนยันได้ว่าใครเป็นผู้กระทำผิดที่แท้จริง ซึ่งการกำหนดมาตรการบังคับให้ผู้ใช้งานสกุลเงินเข้ารหัสทำการลงทะเบียนยืนยันตัวตนผู้ใช้งานกับหน่วยงานของรัฐนี้ เป็นไปตามแนวคิดในการป้องกันอาชญากรรมในมิติของมาตรการทางกฎหมาย คือ **มาตรการระบบอนุญาต จดทะเบียน และจดแจ้ง (Licensing and Registration) ประกอบกับ มาตรการบังคับและควบคุมด้วยการลงโทษ (Command and Control Regulation)** กล่าวคือผลจากการศึกษาได้เสนอหลักการสำคัญให้มีการกำหนดในกฎหมายให้บุคคลที่จะใช้งานสกุลเงินเข้ารหัสประเภทต่างๆที่รัฐกำหนด จะต้องผ่านการยืนยันและแสดงตนต่อเจ้าหน้าที่ของรัฐ โดยหากฝ่าฝืนไม่ทำการยืนยันตัวตนหรือมีการลักลอบยืนยันตัวตนแทนกันหรือกระทำความผิดที่เกี่ยวข้องในลักษณะอื่นๆจะต้องได้รับโทษทางกฎหมาย เพื่อให้รัฐมีข้อมูลว่าบุคคลใดบ้างที่จะใช้งาน

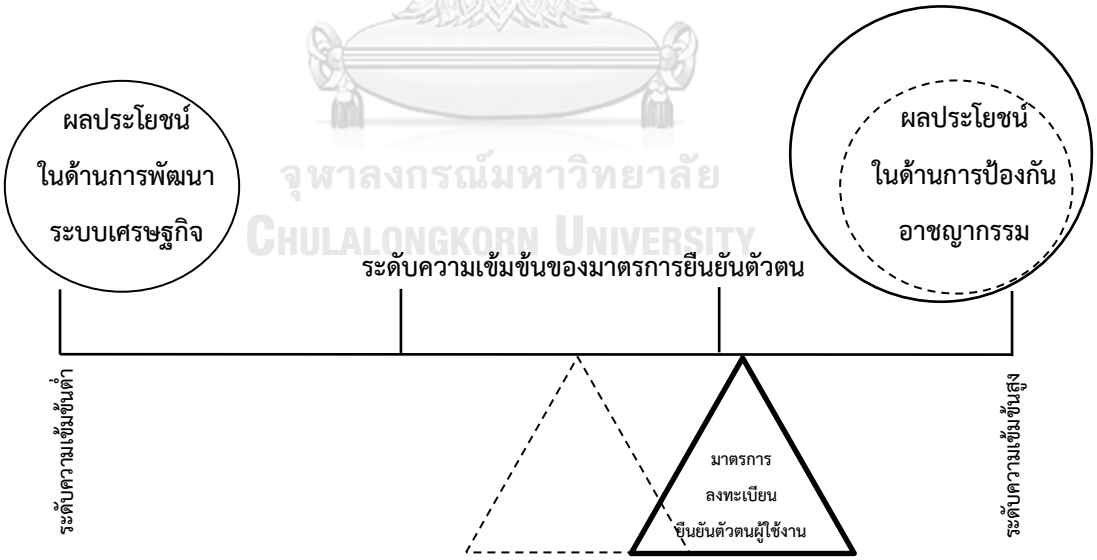
สกุลเงินเข้ารหัสและจะใช้งานจากบัญชีสกุลเงินเข้ารหัสใด ซึ่งหากสามารถดำเนินการตามหลักการและแนวคิดดังกล่าวได้ จะทำให้สภาวะของผู้ใช้งานสกุลเงินเข้ารหัสไม่อยู่ในลักษณะการเป็นบุคคลนิรนามอีกต่อไป อีกทั้งเจ้าหน้าที่ของรัฐจะสามารถตรวจสอบติดตามเพื่อยืนยันตัวผู้กระทำผิดที่แท้จริงโดยอาศัยข้อมูลจากการลงทะเบียนดังกล่าว (Handler) และเมื่อเจ้าหน้าที่ของรัฐสามารถตรวจสอบติดตามบุคคลที่เป็นผู้ใช้งานสกุลเงินเข้ารหัสที่แท้จริงได้แล้วจะส่งผลให้แรงจูงใจที่ทำให้คนร้ายตัดสินใจกระทำผิด (Motivated Offender) ลดหายไปจนอาจส่งผลให้เกิดการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีประสิทธิภาพมากขึ้นเป็นไปตามหลักการในการป้องกันอาชญากรรมตามแนวคิดสามเหลี่ยมอาชญากรรม ที่พัฒนามาจากทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) ว่าหากต้องการจะป้องกันไม่ให้เกิดอาชญากรรมขึ้นจะต้องทำให้องค์ประกอบส่วนของการเสริมแรงจูงใจให้ผู้กระทำผิดหายไป ด้วยการตรวจตราและสอดส่องดูแลผู้กระทำผิดอยู่เสมอ (Handler)

อย่างไรก็ตามจากการเก็บข้อมูลพบว่ามีทั้งผู้ให้ข้อมูลสำคัญที่ให้การสนับสนุนแนวทางการกำหนดมาตรการบังคับให้มีการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานดังกล่าว และในขณะเดียวกันก็มีผู้ที่มีความเห็นแย้งเช่นกัน โดยกลุ่มผู้ให้ข้อมูลที่ให้การสนับสนุนนั้นจะเป็นผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่เป็นฝ่ายที่มีหน้าที่ในการป้องกันปราบปรามอาชญากรรม ซึ่งมีแนวคิดว่าการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสเป็นเรื่องที่จำเป็นเร่งด่วน แม้มาตรการจะกระทบกับสิทธิเสรีภาพและการพัฒนาทางด้านเศรษฐกิจก็ตาม ในขณะที่กลุ่มผู้ให้ข้อมูลที่เป็นผู้เชี่ยวชาญในสกุลเงินเข้ารหัสและเป็นผู้เชี่ยวชาญที่มีหน้าที่กำกับดูแลในเชิงการพัฒนาของภาคเศรษฐกิจยังมองว่าการกำหนดมาตรการบังคับให้มีการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานนี้ยังอาจเกินความจำเป็นและอาจส่งผลกระทบต่อการพัฒนาทางเศรษฐกิจ ซึ่งผู้วิจัยได้วิเคราะห์ก่อนหน้านี้แล้วว่าความขัดแย้งในประเด็นของการป้องกันอาชญากรรมกับการพัฒนาทางเศรษฐกิจนั้น ได้สะท้อนให้เห็นจากความพยายามประนีประนอมของรัฐ เพื่อให้เกิดประโยชน์แก่ประเทศชาติที่สมดุลทั้งสองด้านด้วยการกำหนดนโยบายสาธารณะตามแนวคิดตัวแบบนโยบายสาธารณะแบบกลุ่ม (Group Model) รัฐจึงมีการออก พ.ร.ก.การประกอบธุรกิจดิจิทัล พ.ศ.2561 ดังนั้นผู้วิจัยจึงวิเคราะห์ได้ว่า**การกำหนดมาตรการในการยืนยันตัวตนดังกล่าวจึงจำเป็นจะต้องพิจารณาถึงผลประโยชน์ได้เสียและความเหมาะสมในลักษณะเดียวกัน**

การพิจารณาดังกล่าวสามารถกระทำได้ด้วยการที่**รัฐจะต้องศึกษาและติดตามสถานการณ์การใช้งานสกุลเงินเข้ารหัสต่างๆในประเทศ** ตลอดจนจะต้องรวบรวมข้อมูลที่เกี่ยวข้องเพื่อให้สามารถสรุปข้อมูลสภาพของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสทั้งหมด เพื่อ**ทำการวิเคราะห์ว่าประเด็นปัญหาในเรื่องอาชญากรรมอยู่ในระดับใดเพื่อนำไปชั่งน้ำหนักเปรียบเทียบกับการนำสกุลเงินเข้ารหัสไปใช้ในการพัฒนาระบบเศรษฐกิจ** เพื่อให้ได้ข้อสรุปว่าสถานการณ์ในปัจจุบันนั้น สกุลเงินเข้ารหัสสร้างผลบวกหรือผลเสียให้แก่ประเทศชาติและสังคมส่วนรวมมากกว่ากัน แล้วจึง**กำหนดความเข้มข้นของมาตรการในการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานสกุลเงินเข้ารหัสให้สอดคล้องกับสถานการณ์และสภาพปัญหา** ตัวอย่างเช่นหากรัฐสรุปผลการศึกษาได้ว่า บิทคอยน์ทำให้เกิดการพัฒนาทางเศรษฐกิจส่งผลทำให้รัฐได้ประโยชน์เป็นอย่างมากในขณะที่มีการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมในระดับต่ำ รัฐก็ควรจะกำหนดมาตรการในการยืนยันตัวตนในระดับที่ไม่เข้มข้นมาก เพื่อให้เกิดการใช้งานในด้านการขยายตัวทางเศรษฐกิจ แต่ในทางกลับกันหากข้อมูลที่รัฐศึกษาแสดงให้เห็นว่าสภาพของอาชญากรรมที่ใช้บิทคอยน์เป็นเครื่องมือมีความร้ายแรงกว่าการนำไปใช้ในการพัฒนาทางเศรษฐกิจแล้ว ก็สามารถเปลี่ยนแปลงแนวนโยบายด้วยการเพิ่มความเข้มข้นในมาตรการการยืนยันตัวตน เพื่อเป็นการควบคุมปัญหาอาชญากรรมเป็นสำคัญ ซึ่งแนวคิดดังกล่าวสามารถอธิบายให้เห็นภาพได้ตามหลักแนวคิดตัวแบบนโยบายสาธารณะแบบกลุ่ม (Group Model) ดังนี้



ภาพที่ 30 การวิเคราะห์ข้อมูลเพื่อกำหนดความเข้มข้นของมาตรการในการยืนยันตัวตนผู้ใช้งานสกุลเงินเข้ารหัสตามแนวคิดตัวแบบนโยบายสาธารณะแบบกลุ่ม (Group Model) กรณีที่ผลประโยชน์ในด้านการพัฒนาระบบเศรษฐกิจมีความสำคัญมากกว่า (ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2563)



ภาพที่ 31 การวิเคราะห์ข้อมูลเพื่อกำหนดความเข้มข้นของมาตรการในการยืนยันตัวตนผู้ใช้งานสกุลเงินเข้ารหัสตามแนวคิดตัวแบบนโยบายสาธารณะแบบกลุ่ม (Group Model) กรณีที่ผลประโยชน์ในด้านการป้องกันอาชญากรรมมีความสำคัญมากกว่า (ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2563)

โดยความเข้มข้นของมาตรการการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานในระดับต่างๆ ที่กล่าวถึงนั้น ผู้วิจัยสามารถสรุปและสังเคราะห์ได้จากการศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสของทั้งในต่างประเทศและในประเทศไทย จนสามารถแบ่งเป็นระดับความเข้มข้นซึ่งจะมีความสอดคล้องกันกับรูปแบบของแนวนโยบายที่ได้กล่าวไปแล้ว ดังมีรายละเอียดปรากฏตามตารางต่อไปนี้

แนวนโยบาย/ ระดับความเข้มข้น	**ระดับของ มาตรการยืนยัน ตัวตน**	**รูปแบบของมาตรการ**
แนวนโยบายยอมรับ/ ความเข้มข้นต่ำ	ระดับที่ 1	เปิดเสรีในการใช้งานไม่ต้องยืนยันตัวตนในการใช้งานหรือหากมีก็จะเป็นกรณีเฉพาะรายเท่าที่จำเป็น
แนวนโยบายกึ่งยอมรับกึ่งควบคุม/ ความเข้มข้นปานกลาง	ระดับที่ 2	ยืนยันตัวตนเฉพาะผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่เป็นตัวกลาง
	ระดับที่ 3	ยืนยันตัวตนผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลและผู้ที่ติดต่อซื้อขายแลกเปลี่ยนกับผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่เป็นตัวกลางผ่านมาตรการการรู้จักลูกค้า (Know your Customer หรือ KYC)
	ระดับที่ 4	ยืนยันตัวตนผู้ใช้งานสกุลเงินเข้ารหัสทุกประเภท ทั้งผู้ประกอบธุรกิจและผู้ใช้งานทั่วไปทุกราย
แนวนโยบายไม่ยอมรับ/ ความเข้มข้นสูง	ระดับที่ 5	ห้ามการใช้งานสกุลเงินเข้ารหัสในประเทศ

ตารางที่ 3 ระดับความเข้มข้นและรูปแบบของมาตรการการลงทะเยียนเพื่อ
ยืนยันตัวผู้ใช้งานสกุลเงินเข้ารหัส
(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2563)

นอกจากการวิเคราะห์สภาพปัญหาเพื่อการกำหนดทิศทางและระดับความเข้มข้นของมาตรการในการลงทะเบียนเพื่อยืนยันตัวตนที่เหมาะสมแล้ว เพื่อให้หลักการตามมาตรการดังกล่าว

สามารถนำไปใช้ในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้จริง **จึงจำเป็นจะต้องพัฒนาในด้านเทคนิคคู่ขนานกันไปด้วย** เนื่องจากบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมีลักษณะการใช้งานบนระบบคอมพิวเตอร์หรือระบบเครือข่ายคอมพิวเตอร์ที่ไม่มีศูนย์กลางรวบรวมข้อมูล (Server) ผ่านการใช้งานอุปกรณ์ต่างๆ อย่างเครื่องคอมพิวเตอร์หรือโทรศัพท์มือถือสมารท์โฟน ดังนั้น จึงจำเป็นจะต้องศึกษาและพัฒนาวิธีการทางเทคโนโลยีคอมพิวเตอร์ที่สามารถตรวจสอบและควบคุมผู้ที่ลักลอบใช้งานโดยไม่มีการลงทะเบียนยืนยันตัวควบคู่กันไปด้วย โดยรูปแบบของเครื่องดังกล่าวจะได้กล่าวต่อไป อีกทั้งเพื่อให้การดำเนินการตามมาตรการดังกล่าวเป็นไปอย่างครบถ้วนรอบด้าน รัฐจึงจำเป็น**จะต้องมอบหมายหน้าที่รับผิดชอบให้หน่วยงานของรัฐ หรือจัดตั้งหน่วยงานเฉพาะด้านขึ้นมาเพื่อรับผิดชอบในการ เก็บรวบรวมและรักษาความปลอดภัยข้อมูลที่ได้จากการลงทะเบียนยืนยันตัวตนผู้ใช้งาน** เนื่องจากหากมีการบังคับใช้มาตรการดังกล่าว จะทำให้เกิดข้อมูลผู้ใช้งานสกุลเงินเข้ารหัสเป็นจำนวนมากจึงจำเป็นจะต้องมีผู้รับผิดชอบในการเก็บรวบรวมและรักษาความปลอดภัยข้อมูลดังกล่าวซึ่งถือเป็นข้อมูลบุคคลที่รัฐจะนำไปใช้เพื่อประโยชน์ในการป้องกันอาชญากรรมและรักษาความสงบเรียบร้อยของสังคมส่วนรวมเท่านั้น

