แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

นายวิสูต กัจฉมาภรณ์

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต
สาขาวิชาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา
คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
ปีการศึกษา 2563
ลิขสิทธิ์ของจุฬาลงกรณ์มหาวิทยาลัย

PREVENTION AND SUPPRESSION OF MONEY LAUNDERING BY CRYPTOCURENCY TRANSACTION

Mr. Visoot Kajchamaporn

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

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 2020

Copyright of Chulalongkorn University

หัวข้อวิทยานิพนธ์	แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส
โดย	นายวิสูต กัจฉมาภรณ์
สาขาวิชา	อาชญาวิทยาและงานยุติธรรม
อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก	รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง

คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาศิลปศาสตรดุษฎีบัณฑิต

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

คณะกรรมการสอบวิทยานิพนธ์

..... ประธานกรรมการ
(รองศาสตราจารย์ ดร.จุฑารัตน์ เอื้ออำนวย)

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก
(รองศาสตราจารย์ ดร.สุมนทิพย์ จิตสว่าง)

..... กรรมการ
(รองศาสตราจารย์วันชัย มีชาติ)

..... กรรมการ
(ผู้ช่วยศาสตราจารย์ ดร.ฐิติยา เพชรมุนี)

..... กรรมการภายนอกมหาวิทยาลัย
(ดร.กมล สุปรียสุนทร)

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

วิสูต กัจฉมาภรณ์ : แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส. (PREVENTION AND SUPPRESSION OF MONEY LAUNDERING BY CRYPTOCURENCY TRANSACTION) อ.ที่ปรึกษาหลัก : รศ. ดร.สุมนทิพย์ จิตสว่าง

วิทยานิพนธ์ “แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส” เป็นการศึกษาวิจัยธุรกรรมเงินสกุลเข้ารหัสอันเป็นนวัตกรรมการโอนมูลค่าระหว่างกันโดยตรงแบบไร้พรมแดนได้อย่างรวดเร็วและไม่มีหน่วยงานกลางใดกำกับ เพื่อให้ทราบถึงปัจจัยที่มีอิทธิพลต่ออาชญากรที่อาจเลือกใช้เป็นเครื่องมือในการฟอกเงิน รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส รวมถึงแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม โดยระเบียบวิธีการวิจัยเชิงคุณภาพด้วยการสัมภาษณ์เชิงลึกร่วมกับเทคนิควิธีเดลฟายรูปแบบปรับปรุง

จากการศึกษาพบว่า ระบบนิเวศเงินสกุลเข้ารหัสมีกลไกการปกปิดตัวตนของผู้ใช้งานสามารถกลบเกลื่อนร่องรอยเส้นทางธุรกรรมไม่ให้พิสูจน์ย้อนกลับถึงต้นทางได้ กอรปกับมีช่องว่างทางกฎหมายของแต่ละประเทศที่แตกต่างกัน อาชญากรจึงอาจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน ทั้งนี้ มาตรการป้องกันและปราบปรามที่เหมาะสม คือ ควรเพิ่มประสิทธิภาพการตรวจพิสูจน์ตัวตนของผู้ขอใช้งานโดยจัดทำระบบจัดการฐานข้อมูลกลางของประเทศ เฝ้าระวังธุรกรรมแปรสภาพเงินสกุลเข้ารหัสของผู้ต้องสงสัย พร้อมกับสร้างความร่วมมือกับองค์กรระหว่างประเทศด้านการต่อต้านการฟอกเงิน และปรับปรุงกฎระเบียบในกระบวนการดำเนินคดีเกี่ยวกับธุรกรรมเงินสกุลเข้ารหัส รวมถึงพัฒนาโปรแกรมสืบค้นเส้นทางธุรกรรมบนระบบปฏิบัติการบล็อกเชน และเสริมทักษะความรู้เกี่ยวกับเงินสกุลเข้ารหัสที่ถูกต้องให้แก่เจ้าหน้าที่ทั้งส่วนกลางและส่วนภูมิภาค รวมถึงประชาชนทั่วไป

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

สาขาวิชา อาชญาวิทยาและงานยุติธรรม ลายมือชื่อนิสิต .....

ปีการศึกษา 2563 ลายมือชื่อ อ.ที่ปรึกษาหลัก .....

6181369724 : MAJOR CRIMINOLOGY AND CRIMINAL JUSTICE
KEYWORD: Money Laundering Bitcoin Cryptocurrency Anti-Money Laundering

Visoot Kajchamaporn : PREVENTION AND SUPPRESSION OF MONEY LAUNDERING BY CRYPTOCURENCY TRANSACTION. Advisor: Assoc. Prof. SUMONTHIP CHITSAWANG, Ph.D.

The thesis, “Prevention and Suppression of Money Laundering by Cryptocurrency Transaction”, is a study on innovative cryptocurrency transactions which support energetically Peer-to-Peer global transferring without any controlling agency, for the purpose of identifying influent factors to criminals and cryptocurrency crime pattern for using cryptocurrency as money laundering tool as well as developing proposal guidelines on anti-money laundering by cryptocurrency transactions. The research was conducted by qualitative research methodology with in-depth interviews in conjunction with modified Delphi techniques.

It was found that cryptocurrency ecosystems have been anonymous mechanisms, abstained from traceability to the source and been regulated by various law enforcements therefore may cause criminals apply crypto laundering. The anti-money laundering by cryptocurrency transactions should enhance Know-Your-Customer procedure by KYC big data base, intensively surveillance transaction routing by suspects, corporate with international organizations against money laundering, improve prosecuting procedure on crypto crime, develop crypto forensic programs interfacing with blockchain systems and explode updating knowledge on cryptocurrency not only authorities but also the public.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Field of Study:	Criminology and Criminal Justice	Student's Signature .....
Academic Year:	2020	Advisor's Signature .....

กิตติกรรมประกาศ

วิทยานิพนธ์ฉบับนี้สำเร็จลงได้ด้วยความอนุเคราะห์จากบุคคลหลายท่านที่ให้การสนับสนุนผู้วิจัยมาโดยตลอดระยะเวลาของการศึกษา ขอกราบขอบพระคุณ รศ.ดร.สุมนทิพย์ จิตสว่าง หัวหน้าภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาตร์ จุฬาลงกรณ์มหาวิทยาลัย ผู้เป็นอาจารย์ที่ปรึกษาวิทยานิพนธ์ ซึ่งได้กรุณาให้คำปรึกษาและข้อแนะนำอันมีคุณค่าในการจัดทำวิทยานิพนธ์ ตลอดจนเป็นแรงบันดาลใจในการดำเนินกระบวนการวิจัยให้สำเร็จลุล่วงไปด้วยดี รวมทั้ง รศ.ดร.จุฑารัตน์ เอื้ออำนวย รศ.วันชัย มีชาติ ผศ.ดร.ฐิติยา เพชรมุนี และ ดร.กมล สุปรียสุนทร ผู้ทรงคุณวุฒิด้านอาชญาวิทยาและงานยุติธรรม ที่ให้ข้อแนะนำหลากมุมมองและข้อคิดเห็นที่เป็นประโยชน์ในการปรับปรุงแก้ไขวิทยานิพนธ์ให้มีความครบถ้วนและสมบูรณ์มากยิ่งขึ้น ทั้งนี้ ขอกราบขอบพระคุณ ดร.นัทธี จิตสว่าง ที่เป็นแรงผลักดันให้เกิดความสนใจศึกษาอาชญากรรมเงินสกุลเข้ารหัสเพื่อพัฒนาองค์ความรู้ด้านอาชญากรรมเศรษฐกิจที่มีคุณูปการต่อการพัฒนาด้านอาชญาวิทยาและกระบวนยุติธรรม

นอกจากนี้ ขอขอบพระคุณคณาจารย์ทุกท่านจากภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่ได้ประสิทธิ์ประสาทวิชาความรู้ ตลอดจนได้เสนอแนะแนวทางที่เป็นประโยชน์ในการพัฒนาขีดความสามารถและศักยภาพทางด้านวิชาการแก่ผู้วิจัย รวมทั้ง ขอขอบพระคุณ รศ.ดร.ศรีสมบัติ โชคประจักษ์ชัด ที่ให้ข้อแนะนำด้านเทคนิควิธีเดลฟาย และขอขอบพระคุณ รศ.ขนบพันธ์ เอี่ยมโอภาศ คณะบริหารธุรกิจ มหาวิทยาลัยรามคำแหง ดร.ประพันธ์ วงศ์บางโพ บรรณาธิการ วารสารบริหารธุรกิจและสังคมศาสตร์ มหาวิทยาลัยรามคำแหง ที่ได้ให้ความรู้และคำแนะนำในการตีพิมพ์บทความวิชาการของงานวิจัย ตลอดจนขอขอบคุณ พ.ท.ดิเรกฤทธิ์ บุษยธนากรณ์ พ.ต.หญิง จิตลดา สุจิตต์ และ นางสาวจามีกร แคนนารี่ ที่ให้ความปรารถนาดีและคำแนะนำที่ดีมาตลอด รวมทั้งเพื่อนนิสิตหลักสูตรศิลปศาตร์ดุษฎีบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม และเจ้าหน้าที่ประจำภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาตร์ จุฬาลงกรณ์มหาวิทยาลัย ที่ให้การช่วยเหลือสนับสนุนในด้านเอกสารและข้อมูลที่เป็นประโยชน์แก่ผู้วิจัย

สุดท้ายนี้ ผู้วิจัยขอขอบคุณผู้ที่อยู่เบื้องหลังความสำเร็จในครั้งนี้ โดยเฉพาะครอบครัวที่คอยสนับสนุนอย่างเต็มที่และเป็นกำลังใจเสมอมา ทำให้ผู้วิจัยมีความพยายาม มุ่งมั่น และอดทนต่ออุปสรรคเพื่อการจัดทำวิทยานิพนธ์ฉบับนี้ให้สำเร็จอย่างสมบูรณ์

วิสูต กัจฉมาภรณ์

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

สารบัญ

หน้า

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 1
บทนำ

1.1 ความเป็นมาและความสำคัญของปัญหา

นับตั้งแต่ปี 2008 ซาโตชิ นากาโมโต (Satoshi Nakamoto) ได้นำเสนอนวัตกรรมทางการเงินบนระบบปฏิบัติการบล็อกเชน เพื่อการโอนเงินทางอิเล็กทรอนิกส์ระหว่างบุคคลต่อบุคคลโดยตรง ภายใต้ระบบนิเวศที่สามารถพิสูจน์ยืนยันรายการกันเอง โดยไม่ผ่านการกำกับของหน่วยงานกลางใดในนามเรียกขานว่า ***"บิตคอยน์ (Bitcoin)"*** **ซึ่งถือเป็นเงินสกุลเข้ารหัส (Cryptocurrency) สกุลแรกของโลก** (Nakamoto, 2008) และนับเป็นจุดเริ่มของการปฏิวัติระบบการเงินโลก เนื่องจากคุณลักษณะเฉพาะที่สำคัญของเงินสกุลเข้ารหัส คือ ผู้ใช้งานไม่ต้องเปิดเผยตัวตน การโอนมูลค่าสามารถดำเนินการข้ามเขตแดนประเทศแบบไร้พรมแดน ด้วยความรวดเร็ว ไร้หน่วยงานตัวกลางในการกำกับ และต้นทุนดำเนินงานต่ำ จึงเป็นคุณลักษณะที่ท้าท้ายต่อสถาบันการเงินและระบบการเงินโลกอย่างมาก (FATF, 2019) นอกจากบิตคอยน์แล้ว นักพัฒนาระบบได้นำเสนอเงินสกุลเข้ารหัสใหม่เข้าสู่เครือข่ายอย่างต่อเนื่อง จนกระทั่งปัจจุบันในเดือนมีนาคม 2021 มีเงินสกุลเข้ารหัสหมุนเวียนอยู่ในระบบตลาดเงินอิเล็กทรอนิกส์ไม่น้อยกว่า 8,900 สกุลเงิน ด้วยขนาดตลาดมูลค่ารวมประมาณ 1.8 ล้านล้านเหรียญสหรัฐ หรือประมาณ 54 ล้านล้านบาท อย่างไรก็ตาม บิตคอยน์ก็ยังเป็นเงินสกุลเข้ารหัสที่ได้รับการยอมรับด้วยขนาดตลาดมูลค่าประมาณ 1.0 ล้านล้านเหรียญสหรัฐ หรือประมาณ 31 ล้านล้านบาท และคิดเป็นร้อยละ 59.6 ของมูลค่าทางการตลาดรวม [1]

ทั้งนี้ ด้วยคุณสมบัติเฉพาะที่โดดเด่นของเงินสกุลเข้ารหัสคือ **ธุรกรรมการโอนมูลค่าได้โดยตรงไปยังผู้รับโดยไม่ผ่านการกำกับดูแลของตัวกลาง และการรักษาความเป็นส่วนตัวของผู้ใช้งานโดยไม่ต้องระบุตัวตน** ได้ถูกนำไปเป็นเครื่องมือทางการเงินสำคัญของกลุ่มอาชญากรทางเศรษฐกิจที่นำไปใช้เป็นช่องทางในการโอนมูลค่าระหว่างประเทศ เพื่อส่งต่อผลตอบแทนจากการกระทำผิดกฎหมาย เช่น การค้ายาเสพติด การค้าสิ่งผิดกฎหมายในระบบออนไลน์ การเรียกค่าไถ่ การคอรัปชั่น รวมถึงการฟอกเงิน โดยเฉพาะอย่างยิ่งในปัจจุบันแต่ละประเทศมีบทบัญญัติทางกฎหมายที่ใช้บังคับต่อการดำเนินธุรกรรมเงินสกุลเข้ารหัสที่แตกต่างกัน ส่งผลให้มูลค่าของบิตคอยน์ซึ่งเป็นเงินสกุลเข้ารหัสสกุลแรก และเป็นเงินสกุลหลักมีแนวโน้มราคาเคลื่อนไหวตามปริมาณความต้องการของกลุ่มอาชญากรทางเศรษฐกิจและมีการปรับลดมูลค่าลงอย่างต่อเนื่อง ส่งผลให้หลายประเทศเริ่มมีบทบัญญัติทางกฎหมายในการกำกับดูแลเงินสกุลเข้ารหัสอย่างเคร่งครัดมากขึ้น โดยเริ่มจากปี 2009 เมื่อมีการโอนบิตคอยน์รายการแรกด้วยมูลค่า 1 บิตคอยน์น้อยกว่า 1 เซนต์ หรือกล่าวอีกนัยหนึ่งคือ 1

[1] ข้อมูลจากเว็บไซต์ CoinMarketCap.com ณ Last updated: Sat 20 Mar 2021 15:10:17 UTC

เหรียญสหรัฐมีมูลค่ามากกว่า 10,000 บิตคอยน์ จนกระทั่งบิตคอยน์ไต่ระดับราคาสูงขึ้นไปมีมูลค่าสูงเกือบ 20,000 เหรียญสหรัฐต่อ 1 บิตคอยน์ในปี 2017 ก่อนที่มูลค่าของบิตคอยน์จะลดลงอย่างต่อเนื่อง หลังจากกลุ่มอาชญากรค้าสิ่งผิดกฎหมายทางออนไลน์ (Dark Web) รายใหญ่ถูกกวาดล้างจับกุม จนกระทั่งราคาบิตคอยน์ลดลงมาเคลื่อนไหวอยู่ในระดับ 5,000 - 7,000 เหรียญสหรัฐต่อ 1 บิตคอยน์ ตัวอย่างเช่น Silk Road กลุ่มค้าสิ่งผิดกฎหมายทางออนไลน์ที่ถูกจับกุมและสั่งปิดในปี 2013 และอีกรายหนึ่งคือ AlphaBay ถูกจับกุมและสั่งปิดในปี 2017 (Fanusie & Robinson, 2018)

จากรายงานการศึกษากระบวนการฟอกเงินด้วยบิตคอยน์จากธุรกิจผิดกฎหมาย โดยโปรแกรมประยุกต์เพื่อการตรวจสอบสืบค้นในระบบปฏิบัติการบล็อกเชนชื่อ *“Elliptic”* ของประเทศสหรัฐอเมริกา ในระหว่างปี 2013 ถึงปี 2016 โดย Fanusie and Robinson (2018) ซึ่งได้เผยแพร่เมื่อวันที่ 12 มกราคม 2018 พบว่า ธุรกิจผิดกฎหมายที่มีธุรกรรมฟอกเงินโดยบิตคอย์ในปี 2013 มีจำนวนมากที่สุดคือ Silk Road ซึ่งมีสัดส่วนธุรกรรมฟอกเงินสูงถึงร้อยละ 89.89 ของธุรกรรมรวม สำหรับปี 2014 ธุรกรรมฟอกเงินโดยบิตคอยน์จาก Agora ร้อยละ 42.43 และจาก Silk Road 2.0 ร้อยละ 40.50 ของธุรกรรมรวม (เนื่องจาก Silk Road ถูกจับกุมและสั่งปิดในปี 2013) ส่วนในปี 2015 มีธุรกรรมฟอกเงินโดยบิตคอยน์ผ่านทาง Agora ร้อยละ 47.89 ของธุรกรรมรวม และในปี 2016 มีธุรกรรมฟอกเงินโดยบิตคอยน์จาก AlphaBay ร้อยละ 46.45 และ Nucleus Market ร้อยละ 31.21 ของธุรกรรมรวม ตามลำดับ พร้อมกันนี้ได้รายงานแหล่งการให้บริการธุรกรรมฟอกเงินโดยบิตคอนย์ซึ่งส่วนใหญ่ผ่านศูนย์บริการแลกเปลี่ยนบิตคอยน์ (Bitcoin Exchanger) สูงถึงร้อยละ 45.43 นอกจากนั้นเป็นเว็บไซต์การพนัน (Gambling) ร้อยละ 25.79 และศูนย์บริการแปรสภาพบิตคอยน์ (Bitcoin Mixer) อีกร้อยละ 23.40 ของธุรกรรมรวม ตามลำดับ สำหรับธุรกรรมฟอกเงินโดยบิตคอยน์ที่สามารถตรวจพิสูจน์ตัวตนได้ส่วนใหญ่มาจากกลุ่มประเทศยุโรปมากถึงร้อยละ 37.33 และธุรกรรมที่ไม่สามารถตรวจพิสูจน์ตัวตนได้มีจำนวนสูงถึงร้อยละ 52.03 ของธุรกรรมรวม

นอกจากนี้ผลการศึกษาวิจัยยังพบว่า กลุ่มประเทศยุโรปมีการฟอกเงินโดยบิตคอยน์ซึ่งเกิดจากการกระทำที่เกี่ยวข้องธุรกิจผิดกฎหมายผ่านศูนย์การแปรสภาพบิตคอยน์(Bitcoin Mixers) มากที่สุด และมีสัดส่วนการทำธุรกรรมฟอกเงินโดยบิตคอยน์สูงกว่ากลุ่มประเทศอเมริกาเหนือถึง 5 เท่า ในขณะเดียวกันกลุ่มประเทศแถบเอเชียเริ่มมีสัดส่วนการทำธุรกรรมฟอกเงินโดยบิตคอยน์เพิ่มขึ้นอย่างมีนัยสำคัญตั้งแต่ปี 2015 ทั้งนี้ **กลุ่มผู้ใช้บริการส่วนใหญ่จะมาจากกลุ่มประเทศที่มีการบังคับใช้กฎหมายป้องกันการฟอกเงินอย่างเคร่งครัด** (Fanusie & Robinson, 2018)

นอกจากนี้ ในปี 2013 กระทรวงยุติธรรมของสหรัฐอเมริกาได้ดำเนินคดีฟอกเงินกับธุรกิจบริการแลกเปลี่ยนเงินรายใหญ่ *“Liberty Reserve”* ที่ให้บริการแลกเปลี่ยนเงินตราและการโอนเงินอิเล็กทรอนิกส์ระหว่างประเทศ เข้าข่ายการฟอกเงินอย่างผิดกฎหมายด้วยเงินสกุลเข้ารหัสที่ชื่อ *“Liberty Dollars หรือ LD”* โดยมีจำนวนผู้ใช้บริการในเครือข่ายทั่วโลกหลายล้านราย เฉพาะใน

ประเทศสหรัฐอเมริกามีผู้ใช้บริการจำนวนมากกว่า 2 แสนรายด้วยจำนวนธุรกรรมโอนเงินผิดกฎหมายประมาณ 55 ล้านรายการ และเป็นการสนับสนุนการฟอกเงินไม่น้อยกว่า 6 พันล้านเหรียญสหรัฐ (Dyntu & Dykyi, 2019) ในขณะที่ รอป เวียนไรท์ (Rob Wainwright) ผู้อำนวยการยูโรพอล ได้รายงานว่ามีปริมาณเงินของผู้กระทำผิดกฎหมายในยุโรปจำนวนมากประมาณ 3 ถึง 4 พันล้านปอนด์ที่ทำการฟอกเงินโดยเงินสกุลเข้ารหัส พร้อมให้ทัศนะว่า**ถึงเวลาที่นักอุตสาหกรรมและนักกฎหมายจะต้องเผชิญหน้ากับความท้าทายนี้อย่างจริงจัง** (Kepli & Zulhuda, 2019)

สำหรับกรณีอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสในประเทศไทยมีปรากฏไม่มากนัก แต่เมื่อเกิดเหตุขึ้นมักจะมีขนาดความเสียหายมูลค่าสูง เช่น กรณีการหลอกนักลงทุนชาวฟินแลนด์ ซึ่งประกอบธุรกิจซื้อขายแลกเปลี่ยนเงินสกุลดิจิทัล เพื่อเข้ามาลงทุนในประเทศไทย โดยการชักชวนจากผู้บริหารบริษัทหลักทรัพย์แห่งหนึ่ง ร่วมกับนักธุรกิจและพวกซึ่งมีความสัมพันธ์กับนักแสดงเพื่อการสร้างความน่าเชื่อถือให้แก่เหยื่อตั้งแต่กลางปี 2018 ด้วยข้อเสนอการลงทุนในบริษัท Expay Group ด้วยมูลค่าบิตคอยน์จำนวน 1,259.13 BTC หรือคิดเป็นจำนวนเงินประมาณ 92 ล้านบาท และนำเสนอการลงทุนในเงินสกุลเข้ารหัสสกุลใหม่ในนาม Dragon Coin ด้วยมูลค่าบิตคอยน์อีกจำนวน 2,958.76 BTC หรือคิดเป็นจำนวนเงินประมาณ 440 ล้านบาท พร้อมนำเสนอแผนธุรกิจโดยการลงทุนในบริษัท ดีเอ็นเอ 2002 จำกัด (มหาชน) (DNA) ซึ่งเป็นบริษัทจดทะเบียนในตลาดหลักทรัพย์แห่งประเทศไทย อีกจำนวนเงินประมาณ 265 ล้านบาท เพื่อนำธุรกิจของ Expay Group และ Dragon Coin เข้าควบรวมธุรกิจกับบริษัท DNA สร้างความคาดหวังต่อการเพิ่มมูลค่าเงินลงทุนจำนวนมหาศาล แต่กลุ่มผู้กระทำผิดกลับฉ้อโกงเหยื่อด้วยการนำเงินที่ได้รับจากเหยื่อจำนวนประมาณ 800 ล้านบาทไปทำการกระจายให้แก่เครือญาติและบุคคลใกล้ชิดในลักษณะของการฟอกเงิน (ข่าวการเงิน, 2018) และในอีกกรณีตัวอย่างคือ การหลอกลวงในปี 2019 ด้วยการโฆษณาในเว็บไซต์ Cryptominingfarm ซึ่งเป็นบริษัทผู้ให้เช่าเครื่องมือในการขุดบิตคอยน์ โดยผู้สนใจสามารถทำการลงทุนได้ตั้งแต่ 2,000 บาทขึ้นไป เพื่อเข้าเชื่อมต่อระบบนิเวศและทำหน้าที่ยืนยันรายการธุรกรรมบิตคอยน์ โดยได้รับค่าตอบแทนเป็นบิตคอยน์ ทั้งนี้ผู้กระทำผิดได้นำเงินที่ได้รับจากผู้ลงทุนไปแลกเปลี่ยนเป็นบิตคอยน์และนำไปกระจายส่งมอบเป็นค่าตอบแทนให้แก่นักลงทุน เพื่อสร้างแรงจูงใจให้แก่เหยื่อในการขยายการลงทุนและขยายฐานจำนวนนักลงทุน จนในที่สุดเว็บไซต์นี้ได้ปิดตัวลงโดยสร้างความเสียหายให้แก่นักลงทุนที่หลงเชื่อการหลอกลวงจำนวนรวมสูงถึงประมาณ 500 ล้านบาท (ข่าวอาชญากรรม, 2019)

ดังนั้น การบังคับใช้กฎหมายจึงไม่ควรมุ่งเน้นในการปราบปรามเพียงอาชญากรรมค้าสิ่งผิดกฎหมายทางออนไลน์ที่รับผลตอบแทนเป็นเงินสกุลเข้ารหัสเท่านั้น แต่ควรมีการขยายผลไปสู่การกำกับดูแลระบบเงินสกุลเข้ารหัสที่มีความสำคัญมากขึ้น รวมถึงกลไกการสร้างความร่วมมือในการกำหนดมาตรการป้องกันและปราบปรามอาชญากรรมที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการกระทำผิด และการแบ่งปันประสบการณ์การเรียนรู้ จากกรณีศึกษาพฤติกรรมการฟอกเงินโดยธุรกรรมเงิน

สกุลเข้ารหัสของแต่ละประเทศ เพื่อให้สามารถกำหนดมาตรการกำกับดูแลเงินสกุลเข้ารหัสได้อย่างเหมาะสม และมีองค์ความรู้เท่ากันกับพัฒนาการของผู้กระทำผิด รวมถึงการพัฒนาทักษะเชิงปฏิบัติการได้ทันต่อนวัตกรรมทางเทคโนโลยี่สนับสนุนระบบปฏิบัติการในเครือข่ายเงินสกุลเข้ารหัสที่อาจขยายตัวอย่างรวดเร็ว