5.4.2 แนวทางการป้องกันในด้านการพัฒนากฎหมาย

จากผลการศึกษาทั้งจากการศึกษาค้นคว้าทบทวนวรรณกรรมและการเก็บข้อมูลจากผู้ให้ข้อมูลสำคัญทำให้สามารถเสนอแนวทางในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในมิติทางด้านการพัฒนากฎหมายในประเด็นต่างๆ ได้แก่ **การตีความทางกฎหมายร่วมกันเพื่อกำหนดเป็นหลักปฏิบัติที่ชัดเจนในการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์** เพื่อเป็นการแก้ปัญหาเรื่องสถานภาพของบิทคอยน์ในทางกฎหมายและปัญหาเรื่องการตีความทางกฎหมายที่ไม่ตรงกัน ให้เจ้าหน้าที่ในกระบวนการยุติธรรมมีความเข้าใจในและสามารถปฏิบัติหน้าที่ไปในทิศทางที่ถูกต้องตรงกัน **การบัญญัติกฎหมายเพิ่มเติมเกี่ยวกับการสร้างกระเป๋าเงินอิเล็กทรอนิกส์ (E-Wallet) ของรัฐ** รวมทั้งการกำหนดหลักการและวิธีการในการปฏิบัติเพื่อใช้เป็นเครื่องมือในการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่ถูกใช้ในการกระทำความผิดตลอดจนการปรับปรุงแก้ไขกฎหมายเพิ่มเติมเพื่อรองรับการปฏิบัติหน้าที่ของเจ้าหน้าที่รับผิดชอบให้มีอำนาจในการยึดและอายัดสินตามกฎหมาย ซึ่งผู้วิจัยสามารถวิเคราะห์ได้ว่าแนวทางต่างๆตามที่ได้กล่าวมานี้มีวัตถุประสงค์หลักในการ **สร้างองค์ประกอบที่เหมาะสมในการป้องกันอาชญากรรมตามแนวคิดสามเหลี่ยม**

อาชญากรรมซึ่งพัฒนามาจากทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory) ที่มีหลักการสำคัญว่าหากต้องการจะป้องกันอาชญากรรมต้องทำให้องค์ประกอบที่เกี่ยวกับความเป็นเหยื่อที่เหมาะสมไม่เกิดขึ้นโดยสามารถทำได้ด้วยการทำให้สถานที่ (Place) ที่เป็นเป้าหมายหรือมีความเสี่ยงนั้นมีความปลอดภัยด้วยการบริหารจัดการของผู้ดูแลสถานที่ (Manager) ซึ่งในกรณีนี้การพัฒนากฎหมายให้ครอบคลุมเหมาะสม และสามารถทำหน้าที่เป็นเกราะป้องกันให้แก่สังคมเพื่อไม่ให้สังคมไทยเป็นสถานที่ (Place) หรือสามารถกล่าวอีกนัยหนึ่งได้ว่า การพัฒนาให้กฎหมายไทยให้มีกลไกและมาตรการต่างๆที่มีความพร้อมและครอบคลุมการป้องกันปราบอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสตั้งแต่กระบวนการตีความ การกำหนดขั้นตอนและวิธีการปฏิบัติที่ชัดเจนในการเก็บรวบรวมพยานหลักฐาน ตลอดจนมีหลักกฎหมายที่รับรองการยึดและอายัด จะทำให้สังคมไทยเป็นสังคมที่เข้มแข็งและมีความพร้อมที่จะจัดการกับปัญหาอาชญากรรมเกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ ซึ่งเทียบเคียงได้ว่าถือเป็นการบริหารหรือจัดการ (Manager) ในเรื่องการรักษาความปลอดภัยสังคมเผื่อลดโอกาสการเกิดอาชญากรรมตามแนวคิดสามเหลี่ยมอาชญากรรม

ผลที่จะเกิดขึ้นนอกเหนือจากการสร้างองค์ประกอบในการป้องกันอาชญากรรมตามแนวคิดสามเหลี่ยมอาชญากรรมแล้ว **การที่หลักกฎหมายไทยมีประสิทธิภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสจะทำให้เกิดผลในการข่มขู่ยับยั้งตามทฤษฎีป้องกันหรือทฤษฎีข่มขู่ยับยั้ง (Deterrence Theory)** ที่มีหลักการว่าการที่รัฐมีบทลงโทษที่ชัดเจนจะทำให้เกิดผลในทางการข่มขู่ยับยั้ง 2 ลักษณะคือ การข่มขู่ยับยั้งเฉพาะราย (Specific Deterrence) หมายถึง การที่ผู้กระทำความผิดถูกลงโทษจนเกิดความกลัวและไม่กลับไปกระทำผิดซ้ำอีก และการข่มขู่ยับยั้งทั่วไป (General Deterrence) หมายถึง การที่ประชาชนทั่วไปได้รับรู้รับทราบถึงบทลงโทษที่มีอยู่และเห็นตัวอย่างจากการที่ผู้กระทำผิดถูกลงโทษจนไม่กล้ากระทำผิด โดยในกรณีของการพัฒนากฎหมายไทยดังกล่าวจะทำให้เกิดผลในทางการข่มขู่ยับยั้งทั้งในรูปแบบของ**การข่มขู่ยับยั้งเฉพาะราย (Specific Deterrence)** เช่นในกรณีที่มีการก่ออาชญากรรมเกี่ยวกับสกุลเงินเข้ารหัสขึ้นแล้วเจ้าหน้าที่ที่เกี่ยวข้องมีหลักปฏิบัติที่ชัดเจนจนสามารถตรวจสอบจับกุมและรวบรวมพยานหลักฐานได้อย่างครบถ้วนทั้งยังสามารถยึดและอายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำความผิดได้ จะทำให้เกิดการลงโทษและสร้างผลในการข่มขู่ยับยั้งให้กับตัวผู้กระทำผิดให้เกิดความกลัวและไม่กล้าที่จะกลับไปกระทำความผิดอีก ในขณะที่สังคมทั่วไปจะรับรู้ได้ทั่วไปว่ากฎหมายที่มีอยู่มีหลักปฏิบัติที่ชัดเจนและมีมาตรการในการ

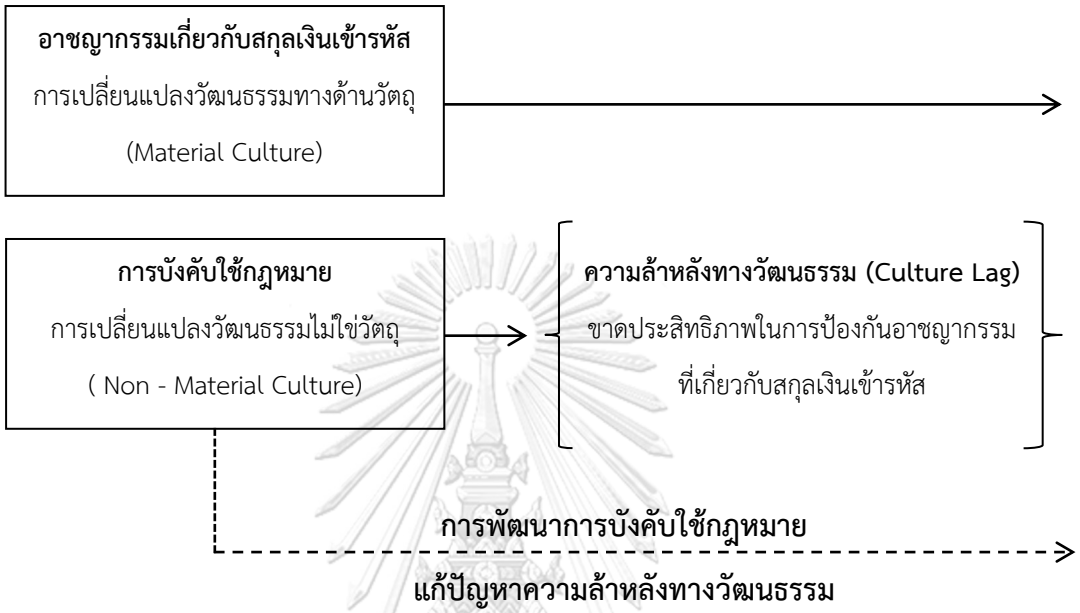
ยึดและอายัดสกุลเงินเข้ารหัสที่มีความพร้อมจนทำให้เกิดผลใน**การข่มขู่ยับยั้งทั่วไป (General Deterrence)** อีกด้วย

5.4.3 แนวทางการป้องกันในด้านการพัฒนาการบังคับใช้กฎหมาย

จากผลการศึกษาสามารถเสนอแนวทางในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในมิติทางด้านการพัฒนาองค์ความรู้ให้แก่ผู้บังคับใช้กฎหมายโดยการ**พัฒนาวิธีการ เครื่องมือหรือกลไกการป้องกันรูปแบบใหม่ที่จะสามารถป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ** สืบเนื่องจากสภาพปัญหาที่ในปัจจุบันเจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องยังขาดวิธีการรวมทั้งยังไม่มีเครื่องมือและกลไกเฉพาะที่จะสามารถตรวจสอบติดตามเส้นทางธุรกรรมทางการเงินและตรวจพิสูจน์ยืนยันตัวบุคคลได้อย่างมีประสิทธิภาพ จึงได้มีการเสนอให้มีการศึกษาวิจัยและพัฒนาเครื่องมือสมัยใหม่ เช่น **โปรแกรมปัญญาประดิษฐ์ที่สามารถตรวจจับการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำความผิด (AI Platform)** และ**การสร้างฐานข้อมูลภาครัฐเกี่ยวกับการป้องกันอาชญากรรม (Big Data)** ขึ้นเพื่อเป็นเครื่องมือและกลไกสมัยใหม่ที่จะสามารถนำไปใช้ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมี ประสิทธิภาพ นอกจากนี้ผู้ให้ข้อมูลสำคัญยังได้เสนอแนวทางใน**การสร้างความร่วมมือระหว่างหน่วยงานภาครัฐและภาคเอกชน รวมทั้งการสร้างความร่วมมือกับหน่วยงานในต่างประเทศ** เพื่อให้เกิดประโยชน์ในเรื่องของการระดมสรรพกำลังและเป็นการดึงเอาศักยภาพและองค์ความรู้ต่างๆมาใช้ร่วมกันเพื่อแก้ปัญหาอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ตลอดจนการส่งต่อข้อมูลสำคัญต่างๆที่จะทำให้การตรวจสอบติดตามเส้นทางธุรกรรมทางการเงิน การพิสูจน์ยืนยันตัวตนผู้กระทำความผิด ตลอดจนกระบวนการดำเนินคดีในกระบวนการยุติธรรมมีประสิทธิภาพมากยิ่งขึ้น

แนวทางการป้องกันอาชญากรรมดังกล่าวนี้ตอบรับ**การแก้ไขปัญหาตามแนวคิดของทฤษฎีความล้าหลังทางสังคม (Culture Lag Theory)** ที่มองว่าอาชญากรรมเป็นผลมาจากการสังคมมีการเปลี่ยนแปลงวัฒนธรรมทางวัตถุ (Material Culture) อย่างรวดเร็ว ซึ่งในที่นี้คือการรับเอานวัตกรรมสมัยใหม่อย่างบิทคอยน์และสกุลเงินเข้ารหัสต่างๆมาใช้ในการกระทำความผิด ในขณะที่การเปลี่ยนแปลงวัฒนธรรมที่ไม่ใช่วัตถุ (Non – Material Culture) คือแนวคิด วิธีการ เครื่องมือและกลไก รวมทั้งการสร้างความร่วมมือต่างๆที่จะใช้ในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสนั้น ยังปรับตัวตามไม่ทันจนเกิดความล้าหลังของกลไกของรัฐทำให้เกิดเป็นช่องว่างและเกิดเป็นปัญหา

อาชญากรรมขึ้น ดังนั้นจึงอาจกล่าวได้ว่าแนวทางนี้เป็น**ความพยายามที่จะพัฒนาและปรับปรุงให้รัฐสามารถปรับตัวก้าวตามปัญหาอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสให้ทันท่วงที** ซึ่งจะเกิดผลในการเพิ่มศักยภาพในการป้องกันอาชญากรรมดังสามารถแสดงให้เห็นได้ตามภาพดังนี้



ภาพที่ 32 การป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ด้วยการพัฒนาวิธีการบังคับใช้กฎหมาย (ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2563)

แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในด้านการพัฒนาการบังคับใช้กฎหมายสร้างนี้ เป็น**แนวทางที่จะทำให้องค์ประกอบการเกิดอาชญากรรมตามแนวคิดสามเหลี่ยมอาชญากรรมซึ่งพัฒนามาจากทฤษฎีกิจวัตรประจำวัน (Routine Activity Theory)** ที่มีหลักการสำคัญว่าหากต้องการจะป้องกันอาชญากรรมต้องทำให้องค์ประกอบที่เกี่ยวกับการเป็นเป้าหมายที่เหมาะสมไม่เกิดขึ้น (Suitable Target) ไม่เกิดขึ้น ด้วยการเพิ่มความสามารถในการป้องกันเป้าหมาย (Capable Guardian) โดยในที่นี้การพัฒนาศักยภาพการบังคับใช้กฎหมายให้เท่าทันกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสจะทำให้เกิดลักษณะของการป้องกันเป้าหมายที่เข้มแข็งและส่งผลให้เกิดการป้องกันอาชญากรรมที่มีประสิทธิภาพ

5.4.4 แนวทางการป้องกันในด้านอื่นๆ

นอกจากแนวทางการกำหนดมาตรการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานสกุลเงินเข้ารหัสซึ่งถือเป็นการแก้ปัญหาลักษณะพิเศษของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ รวมทั้งการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในด้านการพัฒนากฎหมายและการพัฒนาผู้บังคับใช้กฎหมายแล้ว ผู้ให้ข้อมูลสำคัญยังได้เสนอแนวทางที่มีลักษณะเป็นมาตรการเสริม หรือแนวทางที่จะทำให้เกิดประสิทธิภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสมากขึ้น ได้แก่ **การผลักดันให้มีการสร้างสกุลเงินดิจิทัลแห่งชาติและผลักดันให้มีการนำมาใช้งาน** เพื่อสร้างตัวเลือกในด้านเทคโนโลยีทางการเงินให้แก่ประชาชนอันจะนำไปสู่การพัฒนาระบบเศรษฐกิจให้เท่าทันนานาอารยประเทศ และยังถือเป็นการเตรียมความพร้อมกรณีที่รัฐจำเป็นต้องกำหนดนโยบายในการห้ามใช้งานสกุลเงินเข้ารหัสอื่นๆ ในกรณีที่บิทคอยน์และสกุลเงินเข้ารหัสต่างๆสร้างความเสียหายให้แก่สังคมไทยโดยรวม ซึ่งการสร้างสกุลเงินดิจิทัลแห่งชาติอาจมีส่วนช่วยในการแก้ปัญหาการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรม เนื่องจากสกุลเงินดิจิทัลแห่งชาติจะถูกสร้างโดยธนาคารแห่งประเทศไทยและมีการค้ำประกันมูลค่าด้วยเงินบาท ทั้งยังสามารถนำไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการต่างๆได้ในลักษณะคล้ายกันกับสกุลเงินเข้ารหัสแต่มีความน่าเชื่อถือมากกว่า ซึ่งขณะนี้ในประเทศไทยได้เริ่มมีการศึกษาและพัฒนาแล้วภายใต้ชื่อโครงการ “อินทนนท์”

นอกจากนี้ยังจำเป็นจะต้องสร้างความรับรู้ให้แก่ประชาชนและสังคมโดยรวม ในเรื่องที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เพื่อเป็นการสร้างกลไกการป้องกันตัวเองให้แก่ประชาชน ซึ่งตรงกับแนวคิดของการให้ความรู้และการบังคับให้เปิดเผยข้อมูลสำคัญ (Education and Disclosure Regulation) ตามแนวคิดการป้องกันอาชญากรรมด้วยมาตรการทางกฎหมาย (อภิชน จันทรเสน, 2561) โดยสามารถกระทำได้ในรูปแบบต่างๆเช่น การประชาสัมพันธ์ให้ประชาชนได้รับทราบเมื่อมีการแก้ไขปรับปรุงตัวบทกฎหมาย ที่อาจกระทบต่อการใช้ชีวิตตามปกติของประชาชน การจัดอบรมให้ความรู้เกี่ยวกับกฎหมายต่างๆ หรือแม้กระทั่งการรายงานข่าวหรือเผยแพร่ผลการจับกุมและการลงโทษต่างๆ

5.4.5 บทสรุปแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

จากการวิเคราะห์และอภิปรายแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย ทำให้สามารถสรุปผลตามแนวคิดของทฤษฎีกิจวัตรประจำวัน (Routine Activity

Theory) ได้ว่าแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทยนี้ ทำให้เกิดการป้องกันด้วยการสร้างองค์ประกอบสำคัญสามประการ คือ

1) การดูแลสอดส่องอย่างใกล้ชิด (Handler) ผ่านมาตรการการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานสกุลเงินเข้ารหัส

การกำหนดให้มีมาตรการในการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ จะทำให้เกิดการสอดส่องดูแลผู้กระทำผิดหรือผู้ที่จะกระทำผิดอย่างใกล้ชิด และยังทำให้สภาวะความเป็นบุคคลนิรนามของการใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆถูกทำลายไป จึงทำให้ปัจจัยที่เกิดเป็นผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender) ไม่เกิดขึ้น ดังนั้นเมื่อไม่มีผู้กระทำผิดที่ได้รับแรงจูงใจจากบิทคอยน์และสกุลเงินเข้ารหัสต่างๆแล้ว การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมก็จะไม่เกิดขึ้น

2) การทำหน้าที่ในการจัดการด้านการรักษาความปลอดภัยให้แก่สังคมด้วยการพัฒนากฎหมาย (Manager)

การพัฒนาให้กฎหมายไทยให้มีกลไกและมาตรการต่างๆที่มีความพร้อมและครอบคลุมการป้องกันปราบอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสตั้งแต่กระบวนการตีความ การกำหนดขั้นตอนและวิธีการปฏิบัติที่ชัดเจนในการเก็บรวบรวมพยานหลักฐาน ตลอดจนมีหลักกฎหมายที่รับรองการยึดและอายัด จะทำให้สังคมไทยเป็นสังคมที่เข้มแข็งและมีความพร้อมที่จะจัดการกับปัญหาอาชญากรรมเกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ ซึ่งเทียบเคียงได้ว่าถือเป็นการบริหารหรือจัดการ (Manager) ในเรื่องการรักษาความปลอดภัยสังคมเผื่อลดโอกาสการเกิดอาชญากรรมตามแนวคิดสามเหลี่ยมอาชญากรรม

3) การเพิ่มความสามารถในการป้องกันเป้าหมาย (Capable Guardian) ด้วยการพัฒนาการบังคับใช้กฎหมาย

การพัฒนาศักยภาพของผู้บังคับใช้กฎหมายทั้งในมิติของการพัฒนาองค์ความรู้ การปรับแนวทางและทัศนคติให้เกิดการป้องกันเชิงรุก การศึกษาและพัฒนาวิธีการ เครื่องมือหรือกลไกพิเศษที่จะสามารถตรวจสอบติดตามเส้นทางธุรกรรมทางการเงินและการพิสูจน์ยืนยันตัวบุคคลผู้กระทำความผิด ตลอดจนการสร้างความร่วมมือระหว่างหน่วยงานภาครัฐ ภาคเอกชน และการสร้างความร่วมมือกับต่างประเทศ ถือเป็นการเพิ่มความสามารถหรือเพิ่มศักยภาพให้แก่เจ้าหน้าที่ของรัฐซึ่ง

มีหน้าที่ในการป้องกันเป้าหมายหรือสถานที่ ตามแนวคิดการป้องกันอาชญากรรมตามทฤษฎีกิจวัตรประจำวัน

เมื่อองค์ประกอบทั้ง 3 ประการเกิดขึ้นในสังคมไทย ประกอบกับการมีมาตรการเพื่อส่งเสริมต่างๆ ได้แก่ การผลักดันให้มีการสร้างและนำสกุลเงินดิจิทัลแห่งชาติมาใช้งาน การสร้างความตระหนักรู้ให้แก่ประชาชนและสังคมโดยรวม ก็จะส่งผลให้เกิดการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทยที่มีประสิทธิภาพซึ่งสามารถแสดงให้เห็นแนวคิดดังกล่าวตามภาพดังนี้

ภาพที่ 33 แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย ตามแนวคิดทฤษฎีกิจวัตรประจำวัน

(ผู้วิจัย: กิจชัยยะ สุรารักษ์, 2563)

บทที่ 6
สรุปผลการวิจัยและข้อเสนอแนะ

6.1 สรุปผลการศึกษา

การศึกษาเรื่อง “แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: ศึกษากรณีบิทคอยน์” มีวัตถุประสงค์เพื่อศึกษาถึงลักษณะรูปแบบ สภาพปัญหาและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ ศึกษาแนวนโยบาย กฎหมาย และมาตรการต่าง ๆ ที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ การศึกษาครั้งนี้เป็นการวิจัยเชิงคุณภาพ โดยผู้วิจัยได้ใช้วิธีการศึกษาข้อมูลจากเอกสารวิชาการ งานวิจัย บทความ วิทยานิพนธ์ ตลอดจนสื่อต่างๆทั้งในประเทศและต่างประเทศ ประกอบกับการศึกษาวิจัยภาคสนามซึ่งใช้การเก็บข้อมูลด้วยการสัมภาษณ์เชิงลึก (In-depth Interview) จากผู้ให้ข้อมูลสำคัญ 4 กลุ่ม ได้แก่ กลุ่มที่ 1 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในเรื่องสกุลเงินเข้ารหัสทั้งในส่วนภาครัฐและภาคเอกชน กลุ่มที่ 2 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญทางด้านกฎหมายเกี่ยวกับสกุลเงินเข้ารหัส กลุ่มที่ 3 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญหรือผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส และ กลุ่มที่ 4 ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการเสนอแนวทางในการป้องกันอาชญากรรม เพื่อนำข้อมูลมาวิเคราะห์และเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือที่เหมาะสมกับบริบทของประเทศไทย โดยผู้วิจัยสามารถสรุปผลการวิจัยครั้งนี้ตามคำถามการวิจัยและวัตถุประสงค์ของการวิจัยดังต่อไปนี้

6.1.1 ลักษณะรูปแบบ สภาพปัญหาและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ

6.1.1.1 ลักษณะและรูปแบบของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ

จากการศึกษารวบรวมข้อมูลต่างๆพบว่ามีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นเครื่องมือในการก่ออาชญากรรม 2 รูปแบบคือ **การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ก่ออาชญากรรมโดยตรง** ซึ่งเป็นลักษณะที่ผู้กระทำผิดมีการนำบิทคอยน์และสกุลเงินเข้ารหัสไปใช้

งานจริงในรูปแบบต่างๆ ซึ่งการกระทำความผิดที่จัดอยู่ในประเภทนี้ประกอบไปด้วย การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย เช่น การลักลอบซื้อขายยาเสพติด การลักลอบซื้อขายอาวุธปืน การว่าจ้างให้ผู้อื่นกระทำความผิดแล้วชำระค่าจ้างเป็นบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ การซื้อขายสื่อลามกอนาจาร การเรียกค่าไถ่และการใช้โปรแกรมเรียกค่าไถ่ (Ransomware) แล้วเรียกร้องให้ชำระค่าไถ่เป็นบิทคอยน์ การระดมเงินทุนของกลุ่มผู้ก่อการร้ายผ่านบิทคอยน์ และการฟอกเงินด้วยบิทคอยน์ โดยที่การนำบิทคอยน์ไปใช้ในการกระทำความผิดในทางตรงนี้ เป็นลักษณะและรูปแบบที่ผู้วิจัยมุ่งจะศึกษาเนื่องจากเป็นลักษณะการกระทำความผิดที่มีการนำเทคโนโลยีมาพัฒนารูปแบบและวิธีการให้มีความสลับซับซ้อนและยากต่อการตรวจสอบติดตามของเจ้าหน้าที่ของรัฐ

ลักษณะและรูปแบบอีกรูปแบบหนึ่งคือ**การนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมทางอ้อม** ได้แก่ การฉ้อโกงหลอกลวงเพื่อให้เหยื่อหลงเชื่อว่าจะมีการนำเงินไปลงทุนจากการเก็งกำไรในมูลค่าของบิทคอยน์ การหลอกลวงว่าจะมีการนำเงินไปลงทุนในการขุดบิทคอยน์ รวมทั้งการฉ้อโกงหลอกลวงในรูปแบบอื่นๆที่มีการนำเอาชื่อของบิทคอยน์และสกุลเงินเข้ารหัสอื่นๆไปแอบอ้าง ซึ่งการกระทำผิดในลักษณะนี้ไม่อยู่ในขอบเขตของการศึกษาครั้งนี้เนื่องจากผู้วิจัยมีมุมมองว่า **ไม่ได้มีการนำบิทคอยน์ไปใช้ในการกระทำความผิดอย่างแท้จริงแต่อย่างใด** เพียงเป็นการนำชื่อ “บิทคอยน์” หรือชื่อของกิจกรรมการลงทุนที่เกี่ยวกับบิทคอยน์ ไปกล่าวอ้างเพื่อให้เหยื่อหลงเชื่อเท่านั้น หรืออาจกล่าวได้ว่าบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆไม่ใช่สาระสำคัญหรือวัตถุในการกระทำความผิดแต่อย่างใด เพราะวัตถุที่นำมาใช้ในการหลอกลวงหรือฉ้อโกงประชาชนในลักษณะนี้ สามารถเปลี่ยนแปลงไปได้เสมอตามแต่ค่านิยมของคนในสังคมในแต่ละยุคสมัย เช่น เปลี่ยนจากการหลอกลวงให้มาลงทุนในบิทคอยน์ เป็น การหลอกลวงให้นำเงินมาลงทุนใน ราคาน้ำมัน ทองคำ การลงทุนด้วยการเปรียบต่างค่าเงินสกุลต่างๆ (Forex) เป็นต้น

สำหรับในประเทศไทยนั้น พบว่ามีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมโดยตรงที่ปรากฏขึ้นชัดเจน ได้แก่ การฟอกเงินด้วยการนำเอาเงินผลประโยชน์ที่ได้จากการกระทำความผิดมาเปลี่ยนเป็นบิทคอยน์หรือสกุลเงินเข้ารหัสอื่นๆ และการใช้โปรแกรมเรียกค่าไถ่ (Ransomware) เพื่อเข้าโจมตีเครื่องคอมพิวเตอร์หรือระบบคอมพิวเตอร์แล้วเรียกร้องให้มีการจ่ายค่าไถ่เป็นบิทคอยน์ ส่วนที่ยังปรากฏไม่ชัดเจนคือ การนำบิทคอยน์ไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย และรูปแบบของการกระทำผิดที่ผู้วิจัยพบจากการศึกษา

ทบทวนวรรณกรรมและเอกสารทางวิชาการที่เกี่ยวข้องแต่ไม่พบว่ามีการกระทำผิดตามลักษณะดังกล่าวในประเทศไทย คือ การสนับสนุนเงินทุนให้แก่กลุ่มผู้ก่อการร้ายผ่านบิทคอยน์

6.1.1.2 สภาพปัญหาและสาเหตุอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือ

ผลการศึกษาพบว่าอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกลเงินเข้ารหัสเป็นเครื่องมือมีสภาพปัญหาและสาเหตุสำคัญ 3 ปัจจัย คือ

1) สภาพปัญหาและสาเหตุจาก "บิทคอยน์"

คุณลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่ไม่มีรูปร่าง ไม่สามารถจับต้องได้ มีระบบการทำงานและเก็บข้อมูลบนเครือข่ายคอมพิวเตอร์ที่ไม่มีฐานข้อมูลกลาง (Server) แต่ใช้ระบบการกระจายข้อมูลที่ให้ผู้ใช้งานสามารถซื้อขายแลกเปลี่ยนกันได้โดยตรง (Peer – to - Peer) โดยไม่จำเป็นต้องผ่านการตรวจสอบจากรัฐบาลหรือตัวกลางอย่างธนาคารหรือสถาบันการเงิน สามารถนำไปใช้งานได้จากทั่วทุกมุมโลกโดยไม่ติดข้อจำกัดเรื่องเขตแดนของรัฐ (Borderless) และคุณลักษณะพิเศษที่สำคัญคือการที่ผู้ใช้งานไม่จำเป็นต้องทำการยืนยันหรือแสดงตัวตนที่แท้จริง ทำให้เจ้าหน้าที่ของรัฐไม่สามารถตรวจสอบติดตามเส้นทางธุรกรรมทางการเงินและตรวจพิสูจน์ยืนยันตัวบุคคลได้ จนทำให้อาชญากรเล็งเห็นประโยชน์และนำไปก่ออาชญากรรม

2) สภาพปัญหาและสาเหตุจาก “กฎหมาย”

จากการศึกษาสภาพปัญหาและสาเหตุของการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมในประเด็นที่เกี่ยวข้องกับกฎหมาย ทำให้พบว่ากฎหมายต่างๆที่เกี่ยวข้องยังไม่สามารถทำหน้าที่เป็นกลไกในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ และก่อให้เกิดสภาพปัญหาต่างๆทั้งในด้านการกำหนดสถานภาพความเป็นทรัพย์และทรัพย์สิน การตีความเพื่อเก็บพยานหลักฐานต่างๆ ตลอดจนยังขาดกฎหมายที่เกี่ยวข้องที่มีลักษณะเป็นกฎหมายวิธีสบัญญัติที่จะกำหนดขั้นตอนและวิธีการปฏิบัติที่ชัดเจนรวมทั้งให้อำนาจในการดำเนินการต่างๆให้แก่เจ้าหน้าที่ผู้ปฏิบัติงาน อีกทั้งเมื่อศึกษาถึงกฎหมายที่กำกับดูแลเกี่ยวกับสกุลเงินเข้ารหัสโดยตรงอย่าง พ.ร.ก.การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 พบว่าแม้จะมีเจตนารมณ์ในการป้องกันไม่ให้มีการนำสกุลเงินเข้ารหัส ซึ่งถือเป็นสินทรัพย์ดิจิทัลประเภทหนึ่งไปใช้ในการก่ออาชญากรรมหรือนำไปใช้ในกิจกรรมที่ผิดกฎหมายก็ตาม แต่ปรากฏว่ากลไกและมาตรการ

ต่างๆที่บัญญัติในกฎหมายยังเป็นไปเพื่อให้เอื้อต่อการเกิดการพัฒนาทางเศรษฐกิจและการเปิดรับให้เกิดการนำเทคโนโลยีทางการเงินมาใช้ภายใต้การกำกับดูแลของรัฐเป็นวัตถุประสงค์หลัก จึงทำให้ยังไม่สามารถเป็นกลไกในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้

3) สภาพปัญหาและสาเหตุจาก “การบังคับใช้กฎหมาย”