กล่าวโดยสรุป ผู้วิจัยมีความเห็นว่าการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสยังคงเป็นกลไกที่มีระดับความน่าสนใจต่ออาชญากรรมธุรกิจผิดกฎหมาย หรืออาชญากรทางเศรษฐกิจอย่างสูง เนื่องจากนี้ยังปรากฏข้อถกเถียงเรื่องสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส ที่ยังคงมีความเห็นที่แตกต่างกันในมาตรการทางกฎหมายของแต่ละประเทศอย่างเห็นได้ชัด กล่าวคือ บางประเทศไม่ให้การยอมรับเงินสกุลเข้ารหัส และถือว่าธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสเป็นสิ่งต้องห้ามและผิดกฎหมาย เช่น ประเทศจีน สำหรับบางประเทศยอมรับเงินสกุลเข้ารหัสเป็นสิ่งถูกต้องตามกฎหมายรวมถึงส่งเสริมการดำเนินงานของธุรกิจที่เกี่ยวข้อง เช่น ประเทศญี่ปุ่น และบางประเทศยอมรับเงินสกุลเข้ารหัสเป็นสิ่งที่ชอบด้วยกฎหมายในบางลักษณะ แต่จะมีกฎเกณฑ์ในการกำกับอย่างเคร่งครัด เช่น ประเทศไทย ดังนั้นธุรกรรมเงินสกุลเข้ารหัสจึงกลายเป็นโอกาสแก่ผู้กระทำผิดจากการใช้ช่องว่างทางกฎหมายเป็นเงื่อนไขในการเลือกสถานที่หรือประเทศที่จะใช้ทำธุรกรรม อีกประการสำคัญหนึ่ง คือ คุณสมบัติเฉพาะอันเป็นเอกลักษณ์ของเงินสกุลเข้ารหัสที่ใช้ระบบปฏิบัติการบล็อกเชนหรือเทียบเท่าที่รักษาความเป็นส่วนตัวของผู้ใช้บริการโดยไม่ต้องระบุตัวตน ซึ่งถือเป็นการให้ประโยชน์แก่ผู้ใช้งานมีโอกาสหลีกพ้นจากการตรวจพิสูจน์แหล่งที่มาของเงินได้ หรือเจ้าหน้าที่ไม่สามารถตรวจสอบได้สำเร็จ ดังนั้น ผู้วิจัยจึงให้ความสนใจศึกษาคุณลักษณะเฉพาะของเงินสกุลเข้ารหัส และบริบทของเงินสกุลเข้ารหัส ที่เป็นปัจจัยที่มีอิทธิพลต่อผู้กระทำผิดในการเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงินสำหรับผลประโยชน์ที่ได้จากการกระทำผิดกฎหมาย รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส รวมถึงศึกษาแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากล ทั้งนี้กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ถือเป็นประเด็นปัญหาสำคัญในปัจจุบันที่จะส่งผลกระทบต่อความมั่นคงของระบบเศรษฐกิจสากล ซึ่งไม่จำกัดเฉพาะขอบเขตประเทศใด รวมถึงความปลอดภัยมั่นคงต่อบริบททางสังคมโลก โดยเฉพาะอย่างยิ่ง ถ้าพัฒนาการของระบบเงินสกุลเข้ารหัสได้รับการยอมรับในวงกว้างขึ้น จนสามารถใช้เป็นสื่อกลางในการชำระค่าสินค้าและบริการได้โดยตรงอย่างปกติธุระมากขึ้น จะยิ่งยากต่อการตรวจสอบสืบค้นมากขึ้นเช่นกัน ดังนั้น ผู้วิจัยจึงเล็งเห็นความสำคัญของประเด็นปัญหานี้ที่สมควรแก่การศึกษาวิจัยเชิงลึก เพื่อสร้างความเข้าใจให้แก่สังคมและนำเสนอแนวคิดในการกำหนดแนวทางการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัสอย่างเหมาะสมต่อไป

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ในการศึกษาวิจัยนี้ ผู้วิจัยได้กำหนดขอบเขตการศึกษาเฉพาะเงินสกุลเข้ารหัส ซึ่งมีคุณลักษณะเฉพาะบางประการที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสของผู้กระทำผิดกฎหมาย อย่างไรก็ตาม ด้วยคุณลักษณะทางเทคนิคของเงินสกุลเข้ารหัส ซึ่งเป็นหน่วยชุดรหัสข้อมูลอิเล็กทรอนิกส์เพื่อการโอนมูลค่ากันระหว่างบุคคลด้วยระบบนิเวศบนระบบปฏิบัติการบล็อกเชนหรือเทียบเท่า โดยสามารถเชื่อมโยงธุรกรรมข้ามเขตประเทศแบบไร้พรมแดน อันเป็นคุณลักษณะทางเทคนิคสำคัญในทำนองเดียวกับเงินสกุลดิจิทัลหรือสินทรัพย์ดิจิทัล ทั้งนี้การศึกษาวิจัยนี้ คาดหมายว่าจะสามารถนำผลการศึกษาแนวทางการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ไปประยุกต์ปรับใช้เพื่อขยายขอบเขตการบังคับใช้ให้ครอบคลุมถึงการฟอกเงินโดยธุรกรรมของชุดรหัสข้อมูลอิเล็กทรอนิกส์ของเงินสกุลดิจิทัล หรือสินทรัพย์ดิจิทัลอื่นต่อไปได้

1.2 ปัญหาวิจัย

1.2.1 เงินสกุลเข้ารหัสมีรูปแบบและคุณลักษณะเฉพาะ รวมถึงบริบทของกลไกในการทำงานเป็นอย่างไร จึงเป็นปัจจัยที่มีอิทธิพลต่อผู้กระทำผิดในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสสำหรับผลประโยชน์ที่ได้จากการกระทำผิด

1.2.1 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสซึ่งทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสเป็นอย่างไร

1.2.2 แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากลเป็นอย่างไร

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

1.3 วัตถุประสงค์การวิจัย

1.3.1 เพื่อศึกษาคุณลักษณะเฉพาะ กลไกการทำงาน และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส รวมถึงบริบทของเงินสกุลเข้ารหัสที่เป็นปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

1.3.2 เพื่อศึกษารูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และใช้กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสสำหรับผลประโยชน์ที่ได้จากการกระทำผิด

1.3.3 เพื่อศึกษาแนวทางการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากล

1.4 ขอบเขตการิจัย

1.4.1 ขอบเขตด้านเนื้อหา

เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสมีพลวัต และเพิ่มจำนวนสกุลเงินสกุลเข้ารหัสใหม่ขึ้นอย่างต่อเนื่อง รวมถึงบริบททางกฎหมายระหว่างประเทศและในประเทศไทยที่มีต่อเงินสกุลเข้ารหัสยังมีความแตกต่างอย่างมีนัยสำคัญ อีกทั้งเป็นช่วงเวลาที่แต่ละประเทศอยู่ระหว่างการพัฒนาบริบททางกฎหมายเพื่อการกำกับดูแลเงินสกุลเข้ารหัส ดังนั้นการศึกษาวิจัยนี้ จึงมีขอบเขตการศึกษาบริบทของเงินสกุลเข้ารหัส และคุณลักษณะเฉพาะของเงินสกุลเข้ารหัส ที่ดำเนินการบนระบบนิเวศบนระบบปฏิบัติการบล็อกเชนหรือเทียบเท่า โดยกำหนดขอบเขตการศึกษาเฉพาะคุณลักษณะของเงินสกุลเข้ารหัสหลักซึ่งมีขนาดมูลค่าทางการตลาดรวมกันเกินกว่าร้อยละ 80 ของมูลค่าทางการตลาดรวมและเป็นเงินสกุลเข้ารหัสหลักในการชี้นำด้านนวัตกรรมทางเทคโนโลยี่ ซึ่งเป็นตัวแทนของเงินสกุลเข้ารหัสซึ่งดำเนินการบนระบบนิเวศบนระบบปฏิบัติการบล็อกเชนเช่นเดียวกัน อันประกอบด้วยเงินสกุลเข้ารหัสในอันดับต้นได้แก่ บิตคอยน์ อีเทอเรียม และริปเพิล สำหรับการศึกษาแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส มีขอบเขตการศึกษาจำกัดเฉพาะองค์กรในประเทศไทย และองค์กรระหว่างประเทศ 2 แห่ง ได้แก่ Financial Action Task Force on Money Laundering (FATF) ซึ่งเป็นคณะทำงานที่จัดตั้งขึ้นตามมติที่ประชุมกลุ่มประเทศเศรษฐกิจขนาดใหญ่ (G7 Summit) และ European Union Anti-Money Laundering Directives (AMLD) เป็นมาตรการทางกฎหมายที่ออกบังคับใช้โดยสภาสหภาพยุโรป (The European Parliament and of The Council) เพื่อป้องกันการใช้สถาบันการเงินในสหภาพยุโรปเป็นเครื่องในการฟอกเงิน หรือสนับสนุนทางการเงินแก่ผู้ก่อการร้าย นอกจากนี้ได้ทำการศึกษานโยบายและมาตรการทางกฎหมายของนานาชาติที่มีต่อเงินสกุลเข้ารหัส โดยการศึกษาเปรียบเทียบมาตรการของประเทศญี่ปุ่น ประเทศจีน และประเทศไทย ซึ่งเป็นประเทศที่ตั้งอยู่ในเขตภูมิภาคเอเชียร่วมกัน แต่กลับมีมาตราการทางกฎหมายต่อเงินสกุลเข้ารหัสที่แตกต่างกันอย่างมีนัยสำคัญ รวมถึงขอบเขตเนื้อหาการศึกษาวิจัยจากผู้ให้ข้อมูลสำคัญเกี่ยวกับ แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ทั้งด้านมาตรการกำกับดูแลและแนวทางการปฏิบัติงานเพื่อบังคับใช้มาตรการให้เกิดผลสัมฤทธิ์

1.4.2 ขอบเขตด้านผู้เชี่ยวชาญ และผู้ให้ข้อมูลสำคัญ

การศึกษาวิจัยนี้ มีบริบทเกี่ยวกับการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส จึงได้กำหนดขอบเขตด้านผู้เชี่ยวชาญในการมีส่วนร่วมการวิจัยโดยอ้างอิงจากหน่วยงานซึ่งมีความสัมพันธ์และหน้าที่รับผิดชอบเกี่ยวข้องกับการปฏิบัติงาน ตามมาตรการสากลว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย รวมถึงการกำกับดูแลการดำเนินกิจกรรมด้านเทคโนโลยี่ดิจิทัลเพื่อเศรษฐกิจและสังคม โดยได้จัด

กลุ่มผู้เชี่ยวชาญตามภารกิจหน้าที่ความรับผิดชอบของหน่วยงานออกเป็น 4 กลุ่ม ได้แก่ กลุ่มที่ 1 หน่วยงานราชการ กระทรวง คณะกรรมการ หรือหน่วยงานหลักตามมาตรการสากลว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการกำกับดูแลการดำเนินกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม, กลุ่มที่ 2 หน่วยงานองค์กรสถาบันการเงิน, กลุ่มที่ 3 หน่วยงานองค์กรในกระบวนการยุติธรรมและหน่วยปฏิบัติงาน, และกลุ่มที่ 4 หน่วยงานองค์กรธุรกิจ หรือผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงินและด้านอื่นๆ

ทั้งนี้ ในการศึกษาวิจัยได้ใช้วิธีการเลือกผู้ให้ข้อมูลสำคัญแบบเฉพาะเจาะจงจากผู้เชี่ยวชาญในแต่ละกลุ่ม โดยการขอความร่วมมือจากผู้เชี่ยวชาญซึ่งเป็นบุคคลากรประจำหน่วยงานข้างต้นเป็นผู้ให้ข้อมูลสำคัญในขั้นตอนการดำเนินการวิจัย อย่างไรก็ตามในขณะดำเนินการวิจัยมีข้อจำกัดด้านความพร้อมของผู้ให้ข้อมูลสำคัญ เนื่องจากเกิดสถานการณ์การแพร่ระบาดของเชื้อโควิด-19 ไปทั่วโลกรวมถึงประเทศไทย ดังนั้นหลายหน่วยงานได้มีมาตรการป้องกันการแพร่ระบาดของเชื้อโควิด-19 โดยให้บุคคลกรของหน่วยงานส่วนใหญ่ปฏิบัติงานที่บ้าน (Work from Home) จึงเป็นข้อจำกัดในความพร้อมด้านเวลาและวิธีการติดต่อเพื่อเก็บรวบรวมข้อมูลกับผู้ให้ข้อมูลสำคัญ อย่างไรก็ตามในระหว่างการวิจัยได้ทำการปรับวิธีการดำเนินงานบางประการ เพื่อความเหมาะสมต่อสถานการณ์เว้นระยะห่างทางสังคม (Social Distancing) โดยการติดต่อประสานกับผู้ให้ข้อมูลสำคัญส่วนใหญ่ใช้ระบบสื่อสารออนไลน์ รวมถึงการเก็บข้อมูลการสัมภาษณ์เชิงลึกทางโทรศัพท์ Zoom, Microsoft Team, Line และการสำรวจความเห็นตามเทคนิควิธีเดลฟายด้วยการส่งแบบสำรวจทาง Email และการเก็บรวมรวมความเห็นด้วยการตอบกลับทาง Email, Line, Messenger เช่นกัน

1.4.3 ขอบเขตด้านระยะเวลา

เนื่องจาก ธุรกรรมเงินสกุลเข้ารหัสมีพลวัตเปลี่ยนแปลงไปตามสภาพเศรษฐกิจและสังคมที่มีระดับการยอมรับความเป็นสากลของเงินสกุลเข้ารหัสมากขึ้น รวมถึงอาชญากรมีพัฒนาการด้านอาชญากรรมไซเบอร์อย่างต่อเนื่อง ดังนั้น การศึกษาวิจัยนี้จึงจำกัดขอบเขตระยะเวลาการศึกษาวิจัยเชิงเอกสารที่เกี่ยวข้องกับเงินสกุลเข้ารหัส รวมถึงมาตรการกำกับดูแลเงินสกุลเข้ารหัสของหน่วยงานที่ได้ศึกษาซึ่งประกาศบังคับใช้ระหว่างปี 2016 ถึงเดือนมีนาคม 2021 เนื่องจากระบบตลาดเงินสกุลเข้ารหัสได้มีการปรับตัวเมื่อบิตคอยน์ (เงินสกุลเข้ารหัสแรก) มีการเปลี่ยนแปลงเชิงมูลค่าอย่างผันผวน ภายหลังได้รับผลกระทบจากการปราบปรามอาชญากรรมทางเศรษฐกิจที่ทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส จึงส่งผลถึงความปลี่ยนแปลงต่อเนื่อง รวมถึงการเข้าลงทุนในเงินสกุลเข้ารหัสจำนวนมหาศาลของกองทุนการเงินระดับสากล และธุรกิจขนาดใหญ่เริ่มมีนโยบายในการรับชำระราคาค่าสินค้าด้วยเงินสกลุเข้ารหัสมากขึ้น อีกทั้งรัฐบาลหลายประเทศได้ตระหนักถึงความสำคัญ และความจำเป็นในการศึกษาเรียนรู้บริบทของเงินสกุลเข้ารหัสเพื่อเตรียมรับสถานการณ์ที่อาจมีผลกระทบ

ต่อเสถียรภาพของระบบการเงิน โดยอาจประกาศมาตรการเพิ่มเติมในการกำกับดูแลเงินสกุลเข้ารหัส เพื่อสร้างความมั่นคง และความปลอดภัยจากอาชญากรที่ทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

1.5 นิยามศัพท์เฉพาะที่ใช้ในการวิจัย

1.5.1 การฟอกเงิน (Money Laundering)

หมายถึง กระบวนการจัดการซ่อนเร้นผลประโยชน์ที่ผู้กระทำผิดหรืออาชญากรได้รับจากการกระทำผิดกฎหมาย หรือการก่ออาชญากรรมตามความผิดมูลฐานของบทบัญญัติแห่งกฎหมาย เพื่อกลบเกลื่อนร่องรอยเส้นทางการเงิน หรือปิดบังซ่อนเร้นแหล่งที่มาของเงิน หรือทรัพย์สินจากการกระทำที่ไม่ชอบด้วยกฎหมาย รวมถึงการแปรสภาพเงินตราหรือทรัพย์สินดังกล่าวให้เป็นเงินหรือทรัพย์สินที่ชอบด้วยกฎหมาย เพื่อหลีกเลี่ยงการติดตามจับกุม หรือยึดอายัดจากหน่วยงานบังคับใช้กฎหมาย

1.5.2 การฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส
(Money Laundering by Cryptocurrency Transactions)

หมายถึง กระบวนการฟอกเงินเพื่อจัดการซ่อนเร้นผลประโยชน์ที่ผู้กระทำผิด หรืออาชญากรที่ได้รับจากการกระทำผิดกฎหมายหรือการก่ออาชญากรรม เพื่อกลบเกลื่อนร่องรอยเส้นทางธุรกรรมในระบบนิเวศ หลีกเลี่ยงการติดตามจับกุม หรือยึดอายัด รวมถึงการแปรสภาพเป็นเงินตราหรือทรัพย์สินที่ชอบด้วยกฎหมาย โดยใช้เงินสกุลเข้ารหัสซึ่งเป็นชุดรหัสข้อมูลอิเล็กทรอนิกส์และถือเป็นทรัพย์สินไร้รูปร่างทางกายภาพแต่สามารถแสดงมูลค่าในตัวเองได้ เพื่อเป็นเครื่องมือในการทำธุรกรรมการฟอกเงิน

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

1.5.3 กลไกการทำงานของธุรกรรมเงินสกุลเข้ารหัส
(Operation on Cryptocurrency Transaction)

หมายถึง กระบวนการที่ทำให้ระบบนิเวศเงินสกุลเข้ารหัสสามารถดำเนินการขับเคลื่อนระบบปฏิบัติงานได้ โดยมีองค์กร หน่วยงาน กลุ่มบุคคลหรือบุคคล รวมถึงเครื่องมือคอมพิวเตอร์และอุปกรณ์สื่อสาร ซึ่งมีปฏิสัมพันธ์ทางการสื่อสารเชื่อมโยงกันในระบบเครือข่าย เป็นกลไกดำเนินการให้สามารถดำเนินธุรกรรมเงินสกุลเข้ารหัส เพื่อโอนมูลค่าระหว่างกันประสบผลสำเร็จตามเป้าหมาย

1.5.4 เงินสกุลเข้ารหัส (Cryptocurrency)

หมายถึง หน่วยชุดรหัสข้อมูลอิเล็กทรอนิกส์ในระบบนิเวศโครงข่ายการสื่อสารอิเล็กทรอนิกส์ที่สามารถทำธุรกรรมเชื่อมโยงข้ามเขตประเทศแบบไร้พรมแดน เพื่อการโอนมูลค่าระหว่างบุคคลต่อบุคคลโดยตรง ในระบบปฏิบัติการบล็อกเชนซึ่งเป็นระบบงานเปิด และมีระบบจัดเก็บฐานข้อมูลสาธารณะซึ่งบุคคลทั่วไปสามารถเข้าถึงได้ โดยไม่มีหน่วยงานตัวกลางใดในการกำกับดูแล และไม่มีหน่วยงานของรัฐใดให้การรับรองมูลค่าหรือมีระบบการอ้างอิงมูลค่า

1.5.5 ธุรกรรมการเงิน (Financial Transaction)

หมายถึง กิจกรรมที่เกี่ยวกับการทำนิติกรรมสัญญา หรือการดำเนินการใดๆ ทางการเงินกับผู้อื่น รวมถึงข้อตกลงที่เป็นตรรกะอิเล็กทรอนิกส์ ซึ่งเป็นผลบังคับใช้ทางกฎหมาย หรืออยู่บนพื้นฐานการยอมรับของคู่สัญญาทั้งสองฝ่าย ทั้งนี้ให้หมายรวมถึงธุรกรรมการเงินที่กระทำบนระบบนิเวศเงินสกุลเข้ารหัสบนระบบออนไลน์ ในรูปแบบ *“ธุรกรรมการเงินสกุลเข้ารหัส”*

1.5.6 แนวทางการป้องกันและปราบปราม (Prevention and Suppression)

หมายถึง บทบัญญัติตามกฎหมาย นโยบาย มาตรการ แนวปฏิบัติงาน หรือข้อแนะนำซึ่งหน่วยงานของรัฐ รวมถึงองค์กรระหว่างประเทศที่เกี่ยวข้องกับการป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย เพื่อการบังคับใช้ในทางปฏิบัติให้บรรลุวัตถุประสงค์ในการป้องกันเหตุกระทำผิด ลดเหตุแห่งการกระทำผิด หรือการตรวจสอบสืบค้นธุรกรรมของผู้กระทำผิดเพื่อให้เข้าถึงแหล่งผลประโยชน์จากการกระทำผิด และการบรรเทาความเสียหายแก่ผู้ได้รับผลกระทบ รวมถึงการส่งเสริมให้เกิดการตระหนักรู้ต่อสาธารณะถึงผลกระทบจากการกระทำผิด

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

1.5.7 ผู้ใช้งาน (User)

หมายถึง บุคคลหรือกลุ่มบุคคล หน่วยงาน หรือเครื่องมืออุปกรณ์ ซึ่งเป็นผู้ดำเนินการติดต่อเข้าถึงระบบนิเวศเงินสกุลเข้ารหัสเพื่อทำการส่งคำสั่ง รับสั่งคำสั่ง หรือประมวลผลโปรแกรมคำสั่ง โดยใช้คอมพิวเตอร์ โปรแกรมประยุกต์ ระบบการสื่อสารเป็นเครื่องมือดำเนินการให้บรรลุผลตามความประสงค์ ซึ่งหมายรวมถึงแต่ไม่จำกัดเฉพาะ ผู้โอน ผู้รับโอน นักขุด หรือผู้ให้บริการอื่นที่เกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัส

1.5.8 รหัสที่ตั้งของผู้ใช้งาน (IP Address)

หมายถึง หมายเลขเฉพาะประจำแต่ละเครื่องคอมพิวเตอร์ หรืออุปกรณ์สื่อสารที่เชื่อมต่อในระบบนิเวศเพื่อประโยชน์ในการระบุตัวตนของอุปกรณ์คอมพิวเตอร์ หรือแสดงสถานที่ตั้งของอุปกรณ์บนเครือข่าย ซึ่งปัจจุบันหมายเลขแสดงรหัสที่ตั้งของผู้ใช้งานประกอบด้วยเลข 4 ชุด ที่ประกอบเข้าด้วยกันและจะแสดงค่าไม่ซ้ำกันในแต่ละเครื่องคอมพิวเตอร์ หรืออุปรณ์สื่อสาร จึงถือเป็นสิ่งหนึ่งในการแสดงอัตลักษณ์ของคอมพิวเตอร์หรืออุปกรณ์สื่อสารนั้นได้

1.5.9 ระบบนิเวศเงินสกุลเข้ารหัส (Cryptocurrency Ecosystem)

หมายถึง ความสัมพันธ์ระหว่างกลุ่มคอมพิวเตอร์หรืออุปกรณ์สื่อสารชนิดต่างๆ กับระบบปฏิบัติการของเงินสกุลเข้ารหัสที่เชื่อมต่อกันเป็นเครือข่ายออนไลน์บนระบบอินเตอร์เน็ต เพื่อให้ผู้ใช้งานสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และโอนมูลค่าของเงินสกุลเข้ารหัสระหว่างกันได้

1.5.10 ระบบปฏิบัติการบล็อกเชน (Blockchain)

หมายถึง ระบบปฏิบัติในการจัดเก็บข้อมูลธุรกรรมต่างๆบนเครือข่ายฐานข้อมูลสาธารณะแบบกระจายศูนย์ (Distributed Ledger Technology – DLT) และมีลักษณะการจัดเก็บรายการธุรกรรมเป็นชุดข้อมูล (Block) ซึ่งมีกลไกการสร้างความสัมพันธ์ระหว่างรหัสส่วนท้ายของชุดข้อมูลก่อนหน้า กับรหัสส่วนต้นของชุดข้อมูลลำดับถัดไปโดยจัดเก็บเชื่อมโยงกันอย่างต่อเนื่องเป็นห่วงโซ่ของชุดข้อมูล (Chain) ซึ่งมีกระบวนการพิสูจน์ยืนยันชุดข้อมูลจากผู้ร่วมใช้งาน โดยไม่มีหน่วยงานตัวกลางใดในการกำกับดูแลระบบปฏิบัติการ อีกทั้งผู้ใช้งานทั่วไปสามารถเข้าถึงฐานข้อมูลสาธารณะและระบบงานเปิดที่ผู้ใช้งานสามารถพัฒนาโปรแกรมประยุกต์เชื่อมต่อกับระบบปฏิบัติการนี้ได้

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

1.6 ประโยชน์ที่คาดว่าจะได้รับ

1.6.1 ทำให้ทราบถึงคุณลักษณะเฉพาะ และกลไกการทำงานของเงินสกุลเข้ารหัส ปัจจัยที่มีอิทธิพลต่อการทำธุรกรรมการฟอกเงินโดยเงินสกุลเข้ารหัส รวมถึงการเปรียบเทียบกระบวนการฟอกเงินที่ไม่ชอบด้วยกฎหมาย กับกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ในการนำธุรกรรมเข้าสู่ระบบนิเวศเงินสกุลเข้ารหัสเพื่อการปกปิดตัวตน จนถึงขั้นตอนการแลกเปลี่ยนเป็นเงินสกุลเข้ารหัส หรือเงินสกุลดิจิทัลอื่นที่ชอบด้วยกฎหมาย หรือเป็นเงินตราหรือสินทรัพย์อื่นที่ชอบด้วยกฎหมาย

1.6.2 ทำให้ทราบถึงรูปแบบของอาชญกรรมที่เกี่ยวข้องกับการกระทำผิดโดยใช้เงินสกุลเข้ารหัสเป็นสื่อกลาง รวมถึงปัจจัยที่มีอิทธิพลต่อการเลือกใช้การฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

1.6.3 ทำให้ทราบถึงแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสของประเทศซึ่งมีนโยบายและมาตรการทางกฎหมายต่อเงินสกุลเข้ารหัสที่แตกต่างกัน รวมถึงแนวทางการกำหนดกรอบวิธีการปฏิบัติงานอย่างเหมาะสมต่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสของหน่วยงานกำกับที่เกี่ยวข้อง

1.6.4 ทำให้ได้แนวทางการกำกับดูแลเงินสกุลเข้ารหัส แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสอย่างเหมาะสมที่อาจมีโอกาสเกิดขึ้นในบริบทของประเทศไทยและสากล ทั้งนี้แนวทางการกำกับดูแล รวมถึงแนวทางการป้องกันและปราบปรามข้างต้นสามารถนำไปประยุกต์ปรับใช้ในการขยายขอบเขตการกำกับดูแลให้ครอบคลุมเงินสกุลดิจิทัล หรือสินทรัพย์ดิจิทัล ซึ่งมีคุณสมบัติเฉพาะด้านเทคโนโลยีบนระบบนิเวศบนระบบปฏิบัติการบล็อกเชน หรือระบบปฏิบัติการอื่นที่เทียบเคียงกันได้

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 2
การทบทวนวรรณกรรม (แนวคิด ทฤษฎีและงานวิจัยที่เกี่ยวข้อง)