สภาพปัญหาที่เจ้าหน้าที่ของรัฐที่มีหน้าที่เกี่ยวข้องขาดศักยภาพในการบังคับใช้กฎหมายที่มีประสิทธิภาพ อันเกิดจากการขาดองค์ความรู้ที่เกี่ยวข้องกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ การขาดวิธีการ เครื่องมือ กลไกที่สามารถช่วยในการตรวจสอบติดตามเส้นทางธุรกรรมทางการเงินและการตรวจพิสูจน์ยินยันตัวผู้บุคคลผู้กระทำผิด ตลอดจนยังขาดความร่วมมือในการทำงานร่วมกันระหว่างหน่วยงานของรัฐด้วยกันหน่วยงานภาคเอกชน โดยเฉพาะอย่างยิ่งผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ที่ถือเป็นผู้เชี่ยวชาญที่อาจมีส่วนช่วยในกระบวนการป้องกันและปราบปรามอาชญากรรม รวมทั้งยังขาดการประสานงานกับหน่วยงานที่เกี่ยวข้องในต่างประเทศอย่างเป็นรูปธรรม ส่งผลให้การป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสขาดประสิทธิภาพ

6.1.2 แนวนโยบาย กฎหมายและมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสในต่างประเทศและในประเทศไทย

จากการศึกษาพบว่า ประเทศต่างๆมีการกำหนดแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวข้องกับสกุลเงินเข้ารหัสที่แตกต่างกัน อันเนื่องมาจากความแตกต่างทางด้านสถานการณ์ภายในประเทศ แนวความคิดทางการเมือง สภาพเศรษฐกิจและบริบทของสภาพสังคมและวัฒนธรรม โดยสามารถแบ่งแนวนโยบายที่เกี่ยวกับสกุลเงินเข้ารหัสต่างๆออกเป็น 3 แนวนโยบาย ได้แก่ **แนวนโยบายในลักษณะยอมรับ (ระดับความเข้มข้นต่ำ)** จะมีลักษณะของแนวนโยบายที่เปิดกว้างให้ประชาชนในรัฐสามารถใช้งานได้อย่างเสรี มีการออกกฎหมายหรือกำหนดในบทบัญญัติของกฎหมายเพื่อรับรองว่าบิทคอยน์และสกุลเงินเข้ารหัสต่างๆเป็นทรัพย์สินชนิดหนึ่งและสามารถนำไปใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการตามปกติที่ใช้ในชีวิตประจำวันได้ **แนวนโยบายในลักษณะกึ่งยอมรับกึ่งควบคุม (ระดับความเข้มข้นปานกลาง)** คือการรับรองสถานภาพให้กับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ แต่ยังมีการกำกับดูแลที่เข้มงวด เช่น มีระบบการขออนุญาตประกอบกิจการที่เกี่ยวข้อง มีมาตรการยืนยันตัวตนผู้ใช้งานในระดับต่างๆที่เหมาะสมของแต่ละประเทศ และมีมาตรการในการป้องกันนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการฟอกเงินและการสนับสนุนเงินทุนให้ผู้ก่อการร้าย และ **แนวนโยบายในลักษณะการไม่ยอมรับบิทคอยน์และสกุล**

เงินเข้ารหัสต่างๆ (ระดับความเข้มข้นสูง) ที่ไม่อนุญาตให้มีการใช้งานและไม่อนุญาตให้มีการดำเนินการใดๆ รวมทั้งการประกอบธุรกิจและการระดมทุนที่เกี่ยวข้องกับสกุลเงินเข้ารหัสทั้งหมด และมีการกำหนดบทลงโทษสำหรับผู้ฝ่าฝืน โดยในส่วนของประเทศสามารถจัดอยู่ในกลุ่มของประเทศที่มีนโยบายในลักษณะลักษณะกึ่งยอมรับกึ่งควบคุม (ระดับความเข้มข้นปานกลาง)

6.1.3 แนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสเป็นเครื่องมือในประเทศไทย

6.1.3.1 การกำหนดมาตรการบังคับให้มีการลงทะเบียนเพื่อยืนยันตัวตนผู้ใช้งานบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ

เพื่อเป็นการแก้ปัญหาในประเด็นเรื่องของการไม่สามารถยืนยันตัวตนผู้ใช้งานที่แท้จริงของบิทคอยน์และสกุลเงินเข้ารหัสได้ จึงจำเป็นที่ภาครัฐจะต้องกำหนดให้มีมาตรการในการยืนยันตัวตนผู้ใช้งานที่แท้จริง เพื่อประโยชน์ในการเพิ่มศักยภาพในการตรวจสอบติดตามและยืนยันตัวผู้ใช้งานที่แท้จริงที่นำบิทคอยน์และสกุลเงินเข้ารหัสไปใช้ในการกระทำความผิด โดยจำเป็นจะต้องอาศัยวิธีทางเทคนิคหรือองค์ความรู้ทางวิศวกรรมคอมพิวเตอร์มาพัฒนาออกแบบรูปแบบและวิธีการเพื่อให้สามารถนำแนวทางไปปฏิบัติได้จริง ทั้งนี้ยังจะต้องมีการปรับปรุงกฎหมายให้มีบทกำหนดโทษที่มีความรุนแรงเกี่ยวกับการฝ่าฝืนการยืนยันตัวตน หรือการลักลอบยืนยันตัวตนแทนกัน หรือการกระทำความผิดที่มีลักษณะใกล้เคียงกัน เพื่อให้เกิดการบังคับใช้มาตรการที่เกิดประสิทธิภาพ ทั้งนี้การกำหนดมาตรการดังกล่าวอาจกระทบต่อสิทธิเสรีภาพและส่งผลกระทบต่อการพัฒนาทางเศรษฐกิจและเทคโนโลยีทางการเงิน ดังนั้น เพื่อให้การกำหนดมาตรการดังกล่าวมีระดับความเข้มข้นที่เป็นไปอย่างเหมาะสม สามารถสร้างความสมดุลให้เกิดขึ้นสอดคล้องกับสถานการณ์ต่างๆ ภาครัฐหรือเจ้าหน้าที่ของรัฐที่เกี่ยวข้องควรจะต้องทำการศึกษาข้อมูลที่เกี่ยวข้องทั้งในเรื่องของสภาพอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสและประโยชน์ที่จะได้รับในทางการพัฒนาเศรษฐกิจ เพื่อให้สามารถสร้างความสมดุลระหว่างการป้องกันอาชญากรรมและการพัฒนาเศรษฐกิจต่อไป

6.1.3.2 การกำหนดหลักปฏิบัติในการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ที่ชัดเจน

บุคลากรในกระบวนการยุติธรรมจำเป็นอย่างยิ่งที่จะต้องมีกาหารือและตีความทางกฎหมายที่เกี่ยวกับการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ร่วมกัน

เพื่อให้เกิดการกำหนดข้อสรุปที่ชัดเจน อันจะนำไปสู่การกำหนดแนวทางการปฏิบัติที่ชัดเจนว่าเจ้าหน้าที่ที่มีหน้าที่เก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์นั้น จะต้องใช้หลักการตามกฎหมายใดในการปฏิบัติหน้าที่ หรือหากหลักกฎหมายที่มีอยู่ในปัจจุบันยังไม่ครอบคลุมหรือล้าสมัยไม่ทันต่อเหตุการณ์และสภาพปัญหาในปัจจุบันจำเป็นจะต้องมีการพิจารณาแก้ไขเพิ่มเติมอย่างไร โดยหลังจากที่ได้ข้อยุติแล้วจะต้องมีการออกประกาศหรือคำสั่งแจ้งเวียนให้ทุกหน่วยงานที่เกี่ยวข้องทราบ รวมทั้งจัดให้มีการอบรม เผยแพร่ความรู้ ให้เจ้าหน้าที่ในกระบวนการยุติธรรมทุกภาคส่วนรับทราบและมีความเข้าใจที่ถูกต้องตรงกัน อีกทั้งควรจะต้องจัดทำรายละเอียดข้อสรุปดังกล่าวให้อยู่ในรูปแบบของหนังสือ ตำรา หรือ คู่มือการปฏิบัติงานเกี่ยวกับการเก็บรวบรวมพยานหลักฐานที่อยู่ในรูปแบบอิเล็กทรอนิกส์ เพื่อให้เกิดการพัฒนาองค์ความรู้อย่างต่อเนื่องและเป็นการสร้างหลักปฏิบัติที่ชัดเจนให้แก่เจ้าหน้าที่ผู้ปฏิบัติงาน ซึ่งจะส่งผลให้กระบวนการยุติธรรมไทยมีการดำเนินการในเรื่องดังกล่าวที่เป็นไปในทิศทางเดียวกัน

6.1.3.3 การสร้างกระเป๋าเงินอิเล็กทรอนิกส์ (E - Wallet) ของรัฐ เพื่อใช้เป็นเครื่องมือหลักในการยึดหรืออายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่ใช้ในการกระทำผิดกฎหมาย

ประเทศไทยควรมีการออกกฎหมายเกี่ยวกับการสร้างและการใช้งานกระเป๋าเงินอิเล็กทรอนิกส์ (E - Wallet) ของรัฐเพื่อเป็นเครื่องมือหลักในการยึดและอายัด ตลอดจนการเก็บรักษาบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในฐานะของกลาง โดยอาจมีการพิจารณามอบหมายหน่วยงานที่เกี่ยวข้อง เช่น กรมบังคับคดี เป็นผู้รับผิดชอบในการดำเนินการต่างๆ รวมทั้งยังจำเป็นจะต้องตรวจสอบและพิจารณาปรับแก้ไขกฎหมายหรือระเบียบที่เกี่ยวข้องเพื่อให้สามารถนำกระเป๋าเงินอิเล็กทรอนิกส์ (E-wallet) ของรัฐไปใช้งานได้อย่างมีประสิทธิภาพและได้รับการรับรองตามหลักกฎหมาย ซึ่งการดำเนินการตามแนวทางดังกล่าวนี้จะมีผลในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในมิติของการข่มขู่ยับยั้งและยังถือเป็นมาตรการในทางลงโทษในคราวเดียวกันอีกด้วย

6.1.3.4 ส่งเสริมให้มีการศึกษาวิจัย เพื่อค้นหาวิธีการ เครื่องมือหรือกลไกการป้องกันอาชญารูปแบบใหม่ ที่สามารถป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ

ส่งเสริมให้มีการวิจัยและพัฒนาองค์ความรู้เพื่อแสวงหาวิธีการ เครื่องมือและกลไกรูปแบบใหม่ต่างๆที่จะสามารถตรวจสอบและติดตามเส้นทางเส้นทางธุรกรรมทางการเงินและตรวจพิสูจน์ยืนยันตัวบุคคลหรือผู้ที่นำบิทคอยน์และสกุลเงินเข้ารหัสไปกระทำความผิด เช่น การพัฒนาโปรแกรมปัญญาประดิษฐ์ในการวิเคราะห์เส้นทางการเงินของสกุลเงินเข้ารหัส (AI Platform) หรือการสร้างฐานข้อมูลภาครัฐเพื่อป้องกันอาชญากรรม (Big Data) ซึ่งการดำเนินการตามแนวทางนี้จำเป็นจะต้องอาศัยองค์ความรู้ทางด้านวิศวกรรมคอมพิวเตอร์หรือความเชี่ยวชาญเกี่ยวกับการออกแบบและพัฒนาโปรแกรมคอมพิวเตอร์ด้วย

6.1.3.5 การสร้างความร่วมมือระหว่างหน่วยงาน ทั้งภาครัฐและภาคเอกชนในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

เพื่อเป็นการดึงเอาศักยภาพ องค์ความรู้และทรัพยากรที่มีอยู่ทั้งจากหน่วยงานทั้งภาครัฐและภาคเอกชน มาใช้เพื่อให้การป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสเป็นไปอย่างครบถ้วนสมบูรณ์และมีประสิทธิภาพ ตั้งแต่กระบวนการสืบสวนยืนยันตัวตนผู้กระทำความผิด ติดตามตรวจสอบเส้นทางการเงิน ตลอดจนสามารถเก็บรวบรวมพยานหลักฐานที่เกี่ยวข้องจนนำไปสู่การพิจารณาคดีและการยึดอายัดบิทคอยน์หรือสกุลเงินเข้ารหัสต่างๆที่เกี่ยวข้องได้ จึงจำเป็นอย่างยิ่งที่จะต้องมีการบูรณาการร่วมกันของหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องทุกหน่วยงาน โดยรูปแบบของการสร้างความร่วมมือนี้อาจเป็นในลักษณะของการตั้งเป็นคณะทำงานร่วมกันระหว่างหน่วยงานที่เกี่ยวข้อง โดยมีลักษณะเป็นคณะทำงานเฉพาะกิจ กรณีเมื่อเกิดคดีสำคัญที่จำเป็นจะต้องอาศัยทักษะและความชำนาญเฉพาะด้านจากหลากหลายหน่วยงานมาดำเนินการร่วมกัน ไปจนถึงการนำบุคลากรของแต่ละหน่วยงานมาจัดตั้งเป็น “ศูนย์ป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสแห่งชาติ” ที่มีลักษณะของการปฏิบัติหน้าที่ประจำเพื่อกำกับดูแลและแก้ไขปัญหาอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอย่างเป็นรูปธรรมและครบวงจร นอกจากนี้ยังจำเป็นจะต้องขยายความร่วมมือไปสู่ภาคเอกชนโดยเฉพาะอย่างยิ่งผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่ถือเป็นผู้ที่มีความรู้ ความเชี่ยวชาญ ทั้งยังถือเป็นผู้ที่ใกล้ชิดกับข้อมูลผู้ใช้งานที่เป็นลูกค้า เพื่อแสวงหาความร่วมมือทั้งในด้านเทคนิคและการส่งต่อข้อมูลที่เป็นประโยชน์อันจะนำไปสู่การเพิ่มประสิทธิภาพในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสต่อไป

6.1.3.6 การสร้างความร่วมมือกับหน่วยงานในต่างประเทศที่เกี่ยวข้องอย่างเป็นรูปธรรม

เนื่องด้วยลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆที่อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์และมีการทำงานบนระบบคอมพิวเตอร์ ทำให้การใช้งานในการกระทำความผิดนั้นสามารถกระทำได้จากทุกหนแห่งทั่วโลก และไม่อยู่ภายใต้ขอบเขตของเขตแดนระหว่างรัฐในทางกายภาพอีกต่อไป ในขณะที่การดำเนินการของหน่วยงานกระบวนการยุติธรรมทั่วโลกยังถูกกำหนดอำนาจหน้าที่ตามเขตแดนของรัฐ ซึ่งทำให้ขาดประสิทธิภาพและไม่สามารถหยุดยั้งอาชญากรรมสมัยใหม่นี้ได้อย่างทันท่วงที เพื่อเป็นการแก้ไขปัญหาดังกล่าว ประเทศไทยควรมีการสร้างความร่วมมือกับหน่วยงานในต่างประเทศในรูปแบบต่างๆ เช่น การทำข้อตกลงความร่วมมือร่วมกัน (MOU) ในเรื่องของการตกลงแลกเปลี่ยนข้อมูลสำคัญระหว่างกันในกรณีที่จำเป็นที่จะต้องใช้ข้อมูลต่างๆที่คนร้ายทิ้งร่องรอย หรือกระทำความผิดจากในต่างประเทศมาใช้ประกอบการพิจารณาคดี หรือประกอบการสืบสวนเพื่อหาตัวผู้ร่วมกระทำความผิดทั้งในและนอกประเทศ ทั้งนี้การประสานความร่วมมือดังกล่าวจะต้องมีการปฏิบัติให้ได้ผลจริง ไม่เพียงแต่เป็นการสร้างความร่วมมือแต่เพียงในหลักการ เช่น จะต้องมีการระบุตัวตนผู้ประสานงานหลัก (Contact Person) ซึ่งเป็นบุคคลหรือตำแหน่งประจำขึ้น เพื่อให้เกิดความชัดเจนในการประสานงานต่างๆ รวมทั้งจะต้องจัดให้มีวงรอบการติดต่อสื่อสารหรือการประสานงานแลกเปลี่ยนข้อมูลสำคัญกันอย่างสม่ำเสมอ