การวิจัยเรื่อง *“แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส (Prevention and Suppression of Money Laundering by Cryptocurrency Transactions)”* ผู้วิจัยได้ศึกษาข้อมูลจากการทบทวนวรรณกรรม อันประกอบด้วย แนวคิด ทฤษฎี เอกสาร และงานวิจัยที่เกี่ยวข้องกับเนื้อหาในขอบเขตการวิจัย โดยขอนำเสนอตามลำดับดังต่อไปนี้

2.1 แนวคิดเกี่ยวกับบริบทของเงินสกุลเข้ารหัส
- 2.1.1 วิวัฒนาการของเงินสกุลเข้ารหัส
- 2.1.2 คุณลักษณะเฉพาะ และกลไกการทำงานของธุรกรรมเงินสกุลเข้ารหัส
- 2.1.3 ระบบนิเวศของการทำธุรกรรมเงินสกุลเข้ารหัส
- 2.1.4 เงินสกุลเข้ารหัสกับความเป็นเงินตรา
- 2.1.5 สถานภาพทางกฎหมายของเงินสกุลเข้ารหัส
- 2.1.6 นโยบายและมาตรการทางกฎหมายของนานาชาติที่มีต่อเงินสกุลเข้ารหัส

2.2 แนวคิดเกี่ยวกับกระบวนการฟอกเงิน
- 2.2.1 กระบวนการฟอกเงิน
- 2.2.2 กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส
- 2.2.3 ปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส
- 2.2.4 การปกปิดตัวตนของผู้ใช้งานเงินสกุลเข้ารหัสด้วยระบบปฏิบัติการเฉพาะ
- 2.2.5 การกลบเกลื่อนร่องรอยเส้นทางธุรกรรมการโอนเงินสกุลเข้ารหัส

2.3 ทฤษฎีทางสังคมวิทยาที่เกี่ยวข้อง
- 2.3.1 กระบวนทัศน์การเคลื่อนย้าย (Mobility Paradigm)
- 2.3.2 ทฤษฎีความซับซ้อน (Complexity Theory)
- 2.3.3 แนวคิดวัตถุนิยมวิภาษวิธี (Dialectical Materialism)

2.4 ทฤษฎีทางอาชญวิทยาที่เกี่ยวข้อง
- 2.4.1 ทฤษฎีปกตินิสัย (Routine Activity Theory)
- 2.4.2 ทฤษฎีการเลือกกระทำอย่างมีเหตุผล (Rational Choice Theory)
- 2.4.3 ทฤษฎีการป้องกันอาชญากรรม (Situation Crime Prevention)

2.4.4 อาชญากรรมเศรษฐกิจ

2.4.5 อาชญากรรมไซเบอร์และอาชญากรรมองค์กร

2.5 กฎหมายและข้อบัญญัติขององค์กรระหว่างประเทศที่เกี่ยวข้องกับการกำกับดูแล

2.5.1 Financial Action Task Force on Money Laundering (FATF)

2.5.2 European Union Anti-Money Laundering Directives (EU-AMLD)

2.6 กฎหมายไทยที่เกี่ยวข้อง

2.6.1 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน

2.6.2 พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล

2.6.3 พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ

2.7 งานวิจัยที่เกี่ยวข้อง

2.7.1 งานวิจัยเกี่ยวกับมาตรการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

2.7.2 งานวิจัยเกี่ยวกับเทคนิคการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

2.8 กรอบแนวคิดการวิจัย

2.1 แนวคิดเกี่ยวกับบริบทของเงินสกุลเข้ารหัส

2.1.1 วิวัฒนาการของเงินสกุลเข้ารหัส

เงินสกุลเข้ารหัส (Cryptocurrency) ได้เป็นที่รับรู้ครั้งแรกกันในนาม ***"บิตคอยน์ (Bitcoin-BTC)"*** เมื่อปี 2008 โดย ซาโตชิ นากาโมโต (Nakamoto, 2008) ได้นำเสนอรายงานต่อสาธารณะในหัวข้อ *"บิตคอยน์ : ระบบการโอนเงินทางอิเล็กทรอนิกส์ระหว่างบุคคลโดยตรง (Bitcoin: A Peer-to-Peer Electronic Cash System)"* ได้อธิบายถึงระบบการโอนเงินทางอิเล็กทรอนิกส์ระหว่างบุคคลโดยตรงที่ไม่ต้องผ่านการกำกับของสถาบันการเงิน หรือหน่วยงานตัวกลางใด ทำให้สามารถลดต้นทุนค่าธรรมเนียมการทำธุรกรรมที่เกิดจากความเชื่อถือต่อตัวกลาง เป็นการสร้างระบบความน่าเชื่อจากการตรวจพิสูจน์รายการด้วยการถอดรหัสข้อมูลคอมพิวเตอร์ (Proof-of-Work) แทน ทั้งนี้กระบวนการรับรองยืนยันแต่ละรายการจะเกิดขึ้นจากการทำงานของระบบนิเวศคอมพิวเตอร์ของแต่ละบุคคลที่เข้าร่วมเชื่อมต่อเป็นเครือข่าย ทำการถอดรหัสข้อมูลคณิตศาสตร์จนพิสูจน์ได้อย่างถูกต้องตามเงื่อนไข จากนั้นระบบจะทำการรวบรวมรายการดังกล่าวเป็นกลุ่มชุดข้อมูล (Block) เพื่อ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ยืนยันรายการและทำการสร้างรหัสส่วนท้ายของชุดข้อมูล (Nonce) รวมถึงสร้างรหัสส่วนต้นของชุดข้อมูล (Hash) ถัดไป ซึ่งทั้งสองส่วนมีรหัสข้อมูลเชื่อมโยงกัน เมื่อระบบดำเนินการอย่างต่อเนื่อง ความสัมพันธ์ระหว่างรหัสส่วนท้ายของชุดข้อมูลก่อนหน้า กับรหัสส่วนต้นของชุดข้อมูลถัดไปจะเชื่อมโยงกันอย่างต่อเนื่องเป็นห่วงโซ่ของชุดข้อมูล (Chain) จึงทำให้รายการข้อมูลที่ถูกบันทึกเข้าไปในระบบแล้วไม่สามารถแก้ไขเปลี่ยนแปลงได้ เว้นแต่จะต้องดำเนินการถอดรหัสและแก้ไขรหัสย้อนกลับทุกชุดข้อมูลทั้งห่วงโซ่ตามลำดับเท่านั้น ทั้งนี้ ผู้ที่เข้าร่วมพิสูจน์ยืนยันรายการ (Miner) จะได้รับค่าตอบแทนเป็นบิตคอยน์ที่ระบบสร้างขึ้นโดยอัตโนมัติ นอกจากนี้ ระบบนิเวศของบิตคอยน์เป็นระบบปฏิบัติการคอมพิวเตอร์แบบเปิด (Open Source) และรายการข้อมูลที่ถูกบันทึกไว้เป็นรูปแบบกระจายศูนย์ (Distributed Ledger) บันทึกอ้างอิงรหัสที่ตั้งเครื่องคอมพิวเตอร์ (IP Address) ที่ทำการพิสูจน์ยืนยันรายการ อีกทั้งบุคคลทั่วไปสามารถสืบค้นความเคลื่อนไหวของรายการได้โดยสาธารณะ เว้นแต่ ผู้รับโอนบิตคอยน์เท่านั้นที่จะมีรหัสเปิดส่วนบุคคล (Private Key) เพื่อเข้าถึงรหัสข้อมูล หรือรหัสแสดงมูลค่าของตนเอง กล่าวโดยสรุป ซาโตชิ นากาโมโต Nakamoto (2008) ได้แสดงทัศนะว่า

“บิตคอยน์เป็นระบบธุรกรรมการเงินอิเล็กทรอนิกส์ ที่ปราศจากการอ้างอิงความน่าเชื่อถือจากแหล่งใด ทั้งนี้ ระบบปฏิบัติงานจะสร้างเหรียญแสดงมูลค่าในรูปแบบลายมือดิจิทัลพร้อมระบบกำกับการยืนยันความเป็นเจ้าของ ที่สามารถลดทอนค่าธรรมเนียมธุรกรรมที่ถูกเรียกเก็บอย่างซ้ำซ้อนได้”

หลังจากบิตคอยน์ถูกนำเสนอต่อระบบการเงินโลก เงินสกุลเข้ารหัสสกุลแรกนี้ก็ได้รับการตอบรับจากผู้ใช้งานเพิ่มขึ้นอย่างต่อเนื่อง แต่ด้วยข้อจำกัดของระบบการตรวจพิสูจน์รายการแบบ Proof-of-Work (PoW) ที่ผู้ตรวจพิสูจน์หรือนักขุด (Miner) จะต้องใช้หน่วยประมวลผลกลาง (CPU) ของคอมพิวเตอร์ของตนในการเข้าร่วมเครือข่าย ซึ่งเป็นการใช้ทรัพยากรและพลังงานไฟฟ้าจำนวนมากในระหว่างระยะเวลาพิสูจน์ชุดข้อมูล (Block) นานถึงชุดละ 10 นาที ต่อมาในปี 2011 ชาร์ลี ลี (Charles Lee) อดีตพนักงานของกูลเกิลได้พัฒนาต่อยอดระบบปฏิบัติแบบเปิดของบิตคอยน์ และนำเสนอเงินสกุลเข้ารหัสสกุลใหม่ คือ **ไลต์คอยน์ (Litecoin-LTC)** ที่ยังคงรักษาคุณสมบัติสำคัญเดิมของบิตคอยน์ที่ใช้ระบบปฏิบัติการบล็อกเชน (Blockchain) โดยได้พัฒนาเพิ่มประสิทธิภาพของระบบตรวจพิสูจน์ข้อมูลที่มีระยะเวลาการทำงานลดลงจากเดิม 10 นาทีต่อชุดข้อมูล เป็น 2.5 นาทีต่อชุดข้อมูล จึงมีประสิทธิภาพการทำงานเร็วกว่าบิตคอยน์ถึง 4 เท่า รวมถึงได้กำหนดเพดานการสร้างเหรียญดิจิทัลสูงสุดของระบบไว้ที่ 84 ล้านเหรียญ สูงกว่าบิตคอยน์ที่กำหนดเพดานสูงสุดไว้ที่ 21 ล้านเหรียญเช่นกัน (Burniske & Tara, 2017)

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ริปเพิล (Ripple-XRP) เป็นเงินสกุลเข้ารหัสอีกสกุลหนึ่งที่ได้รับความนิยมจากสถาบันการเงินในการใช้งานในปัจจุบัน ซึ่งถูกพัฒนาขึ้นภายใต้ระบบปฏิบัติการบล็อกเชนเช่นกัน โดยในปี 2004 Ryan Fugger ได้สร้างระบบการพิสูจน์รายการขึ้นจากความไว้วางใจที่ส่งทอดต่อกันเป็นลูกโซ่ภายในชุมชนเครือข่ายของระบบนิเวศ หรือที่เรียกว่า *"เกตเวย์ (Gateway)"* ที่ไว้วางใจได้และสามารถตรวจสอบเส้นทางธุรกรรมของผู้ใช้งานได้ ซึ่งแตกต่างจากบิตคอยน์ที่ใช้นักขุดเป็นผู้ตรวจพิสูจน์รายการแบบกระจายศูนย์ที่เรียกว่าโอเพนคอยน์ (Open Coin) (Burniske & Tara, 2017) ส่งผลให้ระยะเวลาการพิสูจน์รายการสามารถทำได้รวดเร็วถึงประมาณแสนรายการต่อนาที เนื่องจากได้พัฒนาระบบปฏิบัติการบล็อกเชน เป็นระบบงานแบบปิดอนุญาตให้เฉพาะสมาชิกในชุมชนเครือข่ายเป็นผู้ใช้งานเท่านั้น อีกทั้งยังสามารถจัดการควบคุมธุรกรรมตลอดเส้นทางได้ ซึ่งต่างจากบิตคอยน์ที่เป็นระบบปฏิบัติการแบบกระจายศูนย์ (Girasa, 2018) โดยเริ่มได้รับความสนใจตั้งแต่ปี 2013 เมื่อบริษัทร่วมทุนขนาดใหญ่แห่งหนึ่งโดย Chris Larsen และ Jed McCaleb ได้ร่วมลงทุนเข้าถือครองเงินสกุลเข้ารหัสนี้ พร้อมทั้งปรับเปลี่ยนชื่อองค์กรเป็น *"ริปเพิลแล็บส์ (Ripple Lab)"* ดังนั้นจึงทำให้ได้รับความไว้วางใจจากธนาคารขนาดใหญ่ระดับโลกหลายแหล่งร่วมเป็นสมาชิก (Burniske & Tara, 2017) รวมถึงธนาคารพาณิชย์ในประเทศไทยหลายแห่ง เพื่อทำธุรกรรมการโอนเงินระหว่างประเทศโดยผ่านระบบการแปลงค่าผ่านริปเพิลที่รวดเร็ว และมีต้นทุนดำเนินการต่ำกว่าระบบการโอนเงินระหว่างประเทศในปัจจุบัน ดังนั้น จึงเป็นประเด็นที่ยังเป็นข้อสังเกตุที่ว่าควรจะเรียกขานริปเพิลอย่างไรระหว่าง *"เงินสกุลเข้ารหัส (Cryptocurrency)"* หรือ *"เงินสกุลดิจิทัล (Digital Currency)"*

วิวัฒนาการของเงินสกุลเข้ารหัสที่น่าสนใจอีกสกุลหนึ่งคือ **อีเทอเรียม หรือ อีเทอ (Ethereum or Ether)** ที่ได้รับการพัฒนาจากระบบปฏิบัติการบล็อกเชนเช่นเดียวกับบิตคอยน์ แต่ด้วยความตั้งใจของ Vitalik Buterin ผู้พัฒนาระบบที่ประสงค์จะให้เกิดความแตกต่างจากบิตคอยน์อย่างมีนัยสำคัญ โดยในปี 2014 ได้นำเสนอโปรแกรมซึ่งพัฒนาให้สามารถเชื่อมต่อสั่งการทำธุรกรรมภายใต้ตรรกะอย่างมีเงื่อนไขที่กำหนดไว้ล่วงหน้าในระบบปฏิบัติการแบบกระจายศูนย์ หรือที่เรียกว่า Smart Contract (Girasa, 2018) ซึ่งถือเป็นนวัตกรรมต่อยอดที่สำคัญของเงินสกุลเข้ารหัส เนื่องจากอีเทอเรียม หรือ อีเทอ ได้ก้าวข้ามความเป็นเงินตราเสมือนสำหรับการโอนมูลค่าระหว่างกัน แต่ได้พัฒนาตนเองขึ้นมาเป็นสินทรัพย์ หรือหลักทรัพย์ดิจิทัล ที่สามารถกำหนดมูลค่าของสินทรัพย์หรือหลักทรัพย์ไปพร้อมกับการกำหนดเงื่อนไขการปฏิบัติงาน ดังนั้นอีเทอจึงไม่เป็นเพียงเงินสกุลเข้ารหัสเท่านั้น แต่ยังสามารถนำไปประยุกต์เพื่อสนับสนุนงานด้านอื่นได้ด้วย การสร้างโปรแกรมตรรกะอย่างมีเงื่อนไขที่ต้องการกำหนดไว้ล่วงหน้า หรือที่เรียกว่า **Smart Contract** (Burniske & Tara, 2017) เช่น ระบบระเบียนโฉนดที่ดิน ระบบการลงคะแนนเสียงเลือกตั้ง เป็นต้น ทั้งนี้ พัฒนาการของระบบปฏิบัติการอีเทอเรียมมีความแตกต่างอย่างมีนัยสำคัญเมื่อเปรียบเทียบกับบิตคอยน์ คือ อีเทอเรียมสามารถประยุกต์ในงานด้านอื่นนอกเหนือจากการโอนมูลค่าทางการเงิน และระยะเวลาในการพิสูจน์รายการ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ใช้เวลาเพียง 14 วินาทีต่อชุดรายการ ในขณะที่บิตคอยน์ใช้เวลาถึง 10 นาทีต่อชุดข้อมูล ส่วนค่าตอบแทนแก่นักขุดของบิตคอยน์จะเกิดจากบิตคอยน์ที่สร้างขึ้นโดยระบบในอัตรา 50 BTC ต่อชุดข้อมูล (แต่ปัจจุบันลดลงเหลือ 6.25 BTC ต่อชุดข้อมูล) ส่วนผลตอบแทนแก่ผู้พิสูจน์รายการในระบบอีเทอเรียมจะเรียกว่าค่าเชื้อเพลิง (Fuel or Gas) ในอัตรา 5 ETC ต่อชุดข้อมูล และระบบการสร้างบิตคอยน์จะเกิดขึ้นจากการให้ผลตอบแทนแก่นักขุด ในขณะที่อีเทอเรียมจะถูกสร้างและนำเสนอขายแก่บุคคลทั่วไปที่สนใจเป็นครั้งแรก (Initial Coin Offering-ICO) (Girasa, 2018)

กล่าวโดยสรุป ในเดือนกันยายน ปี 2020 บิตคอยน์เป็นเงินสกุลเข้ารหัสที่มีขนาดมูลค่าทางการตลาดสูงสุดโดยมีมูลค่าประมาณ 191,500 ล้านเหรียญสหรัฐ หรือคิดเป็นร้อยละ 56.3 ของมูลค่าทางการตลาดรวมที่มีมูลค่าประมาณ 340,000 ล้านเหรียญสหรัฐ สำหรับอิเทอเรียมมีมูลค่าขนาดทางการตลาดเป็นอันดับสองด้วยมูลค่าประมาณ 41,200 ล้านเหรียญสหรัฐ และริปเพิลมีมูลค่าขนาดทางการตลาดด้วยมูลค่าประมาณ 10,900 ล้านเหรียญสหรัฐ[2] ในขณะนั้นมีเงินสกุลเข้ารหัสที่นำเสนอขายและหมุนเวียนในระบบการเงินโลกมีจำนวนมากกว่า 7,000 สกุล โดยเงินสกุลเข้ารหัสส่วนใหญ่จะดำเนินการบนระบบนิเวศบนระบบปฏิบัติการบล็อกเชน แต่อาจมีคุณสมบัติเฉพาะในรายละเอียดที่แตกต่างกันตามข้อกำหนดของแต่ละสกุลของเงินสกุลเข้ารหัส ทั้งนี้ **เงินสกุลเข้ารหัสอื่นนอกเหนือจากบิตคอยน์จะเรียกรวมกันว่า *“Alternative Coin” หรือ “Altcoin”***

อย่างไรก็ตาม เงินสกุลเข้ารหัสที่มีอิทธิพลสูงสุดต่อระบบการเงินในโลกดิจิทัลยังคงเป็นบิตคอยน์ ส่วนอีเทอเรียมและริปเพิลที่มีความสำคัญในลำดับรองลงไปนั้น มีระบบนิเวศหลักของเงินสกุลเข้าหลักบนระบบปฏิบัติการบล็อกเชนเช่นเดียวกัน แต่มีระบบปฏิบัติการเฉพาะเพิ่มเติมจากบิตคอยน์ กล่าวคือ ระบบนิเวศของอิเทอเรียมอนุญาตให้ผู้ใช้งานสามารถพัฒนาสร้างโปรแกรมประยุกต์ซึ่งกำหนดตรรกะเงื่อนไขร่วมปฏิบัติงานได้ หรือที่เรียกว่า Smart Contract บนระบบปฏิบัติการเปิดแบบกระจายศูนย์บนระบบปฏิบัติการบล็อกเชน ในขณะที่ระบบนิเวศของริปเพิลเป็นระบบปฏิบัติการแบบปิดบนระบบปฏิบัติการบล็อกเชนเช่นกัน แต่จำกัดการใช้งานเฉพาะผู้ใช้งานที่เป็นสมาชิก โดยการตรวจพิสูจน์รายการจะดำเนินการเฉพาะกลุ่มภายในระบบงานเครือข่ายเท่านั้น ซึ่งแตกต่างจากบิตคอยน์และอีเทอเรียมที่ใช้รูปแบบการปฏิบัติงานลักษณะกระจายศูนย์ ซึ่งผู้ใช้งานทุกรายในเครือข่ายสามารถเข้ามีส่วนร่วมทำหน้าที่ตรวจพิสูจน์รายการได้ (Hughes, 2017)

2.1.2 คุณลักษณะเฉพาะ และกลไกการทำงานของธุรกรรมเงินสกุลเข้ารหัส

จากรายงานของซาโตชิ ได้นำเสนอข้อมูลกลไกการทำงานของครือข่ายระบบนิเวศของบิตคอยน์ซึ่งเป็นเงินสกุลเข้ารหัสสกุลแรกของโลกด้วยระบบการโอนเงินทางอิเล็กทรอนิกส์โดยตรงหรือที่เรียกว่า *“White Paper”* (Nakamoto, 2008) ซึ่งในระยะเวลาต่อมาได้ถือเป็นธรรมเนียม

[2] ข้อมูลจากเว็บไซต์ CoinMarketCap.com ณ Last updated: Sun, 13 Sep 2020 15:25:18 UTC

ปฏิบัติสำหรับผู้พัฒนาระบบจะต้องนำเสนอรายงานลักษณะดังกล่าวต่อสาธารณะ เมื่อทำการเปิดตัวเงินสกุลเข้ารหัสใหม่ หรือสินทรัพย์ดิจิทัลอื่นที่ใช้ระบบปฏิบัติการบล็อกเชน (Burniske & Tara, 2017) โดยคุณลักษณะเฉพาะ และกลไกการทำงานของเงินสกุลเข้ารหัสแต่ละสกุลอาจมีความแตกต่างเฉพาะตัว แต่โดยทั่วไปจะมีคุณลักษณะเฉพาะและกลไกการทำงานเบื้องต้นเช่นเดียวกัน ดังนี้

2.1.2.1 ระบบการทำงานเป็นการติดต่อ **โอนมูลค่าด้วยรหัสข้อมูลกันโดยตรงระหว่างผู้ใช้งาน (Peer-to-Peer หรือ P2P) โดยไม่มีหน่วยงานกลาง** ตัวแทน หรือผู้ดูแลระบบนิเวศเงินสกุลเข้ารหัสเป็นผู้กำกับจัดการควบคุมระบบการทำงาน ซึ่งระบบจะปฏิบัติงานต่อเนื่องไปตามข้อมูลกลไกการทำงานที่ระบุใน White Paper (Nakamoto, 2008)

2.1.2.2 เนื่องจากกลไกการทำงานแบบไร้การควบคุมจากหน่วยงานใด ระบบได้เปิดกว้างต่อผู้ใช้งานสามารถติดต่อเข้าสู่ระบบได้อย่างไม่มีเงื่อนไข ผู้ใช้งานจึง**ไม่จำเป็นต้องลงทะเบียนอัตลักษณ์ตัวตนแท้จริงของผู้ใช้งานก่อนเข้าสู่ระบบ (Anonymity)** กล่าวคือ ผู้ใช้งานสามารถเลือกใช้นามแฝงเพื่อปิดบังตัวตนได้ ซึ่งถือเป็นคุณลักษณะเฉพาะที่สำคัญ ที่เป็นปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส (Girasa, 2018)

2.1.2.3 ธุรกรรมการโอนมูลค่าเงินสกุลเข้ารหัสระหว่างผู้โอนและผู้รับโอนนั้น โดยระบบจะทำการบันทึกรหัสข้อมูล (Cryptographic) ของรายการลักษณะคล้ายสมุดบัญชีเรียงลำดับข้อมูลเป็นชุด (Block) ซึ่งชุดข้อมูลจะมีรหัสความสัมพันธ์กับชุดข้อมูลในลำดับถัดไปอย่างต่อเนื่องคล้ายห่วงโซ่ (Chain) พร้อมทั้งทำการส่งรหัสเปิดสาธารณะ (Public Key) ซึ่งกำกับชุดข้อมูลที่ถูกบันทึกไปยังรหัสที่ตั้งปลายทางที่ระบุไว้ในระบบนิเวศ เพื่อผู้รับโอนปลายทางใช้รหัสเปิดส่วนบุคคล (Private Key) เสมือนเป็นลายมือดิจิทัลของเจ้าของบัญชีร่วมกับรหัสเปิดสาธารณะทั้งสองส่วนร่วมกันทำการเปิดรายการข้อมูลหรือมูลค่าที่ถูกจัดส่งมา (Burniske & Tara, 2017)

2.1.2.4 **กลไกการทำงานเป็นรูปแบบกระจายศูนย์ (Distributed)** ผู้ใช้งานทุกคนสามารถเข้าถึงฐานข้อมูลสาธารณะที่ถูกบันทึกในสมุดบัญชีอิเล็กทรอนิกส์ของระบบนิเวศได้อย่างไม่มีข้อจำกัด และสามารถติดตามความเคลื่อนไหวของรายการระหว่างผู้ใช้งานต่างๆได้ หรือที่เรียกว่าระบบบัญชีแบบกระจายศูนย์ (Distributed Ledger Technology – DLT) (Burniske & Tara, 2017)

2.1.2.5 **ระบบการตรวจพิสูจน์ยืนยันรายการ (Proof of Work – PoW)** ถือเป็นหัวใจสำคัญของกลไกในการสร้างความน่าเชื่อถือ ต่อระบบการโอนมูลค่าของเงินสกุลเข้ารหัส (Nakamoto, 2008) เนื่องจากระบบปฏิบัติการโอนมูลค่าทางอิเล็กทรอนิกส์ระหว่างผู้โอนและผู้รับโอนที่อาจไม่มีประวัติความสัมพันธ์ต่อกัน และเป็นการโอนมูลค่าในระบบนิเวศที่ข้ามเขตประเทศซึ่งไม่มีหน่วยงานกลางใดเข้ามาทำการรับรอง โดยระบบสร้างกลไกสร้างแรงจูงใจให้ผู้ใช้งานที่กระจายอยู่ทั่วไปทั้งโลก เพื่อเข้าสู่ระบบการแข่งขันเป็นผู้ตรวจพิสูจน์แก้โจทย์รหัสทางคณิตศาสตร์ประจำชุดข้อมูลก่อนการยืนยันด้วยฉันทามติของผู้ร่วมดำเนินการที่เรียกว่า **นักขุด (Miner)** ซึ่งนักขุดจะได้รับ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ค่าตอบแทนเป็นเงินสกุลเข้ารหัสที่ถูกกำหนดไว้ล่วงหน้า (Burniske & Tara, 2017) อย่างไรก็ตาม ระบบการตรวจพิสูจน์ยืนยันรายการ ได้ถูกพัฒนาขึ้นอีกหลายวิธีการสำหรับเงินสกุลเข้ารหัสอื่นที่เกิดขึ้นในภายหลัง ดังเช่นระบบ Proof-of-Stake หรือ PoS ที่ได้รับการยอมรับอันดับรองลงมาจาก PoW โดยวิธีการพิสูจน์ยืนยันรายการจะใช้ฉันทามติของผู้ร่วมดำเนินการตามสัดส่วนได้เสียจากการถือครองเงินสกุลเข้ารหัสนั้น (Girasa, 2018) นอกจากนี้นักพัฒนาระบบได้พัฒนาเทคนิควิธีการพิสูจน์ยืนยันรายการในระบบปฏิบัติการบล็อกเชน เพื่อประยุกต์ให้สอดคล้องกับวัตถุประสงค์ของเงินสกุลเข้ารหัสซึ่งนำเสนออีกหลายวิธีการ เช่น Proof-of-Service, Proof-of-Elapsed Time, Proof-of-Capacity และ Proof-of-Concept เป็นต้น (HouBen & Snyers, 2018)

2.1.2.6 เมื่อรายการรหัสข้อมูลในแต่ละชุดข้อมูลที่ได้รับการพิสูจน์ยืนยันแล้ว จะ**ไม่สามารถแก้ไขเปลี่ยนแปลงได้ (Immutable)** เนื่องจากรหัสที่ได้รับการพิสูจน์ในส่วนท้ายของชุดข้อมูลจะมีความสัมพันธ์ทางคณิตศาสตร์กับรหัสส่วนต้นของชุดข้อมูลถัดไป จึงเป็นการให้ความเชื่อมั่นแก่ผู้ใช้งานในระบบได้โดยเสมือนว่า *“ได้มีการทิ้งร่องรอยอันถาวรเหมือนกับการสลักลงบนแผ่นหินแกรนิต ทันทีที่ข้อมูลได้รับการพิสูจน์ยืนยันในชุดข้อมูลแล้ว ข้อมูลนั้นจะติดแน่นถาวรไม่อาจเปลี่ยนแปลงได้”* (Burniske & Tara, 2017)

2.1.2.7 ทั้งนี้กลไกการทำงานของเงินสกุลเข้ารหัสจะดำเนินการบน**ระบบปฏิบัติการบล็อกเชน (Blockchain) ซึ่งเป็นระบบงานแบบเปิด (Open Source)** ที่ผู้พัฒนาระบบงานสามารถเข้าถึงได้และสามารถนำไปพัฒนาประยุกต์ภายใต้เงื่อนไขเฉพาะของโปรแกรมเงินสกุลเข้ารหัสนั้นๆ เพื่อเชื่อมต่อเข้ากับระบบปฏิบัติการบล็อกเชนต่อไปได้ (Burniske & Tara, 2017)

2.1.3 ระบบนิเวศของการทำธุรกรรมเงินสกุลเข้ารหัส

การดำเนินธุรกรรมเงินสกุลเข้ารหัสโดยการเชื่อมต่อกันในระบบนิเวศ เพื่อให้ผู้ใช้งานสามารถติดต่อสื่อสาร แลกเปลี่ยนข้อมูล และโอนมูลค่าเงินสกุลเข้ารหัสระหว่างกันได้ โดยมีองค์กร หน่วยงาน กลุ่มบุคคลหรือบุคคล รวมถึงเครื่องมือคอมพิวเตอร์และอุปกรณ์สื่อสาร เป็นผู้ดำเนินการให้กลไกของระบบปฏิบัติการของเงินสกุลเข้ารหัสสามารถดำเนินการได้ตามความประสงค์ของผู้ใช้งาน ซึ่งประกอบด้วยบุคคล และเครือข่ายที่เกี่ยวข้อง ดังนี้

2.1.3.1 ผู้พัฒนาเงินสกุลเข้ารหัส (Inventor) หรือผู้ออกเงินสกุลเข้ารหัส (Issuer หรือ Promotor) เป็นบุคคล กลุ่มบุคคล หรือองค์กรที่สร้างระบบกลไกการทำงานของเงินสกุลเข้ารหัสโดยการวางรากฐานโครงสร้างระบบสนับสนุนการปฏิบัติงานภายใต้ระบบปฏิบัติการบล็อกเชน รวมถึงระบบนิเวศที่จะเปิดให้ผู้ใช้งานเข้าถึงได้ และเป็นผู้นำเสนอรายงานระบบนิเวศเงินสกุลเข้ารหัสนั้น เช่น ซาโตชิซึ่งคาดการณ์ว่าเป็นนามแฝงของกลุ่มบุคคลผู้พัฒนาระบบและนำเสนอเงินสกุลเข้ารหัสสกุลแรกของโลกที่เรียกว่า *“บิตคอยน์”* (Dewey, 2018)

2.1.3.2 นักขุด (Miner) เป็นบุคคลที่เข้าสู่ระบบเพื่อร่วมปฏิบัติหน้าที่ในการพิสูจน์ยืนยันรายการด้วยการพิสูจน์รหัสคณิตศาสตร์ของแต่ละชุดข้อมูล โดยได้รับเงินสกุลเข้ารหัสดังกล่าวเป็นค่าตอบแทน จึงถือเป็นกลุ่มบุคคลที่จะได้รับเงินสกุลเข้ารหัสจากระบบปฏิบัติการโดยตรง (Gitlitz, Buerstetta, Edited by, & Dewey, 2019) โดยที่มาของคำว่า *"นักขุด"* เป็นเสมือนกลุ่มคนที่เข้าไปขุดหาอัญมณี โลหะมีค่าในเหมืองเพชร หรือเหมืองทองคำ แต่นักขุดที่กล่าวถึงนี้เป็นนักขุดยุคใหม่ที่ได้รับผลตอบแทนเป็นเงินสกุลเข้ารหัส เนื่องจากต้องใช้ทรัพยากรในระบบคอมพิวเตอร์ของตนเป็นเครื่องมือในการเข้าร่วมพิสูจน์ยืนยัน (Girasa, 2018)

2.1.3.3 ผู้โอน (Sender) เป็นบุคคลที่ประสงค์จะนำเงินสกุลเข้ารหัสเข้าสู่ระบบนิเวศเพื่อส่งไปยังรหัสที่ตั้งปลายทางที่กำหนด โดยระบบไม่มีการกำหนดกฎเกณฑ์หรือเงื่อนไขให้ผู้ใช้งานต้องลงทะเบียนระบุข้อมูลส่วนบุคคล รวมถึงไม่มีระบบการพิสูจน์ตัวตนที่แท้จริงของผู้ใช้งาน ผู้โอนสามารถใช้นามแฝง ซึ่งระบบงานไม่อยู่ภายใต้บังคับในระบบจัดการของหน่วยงานรับผิดชอบใด จึงเป็นอุปสรรคต่อการตรวจสอบตัวตนของผู้ใช้งาน และเป็นปัจจัยที่มีอิทธิพลต่อผู้กระทำผิดที่จะใช้เป็นเครื่องมือในกระบวนการฟอกเงิน (Baath & Zellhorn, 2016)

2.1.3.4 ผู้รับโอน (Receiver) เป็นบุคคลที่จะได้รับเงินสกุลเข้ารหัสตามคำสั่งของผู้โอน โดยระบบงานสามารถปกปิดตัวตนของผู้ใช้งานได้เช่นกัน จึงเอื้อประโยชน์ต่อผู้กระทำผิดที่จะใช้เป็นเครื่องมือในกระบวนการฟอกเงิน ซึ่งในกลไกการป้องปราบการฟอกเงินควรให้ความสำคัญต่อการกำกับผู้รับโอนที่เป็นปลายทางของการถ่ายเทมูลค่า อย่างไรก็ตามระบบกฎหมายที่จะบังคับใช้ต่อเงินสกุลเข้ารหัสในแต่ละประเทศมีความแตกต่างกันและไม่มีความชัดเจนที่เป็นสากล ในขณะที่ระบบนิเวศมีการเชื่อมโยงถึงกันทุกประเทศทั่วโลก และเทคโนโลยีสนับสนุนมีเครือข่ายการทำงานอย่างมีประสิทธิภาพ จึงทำให้สามารถเคลื่อนย้ายมูลค่าระหว่างกลุ่มผู้โอนและกลุ่มผู้รับโอนส่งต่อกันไปได้หลายทอดผ่านหลายประเทศด้วยระยะเวลาเพียงสั้นๆเท่านั้น (Baath & Zellhorn, 2016)

2.1.3.5 กระเป๋าเงินอิเล็กทรอนิกส์ (Wallet) เป็นอุปกรณ์รักษาความปลอดภัยสำหรับบรรจุเงินสกุลเข้ารหัสที่เชื่อมต่อกับระบบนิเวศนั้นๆ เพื่อประโยชน์แก่การถือครอง การโอนและการรับโอนเงินสกุลเข้ารหัส โดยกระเป๋าเงินจะสามารถใช้งานได้ต้องประกอบด้วยรหัสเปิดสาธารณะสำหรับแสดงการติดต่อรหัสที่ตั้งของเงินสกุลเข้ารหัสแต่ละสกุล (ในกรณีที่กระเป๋าเงินมีการถือครองเงินสกุลเข้ารหัสหลายสกุลรวมกัน) และรหัสเปิดส่วนบุคคลที่เป็นข้อมูลรหัสลับเฉพาะสำหรับแสดงความเป็นเจ้าของกระเป๋าเงิน โดยรหัสเปิดสาธารณะที่กระบวนการสร้างขึ้นในขณะทำธุรรมการโอนมูลค่าและจะมีความสัมพันธ์เชิงคณิตศาสตร์กับรหัสเปิดส่วนบุคคลของเจ้าของกระเป๋าเงิน เพื่อเป็นการยืนยันสิทธิในการจัดการกระเป๋าเงินของตน (Gitlitz et al., 2019) ทั้งนี้กระเป๋าเงินอิเล็กทรอนิกส์ มีระบบการทำงานหลายประเภทขึ้นอยู่กับอุปกรณ์สื่อสารที่เชื่อมต่อกับระบบนิเวศ กล่าวคือ (1) **Cold Wallet** กระเป๋าเงินที่อยู่ในอุปกรณ์คอมพิวเตอร์ซึ่งไม่มีการเชื่อมต่อกับเครือข่าย

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

อินเตอร์เน็ต เช่น คอมพิวเตอร์ตั้งโต๊ะ (Desktop Computer) ซึ่งไม่ได้เชื่อมต่อระบบอินเตอร์เน็ตตลอดเวลา ทำให้เป็นการยากต่อการโจรกรรมกระเป๋าเงิน (2) **Hot Wallet** กระเป๋าเงินที่อยู่ในคอมพิวเตอร์ส่วนตัว (Personal Computer หรือ Notebook Computer) ซึ่งเชื่อมต่อกับระบบเครือข่ายพร้อมทั้งอนุญาตให้ระบบนิเวศเข้าถึงกระเป๋าเงินได้เพื่อสะดวกต่อการโอนและการรับโอนเงินสกุลเข้ารหัส (3) **Mobile Wallet** กระเป๋าเงินที่ติดตั้งในระบบปฏิบัติการแอนดรอย (Android) หรือไอโอเอสของแอปเปิล (IOS-Apple) บนโทรศัพท์เคลื่อนที่และอนุญาตให้ติดต่อสื่อสารทำธุรกรรมโอนมูลค่าเงินสกุลเข้ารหัสกับกระเป๋าเงินเคลื่อนที่ รวมถึงร้านค้าระบบออนไลน์ที่ยอมรับเงินสกุลเข้ารหัส และ (4) **Online Wallet** กระเป๋าเงินที่จัดเก็บในระบบเครือข่ายโดยไม่ได้ติดตั้งบนอุปรณ์ใดเป็นการเฉพาะ และจะทำธุรกรรมการโอนมูลค่าด้วยการเข้าทำงานบนเว็บไซต์จากอุปกรณ์สื่อสาร ณ สถานที่ใดก็ได้ (Homeland Security Enterprise, 2014)

2.1.3.6 ผู้ให้บริการเป๋าเงินอิเล็กทรอนิกส์ Wallet Provider เป็นหน่วยงานผู้ให้บริการโดยโปรแกรมประยุกต์ (Software Application) สำหรับการให้บริหารจัดการดูแลรักษาเงินสกุลเข้ารหัส หรือดำเนินการโอน และการรับโอนมูลค่าตามคำสั่งของลูกค้าผู้ใช้บริการที่ไม่มีกระเป๋าเงินเป็นของตนเองโดยเฉพาะ รวมถึงการให้บริการรายงานแสดงข้อมูลสถานะของกระเป๋าเงินและรักษาความปลอดภัยทางไซเบอร์ให้แก่ลูกค้าผู้ใช้บริการ (Girasa, 2018) ทั้งนี้หมายความรวมถึงผู้ให้บริการรับฝากประเป๋าเงินอิเล็กทรอนิกส์ (Custodian Wallet Provider) ซึ่งเป็นหน่วยงานผู้ให้บริการดูแลรักษารหัสเปิดส่วนบุคคลแทนเจ้าของกระเป๋าเงิน รวมถึงให้บริการดูแลรักษา ถือครองและโอนเงินสกุลเข้ารหัสให้แก่บุคคลตามคำสั่งของเจ้าของ (Ciphertrace, 2019; Federico Paesano, 2019)

2.1.3.7 ผู้ให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัส (Cryptocurrency Exchanger) ผู้ให้บริการมีลักษณะการดำเนินการทั้งในรูปแบบบุคคลธรรมดา หรือหน่วยงานที่ให้บริการแก่ลูกค้าผู้ใช้บริการ ในการแลกเปลี่ยนระหว่างเงินสกุลเข้ารหัสกับเงินสกุลเข้ารหัสอื่น หรือแลกเปลี่ยนเงินตราที่ชอบด้วยกฎหมายเป็นเงินสกุลเข้ารหัส รวมถึงการแลกเปลี่ยนในทางกลับกัน โดยได้รับค่าตอบแทนเป็นค่าธรรมเนียมปกติ ซึ่งลักษณะการดำเนินงานคล้ายกับผู้ให้บริการแลกเปลี่ยนเงินตราต่างประเทศ ทั้งนี้ผู้ให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัสที่ได้รับการยอมรับเช่น Bitfinex, HitBTC, Coinbase และผู้ให้บริการบางรายจะให้บริการแลกเปลี่ยนเฉพาะเงินสกุลเข้ารหัสเท่านั้น เช่น Binance นอกจากนี้ ผู้ให้บริการหลายรายยังให้บริการเชื่อมต่อกับระบบการโอนเงินตราปกติทางอิเล็กทรอนิกส์แก่ลูกค้าผู้ใช้บริการที่สามารถส่งคำสั่งการโอนเงินจากระบบ Paypal หรือ บัตรเครดิตได้อีกด้วย (Homeland Security Enterprise, 2014)

2.1.3.8 ผู้ให้บริการค้าเงินสกุลเข้ารหัส (Exchange Market) หน่วยงานที่ดำเนินธุรกิจเป็นตัวกลางในการค้า แลกเปลี่ยนเงินสกุลเข้ารหัส โดยมีลักษณะการดำเนินงานคล้ายกับตลาด

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

หลักทรัพย์ รวมถึงการแปลงมูลค่าระหว่างเงินตราปกติกับเงินสกุลเข้ารหัส เช่น Chicago Mercantile Exchange (CME) และ Chicago Board Options Exchange (CBOE) เป็นต้น (Girasa, 2018)

2.1.3.9 ผู้ให้บริการค้าเงินสกุลเข้ารหัสในรูปแบบอัตโนมัติ (Trading Platform) ผู้ให้บริการในรูปแบบนี้มีลักษณะการดำเนินงานคล้ายกับผู้ให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัส โดยมีความแตกต่างที่สำคัญ คือ ใช้รูปแบบการค้าระบบออนไลน์ที่ดำเนินการโดยอัตโนมัติไม่มีหน่วยงานรับผิดชอบในการจัดการ (Decentralized Exchanger) ดำเนินการจับคู่คำสั่งโอนมูลระหว่างผู้ใช้บริการด้วยโปรแกรมการทำงานอัตโนมัติ (Homeland Security Enterprise, 2014) อย่างไรก็ตาม ผู้ให้บริการในรูปแบบนี้ส่วนใหญ่อยู่ในบัญชีรายชื่อเฝ้าติดตามพฤติกรรมของหน่วยสืบสวนพิเศษของสหรัฐอเมริกา Federal Bureau of Investigation (FBI) โดยเฉพาะอย่างยิ่งรูปแบบพฤติกรรมของผู้ให้บริการการค้าอัตโนมัติที่ดำเนินการด้วยโปรแกรมจัดการ ซึ่งเสนอผลตอบแทนการลงทุนเพื่อการถือครอง หรือการค้าเงินสกุลเข้ารหัสให้แก่ลูกค้าผู้ใช้บริการในอัตราสูงเกินกว่าค่าเฉลี่ยของตลาดมากในลักษณะเข้าข่ายการหลอกลวงผู้ใช้บริการ (Girasa, 2018)

2.1.3.10 ผู้ให้บริการระบบชำระเงิน (Payment System) เป็นผู้ให้บริการระบบการชำระเงินระหว่างผู้ใช้เงินสกุลเงินสกุลเข้ารหัสในการชำระหนี้ค่าสินค้าหรือบริการแก่ผู้ค้า หรือ ผู้ให้บริการโดยตรง ทั้งในรูปแบบเงินสกุลเข้ารหัส หรือการแปลงค่าเป็นเงินตราปกติ ซึ่งมีลักษณะ การดำเนินงานคล้ายระบบการชำระเงินผ่านระบบออนไลน์ของธนาคารในปัจจุบัน (Gitlitz et al., 2019)

2.1.3.11 เครื่องให้บริการเบิกถอนเงินสกุลเข้ารหัส (Cryptocurrency Automatic Teller Machine หรือ Bitcoin ATM) เป็นเครื่องให้บริการอัตโนมัติ (ลักษณะคล้ายตู้เอทีเอ็มที่ให้บริการฝากถอนอัตโนมัติของธนาคาร) ซึ่งผู้ใช้บริการสามารถทำคำสั่งโอน รับโอน แลกเปลี่ยนเงินสกุลเข้ารหัสโดยตรง หรือทำการโอนแลกเปลี่ยนกับเงินตราปกติ เช่น ในประเทศญี่ปุ่นซึ่งเป็นประเทศที่มีกฎหมายรับรองการทำธุรกรรมเงินสกุลเข้ารหัส (Gitlitz et al., 2019)

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

2.1.4 เงินสกุลเข้ารหัสกับความเป็นเงินตรา

2.1.4.1 คำว่า ***"เงินตรา (Currency)"*** นั้นหมายถึง วัตถุ หรือสิ่งของซึ่งมนุษย์กำหนดขึ้น และเป็นที่ยอมรับกันโดยทั่วไปเพื่อวัตถุประสงค์ใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการระหว่างกัน ในอดีตมนุษย์ใช้ระบบเศรษฐกิจการค้าแบบแลกเปลี่ยน (Barter Trade) โดยผู้ต้องการใช้สินค้าหรือบริการต้องใช้ความพยายามในการค้นหา เพื่อจับคู่กับผู้ที่มีความต้องการใช้สินค้าหรือบริการของตน และทำการแลกเปลี่ยนตามสัดส่วนที่จะได้ตกลงกัน ทั้งนี้วิธีการดังกล่าวเป็นอุปสรรคต่อการดำรงชีพ สังคมจึงสร้างฉันทามติร่วมกันโดยกำหนดวัตถุหรือสิ่งของที่จะเป็นสื่อกลางของการแลกเปลี่ยนสินค้าและบริการในขอบเขตของสังคมนั้น เช่น เปลือหอย เครื่องปั้นดินเผา โลหะ ทองคำ รวมถึงธนบัตรกระดาษ เป็นต้น ซึ่งนอกจากหน้าที่หลักของเงินตราที่ใช้เป็น**สื่อกลางในการ**

อำนวยความสะดวกต่อแลกเปลี่ยนสินค้าและบริการ (A Medium of Exchange) ดังกล่าวแล้วนั้น (ธรรมรักษ์ หมื่นจักร รัชพร วงศาโรจน์ กษิดิศ ตันสงวน และเกวลี สันตโยดม, 2018) เงินตรายังมีหน้าที่สำคัญอีก 2 ประการ คือ การรักษามาตรฐานของการเป็น**หน่วยวัดมูลค่าสินค้าและบริการ (A Unit of Account)** เพื่อใช้เป็นหน่วยกลางในการวัดระดับและกำหนดมูลค่า หรืออาจเป็นการวัดค่าเสียโอกาสทางเศรษฐกิจของสินค้าและบริการแต่ละประเภท เช่น วิทยุที่กำหนดราคาเครื่องละ 75 เหรียญสหรัฐ พิซซ่าราคาถาดละ 15 เหรียญสหรัฐ ซึ่งเป็นหน่วยวัดมูลค่าของเงินตราในประเทศสหรัฐอเมริกา ในขณะที่หน่วยวัดมูลค่าของเงินตราไทยเรียกเป็น *“บาท”* เป็นต้น สำหรับอีกหน้าที่คือการดำรงรักษาและ**สะสมความมั่งคั่งทางเศรษฐกิจ (A Store of Value)** กล่าวคือเงินตราถือเป็นเครื่องมือในการเก็บรักษาและสะสมความมั่งคั่ง เพื่อใช้ประโยชน์ทางเศรษฐกิจในอนาคตอย่างมีเสถียรภาพและมั่นคง ไม่ว่าจะเป็นการใช้จ่ายสำหรับสินค้าและบริการ รวมถึงมีศักยภาพเพื่อการชำระหนี้สินในอนาคตได้ แม้ว่าทรัพย์สินบางประเภทจะสามารถทำหน้าที่ในการดำรงรักษามูลค่าได้ เช่น ที่ดิน งานศิลป์ แต่ทรัพย์สินเหล่านี้ก็ยังขาดสภาพคล่องในคุณสมบัติการแลกเปลี่ยนมูลค่ากับสินค้าและบริการอื่น (University of Minnesota Libraries, 2018)

2.1.4.2 เงินสกุลเข้ารหัสกับหน้าที่ความเป็นเงินตรา โดยการวิเคราะห์หน้าที่ของเงินสกุลเข้ารหัสว่าจะมีศักยภาพในการปฏิบัติหน้าที่อย่างเงินตราครบถ้วนทั้ง 3 ประการหรือไม่ อันได้แก่ (1) เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการ (A Medium of Exchange) (2) เป็นหน่วยวัดมูลค่าสินค้าและบริการ (A Unit of Account) และ (3) การดำรงรักษาและสะสมความมั่งคั่งทางเศรษฐกิจ (A Store of Value) เนื่องจากเงินสกุลเข้ารหัสไม่มีมูลค่าในตนเอง หรือมีมูลค่าของสินทรัพย์มีค่าใดหนุนหลัง หากแต่เงินสกุลเข้ารหัสจะมีมูลค่าเท่าใดขึ้นอยู่กับการยอมรับและความต้องการของหน่วยธุรกิจหรือผู้ใช้งานในการแลกเปลี่ยนสินค้าหรือบริการ ซึ่งเป็นหน้าที่สำคัญประการแรกของเงินตราคือ เป็นสื่อกลางในการอำนวยความสะดวกต่อแลกเปลี่ยนสินค้าและบริการ (A Medium of Exchange) โดยเฉพาะหน่วยธุรกิจการค้าทางระบบออนไลน์ การให้บริการเกมส์ระบบออนไลน์ การให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัส รวมถึงนักลงทุนเพื่อการเก็งกำไรจากมูลค่าของเงินสกุลเข้ารหัส แม้ว่าแนวโน้มจะมีผู้ใช้บริการรายใหม่เพิ่มขึ้นแต่ก็ยังอยู่ในวงจำกัด เนื่องจากปริมาณเงินสกุลเข้ารหัสที่หมุนเวียนในระบบนิเวศถูกจำกัดจำนวนอย่างชัดเจน กอรปกับปริมาณธุรกรรมการแลกเปลี่ยนที่เกิดขึ้นประมาณร้อยละ 80 เป็นการทำธุรกรรมเพื่อการเก็งกำไร ไม่ใช่เพื่อการแลกเปลี่ยนสินค้าและบริการ จึงยิ่งเป็นอุปสรรคต่อการทำหน้าที่เป็นเงินตราของเงินสกุลเข้ารหัส (Yermack, 2015)

ในขณะเดียวกันมูลค่าของเงินสกุลเข้ารหัส มีความผันผวนเปลี่ยนแปลงค่าอย่างรวดเร็วตลอดเวลา เนื่องจากระบบนิเวศเชื่อมต่อกับผู้ใช้งานในทุกภูมิภาคของโลกและไม่มีข้อจำกัดด้านเวลา มีผลให้หน้าที่ประการที่สอง คือการรักษามาตรฐานของการเป็นหน่วยวัดมูลค่าสินค้าและ

บริการ (A Unit of Account) ไม่มีความเสถียรเมื่อเปรียบเทียบกับเงินตราปกติ เช่น กาแฟราคาแก้วละ 4 เหรียญสหรัฐ หรือเท่ากับ 0.0068 BTC (บิตคอยน์) ณ ราคาบิตคอยน์เท่ากับ 586 เหรียญสหรัฐต่อ 1 BTC แต่นาทีถัดไปราคาบิตคอยน์เหรียญละ 599.20 เหรียญสหรัฐ หรือคิดเป็นราคากาแฟแก้วละ 4.075 เหรียญสหรัฐ (ข้อมูลราคาบิตคอยน์ ณ ปี 2014) และอีกประการหนึ่งสินค้าอุปโภคบริโภคที่มีปริมาณการค้าประจำวันส่วนใหญ่จะมีมูลค่าไม่สูงนักเมื่อเปรียบเทียบกับมูลค่าต่อ 1 BTC ดังนั้น การตั้งราคาเพื่อการค้าซึ่งเป็นเลขเศษทศนิยมจึงไม่สะดวกต่อระบบการค้า อีกประการหนึ่งหากกำหนดค่าตอบแทนแรงงานด้วยหน่วยเงินสกุลเข้ารหัส ผู้ใช้แรงงานอาจถูกลดค่าจ้างลงอย่างต่อเนื่องสาเหตุจากราคาเงินสกุลเข้ารหัสมีมูลค่าสูงขึ้น ซึ่งจะขัดแย้งต่อบริบทการเสริมแรงจูงใจในการทำงาน อีกประการหนึ่งราคาบิตคอยน์ในเดือนกันยายน 2020 มีค่าเท่ากับ 10,849.59 เหรียญสหัฐต่อ 1 BTC[3] ซึ่งมีมูลค่าสูงขึ้นมากไม่สะดวกต่อการทำธุรกรรม ผู้ใช้งานจึงเริ่มติดต่อกันด้วยหน่วยวัดที่มีขนาดเล็กลง เช่น Mill-Bitcoin (mBTC) หรือ Micro-Bitcoin (uBTC) (Yermack, 2015) และปัจจุบันระบบแลกเปลี่ยนได้กำหนดหน่วยวัดของบิตคอยน์ขนาดเล็กสุดเป็น 1 Shatoshi = 0.00000001 BTC เพื่อเป็นหน่วยวัดที่อำนวยความสะดวกต่อการแลกเปลี่ยนสินค้าและบริการ