6.1.3.7 การสร้างสกุลเงินเข้ารหัสหรือสกุลเงินดิจิทัลแห่งชาติ

การดำเนินการแนวทางนี้ถือเป็นมาตรการเสริมด้วยการสร้างสกุลเงินดิจิทัลแห่งชาติ ที่ได้ถูกพัฒนาโดยธนาคารแห่งประเทศไทย และได้รับการรับรองมูลค่าด้วยการค้ำประกันด้วยเงินบาท ซึ่งจะทำให้เกิดเป็นช่องทางเลือกในการเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการของประเทศไทยที่น่าเชื่อถือ ซึ่งอาจส่งผลในทางอ้อม ซึ่งในปัจจุบันธนาคารแห่งประเทศไทยได้ทำการศึกษาพัฒนาการสร้างสกุลดิจิทัลแห่งชาติภายใต้โครงการชื่อ “อินทนนท์” ซึ่งได้ทำการทดสอบการใช้งานในระยะเริ่มต้น ในรูปแบบของการใช้ระหว่างธนาคารแห่งประเทศไทยและธนาคารพาณิชย์ต่างๆในประเทศ (Wholesale) ซึ่งภาครัฐควรมีการส่งเสริมให้มีการศึกษาและพัฒนาสกุลเงินดิจิทัลแห่งชาตินี้อย่างต่อเนื่องจนสามารถนำมาใช้งานได้ในระบบของการซื้อขายแลกเปลี่ยนสินค้าและบริการ ต่างๆ

อันจะทำให้ประชาชนในประเทศมีความสนใจและอาจส่งผลให้มีระดับการใช้สกุลเงินเข้ารหัสอื่นๆ น้อยลง จนอาจส่งผลให้อัตราการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมลดน้อยลง

6.2 ข้อเสนอแนะ

6.2.1 ข้อเสนอแนะเชิงนโยบาย

จากผลการศึกษา เรื่อง “แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย:ศึกษากรณีบิทคอยน์” ผู้วิจัยจึงขอเสนอข้อเสนอแนะเชิงนโยบายเพื่อเป็นแนวทางในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย ดังนี้

1) ภาครัฐจะต้องทำการศึกษา เก็บรวบรวมข้อมูลและสถิติที่เกี่ยวข้องกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส เพื่อนำไปเป็นฐานข้อมูลในการวิเคราะห์สถานการณ์การเกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ลักษณะและรูปแบบของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส สภาพความรุนแรงหรือความเสียหายที่เกิดขึ้น ตลอดจนวิเคราะห์แนวโน้มการเกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในอนาคต ทั้งจากสถานการณ์ในประเทศและต่างประเทศ ประกอบกับการวิเคราะห์เปรียบเทียบความสำคัญระหว่างการควบคุมการใช้งานสกุลเงินเข้ารหัสในเชิงการป้องกันอาชญากรรมกับผลประโยชน์ในด้านการพัฒนาระบบเศรษฐกิจและการเงิน โดยรัฐจำเป็นจะต้องนำข้อมูลดังกล่าวนี้ ไปใช้ในการพิจารณาตัดสินใจเพื่อกำหนดทิศทางของนโยบายสาธารณธที่เกี่ยวข้องต่างๆ เช่น จะกำหนดให้มาตรการการลงทะเบียนยืนยันตัวตนผู้ใช้งานมีระดับความเข้มข้นมากน้อยเพียงใด จะกำหนดให้บุคคลใดบ้างที่จะต้องดำเนินการตามมาตรการลงทะเบียนยืนยันตัวตน ตลอดจนพิจารณาความจำเป็นในการจัดตั้งศูนย์ปฏิบัติการหรือศูนย์เฉพาะกิจขึ้น เป็นต้น ทั้งนี้ภายหลังจากมีการกำหนดนโยบายต่างๆที่เกี่ยวข้องจะต้องมีกระบวนการการประเมินผลนโยบายประกอบกับข้อมูลต่างๆที่เกี่ยวข้องเพื่อพิจารณาปรับแก้ไขนโยบายต่างๆต่อไป

2) จากสภาพปัญหาและสาเหตุการเกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสที่พบจากการศึกษาซึ่งถือเป็นประเด็นปัญหาหลักและเป็นประเด็นที่ท้าทายประเทศต่างๆทั่วโลก คือ คุณลักษณะของบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ ที่มีลักษณะสำคัญที่เอื้อต่อการถูกนำไปใช้เป็นเครื่องมือในการกระทำความผิดคือ “การปกปิดตัวตนผู้ใช้งานที่แท้จริง” ดังนั้น หากรัฐต้องการที่ป้องกันมิให้อาชญากรรมประเภทนี้เกิดขึ้นในสังคมไทย จึงจำเป็นอย่างยิ่งที่จะต้องมีการกำหนด

มาตรการการลงทะเบียนยืนยันตัวตนผู้ใช้งานและมีการกำหนดขั้นตอนและวิธีการการดำเนินการดังกล่าวที่สามารถดำเนินการได้จริง ทั้งยังสามารถป้องกันการลักลอบยืนยันตัวตนแทนกัน โดยผู้วิจัยขอเสนอแนะขั้นตอนและวิธีการในการดำเนินการดังนี้

ขั้นตอนที่ 1 กำหนดให้มีการมาแสดงตัวเพื่อลงทะเบียนการใช้งานต่อหน้าพนักงานเจ้าหน้าที่ของรัฐที่ได้รับมอบหมาย พร้อมทั้งแสดงเอกสารประจำตัวเพื่อแสดงเจตจำนงเป็นผู้ใช้งานสกุลเงินเข้ารหัสในฐานะต่างๆ เช่น นักลงทุน ผู้ซื้อขาย ตัวแทนผู้ประกอบธุรกิจ เป็นต้น

ขั้นตอนที่ 2 เจ้าหน้าที่ของรัฐที่ได้รับมอบหมาย จะต้องดำเนินการเก็บข้อมูลผู้ที่ลงทะเบียนใช้งานสกุลเงินเข้ารหัสไว้เป็นฐานข้อมูลสำคัญ เพื่อใช้ในการตรวจสอบการใช้งานต่อไป

ขั้นตอนที่ 3 กรณีที่สถานการณ์การเกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสมีความรุนแรงกว่าปกติ หรืออยู่ในระดับที่รัฐกำหนดว่ามีความจำเป็นที่จะต้องยกระดับการตรวจสอบการใช้งานเพื่อประโยชน์ในการป้องกันการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการกระทำผิด อาจกำหนดวิธีการพิเศษเพิ่มเติมได้ เช่น รัฐอาจกำหนดมาตรการเพิ่มเติมในการยืนยันตัวตนผู้ใช้งานให้มีความละเอียดมากยิ่งขึ้น เช่น กำหนดให้การซื้อขาย แลกเปลี่ยน โอน-รับ จะต้องมีการยืนยันตัวตนทั้งต้นทางและปลายทางด้วยวิธีการต่างๆ เช่น การมากระทำต่อหน้าเจ้าหน้าที่ของรัฐ หรือ การยืนยันตัวตนผ่านอุปกรณ์อิเล็กทรอนิกส์ที่สามารถใช้ระบบการสื่อสารทางไกลแบบเห็นใบหน้า (VDO Call) เพื่อเป็นการยืนยันตัวบุคคลว่า ผู้ใดกระทำธุรกรรมที่เกี่ยวกับสกุลเงินเข้ารหัสกับผู้ใด เป็นต้น

ขั้นตอนที่ 4 กำหนดบทลงโทษตามกฎหมายที่เด็ดขาดและรุนแรง ในกรณีที่ตรวจพบว่าบุคคลใดฝ่าฝืนไม่ปฏิบัติตามมาตรการการยืนยันตัวตนของรัฐ หรือ ลักลอบยืนยันตัวตนแทนบุคคลอื่น หรือ ลักลอบกระทำการซื้อขาย แลกเปลี่ยน โอน-รับ ในนามของบุคคลอื่นโดยทุจริต เพื่อเป็นการข่มขู่ยับยั้ง และรักษาความศักดิ์สิทธิ์ให้แก่มาตรการดังกล่าว

ขั้นตอนที่ 5 ภาครัฐจะต้องส่งเสริมให้มีการวิจัยและพัฒนาวิธีการในการยืนยันตัวตนผู้ใช้งานให้เกิดประสิทธิภาพสูงสุด ทั้งนี้ จำเป็นจะต้องอาศัยการพัฒนาร่วมกันระหว่างศาสตร์ที่เกี่ยวกับเทคโนโลยีและวิศวกรรมทางคอมพิวเตอร์ กฎหมายและการบังคับใช้กฎหมาย

อนึ่ง ความเข้มข้นของขั้นตอนและวิธีการตลอดจนกลุ่มบุคคลเป้าหมายที่จะต้องอยู่ภายใต้มาตรการยืนยันตัวตนดังกล่าวนี้นั้น ควรมีการกำหนดให้สอดคล้องกันกับผลการวิเคราะห์ข้อมูลสถานการณ์และแนวโน้มเกี่ยวกับอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสที่ได้กล่าวมาแล้ว เพื่อให้

มาตรการดังกล่าวนี้เกิดความเหมาะสมกับสถานการณ์และกระทบกับการพัฒนาทางด้านเศรษฐกิจน้อยที่สุด

3) ชำระปรับปรุงแก้ไขและพัฒนากฎหมายซึ่งเป็นกลไกหลักในการป้องกันอาชญากรรมของรัฐให้สามารถเท่าทันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส รวมทั้งอาชญากรรมสมัยใหม่รูปแบบต่างๆที่จะเกิดขึ้นในอนาคต โดยภาครัฐและหน่วยงานที่เกี่ยวข้องโดยเฉพาะอย่างยิ่งหน่วยงานในกระบวนการยุติธรรมที่มีหน้าที่เกี่ยวข้องกับการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสจะต้องดำเนินการตรวจสอบกฎหมายที่มีอยู่ในปัจจุบันว่ามีข้อบกพร่อง เช่น ปัญหาในด้านการตีความกฎหมายที่เกี่ยวกับการเก็บพยานหลักฐานทางอิเล็กทรอนิกส์ที่พบในการศึกษาครั้งนี้ หรือมีบทบัญญัติใดบ้างที่ไม่เอื้อต่อการปฏิบัติหน้าที่ รวมทั้งจะต้องศึกษากฎหมายเปรียบเทียบกฎหมายที่เกี่ยวข้องของประเทศต่างๆ เพื่อตรวจสอบว่าในประเทศไทยยังขาดมาตรการทางกฎหมายที่จำเป็นอย่างไร เช่น ในกรณีของการที่ประเทศไทยยังกฎหมายและมาตรการที่ชัดเจนในการยึดและอายัดบิทคอยน์และสกุลเงินเข้ารหัส เป็นต้น

หลังจากที่ได้ทำการตรวจสอบข้อกฎหมายต่างๆที่จำเป็นจะต้องมีการพัฒนาปรับปรุงแล้ว จะต้องดำเนินการปรับปรุง แก้ไข หรือออกกฎหมายที่เกี่ยวข้องโดยเร็ว เช่น ในกรณีปัญหาด้านการตีความกฎหมาย ก็จะต้องจัดให้มีการประชุมใหญ่เพื่อลงความเห็นในประเด็นด้านการตีความกฎหมายเพื่อให้เจ้าหน้าที่ผู้ปฏิบัติและเจ้าหน้าที่ในกระบวนการยุติธรรมเกิดความเข้าใจที่ถูกต้องตรงกัน หรือในกรณีที่พบว่ากฎหมายที่มีไม่สนับสนุนการปฏิบัติหน้าที่ที่เกี่ยวข้องก็จะต้องดำเนินการเสนอแก้ไขปรับปรุง หรือหน่วยงานที่เกี่ยวข้องพิจารณาโดยละเอียดถี่ถ้วนแล้วว่า กฎหมายที่มีอยู่ในปัจจุบันไม่เพียงพอที่จะรองรับสถานการณ์การเกิดของอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้ก็จะต้องเสนอออกกฎหมายตามขั้นตอนโดยเร็ว โดยการดำเนินการดังกล่าวนี้จะส่งผลให้ประเทศไทยมีกฎหมายที่พร้อมรองรับและเป็นเครื่องมือของรัฐในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีประสิทธิภาพ

4) ภาครัฐจะต้องส่งเสริมให้มีการศึกษาค้นคว้าวิจัยเกี่ยวกับการพัฒนาการบังคับใช้กฎหมายที่เกี่ยวกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส เช่น ส่งเสริมให้มีการศึกษาค้นคว้าวิจัยเพื่อพัฒนาวิธีการ เครื่องมือ กลไก หรือ นวัตกรรมต่างๆ ที่จะสามารถตรวจสอบติดตามธุรกรรมทางการเงินของสกุลเงินเข้ารหัสต่างๆ หรือวิเคราะห์พฤติกรรมและรูปแบบการใช้งานเพื่อให้สามารถตรวจสอบติดตามผู้ใช้งานที่มีความเสี่ยงที่จะนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไป

ใช้ในการกระทำผิด เพื่อเป็นการป้องกันเชิงรุกและเป็นเครื่องมือที่มีศักยภาพเพื่อให้เจ้าหน้าที่ของรัฐมีเครื่องมือที่สามารถนำไปใช้ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสได้อย่างมีประสิทธิภาพ

5) ภาครัฐจะต้องกำหนดกรอบความร่วมมือของหน่วยงานภาครัฐและภาคเอกชนที่เกี่ยวข้องกับการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส เพื่อเป็นการส่งเสริมและผลักดันให้หน่วยงานของรัฐมีการบูรณาการการทำงานร่วมกันมากขึ้น โดยผู้วิจัยขอเสนอแนะแนวทางการดำเนินการดังกล่าวในระยะต่างๆ ดังนี้

ระยะที่ 1 กำหนดให้หน่วยงานที่เกี่ยวข้อง เช่น สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานป้องกันและปราบปรามการฟอกเงิน และหน่วยงานอื่นๆ เช่น สำนักงานป้องกันและปราบปรามยาเสพติด ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ เป็นต้น รวมทั้งจะต้องแสวงหาความร่วมมือจากภาคเอกชนอย่างกลุ่มผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลด้วย โดยจะต้องมีการทำความตกลงเพื่อให้เกิดการประสานงานในเรื่องต่างๆ เช่น ทำความตกลงเพื่อประสานความร่วมมือในด้านการสนับสนุน การส่งต่อและการใช้ข้อมูลสำคัญที่เกี่ยวกับการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสร่วมกันอย่างใกล้ชิด โดยจะต้องมีการกำหนดกรอบเวลาในการประสานงานที่ชัดเจนเพื่อให้เกิดความรวดเร็วและสามารถนำข้อมูลที่ได้ไปใช้ในการป้องกันปราบปรามอาชญากรรมได้อย่างทันท่วงที รวมทั้งจะต้องสร้างความร่วมมือในด้านการสนับสนุนบุคลากรผู้มีความรู้ ความเชี่ยวชาญต่างๆมาร่วมบูรณาการกำลังในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสเมื่อได้รับการร้องขอจากภาคีเครือข่าย โดนจะต้องมีการปรับลดขั้นตอนหรือกระบวนการในการประสานงาน หรือยกเว้นการติดต่อตามระเบียบของทางราชการ เพื่อให้การประสานงานและการปฏิบัติหน้าที่ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสเป็นไปด้วยความรวดเร็ว