ประการสุดท้าย ในหน้าที่การดำรงรักษาและสะสมความมั่งคั่งทางเศรษฐกิจ (A Store of Value) นั้น ผู้ถือครองเงินสกุลเข้ารหัสย่อมประสงค์ที่จะสะสมความมั่งคั่งเพื่อใช้ประโยชน์ทางเศรษฐกิจในอนาคต และมูลค่าที่ดำรงรักษาไว้จึงควรมีเสถียรภาพภายใต้สภาพเศรษฐกิจ แต่ด้วยระบบนิเวศเงินสกุลเข้ารหัสที่ผู้ถือครองจัดเก็บเงินดังกล่าวไว้ในกระเป๋าเงินอิเล็กทรอนิกส์ ก็อาจมีค่าใช้จ่ายเพื่อการดูแลรักษาของผู้ให้บริการกระเป๋าเงิน (Wallet Provider) ซึ่งเป็นต้นทุนที่ลดทอนมูลค่า ในขณะเดียวกันราคาของเงินสกุลเข้ารหัสมีความผันผันเปลี่ยนแปลงในระหว่างปีและปีต่อปีอย่างมีนัยสำคัญ ทั้งทิศทางที่มีมูลค่าสูงขึ้นหรือลดมูลค่าลง จึงเป็นความเสี่ยงเข้าข่ายการถือครองเพื่อการเก็งกำไรมากกว่า (Yermack, 2015)

กล่าวโดยสรุป เงินสกุลเข้ารหัสกับหน้าที่การเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่มีลักษณะเข้าข่ายความเป็นเงินตราในประการนี้มากที่สุด อย่างไรก็ตาม การทำธุรกรรมยังอยู่ในวงจำกัดของผู้ใช้งานที่ยอมรับ ซึ่งส่วนใหญ่จะเป็นระบบการค้าและแลกเปลี่ยนที่เกิดขึ้นบนเครือข่ายระบบออนไลน์ ทั้งนี้ความแพร่หลายจึงขึ้นอยู่กับสังคมในขอบเขตประเทศนั้นที่จะยอมรับในวงกว้างเป็นการทั่วไปหรือไม่ ส่วนหน้าที่การเป็นหน่วยวัดมูลค่านั้นขาดเสถียรภาพอย่างมีนัยสำคัญและหน้าที่การสะสมความมั่งคั่งทางเศรษฐกิจ ซึ่งการทำธุรกรรมส่วนใหญ่กลับกลายเป็นการถือครองเพื่อการลงทุนเก็งกำไร ดังนั้น โดยข้อจำกัดทางเทคนิคของระบบนิเวศเงินสกุลเข้ารหัสจึงไม่เข้าลักษณะความเป็นเงินตรา หากแต่มีหน้าที่บางลักษณะเข้าข่ายเป็นทรัพย์สินเพื่อการค้า หรือสินค้า (Commodity) เนื่องจาก Commodity หมายถึงสิ่งของทั้งที่มีรูปร่างหรือไร้รูปร่างที่สามารถนำมา

[3] ข้อมูลจากเว็บไซต์ CoinMarketCap.com ณ Last updated: Sun, 13 Sep 2020 15:25:18 UTC

สร้างคุณค่าทางเศรษฐกิจได้ ซึ่งบางประเทศได้นิยามเงินสกุลเข้ารหัสเข้าข่ายเป็นทรัพย์สินเพื่อการค้า เนื่องจากมีลักษณะเป็นสิ่งของไร้รูปร่างที่จะไม่สูญสลายไปโดยมีมูลค่ากำหนดได้ชัดเจนในแต่ละขณะ และถือเป็นมูลค่าที่มีความรับผิดทางภาษี เช่น ประเทศออสเตเลีย ประเทศอิสราเอล เป็นต้น และโดยหน้าที่ของการสะสมความมั่งคั่งทางเศรษฐกิจในอนาคตสำหรับผู้ถือครองเงินสกุลเข้ารหัส จึงเข้าข่ายเป็นหลักทรัพย์เพื่อการลงทุน (Security) จากการรอรับผลประโยชน์จากกำไรส่วนเกินทุน อย่างไรก็ตาม เงินสกุลเข้ารหัสยังมีระบบการซื้อขายด้วยระบบนิเวศอินเตอร์เน็ตแบบกระจายศูนย์ จึงเป็นระบบที่มีความเสี่ยงภัย ซึ่งแตกต่างจากหลักทรัพย์ที่มีหน่วยงานการกำกับดูแลระบบการซื้อขาย ในขณะที่บางประเทศได้นิยามเงินสกุลเข้ารหัสเป็นทรัพย์สินเพื่อการลงทุน (Property) ที่สามารถซื้อขายและแลกเปลี่ยน หรือการลงทุนโดยได้รับผลประโยชน์คาดหวังจากกำไรส่วนเกินทุน จึงถือเป็นธุรกรรมที่มีความรับผิดทางภาษี รวมถึงผู้ที่เกี่ยวข้องในระบบนิเวศเงินสกุลเข้ารหัสย่อมมีความรับผิดทางภาษีต่อการทำธุรกรรมเช่นกัน เช่น ประเทศสหรัฐอเมริกา เป็นต้น (Cvetkova, 2018)

2.1.5 สถานะทางกฎหมายของเงินสกุลเข้ารหัส

การกำหนดนโยบาย และมาตรการทางกฎหมายในการกำกับดูแลเงินสกุลเข้ารหัสอย่างเหมาะสมภายใต้ปัจจัยพื้นฐาน เพื่อความมั่นคงทางเศรษฐกิจและสังคมแก่ประเทศนั้น ควรพิจารณาเปรียบเทียบคุณสมบัติเฉพาะของเงินสกุลเข้ารหัสกับคุณลักษณะเฉพาะของความเป็นเงินตราที่ชอบด้วยกฎหมายตามแนวคิดทางกฎหมายอื่นประกอบด้วย โดย Sapovadia (2015) ได้นำเสนอกรอบแนวคิดไว้ดังนี้

2.1.5.1 ความเป็นเงินตราที่ชอบด้วยกฎหมาย (Validity of Transaction as a Currency) รัฐบาลของทุกประเทศจะเป็นผู้มีอำนาจที่ชอบด้วยกฎหมายที่จะจัดทำ หรือมอบหมายให้หน่วยงานของภาครัฐใดรับผิดชอบในการจัดทำธนบัตร เหรียญกษาปณ์ เพื่อเป็นสื่อกลางในการชำระหนี้ซึ่งรับประกันการคงมูลค่าโดยรัฐบาล และมีความชอบด้วยกฎหมายภายในอาณาเขตประเทศ ด้วยการระบุข้อความรับรองบนเงินตรา เช่น ธนบัตรเงินตราไทยจะมีข้อความ *“ธนบัตรเป็นเงินที่ชำระหนี้ได้ตามกฎหมาย”* รับรองบนธนบัตร นอกจากนี้รัฐบาลยังมีอำนาจในการกำหนดนโยบายปริมาณเงินตราที่ใช้หมุนเวียนในระบบเศรษฐกิจ โดยมีกลไกในการเพิ่มหรือลดปริมาณเงินเพื่อการบริหารความมั่นคงทางเศรษฐกิจ ในขณะที่เงินสกุลเข้ารหัสมีรูปแบบเป็นรหัสข้อมูลอิเล็กทรอนิกส์ ไร้รูปร่าง และผู้ออกเงินสกุลเข้ารหัส (Promotor) ก็เป็นบุคคลที่ไม่มีอำนาจรัฐาธิปัตย์ในการรับรองความเป็นเงินตราที่ชอบด้วยกฎหมายในขอบเขตประเทศใด อีกทั้งปริมาณเงินสกุลข้ารหัสถูกกำหนดโดยชัดเจนล่วงหน้าไว้ในรายงานนำเสนอเงินสกุลเข้ารหัส (White Paper) นั้น (Sapovadia, 2015)

2.1.5.2 ความเป็นเงินตราต่างประเทศที่ชอบด้วยกฎหมาย (Validity of Transaction as a Foreign Currency) ภายใต้ระบบกฎหมายระหว่างประเทศจะให้การรับรอง

อำนาจอันชอบธรรมของแต่ละอาณาเขตประเทศ รวมถึงบทบัญญัติทางกฎหมายข้ามเขตแดนประเทศจะมีรูปแบบเฉพาะตามความตกลงกันระหว่างประเทศคู่เจรจา หรือกลุ่มประเทศ หรือในระดับสากล อย่างเช่น องค์กรการเงินระหว่างประเทศ (IMF) ที่จะให้การรับรองความเป็นเงินตราของประเทศหนึ่งไปใช้ชำระหนี้นอกเขตประเทศ ซึ่งเป็นการรับรองเงินตราต่างประเทศที่ชอบด้วยกฎหมาย อย่างไรก็ตามความชอบด้วยกฎหมายก็ยังมีข้อจำกัดขึ้นอยู่ความตกลงระหว่างประเทศคู่เจรจา แต่เนื่องจากเงินสกุลเข้ารหัสเป็นรูปแบบรหัสข้อมูลบนระบบนิเวศอินเตอร์เน็ตแบบไร้พรมแดน ที่สามารถทำธุรกรรมข้ามประเทศโดยไม่มีข้อจำกัด แต่ขึ้นอยู่กับระดับการพัฒนาเทคโนโลยีการสื่อสารของประเทศนั้นๆ โดยไม่มีองค์กรใดให้การรับรองทางกฎหมาย เพียงเป็นธุรกรรมที่ผู้ใช้งานให้ความเชื่อถือต่อกันภายใต้ระบบปฏิบัติการเท่านั้น (Sapovadia, 2015)

2.1.5.3 ความรับผิดทางภาษีอากร (Tax Incidences) เนื่องจากเงินตราที่ชอบด้วยกฎหมายทำหน้าที่เป็นสื่อกลางในการชำระหนี้เท่านั้น จึงไม่มีลักษณะเข้าข่ายความรับผิดทางภาษีอากรใด หากแต่เงินสกุลเข้ารหัสที่มีลักษณะเข้าข่ายเป็นทรัพย์สินไร้รูปร่าง ดังนั้น การทำธุรกรรมเกี่ยวกับเงินสกุลเข้ารหัสจึงเข้าข่ายความรับผิดทางภาษีอากรหลายประเภท เช่น ภาษีจากกำไรส่วนเกินทุน, ภาษีเงินได้, ภาษีทรัพย์สิน, ภาษีธุรกิจเฉพาะ ทั้งนี้ ขึ้นอยู่กับมาตรการทางภาษีของแต่ละประเทศจะบัญญัติให้เงินสกุลเข้ารหัสเข้าข่ายต้องเสียภาษีอากรในลักษณะใด แม้ว่าระบบจัดเก็บภาษีอากรจากธุรกรรมเงินสกุลเข้ารหัสตามกฎหมายที่หลายประเทศประกาศบังคับใช้ ก็ไม่ได้เป็นการรับรองสถานะเงินสกุลเข้ารหัสให้มีสถานะชอบด้วยกฎหมายอื่นๆ เช่นกัน (Sapovadia, 2015)

2.1.5.4 การบังคับคดีเมื่อเกิดเหตุละเมิดกฎหมาย (Filing Suit in Legal Disputes) ธุรกรรมเงินสกุลเข้ารหัสเกิดขึ้นโดยความสมัครใจของผู้ใช้งานทั้งสองฝ่ายที่เชื่อถือต่อกัน และต่อระบบปฏิบัติการจึงไม่อาจดำเนินการเรียกร้องความเสียหายหากเกิดเหตุละเมิดกันได้ เว้นแต่ มีเหตุกระทำผิดอื่นที่กฎหมายของประเทศนั้นบัญญัติเป็นความผิด เช่น การขโมย การฉ้อโกงหลอกลวง การฟอกเงิน การคุ้มครองผู้บริโภค รวมถึงการกระทำผิดบนระบบคอมพิวเตอร์ เป็นต้น (Sapovadia, 2015)

2.1.5.5 องค์กรกำกับดูแลการออกและบริหารเงินตรา (Organizational Status of Promoters and Participators) โดยทั่วไปรัฐบาลในหลายประเทศมักจะมอบหมายให้ธนาคารกลางของประเทศเป็นองค์กรที่รับหน้าที่กำกับดูแลการบริหารจัดการระบบหมุนเวียนเงินตรา ในขณะที่เงินสกุลเข้ารหัสไม่มีองค์กรของหน่วยงานรัฐใดให้การรับรอง และทำหน้าที่กำกับตรวจสอบความโปร่งใสของระบบปฏิบัติงาน ดังนั้น ความน่าเชื่อถือของเงินสกุลเข้ารหัสจึงขึ้นอยู่กับการยอมรับของกลุ่มผู้ใช้งาน และบุคคลหรือหน่วยงานของผู้ออกเงินสกุลเข้ารหัสในการปฏิบัติหน้าที่ดูแลบำรุงรักษาระบบเท่านั้น (Sapovadia, 2015)

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

2.1.5.6 การบริหารนโยบายการเงินและการคลัง (Monetary and Fiscal Policies) รัฐบาลจะเป็นผู้ใช้อำนาจในการบริหารราชการแผ่นดิน ซึ่งการบริหารนโยบายการเงินและการคลังเป็นส่วนหนึ่งของภารกิจสำคัญของรัฐบาล ที่จะดำเนินการบริหารปริมาณเงินหมุนเวียนในระบบเศรษฐกิจให้มีประมาณเพิ่มขึ้นหรือลดปริมาณลง เพื่อการรักษาเสถียรภาพทางเศรษฐกิจของประเทศ แต่เงินสกุลเข้ารหัสเป็นการออกหมุนเวียนในระบบปฏิบัติอย่างจำกัดตามปริมาณ ซึ่งได้เผยแพร่ข้อมูลไว้ล่วงหน้าในคู่มือปฏิบัติงาน (White Paper และ Smart Contract) ของเงินสกุลเข้ารหัสแต่ละสกุล ไม่สามารถเปลี่ยนแปลงภายหลังได้ เนื่องจากระบบปฏิบัติการบล็อกเชนจะบริหารจัดการข้อมูลตามชุดคำสั่งปฏิบัติงานที่ระบุไว้ล่วงหน้าเท่านั้น (Sapovadia, 2015)

2.1.6 นโยบายและมาตรการทางกฎหมายของนานาชาติที่มีต่อเงินสกุลเข้ารหัส

เงินสกุลเข้ารหัสเริ่มต้นในปี 2008 หลังจากซาโตชิได้นำเสนอเงินสกุลเข้ารหัสสกุลแรกที่เรียกว่า *“บิตคอยน์”* เข้าสู่ระบบการเงินโลก โดยในปี 2009 ระบบปฏิบัติการได้สร้างบิตคอยน์ชุดแรกเพื่อเป็นค่าตอบแทนแก่นักขุดที่ร่วมพิสูจน์ยืนยันรายการด้วยมูลค่า 50 BTC และมูลค่าเริ่มต้นของบิตคอยน์ในขณะนั้นเท่ากับ 8/100 เซนต์ต่อ 1 BTC หรือประมาณเทียบเท่า 1,309 BTC ต่อ 1 เหรียญสหรัฐ ซึ่งหมายความว่าการลงทุน 1 เหรียญสหรัฐบนบิตคอยน์ในปี 2009 จะเท่ากับมูลค่าในปี 2017 มากกว่า 1 ล้านเหรียญสหรัฐ (Burniske & Tara, 2017) โดยในกลางปี 2020 ได้มีการนำเสนอเงินสกุลเข้ารหัสสู่ระบบการเงินโลกมากกว่า 7,000 สกุลด้วยมูลค่าทางการตลาดรวมประมาณ 340,000 ล้านเหรียญสหรัฐ แต่มีเงินสกุลเข้ารหัสที่ได้รับความนิยมเพียง 10 อันดับแรกซึ่งมีมูลค่ารวมกันเกินกว่าร้อยละ 80 ของมูลค่าทางการตลาดรวม และเงินสกุลเข้ารหัสที่ได้รับความนิยมสูงสุดยังคงเป็นบิตคอยน์ที่มีสัดส่วนสูงถึงร้อยละ 56.0 ด้วยมูลค่าทางการตลาดประมาณ 191,500 ล้านเหรียญสหรัฐ[4]

ดังนั้น หลายประเทศทั่วโลกจึงได้ตื่นตัวถึงนวัตกรรมเงินสกุลเข้ารหัสที่จะส่งผลกระทบต่อระบบเศรษฐกิจของประเทศ และระหว่างประเทศที่มีความเชื่อมโยงอย่างโลกาภิวัตรในปัจจุบันที่ไม่อาจหลีกเลี่ยงได้ โดยให้ความสนใจศึกษาความเหมาะสมในการออกมาตรการทางกฎหมายเพื่อใช้บังคับแก่เงินสกุลเข้ารหัสตามบริบททางเศรษฐกิจและสังคมของแต่ละประเทศ โดยวัตถุประสงค์หลักในการกำกับดูแล เพื่อป้องกันความเสียหายที่จะเกิดขึ้นกับระบบเศรษฐกิจการเงินการคลังระดับมหภาคของประเทศตน และการปกป้องผลประโยชน์ของประชาชนทั่วไปจากความเสี่ยงที่อาจเกิดขึ้น จากการดำเนินงานของผู้ใช้งานที่มีความเชี่ยวชาญและเจตนาไม่สุจริตทั้งภายในประเทศและต่างประเทศในระบบนิเวศแบบไร้พรมแดน รวมถึงการป้องกันและปราบปรามการใช้ช่องทางการจัดการเงินสกุลเข้ารหัสของกลุ่มอาชญากร เพื่อประโยชน์ในการถ่ายโอนเงินที่ไม่ชอบด้วยกฎหมายจาก

[4] ข้อมูลจากเว็บไซต์ CoinMarketCap.com ณ Last updated: Sun, 13 Sep 2020 15:25:18 UTC

การกระทำผิด ดังนั้นสภาพบังคับทางกฎหมายและการกำกับดูแลการบริหารจัดการ เงินสกุลเข้ารหัสอย่างเหมาะสมจะช่วยรักษาดุลยภาพระหว่างผลประโยชน์ทางเศรษฐกิจ และความมั่นคงสงบเรียบร้อยของสังคม

อย่างไรก็ตามความเหมาะสมของการออกมาตรการทางกฎหมายยังขึ้นอยู่กับพื้นฐานของระบบกฎหมายด้านเศรษฐกิจในประเทศนั้น ที่จะให้ความหมายหรือนิยามของเงินสกุลเข้ารหัสว่าควรเข้าข่ายสถานภาพการบังคับใช้กฎหมายในลักษณะใด กล่าวคือควรมีสถานภาพทางกฎหมายของเงินสกุลเข้ารหัสเสมือนเป็น *“เงินตรา (Currency)”* หรือ *“สินทรัพย์ (Property)”* หรือ *“สินค้า (Commodity)”* หรือ *“หลักทรัพย์ (Security)”* (Cvetkova, 2018) รวมถึงการให้ความสำคัญต่อการกำกับระบบนิเวศเงินสกุลเข้ารหัสในรูปแบบการกระจายศูนย์ (Decentralized Digital Currency) หรือในรูปแบบระบบนิเวศที่มีเครือข่ายการปฏิบัติงานแบบรวมศูนย์กลาง (Centralized Digital Currency) (Yang, 2016) ซึ่งจะถือเป็นบรรทัดฐานสำคัญในการปรับใช้มาตรการทางกฎหมายเพื่อการกำกับดูแลในลำดับต่อไป

ทั้งนี้ ในปี 2018 The Law Library of Congress (2018) ได้นำเสนอรายงายผลสำรวจมาตรการทางกฎหมายที่เกี่ยวกับการกำกับดูแลเงินสกุลเข้ารหัสทั่วโลกจำนวน 130 ประเทศ เนื่องจากเงินสกุลเข้ารหัสมีอัตราเติบโตในมูลค่าทางเศรษฐกิจอย่างรวดเร็ว และการให้ความหมายของแต่ละประเทศแตกต่างกันโดยยังไม่มีข้อสรุปอย่างเป็นสากล ทั้งนี้รับรู้กันแต่เพียงว่า เงินสกุลเข้ารหัสมีลักษณะเป็นชุดรหัสข้อมูลอิเล็กทรอนิกส์ ซึ่งผู้ใช้งานสามารถโอนมูลค่าระหว่างกันได้โดยตรงบนระบบปฏิบัติการบล็อกเชนภายใต้ระบบนิเวศอินเตอร์เน็ตในรูปแบบฐานข้อมูลแบบกระจายศูนย์ และไม่มีหน่วยงานกลางในการกำกับดูแลเท่านั้น ดังนั้น จึงมีการใช้คำแทนความหมายของเงินสกุลเข้ารหัสที่หลากหลาย เช่น *“Digital Currency”* สำหรับประเทศอเจนตินา ไทย และออสเตเลีย หรือ *“Virtual Commodity”* สำหรับประเทศแคนาดา จีน และไต้หวัน หรือ *“Crypto-Token”* สำหรับประเทศเยอรมัน หรือ *“Payment Token”* สำหรับประเทศสวิตเซอร์แลนด์ หรือ *“Cyber Currency”* สำหรับประเทศอิตาลี และเลบานอน หรือ *“Electronic Currency”* สำหรับประเทศกัมพูชา และเลบานอน หรือ *“Virtual Assets”* สำหรับประเทศฮอนดูรัส และเม็กซิโก เป็นต้น โดยแต่ละประเทศให้ความสำคัญต่อการสร้างความเข้าใจให้ประชาชนได้ทราบถึง ความเสี่ยงของเงินสกุลเข้ารหัสที่ไม่มีหน่วยงานใดให้การคุ้มครองทางกฎหมาย ผู้ใช้งานจะต้องรับความเสี่ยงภัยด้วยตนเอง รวมถึงการออกมาตรการกำกับดูแลการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส และการออกมาตรการทางภาษีอากรดูแลผลประโยชน์ของประเทศจากผู้ทำธุรกรรมเงินสกุลเข้ารหัส นอกจากนี้ ยังรวมถึงมาตรการกำกับดูแลและกลั่นกรองการให้อนุญาตแก่บุคคลที่ประสงค์ทำธุรกิจเกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัส และการระดมทุนด้วยการนำเสนอออกเงินสกุลเข้ารหัส

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

สกุลใหม่ (Initial Coin Offering - ICO) โดยมีระดับการบังคับใช้กฎหมายที่แตกต่างกันตามบริบทของแต่ละประเทศ (The Law Library of Congress, 2018)

แนวทางการออกมาตรการกำกับดูแลบริหารจัดการเงินสกุลเข้ารหัสตามบริบทของแต่ละประเทศ โดยสามารถจัดกลุ่มมาตรการทางกฎหมายตามลักษณะสภาพบังคับใช้ได้เป็น 3 กลุ่มประเทศ กล่าวคือ

(1) กลุ่มแรก เป็นประเทศที่มีมาตรการทางกฎหมายยอมรับสถานภาพเงินสกุลเข้ารหัส และอนุญาตให้สามารถทำธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสได้อย่างชอบด้วยกฎหมาย โดยประเทศญี่ปุ่นเป็นประเทศแรกที่ยอมรับสถานภาพทางกฎหมายของบิตคอยน์ ในเดือนเมษายน 2017 จนกลายเป็นตลาดธุรกรรมเงินสกุลเข้ารหัสที่มีขนาดใหญ่ระดับโลกในปัจจุบัน และประเทศออสเตรียที่ให้การยอมรับบิตคอยน์ในปีเดียว จากนั้นมีอีกหลายประเทศได้ประกาศมาตรการทางกฎหมายให้การยอมรับเงินสกุลเข้ารหัสมากขึ้น เช่น ประเทศมอร์ต้าซึ่งเป็นศูนย์กลางแลกเปลี่ยนเงินสกุลเข้ารหัสที่สำคัญของโลก และประเทสเยอรมัน บลาซิล เป็นต้น (Kethineni & Cao, 2019)

(2) กลุ่มที่สอง เป็นประเทศที่มีมาตรการต้องห้ามและไม่ยอมรับสถานภาพเงินสกุลเข้ารหัสถือเป็นสิ่งที่ไม่ชอบด้วยกฎหมาย ต้องห้ามสถาบันการเงินไม่ให้ดำเนินธุรกรรมใดๆที่เกี่ยวข้อง รวมถึงการเสนอขายเงินสกุลเข้ารหัสสุกลใหม่ภายในขอบเขตประเทศของตน เช่น ประเทศแอลจิเรีย โบลีเวีย โมรอคโค เนปาล ปากีสถาน และเวียดนาม เป็นต้น ส่วนประเทศการ์ตา และบาเรน จะยกเว้นไม่ต้องห้ามสำหรับธุรกรรมเงินสกุลเข้ารหัสที่ดำเนินการในต่างประเทศ (The Law Library of Congress, 2018) รวมถึงประเทศเศรษฐกิจขนาดใหญ่ที่มีมาตรการต้องห้าม คือประเทศจีน เกาหลีใต้ และรัสเซีย เป็นต้น (Kethineni & Cao, 2019)

(3) กลุ่มประเทศสุดท้าย เป็นประเทศที่มีมาตรการทางกฎหมายยอมรับสถานภาพเงินสกุลเข้ารหัสในบางลักษณะ และอนุญาตให้ดำเนินธุรกรรมที่เกี่ยวข้องบางลักษณะที่อยู่ภายใต้กรอบมาตรการกำกับดูแลที่เคร่งครัด รวมถึงการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ที่มีลักษณะเข้าข่ายหลักทรัพย์ หรือตราสารหนี้ เช่น ประเทศนิวซีแลนด์ และเนเธอร์แลนด์ นอกจากนี้บางประเทศอนุญาตให้ประชาชนถือครองเงินสกุลเข้ารหัสเพื่อการลงทุน แต่อาจมีข้อกำหนดในการกำกับการทำธุรกรรมของสถาบันการเงินที่เกี่ยวข้องกับเงินสกุลเข้ารหัส เช่น ประเทศบังคลาเทศ อิหร่าน ลิตเธอร์เนีย กัมพูชา และไทย เป็นต้น (The Law Library of Congress, 2018)

สำหรับมาตรการทางภาษีอากรนั้น ประเทศส่วนใหญ่จะออกมาตรการจัดเก็บภาษีอากรจากการทำธุรกรรมและผู้ที่เกี่ยวกับการทำธุรกรรมเงินสกุลเข้ารหัส เช่น ธุรกรรมการซื้อขายเงินสกุลเข้ารหัส ค่าตอบแทนนักขุด โดยเข้าข่ายกำไรส่วนเกินทุน ภาษีมูลค่าเพิ่ม และในบางประเทศอาจยินยอมให้นำผลขาดทุนจากการทำธุรกรรมมาหักกลบกับกำไรส่วนเกินทุนก่อนจะถือเป็นฐานภาษีต่อไป (The Law Library of Congress, 2018)

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ดังนั้น การนิยามความหมายของเงินสกุลเข้ารหัสถือเป็นประเด็นที่มีนัยสำคัญต่อการกำหนดนโยบาย และมาตรการทางกฎหมายในการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัสของแต่ละประเทศ ซึ่งในขณะนี้ยังไม่มีแนวปฏิบัติสากลที่ชัดเจน เช่น สหภาพยุโรปให้นิยามตาม มาตรา 4(18) แห่งมาตรการต่อต้านการฟอกเงินฉบับที่ 5 (The Fifth Anti-money Laundering Directive – AMLD5) เป็น *"เงินตราเสมือน (Virtual Currencies) หมายถึง หน่วยข้อมูลดิจิทัลซึ่งได้จัดทำขึ้น หรือค้ำประกันโดยธนาคารกลางหรือหน่วยงานของรัฐ ซึ่งไม่ได้มีมูลค่าผูกติดกับเงินตราที่ชอบด้วยกฎหมายและไม่ได้มีสถานสภาพทางกฎหมาย แต่เป็นที่ยอมรับกันโดยทั่วไปหรือบุคคลตามกฎหมายเพื่อการแลกเปลี่ยน โอนมูลค่า รักษามูลค่า รวมถึงการค้าในเครือข่ายระบบอิเล็กทรอนิกส์"* (Frick, 2019) ส่วนคณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน (Financial Action Task Force) ได้ประกาศข้อแนะนำฉบับปรับปรุงปี 2018 โดยให้นิยามเป็น *"สินทรัพย์เสมือน (Virtual Assets) หมายถึง หน่วยข้อมูลดิจิทัลที่เป็นตัวแทนมูลค่าเพื่อการค้าทางดิจิทัล การโอนมูลค่า และสามารถใช้เพื่อการชำระราคาและการลงทุน"* (Federico Paesano, 2019)

นอกจากนี้ Nian and Chuen (2015) ได้ให้แนวคิดในการนิยามเพิ่มเติม กล่าวคือ เงินตราเสมือน (Virtual Currency) มีลักษณะเชิงความหมายใกล้เคียงหรือเทียบเคียงเงินตราแต่ยังไม่ใช่เงินตราที่ชอบด้วยกฎหมาย ในขณะที่เงินสกุลดิจิทัล (Digital Currency) มีสภาพเป็นเงินตราที่อยู่ในรูปแบบอิเล็กทรอนิกส์หรือมีการลงทะเบียนทางอิเล็กทรอนิกส์ ดังนั้นเงินสกุลดิจิทัลจึงมีความหมายกว้างกว่าเงินตราเสมือน นอกจากนี้ประเด็นที่ต้องพิจารณาประกอบเพื่อให้นิยามลักษณะของหน่วยข้อมูลอิเล็กทรอนิกส์ที่แสดงมูลค่า กล่าวคือ ลักษณะมีรูปร่างทางกายหรือไร้รูปร่างทางกายภาพ ซึ่งจะประกอบการกำหนดความเป็นทรัพย์สินเพื่อการค้า (Commodity) หรือเงินตรา (Money) รวมถึงเครือข่ายระบบปฏิบัติแบบมีศูนย์กลางกำกับดูแล (Centralized Digital Currency) หรือเครือข่ายระบบปฏิบัติการแบบกระจายศูนย์ไม่มีหน่วยงานกำกับดูแล (Distributed or Decentralized Digital Currency) เป็นต้น (Nian & Chuen, 2015)

จากการศึกษาพบว่า เงินสกุลดิจิทัล (Digital Currency) อาจให้นิยามความหมายเป็นหน่วยชุดรหัสข้อมูลอิเล็กทรอนิกส์ในระบบนิเวศเทคโนโลยีการสื่อสาร ที่เชื่อมโยงข้ามเขตแดนประเทศแบบไร้พรมแดน เพื่อการส่งและรับชุดรหัสข้อมูลซึ่งแสดงมูลค่าระหว่างผู้ใช้งาน ทั้งในระบบงานแบบเปิด ซึ่งเป็นฐานข้อมูลสาธารณะที่บุคคลทั่วไปสามารถเข้าถึงได้โดยไม่มีตัวกลางในการกำกับดูแล และในระบบปิดที่มีหน่วยงานกำกับดูแลการปฏิบัติงาน รวมถึงลักษณะการประยุกต์ของหน่วยชุดรหัสข้อมูลที่เทียบเสมือนเป็นทรัพย์สินเพื่อการค้า (Commodity) หรือทรัพย์สินเพื่อลงทุน (Security) หรือเงินตรา (Currency) ซึ่งจะมีความหมายแบบกว้าง

เงินตราเสมือน (Virtual Currency) ซึ่งเป็นระบบเงินตราเสมือนที่ไม่หน่วยงานของรัฐใดให้การรับรองมูลค่าอย่างถูกต้องตามกฎหมาย หรือเป็นเงินดิจิทัลในรูปแบบที่เป็นเงินตราเสมือน

ที่มีรัฐบาลให้การรับมูลค่าอย่างถูกต้องตามกฎหมาย (Real Currency) สามารถใช้ชำระราคาค่าสินค้า บริการ และชำระหนี้ในระบบเศรษฐกิจได้อย่างชอบด้วยกฎหมาย ซึ่งมีระบบการดำเนินงานเป็น 2 ลักษณะ คือ *"Centralized Currency"* หรือเงินตราเสมือนที่ไม่มีหน่วยงานรัฐบาลใดรับรอง แต่มีองค์กรเอกชน หรือหน่วยงานที่ไม่ใช่ภาครัฐปฏิบัติหน้าที่ในการออกระเบียบการกำกับและดูแลการบริหารจัดการระบบนิเวศออนไลน์ รวมถึงการจัดการระบบฐานข้อมูลกลางของผู้ดูแลระบบนิเวศ และ "Decentralized Currency" เงินตราเสมือนที่ไม่มีหน่วยงานกลางใดทำหน้าที่กำกับดูแลบริหารจัดการระบบนิเวศ แต่ระบบจะปฏิบัติงานตามชุดคำสั่งเองโดยอัตโนมัติ (White Paper) หรือเงื่อนไขข้อตกลงการดำเนินงาน (Smart Contract) ที่ได้ระบุล่วงหน้าตั้งแต่นำเงินดิจิทัลนั้นเข้าสู่ระบบนิเวศ

ทั้งนี้ Decentralized Currency เป็นระบบปฏิบัติการเพื่อการรับส่งมูลค่าด้วยชุดรหัสข้อมูลในระบบงานแบบเปิดบนฐานข้อมูลสาธารณะที่ไม่มีศูนย์กลางในการกำกับดูแล โดยส่วนใหญ่ประกอบด้วยเงินสกุลเข้ารหัส (Cryptocurrency) หรือ สินทรัพย์เข้ารหัส (Crypto Token) ซึ่งหมายถึง ชุดรหัสข้อมูลเพื่อการรับส่งสิทธิประโยชน์ทางเศรษฐกิจอื่นใดระหว่างผู้ใช้งาน เช่น การแลกเปลี่ยนเป็นเงินสกุลเข้ารหัสอื่น การแลกเปลี่ยนเป็นสินค้าและบริการ ทั้งที่มีรูปร่างทางกายภาพหรือไร้รูปร่างในลักษณะดิจิทัล

และ ลำดับสุดท้าย เงินสกุลเข้ารหัส (Cryptocurrency) หมายรวมถึง *"บิตคอยน์"* เงินสกุลเข้ารหัสแรก ซึ่งเป็นกรอบความหมายแบบแคบ เนื่องจากเป็นหน่วยชุดรหัสข้อมูลแสดงมูค่าที่มีคุณลักษณะเฉพาะบางประการที่เป็นปัจจัยที่มีอิทธิพลต่อการใช้เป็นเครื่องมือในการฟอกเงิน อย่างไรก็ตามแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม ยังสามารถขยายขอบเขตการบังคับใช้แบบกว้างครอบคลุมเงินสกุลดิจิทัล (Digital Currency) หรือสินทรัพย์ดิจิทัล (Digital Asset) ได้ในทำนองเดียวกัน เนื่องด้วยเงินสกุลดิจิทัลหรือสินทรัพย์ดิจิทัล มีคุณลักษณะร่วมกันทางเทคโนโลยี่หลายประการ โดยเฉพาะอย่างยิ่งเป็นการสื่อกลางในการโอนมูลค่าแบบไร้พรมแดนด้วยความรวดเร็วในระบบนิเวศบนระบบปฏิบัติการบล็อกเชน เช่นเดียวกับเงินสกุลเข้ารหัส ดังเช่น ความเห็นของ FATF ได้ให้ข้อแนะนำในการให้ความหมายของหน่วยชุดรหัสข้อมูลแสดงมูลค่านี้ โดยกรอบแนวคิดความเป็นกลางที่ครอบคลุมความแตกต่างทางเทคโนโลยี่ และสามารถขยายความครอบคลุมถึงพัฒนาการในอนาคต (Ciphertrace, 2019) ไม่ว่าจะใช้คำว่า *"สินทรัพย์เสมือน (Virtual Assets)"* หรือ *"เงินเสมือน (Virtual Currency)"* หรือ *"สินทรัพย์เข้ารหัส (Crypto Assets)"* ก็ควรจะมีสภาพบังคับทางกฎหมายในลักษณะทำนองเดียวกันของทุกประเทศสมาชิก

2.1.6.1 กรณีศึกษา: นโยบายและมาตราการทางกฎหมายของประเทศญี่ปุ่น

ประเทศญี่ปุ่นถือเป็นประเทศเปิดกว้างต่อธุรกิจเงินสกุลเข้ารหัส และเป็นประเทศแรกที่ยอมรับสถานภาพทางกฎหมายของเงินสกุลเข้ารหัสที่เรียกว่า *"Virtual Currency"* เป็นเงินตรา

ที่ชอบด้วยกฎหมาย (Awataguchi, Edited by, & Dewey, 2019) โดยรวมถึงบิตคอยน์ซึ่งเป็นเงินสกุลเข้ารหัสแรกของโลกที่เริ่มนำเข้าสู่ระบบการเงินโลกในปี 2009 และการยอมรับให้ผู้ประกอบการต่างชาติสามารถทำธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัสในประเทศญี่ปุ่นได้ จนกระทั่งได้รับการตอบรับจากกลุ่มนักลงทุนหลายประเทศทั่วโลก ส่งผลให้ธุรกิจเงินสกุลเข้ารหัสเติบโตอย่างต่อเนื่อง และด้วยการขยายตัวของธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัสดังกล่าว ทำให้ประเทศญี่ปุ่นเป็นตลาดเงินสกุลเข้ารหัสที่มีขนาดใหญ่ที่สุดในโลก (Kawai, Nagase, Edited by, Sachheim, & Howell, 2019) และต่อมาในปี 2014 ธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัสอันดับหนึ่งของโลกได้แก่ Mt.Gox Co.,Ltd ซึ่งให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัสเป็นเงินตราปกติและระหว่างเงินสกุลเข้ารหัสอื่น ประสบปัญหาการถูกขโมย (Hack) บิตคอยน์จากกระเป๋าเงินอิเล็กทรอนิกส์ (Wallet) จำนวนประมาณกว่า 800,000 บิตคอยน์หรือมูลค่าประมาณ 640 ล้านเหรียญสหรัฐ ส่งผลให้บริษัทขาดสภาพคล่องและผลประกอบการขาดทุนจนถึงขั้นอาจล้มละลาย และต้องนำกิจการเข้าสู่กระบวนการฟื้นฟูกิจการ โดยนักลงทุนและบุคคลที่เกี่ยวข้องได้รับการชดเชยคืนเงินลงทุนบางส่วนตามสัดส่วน จากการเฉลี่ยมูลค่าบังคับขายบิตคอยน์และทรัพย์สินอื่นที่ถือครอง ซึ่งถือเป็นกรณีศึกษาสำคัญของรัฐบาลญี่ปุ่น โดยได้นำประเด็นปัญหาดังกล่าวมาเป็นแนวทางการวางมาตรการกำกับดูแลเงินสกุลเข้ารหัส เพื่อป้องกันผลประโยชน์แก่นักลงทุน (Awataguchi et al., 2019)

ในปี 2015 กลุ่มประเทศพัฒนา (G7) ได้จัดตั้งคณะทำงาน Financial Action Task Force (FATF) เพื่อทำการศึกษาและออกแนวปฏิบัติสำหรับการจัดการความเสี่ยงจากธุรกรรมเงินสกุลเข้ารหัส โดยกำหนดให้บุคคลที่เกี่ยวข้องกับธุรกรรมการแลกเปลี่ยนเงินสกุลเข้ารหัส ซึ่งอยู่ในข่ายที่จะต้องรายงานธุรกรรมตามมาตรการป้องกันการฟอกเงิน และการต่อต้านการสนับสนุนการก่อการร้ายเพื่อให้ประเทศสมาชิกได้นำไปเป็นแนวปฏิบัติ และปรับใช้ให้เหมาะสมกับบริบทของแต่ละประเทศ ทั้งนี้ รัฐบาลญี่ปุ่นได้ตระหนักถึงความจำเป็นในการออกมาตรการทางกฎหมายในการกำกับดูแลเงินสกุลเข้ารหัส ภายใต้หลักการที่จะปกป้องผลประโยชน์ของนักลงทุนจากธุรกรรมแลกเปลี่ยนเงินสกุลเข้ารหัส และยึดถือตามแนวปฏิบัติสากลเพื่อการป้องกันการฟอกเงินและการต่อต้านการสนับสุนนทางการเงินแก่การก่อการร้าย (AML/CFT) โดยได้นำสาระสำคัญเกี่ยวกับธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัสไปปรับปรุงแก้ไขเพิ่มเติมกฎหมายเกี่ยวกับธุรกิจบริการทางการเงิน The Payment Services Act and The Act on Prevention of Transfer of Criminal Proceeds ซึ่งมีผลบังคับใช้ตั้งแต่เดือนเมษายน 2017 และ Financial Services Agency (FSA) ได้ดำเนินการให้ 16 กิจการธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัสต้องเข้าจดทะเบียนทันทีตามกฎหมายที่กำหนด (Awataguchi et al., 2019)

อย่างไรก็ตาม ในปี 2018 ยังคงปรากฏเหตุการณ์ขโมย (Hack) เงินสกุลเข้ารหัสจากระบบปฏิบัติการของ Coincheck Inc. ซึ่งประกอบธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัสรายใหญ่เป็น

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

มูลค่าประมาณ 530 ล้านเหรียญสหรัฐ จนส่งผลกระทบเป็นวงกว้างต่อนักลงทุนจำนวนมาก เนื่องจากนักลงทุนให้ความสนใจลงทุน เพื่อการเก็งกำไรมากกว่าใช้เงินสกุลเข้ารหัสเพื่อการชำระค่าสินค้าและบริการ (Kawai et al., 2019) ทำให้หน่วยงาน FSA ต้องเข็มงวดด้วยการเข้าตรวจสอบระบบการปฏิบัติงานของกิจการที่ได้รับอนุญาตอย่างต่อเนื่อง อีกทั้งได้มีคำสั่งให้กิจการที่ถูกตรวจพบและมีประเด็นปัญหาในการดำเนินงานให้เร่งแก้ไขเพื่อป้องกันความเสียหายที่อาจเกิดขึ้น รวมถึงเร่งเพิ่มประสิทธิภาพการกำกับดูแลระบบการควบคุมการปฏิบัติงานภายในที่เกี่ยวข้องกับการป้องกันการฟอกเงิน โดยได้จัดตั้งคณะทำงานขึ้นศึกษาประเด็นปัญหาที่พบในระหว่างการตรวจสอบเพื่อการออกแนวปฏิบัติที่เหมาะสมแก่ผู้ประกอบการ โดยการเพิ่มประเด็นการตรวจสอบคุณสมบัติผู้ประกอบการจาก 166 รายการเป็นประมาณ 400 รายการ ในขณะเดียวกันธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัสที่ได้รับการจดทะเบียนรายใหญ่ 16 รายได้รวมตัวกันจัดตั้งสมาคม Japan Virtual Currency Exchange Association (JVCEA) เพื่อเป็นองค์กรวิชาชีพในการกำกับดูแลกิจการจดทะเบียนความเป็นสามาชิกกันเองภายใต้บทบัญญัติของกฎหมาย (Awataguchi et al., 2019)

ภายใต้กฎหมายกำกับดูแลเงินสกุลเข้ารหัสของประเทศญี่ปุ่น ได้บัญญัติให้เงินสกุลเข้ารหัสเป็นเงินตราเสมือน *“Virtual Currency”* ที่ไม่มีลักษณะเป็นหลักทรัพย์ *“Security”* ตามกฎหมายว่าด้วยหลักทรัพย์ แต่อยู่ภายใต้บังคับกฎหมายว่าด้วยบริการทางการเงินที่กำหนดให้มีสภาพเป็นเงินตราเสมือน กล่าวคือ มูลค่าซึ่งผู้ครอบครองสามารถใช้เพื่อการซื้อสินค้าและบริการ รวมถึงการชำระหนี้ให้แก่บุคคล หรือการแลกเปลี่ยนมูลค่ากับผู้ถือครองรายอื่นภายใต้เครือข่ายระบบปฏิบัติการคอมพิวเตอร์ รวมถึงกำหนดให้ผู้ประกอบการธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัสที่จะได้รับการอนุญาตต้องเป็นกิจการสัญชาติญี่ปุ่น หรือเป็นกิจการต่างชาติที่ต้องมีสาขาประกอบกิจการในประเทศญี่ปุ่นรวมถึงอยู่ในกำกับดูแลการดำเนินงานโดย FSA ทั้งนี้กฎหมายได้กำหนดให้ผู้ประกอบการขุดเงินสกุลเข้ารหัสหรือนักขุด (Miners) ได้รับการยกเว้นไม่อยู่ในบังคับที่ต้องจดทะเบียน และปฏิบัติตามกฎหมายนี้ (Awataguchi et al., 2019)

นอกจากนี้ รัฐบาลญี่ปุ่นได้ขยายการบังคับใช้กฎหมายที่เกี่ยวกับเงินสกุลเข้ารหัสให้ครอบคลุมการระดมเงินทุนที่เรียกว่า *“Crypto-assets”* ซึ่งมีความหมายรวมถึง *“Virtual Currency”* โดยให้ความสำคัญในการแก้กฎระเบียบกำกับการออกเงินสกุลเข้ารหัสสกุลใหม่ เพื่อการเสนอขายแก่ประชาชนทั่วไป (Initial Coin Offering – ICO) รวมถึงอนุพันธ์เงินสกุลเข้ารหัส (Token) และระเบียบว่าด้วยความคุ้มครองจากการปฏิบัติที่ไม่เป็นธรรมต่อนักลงทุน ด้านการบริหารความเสี่ยงที่อ้างอิงกับเงินสกุลเข้ารหัสสกุลอื่น ทั้งความเสี่ยงจากความผันผวนของราคาและความเสี่ยงจากการฉ้อโกงในการเสนอขายเงินสกุลเข้ารหัส (Kawai et al., 2019)

ทั้งนี้ในระยะแรก กฎหมายภาษีอากรไม่มีข้อบัญญัติเฉพาะที่เกี่ยวกับการทำธุรกรรมเงินสกุลเข้ารหัส รัฐบาลจึงได้ปรับใช้กฎหมายลักษณะทั่วไปเป็นภาษีบริโภค (Consumption Tax) ที่มี

ระบบการจัดเก็บคล้ายภาษีมูลค่าเพิ่มในประเทศไทย แต่ต่อมารัฐบาลได้มีการปรับปรุงแก้ไขกฎหมายภาษีอากรในปี 2017 บัญญัติให้ธุรกรรมการซื้อขายแลกเปลี่ยนเงินสกุลเข้ารหัส ถือเป็นรายได้อื่นแทน (Miscellaneous Income) และไม่ถือเป็นรายได้กำไรจากส่วนเกินทุน (Capital Gain) โดยผู้ทำธุรกรรมมีหน้าที่สำแดงรายการ เพื่อชำระภาษีเฉพาะกำไรจากการทำธุรกรรมซื้อขายแลกเปลี่ยนเงินสกุลเข้ารหัส และต้องห้ามไม่ให้นำผลขาดทุนมาหักกลบโดยให้นำรายการดังกล่าวไปนับรวมกับแบบแสดงรายการภาษีรายได้บุคคลธรรมดาประจำปี (Kawai et al., 2019)

ส่วนในระดับปัจเจกบุคคลเกี่ยวกับกฎหมายว่าด้วยมรดกนั้น กฎหมายไม่ได้มีลักษณะบังคับเป็นการเฉพาะเกี่ยวกับเงินสกุลเข้ารหัส แต่จะถือเป็นทรัพย์สินของผู้วายชนม์ที่จะตกทอดไปยังทายาทตามประมวลกฎหมายแพ่ง อย่างไรก็ตามด้วยระบบนิเวศเงินสกุลเข้ารหัสนั้นผู้ที่จะสามารถเปิดกระเป๋าเงินอิเล็กทรอนิกส์ในระบบปฏิบัติการบล็อกเชนได้ จะต้องเป็นผู้ที่รู้รหัสเปิดส่วนบุคคลเท่านั้น หากรหัสเปิดส่วนบุคคลดังกล่าวไม่ได้ถูกบันทึกให้ทราบไว้ก็จะไม่สามารถดำเนินการใดๆได้ ในกรณีนี้คาดว่ารัฐบาลญี่ปุ่น จะได้ทำการศึกษาถึงมาตรการทางกฎหมายที่จะสามารถให้เข้าถึงรหัสเปิดส่วนบุคคลสำหรับการเป๋าเงินอิเล็กทรอนิกส์ของผู้วายชนม์ได้ภายใต้เงื่อนไขทางเทคโนโลยี่ต่อไป (Awataguchi et al., 2019)

2.1.6.2 กรณีศึกษา: นโยบายและมาตราการทางกฎหมายของประเทศจีน

ประเทศจีน ถือเป็นประเทศที่มีระบบเศรษฐกิจเติบโตต่อเนื่องและมีขนาดใหญ่เป็นอันดับสองรองจากสหรัฐอเมริกา โดยเฉพาะอย่างยิ่งการเติบโตของตลาดเทคโนโลยี่การเงิน (FinTech) อันทันสมัยซึ่งเป็นกลไกผลักดันการเติบโตทางเศรษฐกิจ (Alvarez, 2018) รวมถึงระบบนิเวศเงินสกุลเข้ารหัสอย่างบิตคอยน์ที่ระบบเศรษฐกิจจีนให้การตอบรับเป็นอย่างดี จนกลายเป็นศูนย์รวมนักขุดขนาดใหญ่ของโลกทั้งระดับบุคคลและองค์กรธุรกิจ ตั้งแต่ปี 2009 เมื่อบิตคอยน์เริ่มเปิดตัวครั้งแรก (Panova, Leheza, Ivanytsia, Marchenko, & Oliukha, 2019) เนื่องจากผลตอบแทนของนักขุดที่ได้รับเป็นบิตคอยน์มีอัตราสูง และต้นทุนพลังงานไฟฟ้าในประเทศจีนเพื่อใช้ในระบบคอมพิวเตอร์ของนักขุดมีราคาถูกกว่าประเทศอื่น จนรัฐบาลจีนได้รับผลกระทบจากการขาดแคลนพลังงานไฟฟ้าเพื่อการผลิตโภคภัณฑ์อื่น ซึ่งนับเป็นอีกปัจจัยหนึ่งที่มีผลต่อการออกมาตราการกำกับดูแลเงินสกุลเข้ารหัส (Jonge & Jonge, 2018) โดยในปี 2013 ธนาคารกลางจีน (People's Bank of China – PBOC) และสถาบันการเงินหลักของจีน ได้ออกประกาศเตือนประชาชนถึงความเสี่ยงของเงินสกุลเข้ารหัสอย่างบิตคอยน์ เนื่องจากลักษณะสำคัญ 4 ประการของบิตคอยน์ (1) ไม่มีองค์กรที่ชัดเจนในการกำกับดูแล (2) มีปริมาณหมุนเวียนจำกัด (3) ระบบนิเวศแบบไร้พรมแดน และ (4) ไม่เปิดเผยตัวตนผู้ใช้งาน โดยบัญญัติให้บิตคอยน์ไม่มีลักษณะเป็นเงินตรา (Currency) ตามมาตรา 20 ของกฎหมายธนาคารกลางจีนที่ระบุ *"No units or individuals may print or sell promissory notes as substitutes for*

Renminbi to circulate in the market" จึงต้องห้ามไม่ให้สถาบันการเงินและสาธารณชนใช้บิตคอยน์ในการชำระราคาค่าสินค้าและบริการ แต่ให้ถือเสมือนเป็นสินค้าไร้รูปร่าง (Virtual Commodity) (Gong, Yu, Edit by, & Dewey, 2019)

ต่อมาในปี 2017 ธนาคารกลางจีนและสำนักงานกำกับหลักทรัพย์จีนได้ออกประกาศห้ามสถาบันการเงิน หรือธุรกิจหลักทรัพย์รวมถึงธุรกิจที่เกี่ยวข้องทำการระดมทุนด้วยการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ (ICO) แก่ประชาชนทั่วไป และให้ถือเป็นธุรกรรมการเงินที่ไม่ชอบด้วยกฎหมาย (The Law Library of Congress, 2018) รวมถึงการห้ามการดำเนินธุรกิจซื้อขายแลกเปลี่ยนระหว่างเงินสกุลเข้ารหัสต่างสกุล และเงินสกุลเข้ารหัสกับเงินหยวน เว้นแต่การถือครอง การได้มา การซื้อขายเงินสกุลดิจิทัลโดยบุคคลธรรมดาให้ถือเสมือนเป็นการค้าสินค้าไร้รูปร่าง หรือการทำธุรกรรมกับเครือข่ายการค้าระบบออนไลน์ของต่างประเทศ (Gong et al., 2019) แต่ด้วยขนาดพื้นที่ของประเทศจีนที่กว้างใหญ่ และการพัฒนาเทคโนโลยีขั้นสูงของประเทศกลับเป็นปัจจัยส่งเสริมให้ธุรกรรมเงินสกุลเข้ารหัสได้รับความนิยมและมีอัตราเติบโต โดยข้อมูลจากรายงาน China Internet Watch ณ เดือนมิถุนายน 2015 นำเสนอผลสำรวจผู้ใช้งานอินเตอร์เน็ตในประเทศจีนมีจำนวนสูงถึง 667 ล้านราย ทำให้การเข้าถึงระบบเครือข่ายออนไลน์เป็นไปด้วยความสะดวกรวดเร็ว นอกจากนี้มีผู้ใช้งานอินเตอร์เน็ตในเขตชนบทมีจำนวนกว่า 27.9% หรือประมาณกว่า 180 ล้านรายซึ่งส่วนหนึ่งเป็นประชากรจีนที่ไม่สามารถเข้าถึงบัญชีของสถาบันการเงินมีจำนวนหลายร้อยล้านราย (Alvarez, 2018) ธุรกรรมเงินสกุลเข้ารหัสจึงเป็นทางเลือกหนึ่งที่อำนวยความสะดวกในการธุรกรรมการเงิน ทั้งนี้ในระหว่างปี 2016 – 2018 จำนวนธุรกรรมการแลกเปลี่ยนเงินสกุลเข้ารหัสผ่านเครือข่ายการค้าบนระบบออนไลน์สัญชาติจีน (Platform Network) มีสูงกว่า 70% ส่วนที่เหลือจะเป็นการทำธุรกรรมผ่านระบบโครงข่ายการค้าของต่างประเทศ ทั้งนี้มีธุรกรรมเงินสกุลเข้ารหัสที่เกิดขึ้นในขอบเขตประเทศจีนและเป็นธุรกรรมที่ไม่ชอบด้วยกฎหมายมีจำนวนสูงถึง 40% (Panova et al., 2019)