ระยะที่ 2 พิจารณาความจำเป็นในการจัดตั้งหน่วยงานเฉพาะทางที่มีหน้าที่เกี่ยวกับการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส ทั้งในรูปแบบของการตั้งเป็นชุดเฉพาะกิจโดยการนำบุคลากรที่เป็นผู้เชี่ยวชาญในแต่ละด้าน จากหน่วยงานที่กล่าวถึงข้างต้นมาร่วมปฏิบัติหน้าที่เป็นการชั่วคราว และในรูปแบบของการตั้งเป็นหน่วยงานถาวรที่มีหน้าที่รับผิดชอบในเรื่องดังกล่าวโดยตรง ในกรณีที่เกิดปัญหาหรือสถานการณ์การเกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสขึ้นในระดับที่

ภาครัฐประเมินสถานการณ์ว่าจำเป็นจะต้องมีหน่วยงานดังกล่าว โดยในการพิจารณาดำเนินการตามข้อเสนอแนะ เห็นควรให้ภาครัฐหรือผู้มีอำนาจนำข้อมูลที่ได้จากการวิเคราะห์แนวโน้มสถานการณ์การเกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสมาประกอบการพิจารณาถึงความจำเป็นดังกล่าว เพื่อให้สอดคล้องเหมาะสมกับสถานการณ์

ระยะที่ 3 พิจารณาถึงความจำเป็นและความเป็นไปได้ที่จะดำเนินการตามข้อเสนอจากการศึกษาในประเด็นเกี่ยวกับการจัดทำฐานข้อมูลขนาดใหญ่ (Big Data) ที่รวบรวมข้อมูลสำคัญของหน่วยงานต่างๆที่เกี่ยวข้องเพื่อให้เป็นฐานข้อมูลในการป้องกันอาชญากรรมระดับประเทศ โดยรัฐควรจะต้องมอบหมายให้หน่วยงานที่รับผิดชอบพิจารณาศึกษาความเป็นไปได้และความเหมาะสม โดยหากเห็นสมควรว่าจะต้องมีการดำเนินการสร้างเครื่องมือและกลไกดังกล่าวแล้ว จำเป็นจะต้องให้หน่วยงานต่างๆทำการศึกษาพัฒนาและออกแบบระบบการใช้งานให้มีความปลอดภัยสูงสุด โดยกำหนดหลักเกณฑ์และวิธีการใช้งานข้อมูลดังกล่าวเพื่อประโยชน์ในการป้องกันอาชญากรรมและประโยชน์ส่วนรวมของประเทศเท่านั้น รวมทั้งจะต้องออกแบบมาตรการและวิธีการในการรักษาความปลอดภัยข้อมูลดังกล่าว เช่น กำหนดชั้นความลับและสิทธิ์การเข้าถึงข้อมูลให้เฉพาะกับเจ้าหน้าที่ที่เกี่ยวข้องเท่านั้น เป็นต้น

6) ส่งเสริมให้เกิดการสร้างความร่วมมือระหว่างประเทศในประเด็นที่เกี่ยวกับการประสานงานในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในรูปแบบต่างๆ เช่น ควรมีการทำข้อตกลงระหว่างประเทศ เพื่อกำหนดตัวแทนบุคคลของหน่วยงานที่เกี่ยวข้องของแต่ละประเทศ และกำหนดวิธีการพิเศษที่ตัวแทนดังกล่าวจะสามารถติดต่อสื่อสารกันได้ด้วยความรวดเร็วไม่ผ่านพิธีการทางการฑูตหรือธรรมเนียมการปฏิบัติระหว่างประเทศ เพื่อให้สามารถระงับยับยั้งความเสียหาย หรือ เพื่อให้เท่าทันต่อการทำลายพยานหลักฐานที่เกี่ยวกับการกระทำความผิดเกี่ยวกับสกุลเงินเข้ารหัส รวมทั้งกำหนดขอบเขตและกรอบความร่วมมือที่ชัดเจน เพื่อให้แต่ละชาติสามารถประเมินขีดความสามารถในการขอความร่วมมือได้อย่างถูกต้อง และลดระยะเวลาในการดำเนินการประสานงาน เป็นต้น

7) กำหนดแผนงานหรือโครงการในการประชาสัมพันธ์ให้ความรู้แก่ประชาชนให้ตระหนักถึงภัยจากอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอย่างเป็นรูปธรรม โดยมุ่งเน้นให้ประชาชนเกิดความรู้ความเข้าใจว่า บิทคอยน์และสกุลเงินเข้ารหัสต่างๆคืออะไร มีรูปแบบการทำงานอย่างไร และปัจจุบันอาชญากรมีการนำบิทคอยน์และสกุลเงินเข้ารหัสต่างๆไปใช้ในการก่ออาชญากรรมใน

ลักษณะและรูปแบบใดบ้าง อีกทั้งยังจำเป็นจะต้องประชาสัมพันธ์ให้ทราบถึงโทษทางกฎหมายที่จะได้รับหากเป็นผู้กระทำผิด โดยการประชาสัมพันธ์ผ่านช่องทางต่างๆ เช่น สื่อหลัก สื่อสังคมออนไลน์ เพื่อสร้างความรับรู้ให้แก่ประชาชนทั่วไปและยังถือเป็นกลไกในการสร้างการป้องกันตนเองให้กับประชาชนอีกด้วย

6.2.2 ข้อเสนอแนะเชิงวิชาการ

1) การศึกษาวิจัยครั้งนี้ เป็นการศึกษาเพื่อเสนอแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในมิติมุมมองทางอาชญาวิทยาและกระบวนการยุติธรรม ซึ่งการจะดำเนินการตามแนวทางการป้องกันอาชญากรรมเกี่ยวกับสกุลเงินเข้ารหัสแนวทางต่างๆ เช่น การพัฒนาวิธีการ เครื่องมือหรือกลไกต่างๆ เพื่อให้สามารถตรวจสอบติดตามเส้นทางธุรกรรมทางการเงินหรือการพิสูจน์ยืนยันตัวบุคคลผู้กระทำผิด จำเป็นจะต้องอาศัยศาสตร์ในเชิงวิศวกรรมคอมพิวเตอร์หรือองค์ความรู้ที่เกี่ยวกับระบบคอมพิวเตอร์ชั้นสูง ดังนั้น การนำแนวคิดดังกล่าวไปใช้ในการศึกษาวิจัยและพัฒนาวิธีการ เครื่องมือหรือกลไกเหล่านี้ต่อไป จะก่อให้เกิดประโยชน์ต่อประเทศชาติและสังคมโดยรวมเป็นอย่างมาก ตลอดจนยังสามารถนำองค์ความรู้ที่ได้ไปเป็นรากฐานในการป้องกันประเทศและการพัฒนาเทคโนลีเพื่อความมั่นคงปลอดภัยต่อไปในอนาคต

2) การศึกษาวิจัยครั้งนี้ เป็นลักษณะของการศึกษาที่เป็นการนำปัญหา ณ ช่วงขณะเวลาหนึ่งมาศึกษาวิจัย ซึ่งประเด็นปัญหาในเรื่องของเทคโนโลยีและนวัตกรรมลักษณะนี้จะมีพลวัตที่รวดเร็ว ประกอบกับสภาพสังคมที่ถูกผลักดันให้เกิดสังคมไร้เงินสด ทั้งสถานการณ์การแพร่ระบาดของโรคโควิด - 19 ที่อาจทำให้ประเด็นปัญหานี้เกิดความรุนแรงเพิ่มมากขึ้นกว่า ณ ขณะที่มีการศึกษาหรืออาจทำให้เกิดประเด็นปัญหาใหม่ จึงจำเป็นอย่างยิ่งที่การศึกษาวิจัยจะต้องไปพัฒนาและต่อยอดให้เกิดองค์ความรู้ใหม่ที่ยั่งยืน ในมิติของการป้องกันปราบปรามอาชญากรรมสมัยใหม่

ภาคผนวก

คำชี้แจง

แบบสัมภาษณ์นี้เป็นเครื่องมือในการเก็บรวบรวมข้อมูลประกอบการทำวิทยานิพนธ์ เรื่อง “แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์” มีวัตถุประสงค์ในการศึกษา คือ 1) เพื่อศึกษาสภาพปัญหา ลักษณะ รูปแบบและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัส 2) เพื่อศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ และ 3) เพื่อเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสในประเทศไทย โดยแบบสัมภาษณ์แบ่งออกเป็น 4 ชุด ดังนี้

ชุดที่ 1 สำหรับผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในเรื่องสกุลเงินเข้ารหัสทั้งในส่วนภาครัฐและภาคเอกชน ได้แก่

1. รองผู้ว่าการธนาคารแห่งประเทศไทย หรือ ผู้แทน จำนวน 1 ท่าน
2. ผู้ช่วยเลขาธิการ คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ หรือผู้แทน จำนวน 1 ท่าน
3. ผู้เชี่ยวชาญภาคเอกชนหรือผู้ประกอบธุรกิจเกี่ยวกับบิทคอยน์หรือสกุลเงินเข้ารหัส จำนวน 2 ท่าน

ชุดที่ 2 สำหรับผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญทางด้านกฎหมายเกี่ยวกับสกุลเงินเข้ารหัส ได้แก่

1. ผู้พิพากษา จำนวน 1 ท่าน
2. พนักงานอัยการ จำนวน 1 ท่าน

ชุดที่ 3 สำหรับผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญหรือผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส ได้แก่

1. ผู้บังคับการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (ผบก.ปอท.) หรือ ผู้แทน จำนวน 1 ท่าน
2. ผู้บังคับการกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (ผบก.ปอศ.) หรือ ผู้แทน จำนวน 1 ท่าน
3. ผู้อำนวยการกองคดีการเงินการธนาคารและการฟอกเงิน กรมสอบสวนคดีพิเศษ หรือผู้แทน จำนวน 1 ท่าน

4. รองเลขาธิการสำนักงานป้องกันและปราบปรามการฟอกเงิน หรือ ผู้แทน จำนวน 1 ท่าน

ชุดที่ 4 สำหรับผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการเสนอแนวทางในการป้องกันอาชญากรรม ได้แก่ รองผู้บัญชาการตำรวจแห่งชาติหรือผู้ช่วยผู้บัญชาการตำรวจแห่งชาติ ที่รับผิดชอบงานป้องกันปราบปรามอาชญากรรม หรือ ผู้แทน จำนวน 2 ท่าน

แบบสัมภาษณ์ ชุดที่ 1

(สำหรับผู้ให้ข้อมูลสำคัญ: ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญในเรื่องสกุลเงินเข้ารหัสทั้งในส่วนภาครัฐและภาคเอกชน**)**

เรื่อง แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์

คำชี้แจง

แบบสัมภาษณ์เป็นเครื่องมือในการเก็บรวบรวมข้อมูลประกอบการทำวิทยานิพนธ์ เรื่อง “แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์” มีวัตถุประสงค์ในการศึกษาคือ 1) เพื่อศึกษาสภาพปัญหา ลักษณะ รูปแบบและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัส 2) เพื่อศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ และ 3) เพื่อเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสในประเทศไทย โดยแบบสัมภาษณ์แบ่งออกเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคล

1. ชื่อ-นามสกุล
2. ตำแหน่งและหน้าที่ความรับผิดชอบ
3. ประสบการณ์การทำงาน

ส่วนที่ 2 ข้อมูลเกี่ยวกับบิทคอยน์

1.บิทคอยน์มีคุณลักษณะพิเศษอย่างไร และมีคุณลักษณะใดบ้างที่เอื้อต่อการถูกนำไปใช้เป็นเครื่องมือในการก่ออาชญากรรม

2 สถานการณ์การใช้บิทคอยน์ของประเทศไทยในปัจจุบันเป็นอย่างไร และมีแนวโน้มเป็นอย่างไรในอนาคต

3.จากสถานการณ์และแนวโน้มการใช้บิทคอยน์ในประเทศไทยดังกล่าว จะส่งผลกระทบต่อการนำบิทคอยน์ไปใช้ในการก่ออาชญากรรมหรือไม่ อย่างไร

ส่วนที่ 3 นโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวข้องกับสกุลเงินเข้ารหัสในปัจจุบัน

1.ในปัจจุบัน**หน่วยงาน องค์กร บริษัทหรือกิจการของท่าน**มีการกำหนด/มีการดำเนินงานภายใต้นโยบาย กฎหมาย และมาตรการต่างๆเกี่ยวกับสกุลเงินเข้ารหัส อย่างไร

2. นโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวข้องกับสกุลเงินเข้ารหัสดังกล่าว มีประเด็นเกี่ยวกับการป้องกันการนำสกุลเงินเข้ารหัสไปใช้ในการก่ออาชญากรรมประเภทต่างๆหรือไม่ อย่างไร

3. ท่านคิดว่าควรมีการพัฒนา เปลี่ยนแปลง หรือ แก้ไขเพิ่มเติม นโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวข้องกับสกุลเงินเข้ารหัสในปัจจุบัน หรือไม่ อย่างไร

ส่วนที่ 4 ข้อเสนอแนะ

1.ข้อเสนอแนะเกี่ยวกับแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในประเทศไทย

2.ข้อเสนอแนะอื่นๆ

แบบสัมภาษณ์ ชุดที่ 2

(สำหรับผู้ให้ข้อมูลสำคัญ: ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญทางด้านกฎหมายเกี่ยวกับสกุลเงินเข้ารหัส**)**

เรื่อง แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์

คำชี้แจง

แบบสัมภาษณ์เป็นเครื่องมือในการเก็บรวบรวมข้อมูลประกอบการทำวิทยานิพนธ์ เรื่อง “แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์” มีวัตถุประสงค์ในการศึกษาคือ 1) เพื่อศึกษาสภาพปัญหา ลักษณะ รูปแบบและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัส 2) เพื่อศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ และ 3) เพื่อเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสในประเทศไทย โดยแบบสัมภาษณ์แบ่งออกเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคล

1. ชื่อ-นามสกุล
2. ตำแหน่งและหน้าที่ความรับผิดชอบ
3. ประสบการณ์การทำงาน

ส่วนที่ 2 ประเด็นเกี่ยวกับสถานภาพทางกฎหมายของบิทคอยน์

1. สถานภาพทางกฎหมายของบิทคอยน์เป็นอย่างไร และบิทคอยน์ถือเป็นทรัพย์ตามกฎหมายอาญา หรือ กฎหมายอื่นใดหรือไม่ อย่างไร

2. สถานภาพของบิทคอยน์ดังกล่าว ทำให้เกิดปัญหาในการวิเคราะห์ ตีความในทางกฎหมายหรือไม่ อย่างไร

ส่วนที่ 3 ข้อกฎหมายและกระบวนการทางกฎหมายที่เกี่ยวข้องกับบิทคอยน์

1.ปัจจุบันมีกฎหมายใดบ้าง ที่เกี่ยวข้องกับการป้องกันการนำบิทคอยน์ไปใช้เป็นเครื่องมือในการก่ออาชญากรรม