ด้วยนโยบายของจีนที่ยึดหลักการกีดกันและต้องห้ามการทำธุรกรรมเงินสกุลเข้ารหัส รวมถึงธุรกิจที่เกี่ยวเนื่องถือเป็นการกระทำที่ไม่ชอบด้วยกฎหมาย กลับกลายเป็นการเปิดช่องว่างทางกฎหมายให้แก่ผู้ทำธุรกรรมต้องห้าม เป็นผลให้ไม่มีหน่วยงานรับผิดชอบใดออกมาตรการกำกับดูแลรายงานทำธุรกรรมเงินสกุลเข้ารหัส การตรวจสอบฐานะของผู้ทำรายการ (KYC) รวมถึงการป้องกันการฟอกเงิน (AML) ทำให้ประเทศจีนกลายเป็นทางผ่านของธุรกรรม หรือแหล่งฟอกเงินด้วยธุรกรรมเงินสกุลเข้ารหัสจากเงินที่ไม่ชอบด้วยกฎหมาย (Yang, 2016) นอกจากนี้รัฐบาลจีนยังเสียโอกาสในการออกมาตรการจัดเก็บภาษีอากรจากธุรกรรมเงินสกุลเข้ารหัส เพื่อรักษาผลประโยชน์อันมหาศาลของประเทศ อีกทั้งผลกระทบจากการขาดกฎหมายรับรองในระดับปัจเจกชน เมื่อเกิดข้อพิพาทเกี่ยวกับธุรกรรมเงินสกุลเข้ารหัสก็จะไม่มีกฎหมายใดสามารถบังคับใช้เพื่อการระงับข้อพิพาท รวมถึงการขาด

CHULALONGKORN UNIVERSITY

สิทธิตกทอดทางมรดก ในการร้องขอรหัสเปิดส่วนบุคคลของกระเป๋าเงินอิเล็กทรอนิกส์ในกรณีที่เจ้าของเสียชีวิต เป็นต้น (Gong et al., 2019)

อย่างไรก็ตาม ตั้งแต่ปลายปี 2017 รัฐบาลจีนเริ่มตระหนักถึงผลกระทบจากนโยบายการกีดกันและต้องห้ามธุรกรรมเงินสกุลดิจิทัล โดยได้ให้คำนิยามเงินสกุลเข้ารหัส เป็น *"Virtual Currency"* เทียบเสมือนสินค้าที่เป็นทรัพย์สินไร้รูปร่าง ซึ่งจะได้รับความคุ้มครองภายใต้กฎหมาย (Gong et al., 2019) นอกจากนี้รัฐบาลจีนได้ปรับนโยบาย โดยมอบหมายให้ธนาคารกลางแห่งชาติจีนรับผิดชอบโครงการศึกษาพัฒนาเงินสกุลเข้ารหัสของชาติหรือเรียกว่า*"Sovereign Cryptocurrency"* (Yang, 2016) บนระบบนิเวศแบบเปิดทำนองเดียวกับระบบปฏิบัติการบล็อกเชนเพื่อให้บริการโอนมูลค่าแก่ผู้ใช้งานระหว่างกันโดยตรงเช่นเดียวกับเงินสกุลเข้ารหัสทั่วไป เพื่อสนับสนุนภาคการเงินการธนาคารของจีน แต่จะมีกระบวนการกำกับปริมาณการหมุนเวียนของเงินสกุลเข้ารหัสนี้โดยธนาคารกลางจีน จึงถือเป็นเงินสกุลเข้ารหัสในลักษณะแบบรวมศูนย์ (Centralized Cryptocurrency) หรือที่เรียกว่า *"Central Bank Digital Currency – CBDC"* ทั้งนี้เงินสกุลเข้ารหัสที่รัฐบาลจีนจะนำออกทดสอบระบบนั้นจะต้องอำนวยความสะดวก เข้าถึงง่าย ปลอดภัยสูง ต้นทุนต่ำ และสามารถให้บริการประชาชนครอบคลุมวงกว้าง (Jonge & Jonge, 2018) พร้อมได้กำหนดแผนนำเสนอเงินสกุลเข้ารหัสที่จะออกและรับรองโดยรัฐบาล เพื่อใช้หมุนเวียนในระบบการเงินแทนเงินหยวนจีนในการรองรับนโยบายสังคมไร้เงินสด เนื่องจากปัจจุบันสังคมจีนมีการใช้งานธุรกรรมการค้าระบบออนไลน์และเงินอิเล็กทรอนิกส์อย่างแพร่หลายอยู่แล้ว ด้วยการปรับหลักการเป็นมุ่งสร้างความสมดุลระหว่างการเสริมสร้างนวัตกรรมกับการป้องกันการเก็งกำไรโดยไม่เป็นธรรม ทั้งนี้รัฐบาลจีนกำลังมีแผนพัฒนามาตรการทางกฎหมายที่จะรับรองธุรกรรมเงินสกุลเข้ารหัส เมื่อรัฐบาลได้ออกเงินสกุลเข้ารหัสของรัฐบาลจีนเองภายใต้แนวปฏิบัติกำกับดูแลที่เคร่งครัดต่อไป (Gong et al., 2019)

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

2.1.6.3 กรณีศึกษา: นโยบายและมาตราการทางกฎหมายของรัฐบาลไทย

สำหรับประเทศไทย การรู้จักบิตคอยน์เงินสกุลเข้ารหัสแรกค่อนข้างอยู่ในวงจำกัด เนื่องจากระดับความซับซ้อนทางเทคโนโลยี่ของระบบนิเวศเงินสกุลเข้ารหัส และผลกระทบต่อระบบเศรษฐกิจไทยและระดับสากลในช่วงแรกยังไม่สามารถสร้างความรับรู้ต่อสาธารณะได้ จนกระทั่งในปี 2017 เป็นต้นมา เมื่อกลุ่มอาชญากรทางเศรษฐกิจ Alphabay ที่มีระบบเครือข่ายการค้ายาเสพติดและสิ่งผิดกฎหมายบนระบบออนไลน์รายใหญ่ของโลก ได้อาศัยบิตคอยน์เป็นช่องทางในการโอนมูลค่าการค้าระหว่างกันโดยตรง ซึ่งกลุ่มผู้กระทำผิดดังกล่าวถูกหน่วยสืบราชการลับของสหรัฐอเมริการ่วมกับสำนักงานตำรวจแห่งชาติสืบสวนจับกุมได้ในประเทศไทย (สถาบันเพื่อการยุติธรรมแห่งประเทศไทย, 2018) จนเกิดเป็นกระแสการค้นหาความหมายของบิตคอยน์ในสายตาของสาธารณชนไทยมากขึ้น

ทั้งนี้ การรับรู้เกี่ยวกับเงินสกุลเข้ารหัสโดยเฉพาะอย่างยิ่งบิตคอยน์ของประชาชนในประเทศไทยยังขาดองค์ความรู้ที่ชัดเจน โดยในปี 2014 ธนาคารแห่งประเทศไทยได้ออกประกาศข่าว ธปท ฉบับที่ 8/2557 เรื่อง ข้อมูลเกี่ยวกับ Bitcoin และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่นๆ ที่มีลักษณะใกล้เคียงเพื่อให้คำแนะนำต่อประชาชนในการสร้างความเข้าใจถึงลักษณะของเงินสกุลเข้ารหัสและกลไกการทำงานของระบบการโอนมูลค่าระหว่างผู้ใช้งานโดยตรง รวมถึงความเสี่ยงจากการเปลี่ยนแปลงมูลค่าอย่างรวดเร็วเข้าข่ายการเก็งกำไร และความเสี่ยงจากการโจรกรรมทางระบบคอมพิวเตอร์ อีกทั้งได้แจ้งเตือนประชาชนถึงเงินสกุลเข้ารหัส *“ไม่ถือเป็นเงินที่ใช้ชำระหนี้ได้ตามกฎหมายไทย”* และไม่มีหน่วยงานใดให้ความคุ้มครองตามกฎหมาย (ธนาคารแห่งประเทศไทย, 2014)

ในเดือนกุมภาพันธ์ ปี 2018 ธนาคารแห่งประเทศไทยได้ออกหนังสือเวียนถึงสถาบันการเงินทุกแห่ง ที่ 276/2561 เรื่อง ขอความร่วมมือสถาบันการเงินไม่ให้ทำธุรกรรมที่เกี่ยวข้องกับคริปโตเคอเรนซี (ธนาคารแห่งประเทศไทย, 2019b) เนื่องจากเกิดความกังวัลต่อความเสี่ยงจากนวัตกรรมด้านเทคโนโลยี่การเงินที่ก้าวหน้าอย่างรวดเร็ว จนกระทั่งปรากฏเงินสกุลเข้ารหัสหมุนเวียนในระบบการเงินโลกหลายสกุล แต่เงินสกุลเข้ารหัสไม่มีสินทรัพย์ใดอ้างอิง และไม่มีคุณสมบัติเป็นเงินที่ใช้ในการชำระหนี้ได้ตามกฎหมาย รวมถึงยังไม่มีกฎหมายกำหนดให้อยู่ภายใต้การกำกับดูแลของหน่วยงานใดเป็นการเฉพาะ ผู้ทำธุรกรรมที่เกี่ยวข้องอาจไม่ได้รับความคุ้มครอง จึงขอความร่วมมือสถาบันการเงินทุกแห่งไม่ทำธุรกรรม หรือเข้าไปมีส่วนร่วมในการสนับสนุนการทำธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส (The Law Library of Congress, 2018) รวมถึงได้เพิ่มมาตรการรู้จักตัวตนลูกค้า (Know Your Customer – KYC) และตรวจสอบข้อเท็จจริงเกี่ยวกับลูกค้า (Customer Due Diligence – CDD) ที่ขอเปิดบัญชีหรือใช้บัญชีธนาคารของตนทำธุรกรรมการเงินกับเงินสกุลเข้ารหัส (หนังสือเวียนธนาคารแห่งประเทศไทย, กุมภาพันธ์ 2019) แต่ในขณะเดียวกันธนาคารแห่งประเทศไทยได้ดำเนินการโครงการศึกษาวางระบบเงินสกุลเข้ารหัสในลักษณะ Central Bank Digital Currency (CBDC) บนระบบนิเวศแบบกระจายศูนย์ (Distributed Ledger Technology – DLT) ในนามโครงการ *“อินทนนท์”* ซึ่งได้เริ่มทดสอบระบบการทำธุรกรรมซื้อขายพันธบัตร โดยใช้วิธีการชำระเงินแบบ Wholesale CBDC (ธรรมรักษ์ หมื่นจักร รัชพร วงศาโรจน์ กษิดิศ ตันสงวน และเกวลี สันตโยดม, 2018)

ต่อมา ในเดือนพฤษภาคม ปี2018 รัฐบาลไทยได้ตราพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 เพื่อกำกับดูแลการระดมทุนผ่านสินทรัพย์ดิจิทัลรวมถึงการประกอบธุรกิจและการดำเนินกิจกรรมที่เกี่ยวกับสินทรัพย์ดิจิทัล รวมถึงการดูแลผลกระทบต่อเสถียรภาพทางการเงิน ป้องกันการกระทำอันไม่เป็นธรรมต่อการดำเนินธุรกรรม และป้องกันการนำเงินสกุลเข้ารหัสไปสนับสนุนธุรกรรมที่ผิดกฎหมาย โดยให้อำนาจแก่คณะกรรมการกำกับทรัพย์และตลาดหลักทรัพย์ปฏิบัติหน้าที่กำกับควบคุมสินทรัพย์ดิจิทัลและผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัล รวมถึงการวาง

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

นโยบายส่งเสริมพัฒนากิจการที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล (สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2018) แม้ว่าพระราชกำหนดนี้จะได้บัญญัติให้หลักทรัพย์ตามพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ที่อาจอยู่ในรูปข้อมูลอิเล็กทรอนิกส์ ไม่ให้ถือเป็นสินทรัพย์ดิจิทัลตามพระราชกำหนดนี้ก็ตาม (พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561, 2018) แต่ถือว่าแนวนโยบายของไทยมีลักษณะการกำกับสินทรัพย์ดิจิทัลหรือเงินสกุลเข้ารหัสเข้าข่ายเป็นหลักทรัพย์เพื่อการลงทุน หรือ *“Security”*

ในช่วงเวลาต่อมาเดือนสิงหาคม ปี 2018 ธนาคารแห่งประเทศไทยได้ออกหนังสือเวียนแจ้งสถาบันการเงินทุกแห่ง ที่ 1759/2561 เรื่อง แนวทางการประกอบธุรกิจสินทรัพย์ดิจิทัลของสถาบันการเงินและบริษัทในกลุ่มธุรกิจทางการเงินของสถาบันการเงิน (ธนาคารแห่งประเทศไทย, 2019a) เพื่อแจ้งยกเลิกหนังสือเวียนที่ 276/2561 ที่สั่งห้ามไม่ให้ทำธุรกรรมที่เกี่ยวข้องกับเงินสกุลดิจิทัล ด้วยเหตุที่พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัลได้กำหนดอำนาจหน้าที่ในการกำกับดูแลเป็นของคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ธนาคารแห่งประเทศไทยจึงขอความร่วมมือในการให้การสนับสนุนการประกอบธุรกิจดังกล่าว ตามแนวปฏิบัติของคณะกรรมการกำกับทรัพย์และตลาดหลักทรัพย์ แต่ยังคงให้สถาบันการเงินได้ดูแลความเสี่ยงของกลุ่มธุรกิจการเงินในภาพรวม และปฏิบัติตามหลักเกณฑ์การป้องกันปราบปรามการฟอกเงินและต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้ายอย่างเคร่งครัดต่อไป (ธนาคารแห่งประเทศไทย, 2019a)

ขณะเดียวกันในเดือนพฤษภาคม ปี2018 เมื่อรัฐบาลได้ประกาศพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัลให้มีผลบังคับใช้ กรมสรรพากรจึงได้ออกประกาศพระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากรที่ 19/2561 เพื่อเพิ่มเติมประเภทของเงินได้ตามมาตรา 40(4) ซึ่งเป็นประเภทเงินได้ที่ได้รับผลตอบแทนจากเงินทุน โดยได้บัญญัติมาตรา 40(4)(ซ) เงินส่วนแบ่งของกำไรหรือผลประโยชน์อื่นใดในลักษณะเดียวกันที่ได้จากการถือหรือครอบครองโทเคนดิจิทัล และ 40(4)(ฌ) ผลประโยชน์ที่ได้รับจากการโอนคริปโทเคอร์เรนซีหรือโทเคนดิจิทัล ทั้งนี้ เฉพาะซึ่งตีราคาเป็นเงินได้เกินกว่าเงินที่ลงทุน โดยให้จัดเก็บภาษีจากเงินได้ประเภทดังกล่าวในอัตราร้อยละ 15.0 ซึ่งเป็นอีกหนึ่งมาตรการในการควบคุมการประกอบธุรกิจสินทรัพย์ดิจิทัล (พระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19) พ.ศ.2561, 2018)

2.1.6.4 สรุปเปรียบเทียบนโยบายและมาตรการทางกฎหมายที่มีต่อเงินสกุลเข้ารหัสของญี่ปุ่น จีน และไทย

การศึกษาเปรียบเทียบ มาตรการทางกฎหมายของต่างประเทศที่มีต่อการกำกับดูแลเงินสกุลเข้ารหัสนี้ ได้เลือกกรณีศึกษาจากประเทศในภูมิภาคเอเชียที่มีมาตราการทางกฎหมายที่

แตกต่างกัน โดยประเทศญี่ปุ่นเป็นประเทศที่ให้การยอมรับและรับรองธุรกรรมเงินสกุลเข้ารหัสชอบด้วยกฎหมาย ประเทศจีนเป็นประเทศที่ต้องห้ามธุรกรรมเงินสกุลเข้ารหัสและถือเป็นธุรกรรมที่ไม่ชอบด้วยกฎหมาย สำหรับประเทศไทยนั้นเป็นประเทศที่มีการรับรองธุรกรรมเงินสกุลเข้ารหัสชอบด้วยกฎหมายในบางลักษณะ ทั้งนี้เพื่อการเปรียบเทียบและสร้างความเข้าใจถึงมาตรการทางกฎหมายมากขึ้น ผู้ทำวิจัยจึงได้สังเคราะห์ สรุปเป็นประเด็นพิจารณาที่อาจมีผลต่อการกำหนดมาตรการทางกฎหมายตามบริบททางเศรษฐกิจและสังคมของแต่ละประเทศของกรณีศึกษา ดังนี้

สรุปเปรียบเทียบมาตรการทางกฎหมายที่มีต่อเงินสกุลเข้ารหัสของญี่ปุ่น จีน และไทย

ประเด็นพิจารณา	ประเทศญี่ปุ่น[5]	ประเทศจีน[6]	ประเทศไทย
คำเรียกเงินสกุลเข้ารหัส	Virtual Currency	Virtual Commodity	Digital Currency
ลักษณะของเงินสกุลเข้ารหัส	เข้าข่าย *“เงินตรา”*	เข้าข่าย *“สินค้า”*	เข้าข่าย *“หลักทรัพย์”*
สถานภาพทางกฎหมายของเงินสกุลเข้ารหัส	ถือเป็นสินทรัพย์ดิจิทัลที่ชอบด้วยกฎหมายซึ่งมีมูลค่า และมีสภาพบังคับใช้ในการชำระหนี้ค่าสินค้าและบริการได้ ถูกต้องตามกฎหมาย แม้ว่าการซื้อขายและการชำระราคาดังล่าวดำเนินการกับบุคคลที่ไม่ระบุตัวตน รวมถึงการโอนมูลค่าให้บุคคลที่ไม่ระบุตัวตนผ่านระบบนิเวศเงินสกุลเข้ารหัส	ถือเป็นสิ่งไม่ชอบด้วยกฎหมาย ต้องห้ามไม่ให้ทำธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสภายในประเทศ แต่ไม่ต้องห้ามกรณีดำเนินธุรกรรมลักษณะดังกล่าวนอกประเทศ อย่างไรก็ตามรัฐบาลจีนกำลังพัฒนาเงินสกุลเข้ารหัสของธนาคารกลางเพื่อสนับสนุนระบบเศรษฐกิจด้วยระบบสังคมไร้เงินสด ที่กำกับดูแลด้วยเงินสกุลเข้ารหัสโดยรัฐบาลจีน	ถือเป็นสิ่งที่ชอบด้วยกฎหมายในลักษณะเทียบเคียงหลักทรัพย์ โดยในปี 2018 ได้มีการตราพระราชกำหนดการประกอบกิจการธุรกิจสินทรัพย์ดิจิทัล เพื่อการกำกับดูแลธุรกรรมและผู้ประกอบการที่เกี่ยวข้องกับเงินสกุลดิจิทัล โดยมุ่งให้ความคุ้มครองต่อการระดมเงินทุน

[5](Awataguchi et al., 2019; Kawai et al., 2019)

[6] (Gong et al., 2019)

ประเด็นพิจารณา	ประเทศญี่ปุ่น	ประเทศจีน	ประเทศไทย
หน่วยงานกำกับดูแล	สถาบันกำกับสถาบันการเงิน (Financial Services Agency – FSA)	ไม่มีหน่วยงานใดกำกับดูแล เนื่องจากต้องห้ามตามกฎหมาย แต่ธนาคารกลางจะทำหน้าที่เฝ้าระวังดูแลความเคลื่อนไหวของการทำธุรกรรมเงินสกุลเข้ารหัส	สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
ธุรกิจแลกเปลี่ยนเงินสกุลเข้ารหัส	ไม่ต้องห้ามแต่ผู้ประกอบการจะต้องได้รับอนุญาตจากหน่วยงานกำกับ Financial Services Agency – FSA) และนำเสนอรายงานธุรกรรมรวมถึงรายงานอื่นต่อ FSA และบังคับใช้มาตรการป้องกันการฟอกเงิน โดยผู้ให้บริการจะต้องตรวจสอบตัวตนของผู้ขอใช้บริการรวมถึงรายงานธุรกรรมที่เข้าข่ายมีข้อต้องสงสัยต่อหน่วยงานกำกับ	ถือเป็นธุรกิจต้องห้ามตามกฎหมาย ไม่สามารถดำเนินการไม่ว่าจะเป็นในธุรกิจเครือข่ายออนไลน์ทั้งระบบการชำระเงินของสถาบันการเงินและไม่ใช่สถาบันการเงิน อย่างไรก็ตามปรากฏว่ามีชาวจีนจำนวนหนึ่งยังคงดำเนินธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสโดยผ่านระบบนิเวศออนไลน์ของต่างประเทศที่รัฐบาลจีนไม่สามารถเข้าถึงและกีดกันได้	ไม่ต้องห้ามแต่ผู้ประกอบการจะต้องได้รับอนุญาตจากสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และนำเสนอรายงานธุรกรรมต่อ สำนักงาน กลต. แต่ยังไม่มีมาตราการป้องกันการฟอกเงินโดยเงินสกุลเข้ารหัสโดยตรงออกมาบังคับใช้

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ประเด็นพิจารณา	ประเทศญี่ปุ่น	ประเทศจีน	ประเทศไทย
การเสนอขายเงินสกุลเข้ารหัสใหม่ (Initial Coin Offering)	สามารถดำเนินการได้ตามกฎหมายโดยเมื่อต้นปี 2018 FSA ได้ตั้งคณะทำงานร่วมภาคเอกชนในสายธุรกิจการธนาคารและหลักทรัพย์เพื่อศึกษาการออกมาตรการกำกับดูแลการเสนอขายเงินสกุลเข้ารหัสใหม่ต่อสาธารณะ	ต้องห้ามไม่ให้สถาบันการเงินเข้าไปร่วมธุรกรรมดังกล่าว อย่างไรก็ตามธนาคารกลางจีนได้จัดตั้งสถาบันเงินสกุลเข้ารหัส (Institute of Digital Money) เพื่อเตรียมการพัฒนาระบบเทคโนโลยี่ของตนเองในการออกเงินสกุลเข้ารหัสกลางของประเทศจีนเอง ทั้งนี้ในปี 2017 ธนาคารกลางจีนได้เริ่มทดสอบระบบนิเวศเงินสกุลเข้ารหัสของจีนที่จะมีสถานภาพทางกฎหมายเทียบเท่ากับเงินหยวน	สามารถดำเนินการได้ตามกฎหมายโดยสำนักงาน กลต. เป็นหน่วยงานกำกับดูแลและให้ใบอนุญาตประกิจการแก่ผู้ประกอบที่ปรึกษาคัดกรองโครงการเสนอขายสินทรัพย์ดิจิทัล (ICO Portal) และ ผู้ให้บริการระดมทุนจากเสนอขายสินทรัพย์ดิจิทัลต่อประชาชน (ICO Issuer)
ภาษีอากร	กำหนดให้ถือเป็นรายได้อื่นที่เข้าข่ายต้องชำระภาษีเงินได้ตามกฎหมาย และไม่ถือเป็นกำไรจากส่วนเกินเงินลงทุน (Capital Gain)	ไม่มีมาตรการทางภาษีใดๆ เนื่องจากต้องห้ามการถือครอง รวมถึงการดำเนินธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสในประเทศจีน	กำหนดให้ถือเป็นกำไรจากส่วนเกินเงินลงทุน (Capital Gain) ที่เข้าข่ายต้องชำระภาษีเงินได้

แหล่งที่มา : สรุปเปรียบเทียบโดยผู้วิจัย

2.2 แนวคิดเกี่ยวกับกระบวนการฟอกเงิน

2.2.1 กระบวนการฟอกเงิน

กระบวนการฟอกเงินไม่ใช่ลักษณะการกระทำผิดทางอาญาที่เกิดขึ้นในตัวเอง (Mala Inse) หากแต่เป็นการกระทำที่กฎหมายได้บัญญัติให้การกระทำนั้นเป็นความผิดทางอาญา (Mala Prohibita) ทั้งนี้การนิยามให้ความหมายของการฟอกเงินจะมีความแตกต่างกัน ดังเช่น สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

– UNODC) ให้ความหมายการฟอกเงิน คือ *“กระบวนการจัดการซ่อนเร้นผลประโยชน์ที่อาชญากรได้รับจากการกระทำผิด ไม่ว่าจะเป็นการค้ายาเสพติด ฉ้อราษฎร หรือบังหลวง เพื่อกลบเกลื่อนร่องรอย ปิดบังที่ซ่อนแหล่งเงินจากการกระทำผิด ป้องกันการติดตามจับกุม โดยกลไกการฟอกเงินประกอบด้วย 3 ขั้นตอน คือ (1) การเคลื่อนย้ายเงินจากการกระทำผิดเข้าสู่ระบบ (Placement) (2) การกลบเกลื่อนร่องรอยเส้นทางการเงิน (Layering) และ (3) การรวบรวมเป็นเงินที่ชอบด้วยกฎหมายกลับให้แก่ผู้กระทำผิด (Integration)”* (Unite Nations Office on Drugs and Crime, 2020) และคณะกรรมการธิการยุโรป (European Commission) ได้ให้ความหมาย *“การฟอกเงินเป็นกระบวนการที่อาชญากรใช้เพื่อการสร้างความชอบด้วยกฎหมายให้แก่เงินจากการกระทำผิด ซึ่งส่วนใหญ่จะเกี่ยวข้องกับอาชญากรรมองค์กร ที่สามารถสร้างผลประโยชน์มหาศาลจากการค้ายาเสพติด การค้าอาวุธ การค้ามนุษย์ รวมถึงการฉ้อโกง”* (European Commission, 2020)