2.กระบวนการในการดำเนินคดี/พิจารณาคดีอาญาที่เกี่ยวข้องกับบิทคอยน์ รวมทั้งกระบวนการขั้นตอนและวิธีการในการลงโทษผู้กระทำผิดเป็นอย่างไร เหมือนหรือแตกต่างจากคดีอาญาทั่วไปหรือไม่ อย่างไร

3. กฎหมายและกระบวนการในทางอาญาที่เกี่ยวข้องกับบิทคอยน์ดังกล่าว มีปัญหาและอุปสรรคหรือไม่ อย่างไร และท่านคิดว่าควรมีการแก้ไขเพิ่มเติมกฎหมายและกระบวนการในทางอาญาดังกล่าวหรือไม่ อย่างไร

ส่วนที่ 4 ข้อเสนอแนะ

1.ข้อเสนอแนะเกี่ยวกับแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในประเทศไทย

2.ข้อเสนอแนะอื่นๆ

แบบสัมภาษณ์ ชุดที่ 3

(สำหรับผู้ให้ข้อมูลสำคัญ: ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญหรือผู้ที่ปฏิบัติหน้าที่เกี่ยวกับการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวข้องกับสกุลเงินเข้ารหัส**)**

เรื่อง แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์

คำชี้แจง

แบบสัมภาษณ์เป็นเครื่องมือในการเก็บรวบรวมข้อมูลประกอบการทำวิทยานิพนธ์ เรื่อง “แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์” มีวัตถุประสงค์ในการศึกษาคือ 1) เพื่อศึกษาสภาพปัญหา ลักษณะ รูปแบบและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัส 2) เพื่อศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ และ 3) เพื่อเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสในประเทศไทย โดยแบบสัมภาษณ์แบ่งออกเป็น 4 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคล

1. ชื่อ-นามสกุล
2. ตำแหน่งและหน้าที่ความรับผิดชอบ
3. ประสบการณ์การทำงาน

ส่วนที่ 2 อาชญากรรมที่เกี่ยวกับบิทคอยน์

1. ในปัจจุบัน มีคดีอาญาที่มีการใช้บิทคอยน์เป็นเครื่องมือในการกระทำความผิดหรือเป็นคดีที่เกี่ยวข้องกับบิทคอยน์ที่อยู่ในความรับผิดชอบของหน่วยงานของท่าน หรือที่หน่วยงานของท่านได้รับแจ้งไว้หรือไม่ หากมี มีจำนวนเท่าใด และคดีต่างๆดังกล่าว มีรูปแบบและลักษณะการกระทำความผิดอย่างไร

2. ท่านคิดว่าคดีอาญาที่เกี่ยวกับบิทคอยน์ดังกล่าวเกิดจากสาเหตุใด

3. ท่านคิดว่าคดีอาญาที่เกี่ยวกับบิทคอยน์ดังกล่าว มีความแตกต่างจากอาชญากรรมในรูปแบบเดิมหรือไม่ อย่างไร

4. ท่านคิดว่าในอนาคตจะมีแนวโน้มการเกิดอาชญากรรมที่เกี่ยวกับบิทคอยน์ หรืออาชญากรรมที่ใช้บิทคอยน์เป็นเครื่องมือในการกระทำความผิด อย่างไร

ส่วนที่ 3 บุคลากรและเครื่องมือที่ใช้ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์

1.หน่วยงานของท่านมีบุคลากรที่มีความรู้ ความเข้าใจในเรื่องบิทคอยน์ที่เพียงพอต่อการปฏิบัติงานในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์หรือไม่ อย่างไร

2.หน่วยงานของท่านมีอุปกรณ์และเครื่องมือพิเศษต่างๆ เพียงพอต่อการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์หรือไม่ อย่างไร

3.ท่านคิดว่า มีปัญหาอุปสรรคใดบ้าง ที่เกิดขึ้นจากการปฏิบัติหน้าที่ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์

4.ท่านต้องการให้มีการพัฒนาหรือเพิ่มศักยภาพในด้านวิธีการ บุคลากรหรือเครื่องมือต่างๆ เพื่อให้เกิดการพัฒนาทางด้านประสิทธิภาพในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์หรือไม่ อย่างไร

ส่วนที่ 4 นโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับบิทคอยน์

1. ปัจจุบันหน่วยงานของท่าน ได้ดำเนินการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์ภายใต้นโยบาย กฎหมาย หรือมาตรการใดบ้าง อย่างไร

2. นโยบาย กฎหมาย และมาตรการต่างๆดังกล่าว เอื้ออำนวย หรือ เป็นอุปสรรคต่อการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์หรือไม่ อย่างไร

3. ท่านคิดว่า ควรมีการแก้ไขปรับปรุงนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆ เพื่อให้เกิดประโยชน์ต่อการปฏิบัติหน้าที่ในการป้องกันปราบปรามอาชญากรรมที่เกี่ยวกับบิทคอยน์หรือไม่ อย่างไร

4.ข้อเสนอแนะเกี่ยวกับแนวทางการป้องกันอาชญากรรมที่เกี่ยวกับบิทคอยน์และสกุลเงินเข้ารหัสต่างๆในประเทศไทย

5. ข้อเสนอแนะอื่นๆ

แบบสัมภาษณ์ ชุดที่ 4

(สำหรับผู้ให้ข้อมูลสำคัญ: ผู้ทรงคุณวุฒิหรือผู้เชี่ยวชาญที่มีองค์ความรู้และประสบการณ์เกี่ยวกับการเสนอแนวทางในการป้องกันอาชญากรรม**)**

เรื่อง แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์

คำชี้แจง

แบบสัมภาษณ์เป็นเครื่องมือในการเก็บรวบรวมข้อมูลประกอบการทำวิทยานิพนธ์ เรื่อง “แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิทคอยน์” มีวัตถุประสงค์ในการศึกษาคือ 1) เพื่อศึกษาสภาพปัญหา ลักษณะ รูปแบบและสาเหตุของอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัส 2) เพื่อศึกษาแนวนโยบาย กฎหมาย และมาตรการต่างๆที่เกี่ยวกับสกุลเงินเข้ารหัสที่มีอยู่ในประเทศไทยและในต่างประเทศ และ 3) เพื่อเสนอแนวทางการป้องกันอาชญากรรมที่ใช้บิทคอยน์ในฐานะสกุลเงินเข้ารหัสในประเทศไทย โดยแบบสัมภาษณ์แบ่งออกเป็น 3 ส่วน ดังนี้

ส่วนที่ 1 ข้อมูลส่วนบุคคล

1. ชื่อ-นามสกุล
2. ตำแหน่งและหน้าที่ความรับผิดชอบ
3. ประสบการณ์การทำงาน

ส่วนที่ 2 อาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส

1. ท่านคิดว่าอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัส มีความร้ายแรงและส่งผลกระทบต่อความสงบสุขของประชาชนได้มากกว่าอาชญากรรมตามปกติหรือไม่ อย่างไร

2. ท่านคิดว่าในอนาคตจะมีแนวโน้มการเกิดอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสเป็นอย่างไร

ส่วนที่ 3 แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย

1. ท่านคิดว่าประเทศไทย ควรมีแนวทางในการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสอย่างไร

2. ข้อเสนอแนะอื่นๆ

บรรณานุกรม

หนังสือ

ทศพร ศิริสัมพันธ์. (2539). *ความรู้เบื้องต้นเกี่ยวกับนโยบายสาธารณะ*. กรุงเทพฯ : สำนักพิมพ์จุฬาลงกรณ์มหาวิทยาลัย.

พรชัย ขันตี. (2558). *ทฤษฎีอาชญาวิทยา: หลักการ งานวิจัย และนโยบายประยุกต์*. กรุงเทพฯ: ส.เจริญการพิมพ์

มยุรี อนุมานราชธน. (2556). *นโยบายสาธารณะ.* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: เอ็กซเปอร์เน็ท.

วีระพงษ์ บุญโญภาส. (2552). *อาชญากรรมเศรษฐกิจ.* (พิมพ์ครั้งที่ 6). กรุงเทพฯ: สำนักพิมพ์นิติธรรม

ศุภชัย ยาวะประภาษ. (2550). *นโยบายสาธารณะ*. (พิมพ์ครั้งที่ 7.)กรุงเทพฯ: สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย.

สุดสงวน สุธีสร. (2547). *อาชญาวิทยา.* (พิมพ์ครั้งที่ 2). กรุงเทพฯ: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์

Antonopoulus, A.M. (2017). *Mastering Bitcoin Programming the Open Blockchain.* (Second Edition). Newton, MA: O'reilly Media.

Clarke, R. V. G., & Eck, J. (2003). *Become a problem-solving crime analyst : in 55 small steps*. London: Jill Dando Institute of Crime Science.

Lilly, J. R., Cullen, F. T., & Ball, R. A. (2011). *Criminological theory: Context and consequences.* (Sixth edition). Thousand Oaks, Calif: SAGE Publications.

Siegel, L. J. (2016). *Criminology : theories, patterns, and typologies.* (Twelfth edition). Boston, MA: Cengage Learning.

วิทยานิพนธ์

จุฑารัตน์ ชวดนุช. (2556). *ปัญหากฎหมายในการนำบิทคอยน์มาใช้สำหรับทำธุรกรรมออนไลน์ในประเทศไทย.*(การค้นคว้าอิสระปริญญานิติศาสตรมหาบัณฑิต, มหาวิทยาลัยกรุงเทพ).

ฉัทปณัย รัตนพันธ์. (2547). *อาชญากรรมคอมพิวเตอร์: ศึกษาการกำหนดฐานความผิดและการดำเนินคดีอาชญากรรมทางคอมพิวเตอร์*. (สารนิพนธ์ปริญญานิติศาสตรมหาบัณฑิต, มหาวิทยาธรรมศาสตร์).

ชาลี ธรรมรัตน์. (2554). *ความมั่นคงปลอดภัยการรับส่งแฟ้มข้อมูลและการจัดการการเข้ารหัสลับภายในองค์กร.*(สารนิพนธ์ปริญญาวิทยาศาสตรมหาบัณฑิต, มหาวิทยาลัยเทคโนโลยีมหานคร).

ณหทัย สุขเสนา. (2560). *มาตรการกำกับดูแลเงินสกุลดิจิทัลและการปรับใช้กฎหมายไทยกับเงินสกุลดิจิทัล:บิทคอยน์.* (วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต, สถาบันบัณฑิตพัฒนบริหารศาสตร์).

ดลพร ประสงค์สุทธิพร. (2557). *แนวทางการกำกับดูแลการใช้เงินเสมือน : กรณีศึกษาบิทคอยน์.* (เอกัตศึกษาปริญญานิติศาสตรมหาบัณฑิต,จุฬาลงกรณ์มหาวิทยาลัย).

สิรวิศ ศรีวิลาส. (2561). *มาตรการในการกำกับดูแลสินทรัพย์ดิจิทัล.* (วิทยานิพนธ์ปริญญานิติศาสตรมหาบัณฑิต, มหาวิทยาลัยอัสสัมชัญ).

งานวิจัยและบทความวิชาการ

ทวีชัย มีลาภ. (2559). การใช้บิทคอยน์ในประเทศไทยกับกฎหมายของประเทศที่ให้การยอมรับการใช้บิทคอยน์(สกุลเงินเสมือน). วารสารวิชาการ คณะนิติศาสตร์ มหาวิทยาลัยหอการค้าไทย, 8(1), 107.

พรรณทิพย์ เต็มเจริญ. (2561). ระวังกระแสบิทคอยน์. DSIไตรสาร , 10(2), 69.

ยอดชาย วิถีพานิช. (2558). ไอเอส (IS): กลุ่มก่อการร้ายที่โลกต้องจับตามอง. กรุงเทพมหานคร: สำนักวิชาการ สำนักงานเลขาธิการสภาผู้แทนราษฎร.

ลักษนันท์ พลอยวัฒนาวงศ์. (2561). บิตคอยน์และเทคโนโลยีบล็อกเชน. วารสารวิจัยมหาวิทยาลัยขอนแก่น, 18(3), 1-12.

สนธิกาญจน์ เพื่อนสงคราม. (2560). กรอบนโยบายสาธารณะที่ดีที่พรรคการเมืองของไทยควรนำมาประกอบการจัดทำนโยบายการบริหารประเทศ. รัฐสภาสาร 65(11), 9-44.

สุชาญ ไวยชีตา. (2560). Bitcoin เงินตราสกุลใหม่ของโลกหรือกลลวงเล็กๆของระบบเงินตรา. วารสารการค้าระหว่างประเทศ, 4(17), 23.

สำนักวิชาการ. สำนักงานเลขาธิการสภาผู้แทนราษฎร. (2561). บิทคอยน์(bitcoin)สกุลเงินเสมือนจริงแห่งอนาคต.กรุงเทพมหานคร:สำนักงานเลขาธิการสภาผู้แทนราษฎร.

อภินพ อติพิบูลย์สิน. (2557). บิทคอยน์ (Bitcoin): ความท้าทายในการกำกับดูแลนวัตกรรมเงินเสมือน.วารสารนิติศาสตร์, 43(3), 692 – 701.

อัญชนา เหมือนคิด, ธนพล พุกเส็ง, ระดม เจือจันทร์ และ ศิรปัฐช์ บุญครอง. (2557). Bitcoin: สกุลเงินของการเข้ารหัสลับที่น่าจับตามอง. วารสารวิทยาศาสตร์และเทคโนโลยี มหาวิทยาลัยมหาสารคาม, 33(6), 739-745.

เอกสารอื่นๆ

ธนาคารแห่งประเทศไทย. (2557). ประกาศของธนาคารแห่งประเทศไทย ฉบับที่ 8/2557 เรื่อง ข้อมูลเกี่ยวกับ Bitcoin และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่นๆ ที่ลักษณะใกล้เคียง (น. 1-2)

_____. (2561). ขอความร่วมมือสถาบันการเงินไม่ให้ทำธุรกรรมที่เกี่ยวข้องกับคริปโตเคอเรนซี (Cryptocurrency) (น.1-2)

สื่ออิเล็กทรอนิกส์

กรมสอบสวนคดีพิเศษ. ประวัติกรมสอบสวนคดีพิเศษ. [ออนไลน์]. 2559. แหล่งที่มา: https://www.dsi.go.th/th/Detail/History-of-DSI [9 กรกฎาคม 2562]

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม. กระทรวง DE เตือนภัย มัลแวร์เรียกค่าไถ่ WannaCry ระบาดผ่านช่องโหว่ของวินโดว์. [ออนไลน์]. 2560. แหล่งที่มา: https://www.etda.or.th/content/wannacry-ransomware-outbreak.html [15 กรกฎาคม 2562]

กรุงเทพธุรกิจ. ร้องปอท. ถูกหลอกลงทุน 'บิทคอยน์' สูญเงินร่วม 500 ล้าน. [ออนไลน์]. 2562. แหล่งที่มา: https://www.bangkokbiznews.com/news/detail/827193 [20 กันยายน 2562]

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี (บก.ปอท.). เกี่ยวกับหน่วยงาน. [ออนไลน์]. 2559. แหล่งที่มา: https://tcsd.go.th/เกี่ยวกับหน่วยงาน/ [1 กันยายน 2562]

กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (บก.ปอศ.). อำนาจหน้าที่. [ออนไลน์]. 2561. แหล่งที่มา: https://www.ecdpolice.com/ [1 กันยายน 2562]

กองวิจัย สำนักงานยุทธศาสตร์ตำรวจ สำนักงานตำรวจแห่งชาติ. การวิจัยเพื่อพัฒนากระบวนการสืบสวนและสอบสวนของเจ้าหน้าที่ตำรวจในการรับมือกับอาชญากรรมคอมพิวเตอร์. [ออนไลน์]. 2559. แหล่งที่มา: http://research.police.go.th/index.php/datacenter/research/2558/-2559-1/342---67/file [5 พฤษภาคม 2563]

กองวิจัยและพัฒนา สำนักงานตำรวจแห่งชาติ. รายงานการวิจัยการมีส่วนร่วมของผู้ขับขี่รถจักรยานยนต์รับจ้างในการป้องกันและปราบปรามอาชญากรรม. [ออนไลน์]. 2550. แหล่งที่มา : http://research.police.go.th/index.php/datacenter/research/--1/2550/94--2550/file [15 มิถุนายน 2562]

จิรายุส ทรัพย์ศรีโภคา. บิทคับ มอง Libra ของเฟซบุ๊ก เป็นอินฟราสตรัคเจอร์ใหม่ของโลกการเงิน. [ออนไลน์]. 2562. แหล่งที่มา: https://www.efinancethai.com/LastestNews/LatestNewsMain.aspx?release=y&ref=M&id=d1pDVEtOWUJNMjg9 [10 สิงหาคม 2562]

ณรัณ โพธิ์พัฒนชัย. Cryptocurrency สำหรับนักกฎหมายตอนที่ 3 เงินดิจิทัลกับประเด็นด้านสังคมและเศรษฐกิจที่ควรทราบ. [ออนไลน์]. 2561. แหล่งที่มา: https://www.facebook.com/thailawreform/posts/1731991000199221 [10 สิงหาคม 2562]

บุญชัย ธนะไพรินทร์. มหันตภัยบิทคอยน์!!! แก๊งขี้ยาใช้ซื้อขายในตลาดมืด-ออนไลน์.[ออนไลน์]. 2561. แหล่งที่มา: https://www.tnews.co.th/contents/424080 [17 สิงหาคม 2562]

ประพัทธ์โชต งามขำ. องค์กรภาคเอกชนกับการแก้ไขปัญหาอาชญากรรมทางเศรษฐกิจ: ศึกษากรณีอาชญากรรมคอมพิวเตอร์. [ออนไลน์]. 2548. แหล่งที่มา: http://www.library.coj.go.th/Info/42069?c= 47407935 [9 สิงหาคม 2563]

พรชัย ชุนหจินดา. บทเรียนจากทศวรรษแรกของคริปโทเคอร์เรนซี. [ออนไลน์]. 2561. แหล่งที่มา: https://e-jodil.stou.ac.th/filejodil/17_1_641.pdf [25 สิงหาคม 2563]

มติชนออนไลน์. ปปง.รุกแก้ไข กม.เงินดิจิทัล 'บิทคอยน์' ต้องรายงานธุรกรรมปิดทางมิจฉาชีพ. [ออนไลน์]. 2561. แหล่งที่มา: https://www.matichon.co.th/local/crime/news_822213 [22 กรกฎาคม 2562]

มหาวิทยาลัยสุโขทัยธรรมาธิราช. วิกฤตเศรษฐกิจในหรัฐอเมริกา. [ออนไลน์]. 2556. แหล่งที่มา: https://www.stou.ac.th/stouonline/lom/data/sec/Lom6/04-01.html [1 กรกฎาคม 2562]

มาณพ เสงี่ยมบุตร. จับตา "เงินหยวนดิจิทัล" นวัตกรรมการเงินครั้งสำคัญหลังเกิด "โควิด-19". [ออนไลน์]. 2563. แหล่งที่มา: https://www.prachachat.net/finance/news-463004 [6 มิถุนายน 2563]

ศูนย์วิจัยกฎหมายและพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. โครงการศึกษาเรื่องการบังคับคดีกับสินทรัพย์ดิจิทัล. [ออนไลน์]. 2561. แหล่งที่มา: http://www.led.go.th/articles/pdf/uO5ivavpioXiwe0zVD7ZS4DVtO0m3M27shbWXJzP2933110119024416.pdf [29 มิถุนายน 2562]

สถานีโทรทัศน์ไทยทีวีสีช่อง 3. เตือนภัยแอบอ้างบิทคอยน์หลอกเหยื่อลงทุนสูญหลายล้าน. [ออนไลน์]. 2561. แหล่งที่มา: http://news.ch3thailand.com/rerun/8/128652 [6 กรกฎาคม 2562]

สปริงนิวส์. ผู้การฯ กองปราบแจงดาราหนุ่มบูมโดนจับเหตุเปิดบัญชีรับโอนเงินลงทุน bitcoin แทนพี่. [ออนไลน์]. 2561. แหล่งที่มา: https://www.springnews.co.th/crime/323274 [10 ตุลาคม 2562]

สยามบล็อคเชน. จีนจะวางกฎระเบียบสำหรับเงินคริปโตอย่างค่อยเป็นค่อยไปโดยผู้ว่าฯธนาคารกลางจีน. [ออนไลน์]. 2561. แหล่งที่มา: https://siamblockchain.com/3/11/2018/china-will-move-slowly-to-regulate-crypto-central-bank-governor-says/ [11 พฤศจิกายน 2562]

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์(ก.ล.ต.). ประกาศสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ที่ สจ. 12/2562 เรื่อง บัญชีรายชื่อคริปโทเคอร์เรนซีที่สำนักงาน ก.ล.ต.ประกาศกำหนด ฉบับที่ 2. [ออนไลน์]. 2561. แหล่งที่มา: http://capital.sec.or.th/webapp/data/7997s.pdf [25 มกราคม 2563]

สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.). เกี่ยวกับสำนักงาน ปปง. [ออนไลน์]. 2557. แหล่งที่มา: http://www.amlo.go.th/ [1 กันยายน 2562]

อภิชน จันทรเสน. รูปแบบของมาตรการและประสิทธิภาพในการบังคับใช้. [ออนไลน์]. 2561. แหล่งที่มา:https://www.facebook.com/thailawreform/photos/pcb.1881158315282488/1881149831950003/ [15 กันยายน 2562]

Alexandre, A. Brazilian police arrest suspect for money laundering with Bitcoin. [Online]. 2019. Available from : https://cointelegraph.com/news/brazilian-police-arrest-suspect-for-money-laundering-with-bitcoin [2019,July 21]

Australian Federal Police. Brisbane woman charged over dangerous drug parcel post imports. [Online]. 2018. Available from : https://www.afp.gov.au/news-media/media-releases/Brisbane-woman-charged-over-dangerous-drug-parcel-post-imports [2019,September 2]

Berr, J. "WannaCry" ransomware attack losses could reach $4 billion. [Online]. 2017. Available from : https://www.cbsnews.com/news/wannacry-ransomware-attacks-wannacry-virus-losses/ [2020,February 19]

Bischoff, P. How Asia uses Bitcoin in one color-coded map. [Online]. 2015. Available from : https://www.techinasia.com/asia-bitcoin-colorcoded-map [2020,May 5]

Buck, J. Woman in Denmark Imprisoned for Hiring Hitman Using Bitcoin.[Online]. 2017. Available from : https://cointelegraph.com/news/woman-in-denmark-imprisoned-for-hiring-hitman-using-bitcoin [2019, August 28]

Burke, J. South Africa kidnappers make ransom demand in bitcoin. [Online]. 2018. Available from : https://www.theguardian.com/world/2018/may/22/south-africa-kidnappers-ransom-demand-bitcoin [2020,April 6]

Buy Bitcoin Worldwide. Bitcoin Price History [Online]. 2019. Available from : https://www.buybitcoinworldwide.com/th/price/ [2019,December 19]

Canellis, D. 76% of laundered cryptocurrency was washed with an exchange service. [Online]. 2018. Available from : https://thenextweb.com/hardfork/2019/01/29/cryptocurrency-laundering-chainalysis/ [2020,April 6]

Clark, J. R., Niederjohn, M. S. and Wood, W. C. Understanding Bitcoin: Money, Asset, or Bubble?. [Online]. 2018. Available from : https://www.researchgate.net/publication/2518050_Understanding_Bitcoin_Money_Asset_or_Bubble/citation/download [2020,April 20]

Coinmarketcap. Top 100 Cryptocurrencies by Market Capitalization. [Online]. 2020. Available from : https://www.coinmarketcap.com/ [2020,July 31]

Coinnounce. Top 6 porn websites that accept cryptocurrencies. [Online]. 2018. Available from : https://coinnounce.com/porn-websites-accepting-cryptocurrencies [2020,July 20]

Council of Europe. Convention on Cybercrime. [Online]. 2001. Available from : https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561 [2019,November 11]

European Central Bank. What is Bitcoin?. [Online]. 2018. Available from : https://www.ecb.europa.eu/explainers/tell-me/html/what-is-bitcoin.en.html [2020,June 30]

Federal Bureau of Investigation. Bitcoin Virtual Currency : Unique Features Present Distinct Challenges for Deterring Illicit Activity. [Online]. 2012. Available from : https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf [2019,September 26]

Fijnaut, C. J. C. F. Transnational Crime and the Role of the United Nations in its Containment through International Cooperation: A Challenge for the 21st Century. [Online]. 2000. Available from : https://brill.com/view/journals/eccl/8/2/article-p119_2.xml?language=en [2020,May 19]

Financial Action Task Force [FATF]. Guidance for a risk-based approach Virtual Currency. [Online]. 2015. Available from : https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-RBA-Virtual-Currencies.pdf [2020,July 2]

Gesley, J. Regulation of Cryptocurrency: Switzerland. [Online]. 2018. Available from : https://www.loc.gov/help/cryptocurrency/switzerland.php#II [2020,May 31]

Gulled & Hossain. Bitcoins Challenge to the Financial Institutions. [Online]. Available from : https://pdfs.semanticscholar.org/07fb/51cf2d8d180c7db4d4615821473e233d02e1.pdf [2020,June 15]

Helms, K. Putin's Order: Russia to Adopt Crypto Regulation by July. [Online]. 2019. Available from : https://news.bitcoin.com/putins-order-russia-cryptocurrency-regulation/ [2020,April 20]

Hileman, G. and Rauchs, M. 2017 Global Blockchain Benchmarking Study. [Online]. 2017. Available from : https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/alternative-finance/downloads/2017-09-27-ccaf-globalbchain.pdf [2019,October 11]

Hundeyin, D. Scotland: Man Jailed after Using Bitcoin to Buy Handgun on Dark Web. [Online]. 2019. Available from : https://www.ccn.com/scotland-man-jailed-after-using-bitcoin-to-buy-handgun-on-dark-web/ [2020,July 4]

Interpol. Financial Crime. [Online]. 2020. Available from : https://www.interpol.int/Crimes/Financial-crime [2020,August 30]

Liu, S. Size of the Bitcoin blockchain from 2010 to 2019 by quarter (in megabytes). [Online]. 2019. Available from : https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/ [2020,June 13]

Norry, A. The History of Mt Gox Hack: Bitcoin's Biggest Heist. [Online]. 2019. Available from : https://blockonomi.com/mt-gox-hack/ [2020,July 19]

Ogburn, W. F. Social Change with Respect to Culture and Original Nature. [Online]. 1922. Available from : https://archive.org/stream/socialchangewith00ogburich?ref=ol [2020,September 2]

Partz, H. Danish man faces over 4 years in prison for laundering 450k with Bitcoin. [Online]. 2019. Available from : https://cointelegraph.com/news/danish-man-faces-over-4-years-in-prison-for-laundering-450k-with-bitcoin [2020, July 6]

Polityuk, P. Ukraine kidnappers free bitcoin analyst after $1 mln ransom paid. [Online]. 2017. Available from : https://www.reuters.com/article/us-ukraine-kidnapping/ukraine-kidnappers-free-bitcoin-analyst-after-1-mln-ransom-paid-idUSKBN1EN1QB [2019,August 20]

Regional Organized Crime Information Center. Bitcoin and Cryptocurrencies : Law Enforcement Investigative Guide. [Online]. 2018. Available from : http://www.iacpcybercenter.org/wp-content/uploads/2018/03/Bitcoin.pdf [2020,january 26]

Reuters. Crypto Terror Financing: Hamas shifts tactics in Bitcoin Fundraising. [Online]. 2019. Available from : https://www.jpost.com/Middle-East/Crypto-terror-financing-Hamas-shifts-tactics-in-bitcoin-fundraising-587930 [2020,June 5]

Rushe, D. Silk Road 2.0's alleged owner arrested as drugs website shuttered by FBI. [Online]. 2014. Available from : https://www.theguardian.com/technology/2014/nov/06/silk-road-20-owner-arrested-drugs-website-fbi [2020,July 29]

Salomon, E. The Story Behind "Bitcoin Pizza Day". [Online]. 2019. Available from : https:// www.cbsnews.com/news/the-story-behind-bitcoin-pizza-day-2019-05-22/ [2020,November 17]

Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. [Online]. 2008. Available from : https://bitcoin.org/bitcoin.pdf [2020,Mar 4]

Statista. Number of Blockchain wallet users globally 2016-2019. [Online]. 2019. Available from : https://www.statista.com/statistics/644874/worldwide-blockchain-wallet-users/ [2020,December 21]

Thomas, W. Create legal security for Bitcoin. [Online]. 2013. Available from : https://www.parlament.ch/de/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20134070 [2021,March 13]

Turner, A. and Irwin A. S. M. Bitcoin transaction: a digital discovery of illicit activity on the blockchain. [Online]. 2018. Available from : https://researchers.mq.edu.au/en/publications/bitcoin-transactions-a-digital-discovery-of-illicit-activity-on-t [2019, October 1]

United Nations. UN Convention Against Transanational Organized Crime. [Online]. 2000. Available from : https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC20Convention/TOCebook-e.pdf [2020,May 7]

Vondráčková, A. Regulation of Virtual Currency in the European Union. [Online]. 2018. Available from : https://ssrn.com/abstract=2896911 [2020,July 3]

Wilusz, L. Woman paid 10k in Bitcoin on 'dark web' in murder-for-hire plot. [Online]. 2018. Available from : https://chicago.suntimes. com/crime/woman-paid-10k-in-bitcoin-on-dark-web-in-murder-for-hire-plot-prosecutors/ [2020,May 7]

ประวัติผู้เขียน

ชื่อ-สกุล	พ.ต.ต.กิจชัยยะ สุรารักษ์
วัน เดือน ปี เกิด	4 มีนาคม 2532
สถานที่เกิด	กรุงเทพมหานคร
วุฒิการศึกษา	ปริญญาตรี : รัฐประศาสนศาสตรบัณฑิต (ตร.) โรงเรียนนายร้อยตำรวจ ปริญญาโท : ศิลปศาสตรมหาบัณฑิต (บริหารงานยุติธรรม) มหาวิทยาลัยธรรมศาสตร์
ที่อยู่ปัจจุบัน	90/1111 หมู่ 7 ตำบลสามพราน อำเภอสามพราน จังหวัดนครปฐม
ผลงานตีพิมพ์	บทความเรื่อง "บิทคอยน์: สินทรัพย์ในยุคดิจิทัลกับการตกเป็นเครื่องมือประกอบอาชญากรรม" ในวารสารสถาบันวิชาการป้องกันประเทศ ปีที่ 11 ฉบับที่ 2 ประจำเดือน พฤษภาคม - สิงหาคม 2563