ในขณะที่ประเทศไทย มีกฎหมายบัญญัติให้การฟอกเงินที่เกี่ยวกับการกระทำความผิดมูลฐานเป็นความผิดทางอาญา ตามมาตรา 5 แห่งพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 ที่กล่าวว่า *“ผู้ใด (1) โอน รับโอน หรือเปลี่ยนสภาพทรัพย์สินที่เกี่ยวกับการกระทำผิดเพื่อซุกซ่อน หรือปกปิดแหล่งที่มาของทรัพย์สินนั้น หรือเพื่อช่วยเหลือผู้อื่นไม่ว่าก่อน ขณะหรือหลังการกระทำผิด มิให้ต้องได้รับโทษหรือได้รับโทษน้อยลงในความผิดมูลฐาน หรือ (2) กระทำการด้วยประการใดๆ เพื่อปกปิดหรืออำพรางลักษณะที่แท้จริงของการได้มาจากแหล่งที่ตั้ง การจำหน่าย การโอน การได้สิทธิใดๆ ซึ่งทรัพย์สินที่เกี่ยวข้องกับการกระทำผิด (3) ได้มา ครอบครอง หรือใช้ทรัพย์สินโดยรู้ในขณะที่ได้มา ครอบครองหรือใช้ทรัพย์สินนั้นว่าเป็นทรัพย์สินที่เกี่ยวกับการกระทำผิด ผู้นั้นกระทำผิดฐานฟอกเงิน”* หรือกล่าวอีกนัยหนึ่ง คือ การยักย้ายถ่ายโอนทรัพย์สินมีลักษณะเช่นเดียวกับมาตรา 5 ของพระราชบัญญัตินี้จะต้องรับผิดทางอาญาก็ต่อเมื่อผู้นั้นได้กระทำกับทรัพย์สินที่เกี่ยวกับหรือได้มาจากกระทำความผิดมูลฐานที่บัญญัติไว้ในมาตรา 3 ซึ่งได้บัญญัติความผิดมูลฐานแรกเริ่มไว้ 10 ลักษณะ และได้มีการแก้ไขเพิ่มเติมอย่างต่อเนื่องจนถึงปัจุบันเป็นการแก้ไขเพิ่มฉบับที่ 5 ได้บัญญัติขยายความผิดมูลฐานไว้ถึง 29 ลักษณะ (พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542, 2017) กล่าวโดยสรุป การฟอกเงินเป็นกระบวนการในการแปรสภาพของเงินผิดกฎหมาย หรือเงินที่ได้มาจากการกระทำผิดกฎหมาย เช่น การค้าอาวุธ การค้ายาเสพติด การฉ้อโกง เป็นต้น ซึ่งเงินดังกล่าวนี้จะเรียกว่า *“เงินสกปรก”* (Taint Money) ให้เป็นเงินที่ชอบด้วยกฎหมาย หรือที่เรียกว่า *“เงินสะอาด”* (Clean Money) ทั้งนี้ ความหมายของการฟอกเงินยังขยายความไปถึงทรัพย์สินที่มีมูลค่าอื่นนอกเหนือจากเงินตรา เช่น ที่ดิน ทองคำ รถยนต์ หลักทรัพย์ รวมถึงเงินสกุลเข้ารหัส เช่น บิตคอยน์ซึ่งมีลักษณะทรัพย์สินที่ไร้รูปร่างแต่มีมูลค่าสามารถแลกเปลี่ยนเป็นเงินตราที่ชอบด้วยกฎหมายได้ในที่สุด

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ทั้งนี้ กระบวนการฟอกเงินประกอบไปด้วยขั้นตอนการดำเนินการเพื่อแปรสภาพจากเงินที่ไม่ชอบด้วยกฎหมายให้เป็นเงินที่ชอบด้วยกฎหมาย ซึ่งมี 3 ขั้นตอน คือ

(1) **การนำเงินสกปรกเข้าสู่ระบบ (Placement Stage)** เป็นขั้นตอนแรกที่ผู้กระทำผิด หรืออาชญากรได้รับเงินจากการกระทำผิดกฎหมาย ใช้ความพยายามนำเงินดังกล่าวเข้าสู่ระบบสถาบันการเงิน หรือแปรสภาพเป็นทรัพย์สินที่สามารถหลบเลี่ยงการตรวจพิสูจน์ตัวตนโดยหน่วยงานรัฐ (Breing, Accorsi, & Muller, 2015) ในกรณีที่เงินสกปรกมีมูลค่าสูง หรือเป็นทรัพย์สินรายการใหญ่ซึ่งเป็นที่สังเกตได้โดยง่าย ก็จะยิ่งเพิ่มความเสี่ยงจากการตรวจสอบแก่ผู้ถือครอง ดังนั้นผู้กระทำผิดจึงพยายามถ่ายโอนไปยังขั้นตอนต่อไปให้เร็วที่สุดก่อนที่จะถูกตรวจสอบ หรือถูกอายัดทรัพย์สินตามกระบวนการป้องกันและปราบปรามการฟอกเงิน โดยทำการกระจายจำนวนผู้ถือครองทรัพย์สิน (Smurfs) ด้วยการแบ่งแยกย่อยจำนวนเงิน หรือทรัพย์สินให้แก่ผู้ถือครองจำนวนมากรายและผู้ถือครองแต่ละรายจะถือครองทรัพย์สิน ที่มีมูลค่าไม่เกินกว่าจำนวนที่กฎหมายยกเว้นการตรวจสอบ หรือกฎหมายไม่กำหนดให้เป็นประเด็นต้องตรวจสอบ (Baath & Zellhorn, 2016)

(2) **การกลบเกลื่อนร่องรอยเส้นทางการเงิน (Layering)** เป็นขั้นตอนต่อเนื่องหลังจากผู้กระทำผิดได้รับเงินสกปรกจากการกระทำที่ไม่ชอบด้วยกฎหมาย จะเป็นขั้นตอนในการแปรสภาพจากเงินที่สามารถตรวจพิสูจน์เส้นทางการเงิน หรือพิสูจน์ตัวตนของผู้ถือครองทรัพย์สินได้ไปสู่ขั้นตอนจัดการกลบเกลื่อนร่องรอย ยักย้าย ถ่ายโอน แปรสภาพทรัพย์สินเป็นทรัพย์สินรูปแบบอื่นที่ไม่สามารถตรวจพิสูจน์ติดตามแหล่งที่มาของทรัพย์สินได้ (Breing et al., 2015) เช่น การนำเงินจากการกระทำผิดไปซื้อเพชรพลอย ทองคำ รถยนต์หรู งานศิลปะ หรือวัตถุโบราณ โดยไม่ระบุแหล่งที่มาของเงินในการซื้อทรัพย์สินดังกล่าว รวมถึงการถ่ายโอนทรัพย์ที่ถือครองไปหลายลำดับขั้น การให้กู้ยืมเงินแก่บุคคลรายย่อย การทยอยโอนเงินระหว่างประเทศ จนในที่สุดไม่สามารถตรวจสอบย้อนกลับไปยังแหล่งที่มาของเส้นทางการเงินตั้งต้นได้ (Baath & Zellhorn, 2016)

(3) **การรวบรวมเป็นเงินสะอาดที่ชอบด้วยกฎหมาย (Integration Stage)** เป็นขั้นตอนในการรวบรวมเงิน หรือทรัพย์สินที่ได้กระจายผ่านผู้ถือครองหลายราย (Smurfs) หรือจัดการกลบเกลื่อนร่องรอย ยักย้อย ถ่ายโอนทรัพย์สิน (Layering) ส่งมอบกลับคืนไปยังผู้กระทำความผิดซึ่งเป็นเจ้าของเงินดังกล่าว (Breing et al., 2015) โดยผ่านระบบสถาบันการเงิน หรือกระบวนการอื่นที่กฎหมายให้การรับรอง เพื่อให้เป็นเงินที่ชอบด้วยกฎหมาย เช่น การขายทรัพย์สินที่ลงทุนซื้อในขั้นตอนที่ 2 หรือการถอนและฝากเงินสดจำนวนย่อยในวงเงินที่ไม่อยู่ในการบังคับของกฎหมายป้องกันและปราบปรามการฟอกเงิน (Baath & Zellhorn, 2016)

ขั้นตอนการกลบเกลื่อนร่องรอยเส้นทางการเงิน นับว่าเป็นขั้นตอนสำคัญต่อกระบวนการฟอกเงิน ดังนั้นผู้กระทำผิดมักจะหาแหล่งที่ให้บริการช่องทางในการแปรสภาพเงินหรือทรัพย์สิน โดยอาศัยช่องว่างของมาตราการทางกฎหมายการเงินและความไม่เข็มงวดของการบังคับใช้กฎหมายต่อต้านการฟอกเงิน ณ แหล่งที่ตั้งนั้น ซึ่งมักเป็นแหล่งหรือสถานที่ที่มีลักษณะการให้บริการเงินทุนหมุนเวียนสะพัดจนยากต่อการตรวจสอบสืบค้นแหล่งที่มาของธุรกรรมการเงิน อันเป็นช่องทางอำนวยความสะดวกในการฟอกเงิน ซึ่งประกอบด้วยแหล่งที่ตั้งนอกประเทศและในประเทศ ดังนี้ (ไชยยศ เหมาะรัชตะ, 1997)

(1) ธนาคารในบางประเทศที่มีกฎหมายคุ้มครองความลับข้อมูลบัญชีธนาคารของลูกค้าอย่างเข็มงวด เช่น ธนาคารในประเทศสวิตเซอร์แลนด์

(2) สถาบันการเงินในหมู่เกาะแคริเบียน ซึ่งเป็นแหล่งสำคัญในการอำนวยความสะดวกในการฟอกเงิน เนื่องจากมีอาณาเขตใกล้กับประเทศสหรัฐอเมริกาซึ่งเป็นศูนย์กลางการเงินสำคัญของโลก

(3) ประเทศขนาดเล็กในทวีปยุโรปซึ่งไม่มีรายได้หลักของประเทศชัดเจน แต่อาศัยรายได้จากบริการการพนันบ่อนคาสิโน และให้บริการรับจดทะเบียนจัดตั้งบริษัทบังหน้าที่ไม่ประกอบกิจการชัดเจน แต่เพื่อเป็นแหล่งอำนวยความสะดวกในการรักษาความลับของผู้ประกอบการและปิดบังแหล่งที่มาของธุรกรรมการเงินในการฟอกเงิน

(4) ประเทศรัฐอิสระซึ่งเป็นอดีตประเทศอาณานิคมของยุโรป ตั้งอยู่ในหมู่เกาะขนาดเล็กแถบทะเลแปซิฟิกตอนใต้ และในทะเลเมดิเตอร์เรเนียน ที่มีอาณาเขตใกล้ชายฝั่งทะเลของประเทศฝรั่งเศสและประเทศอังกฤษซึ่งถือเป็นอีกหนึ่งในศูนย์กลางการเงินโลก โดยอาจมีนโยบายเอื้อประโยชน์ทางภาษี และความสะดวกในการยักย้ายถ่ายเททรัพย์สินข้ามเขตประเทศด้วยเหตุแห่งความเป็นอดีตอาณานิคม

(5) บ่อนการพนันทั้งที่ถูกต้องตามกฎหมายและที่ผิดกฎหมาย เนื่องจากบ่อนการพนันเป็นแหล่งหมุนเวียนเงินสดปริมาณมากและรวดเร็ว โดยเฉพาะอย่างยิ่งบ่อนการพนันในบางประเทศที่อนุญาตให้จัดตั้งได้ตามกฎหมาย มักถูกใช้เป็นเครื่องมือในการฟอกเงินด้วยการสมคบคิดกับเจ้าของบ่อนการพนัน ด้วยการกำหนดให้ผู้กระทำผิดชนะพนัน ซึ่งเงินรางวัลที่ได้รับจึงเป็นเงินที่ชอบด้วยกฎหมาย โดยเจ้าของบ่อนการพนันได้รับค่าตอบแทน หรือในบางกรณีผู้กระทำผิดอาจลงทุนจัดตั้งบ่อนการพนันเองเพื่อบังหน้าในการฟอกเงินของตน

(6) ตลาดหลักทรัพย์ ซึ่งเป็นศูนย์กลางในการซื้อขายหลักทรัพย์จดทะเบียน โดยปริมาณหมุนเวียนเปลี่ยนมือหลักทรัพย์ระหว่างผู้ลงทุนจำนวนมากและรวดเร็ว อาจถือเป็นอีกช่องทาง

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

หนึ่งที่ผู้กระทำผิดใช้ช่องทางการค้าหลักทรัพย์ ในการเปลี่ยนสภาพเงินที่ได้จากการกระทำผิดได้โดยง่าย โดยเฉพาะอย่างยิ่งตลาดหลักทรัพย์ในบางประเทศที่มีสภาวะตลาดเพื่อการเกร็งกำไร

(7) การค้าอสังหาริมทรัพย์ หรือสังหาริมทรัพย์ที่มีมูลค่าสูง เนื่องจากเป็นธุรกรรมที่สามารถเปลี่ยนสภาพเงินได้คราวละจำนวนมาก ซึ่งสถาบันการเงินในประเทศกำลังพัฒนามักให้ความสำคัญต่ออสังหาริมทรัพย์ อีกทั้งอัญมณีและทองคำซึ่งเป็นสังหาริมทรัพย์ที่มูลค่าสูงสามารถเคลื่อนย้ายและส่งมอบให้แก่กันได้โดยง่ายด้วยการซื้อบังหน้าในราคาต่ำและขายต่ออีกทอดในราคาสูง

(8) การเปลี่ยนเป็นเงินตราสกุลอื่น เนื่องด้วยบริบททางสังคมมีการเปลี่ยนเชื่อมโยงกันเป็นโลกาภิวัตร ส่งผลให้เกิดธุรกรรมการค้าระหว่างประเทศ หรือการเดินทางท่องเที่ยวข้ามประเทศกันเป็นจำนวนมาก รวมถึงการเปิดเสรีการเงินระหว่างประเทศ หลายประเทศลดข้อจำกัดในการควบคุมการเคลื่อนย้ายเงินทุน ดังนั้นจึงเกิดช่องโอกาสในการแลกเปลี่ยนเงินเป็นเงินตราสกุลอื่น เพื่อการส่งมอบผ่านการค้าระหว่างประเทศ และการท่องเที่ยวต่างประเทศ รวมถึงบริการชำระเงินระหว่างประเทศทางอิเล็กทรอนิกส์หรือบัตรเครดิต

(9) การโอนย้าย ถ่ายเท ทรัพย์สินให้ผู้อื่นถือแทน ซึ่งเป็นวิธีการพื้นฐานในการกระจายทรัพย์สิน โอนย้ายให้แก่บุคคลที่ตนไว้วางใจและสมรู้ร่วมคิดกันครอบครองทรัพย์สิน ดูแลผลประโยชน์แทน จนกว่าจะสบโอกาสในการโอนย้ายคืนแก่ผู้กระทำผิดในอนาคต

ทั้งนี้ Tax Justic Network (2020) เครือข่ายหน่วยงานระหว่างประเทศในการตรวจสอบการหลีกเลี่ยงภาษีและการสนับสนุนการฟอกเงิน ได้นำเสนอรายงานดัชนีความโปร่งใสของระบบการเงินระหว่างประเทศประจำปี 2020 หรือที่เรียกว่า *“Financial Secrecy Index 2020 Reports Progress on Global Transparency”* ซึ่งเป็นรายงานดัชนีการจัดอันดับความโปร่งใสของระบบการเงิน โดยประเมินจากบรรทัดฐานการปกปิดความลับทางการเงินของผู้ใช้บริการของแต่ละประเทศ ซึ่งมีปัจจัยตัวชี้วัด 20 เกณฑ์ ประกอบด้วย 4 กลุ่มคือ (1) การลงทะเบียนตัวตนผู้ใช้บริการ (2)ความโปร่งใสของหน่วยงานบังคับใช้กฎหมาย (3) หลักคุณธรรมต่อระเบียบปฏิบัติทางภาษีอากรและการเงิน และ (4) มาตรฐานและความร่วมมือระหว่างประเทศ ซึ่งแต่ละเกณฑ์มีระดับคะแนนตั้งแต่ 0 คือมีความโปร่งใสสูง และ 100 คือปกปิดความลับข้อมูลผู้ใช้บริการ

รายงานดัชนีนี้เป็นการประเมินประสิทธิภาพของระเบียบปฏิบัติ และการบังคับใช้มาตรการทางกฎหมายในการให้บริการทางการเงินแก่เจ้าของบัญชีผู้ที่มีถิ่นฐานอยู่นอกประเทศ ในกรณีที่ประเทศใดมีคะแนนประเมิน Secrecy Score สูง แสดงว่าประเทศนั้นมีแนวโน้มในการปกปิดข้อมูลทางการเงินของเจ้าของบัญชีผู้ใช้บริการซึ่งเป็นชาวต่างประเทศ อันอาจเป็นช่องทางในการเอื้อประโยชน์แก่ผู้กระทำผิดที่ต้องการซ่อนเร้นแหล่งเงินที่ไม่ชอบด้วยกฎหมายหรือถือเป็นแหล่งสนับสนุน

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

การฟอกเงิน ในทางกลับกันประเทศที่มีคะแนนประเมิน Secrecy Score ต่ำ แสดงว่าประเทศนั้นมีความโปร่งใสในการให้บริการทางการเงิน โดยสามารถตรวจสอบเข้าถึงข้อมูลผู้ใช้บริการได้

จากรายงานผลการประเมิน 10 อันดับแรกของประเทศที่มีแนวโน้มเป็นแหล่งสนับสนุนการฟอกเงิน ปรากฏว่า อันดับ 1 คือหมู่เกาะเคย์แมนแต่มีสัดส่วนปริมาณธุรกรรมการเงินที่ให้บริการแก่ผู้มีถิ่นที่อยู่นอกประเทศเพียง 4.58% ของธุรกรรมการเงินรวมทั้ง 133 ประเทศ ในขณะที่อันดับ 2 ประเทศสหรัฐอเมริกาสัดส่วนปริมาณธุรกรรมการเงินสูงสุดถึง 21.37% สำหรับประเทศสวิตเซอร์แลนด์ซึ่งในอดีตถือเป็นแหล่งสนับสนุนการฟอกเงินที่สำคัญของโลก ได้ขยับอันดับลงมาเป็นอันดับ 3 หลังจากรัฐบาลยอมรับมาตรการต่อต้านการฟอกเงินโดยการปรับแนวปฏิบัติในการรักษาความลับของบัญชีผู้ใช้บริการทางการเงิน ส่วนอันดับ 4 อันดับ 5 และอันดับ 7 เป็นแหล่งประเทศในภูมิภาคเอเชียแปซิฟิค อันได้แก่ เขตปกครองฮ่องกง ประเทศสิงค์โปร์ และประเทศญี่ปุ่น ตามลำดับ สำหรับอันดับ 6 เป็นประเทศขนาดเล็กในทวีปยุโรปได้แก่ประเทศลักเซมเบิร์กซึ่งให้บริการธุรกรรมการเงินสัดส่วนสูงถึง 12.36% นอกจากนี้ประเทศอังกฤษซึ่งถูกจัดอยู่ในอันดับ 12 ปรับอันดับสูงขึ้นอย่างก้าวกระโดดจากปี 2018 ที่ถูกจัดอยู่ในอันดับ 28 โดยมีสัดส่วนปริมาณธุรกรรมการเงินถึง 15.94% และหากรวมประเทศในเครือจักรภพอังกฤษเป็นเสมือนรัฐเดียวกัน ซึ่งหมายรวมถึงหมู่เกาะเคย์แมนและหมู่เกาะบริติชเวอร์จินด้วยแล้ว จะส่งผลให้เป็นรัฐในเครือจักรภพอังกฤษเป็นแหล่งสนับสนุนการฟอกเงินสำคัญและมีสัดส่วนปริมาณธุรกรรมการเงินสูงสุดเป็นอันดับหนึ่งของโลก

ในขณะที่ประเทศไทยถูกจัดอยู่ในอันดับ 17 ด้วยคะแนนประเมิน Secrecy Score ระดับ 73.25 เปรียบเทียบกับค่าเฉลี่ยของคะแนนประเมินที่ 63.0 นอกจากนี้รายงานได้นำเสนอภูมิภาคที่เป็นแหล่งสนับสนุนการฟอกเงินสำคัญที่สุดคือภูมิภาคยุโรปและเอเชียกลาง โดยมีสัดส่วนปริมาณธุรกรรมการเงินที่ระดับ 51.54% หรือมีขนาดเกินกว่าครึ่งหนึ่งของปริมาณธุรกรรมการเงินทั้งโลก ส่วนภูมิภาคอเมริกาเหนือมีสัดส่วนปริมาณธุรกรรมการเงินที่ระดับ 22.97% โดยเป็นสัดส่วนปริมาณธุรกรรมของประเทศสหรัฐอเมริกามากถึง 21.37% สำหรับภูมิภาคเอเชียตะวันออกและเขตทะเลแปซิฟิคซึ่งรวมถึงประเทศไทยมีสัดส่วนปริมาณธุรกรรมทางการเงินที่ระดับ 15.14% ดังนั้นผู้กระทำผิดอาจเลือกแหล่งสนับสนุนการฟอกเงิน ซึ่งมีมาตรการการรักษาความลับข้อมูลทางการเงินของผู้ใช้บริการในระดับสูง เพื่อการซ่อนเร้นแหล่งเงินที่ได้จากการกระทำผิดและหลีกเลี่ยงการดำเนินการในแหล่งประเทศที่มีระดับความโปร่งใสสูง ซึ่งมีมาตรการอนุญาตให้เข้าถึงข้อมูลผู้ใช้บริการทางการเงินได้โดยง่าย (Tax Justic Network, 2020)

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

การจัดอันดับ 10 ประเทศแรกของดัชนี The Financial Secrecy Index 2020

อันดับ	ประเทศ	FSI Value[7]	FSI Share[8]	Secrecy Score[9]	Global Scale Weight[10]
1	หมู่เกาะเคย์แมน	1575.19	4.62%	76.08	4.58%
2	สหรัฐอเมริกา	1486.96	4.36%	62.89	21.37%
3	สวิตเซอร์แลนด์	1402.10	4.11%	74.05	4.12%
4	เขตปกครองฮ่องกง	1035.29	3.04%	66.38	4.44%
5	สิงคโปร์	1022.12	3.00%	64.98	5.17%
6	ลักเซมเบิร์ก	849.36	2.49%	55.45	12.36%
7	ญี่ปุ่น	695.59	2.04%	62.85	2.20%
8	เนเธอร์แลนด์	682.20	2.00%	67.40	1.11%
9	หมู่เกาะบริติชเวอร์จิน	619.14	1.82%	71.30	0.50%
10	สหรัฐอาหรับเอมิเรตส์	605.20	1.78%	77.93	0.21%
17	**ไทย**	**448.86**	**1.32%**	**73.25**	**0.15%**

ดัชนี the Financial Secrecy จำแนกตามภูมิภาค

ภูมิภาค	Sum of FSI Value	Sum of FSI Share	Avg.Secrecy Score	Sum of Global Scale Weight
ยุโรป-เอเชียกลาง	10109.00	29.90%	55.80	51.54%
เอเชียตะวันออก-แปซิฟิก	6822.60	20.00%	65.60	15.14%
ลาตินอเมริกา-แคริเบียน	6615.10	19.40%	68.00	5.91%
ตะวันออกกลาง-แอฟาริกาเหนือ	4118.00	12.10%	69.40	1.92%
แอฟาริกา	3261.00	9.60%	69.50	0.62%
ลาตินอเมริกา	2459.60	7.20%	62.50	0.67%
แอฟริกาใต้สะฮารา	2313.60	6.80%	68.90	0.52%
อเมิรกาเหนือ	1925.30	5.70%	59.40	22.97%
เอเชียใต้	1011.40	3.00%	65.50	1.13%
แหล่งที่มา: Financial Secrecy Index 2020 reported by Tax Justice Network on 18 February 2020				

[7] เป็นค่าที่ได้จากการคำนวณระหว่าง Secrecy Score กับ Global Scale Weight

[8] เป็นค่าสัดส่วนของ FSI Value เทียบกับผลรวมของค่า FSI Value ของทั้ง 133 ประเทศ

[9] เป็นค่าประเมินการรักษาความลับทางการเงินรวม 20 เกณฑ์ (เกณฑ์ละ 100 คะแนน)

[10] สัดส่วนปริมาณธุรกรรมการเงินที่ให้บริการแก่ผู้มีถิ่นที่อยู่นอกประเทศเทียบกับปริมาณรวม

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

2.2.2 กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

ดังที่กล่าวมาข้างต้นเป็นกระบวนการฟอกเงินโดยผ่านทรัพย์สินที่มีรูปร่าง แต่ในกรณีการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ซึ่งเป็นเพียงรหัสข้อมูลอิเล็กทรอนิกส์ในระบบนิเวศอินเตอร์เน็ตภายใต้ระบบปฏิบัติการบล็อกเชน และมีลักษณะเป็นทรัพย์สินไร้รูปร่าง แต่ด้วยคุณสมบัติเฉพาะที่โดดเด่นของเงินสกุลเข้ารหัส ที่สามารถทำธุรกรรมโดยตรงระหว่างผู้โอนและผู้รับโอนโดยไม่ผ่านการกำกับดูแลของตัวกลางหรือสถาบันการเงิน รวมถึงการรักษาความเป็นส่วนตัวของผู้ใช้งานโดยไม่จำเป็นต้องระบุตัวตน ดังจะเห็นได้จากรายงานผลการดำเนินงานครบรอบ 30 ปีของ Financial Action Task Force (FATF) ที่ให้ความสำคัญต่อนวัตกรรมที่มีผลกระทบต่อระบบการเงิน*โลก “โดยเฉพาะอย่างยิ่งเงินสกุลเข้ารหัส ซึ่งมีกลไกการดำเนินการที่สามารถปิดบังตัวตนผู้ใช้งาน ข้ามเขตประเทศแบบไร้พรมแดนด้วยความรวดเร็ว จึงเป็นมูลเหตุจูงใจที่สำคัญต่อผู้กระทำผิดหรืออาชญากรทางเศรษฐกิจให้ความสนใจในการนำไปใช้เป็นเครื่องมือในการทำธุรกรรมฟอกเงินที่ไม่ชอบด้วยกฎหมาย”* (FATF, 2019)

กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ก็มีขั้นตอนเช่นเดียวกับการฟอกเงินหรือทรัพย์สินที่มีรูปร่าง โดยขั้นตอนแรกผู้กระทำผิดได้รับผลประโยชน์จากธุรกรรมที่เกี่ยวกับการกระทำที่ไม่ชอบด้วยกฎหมายเป็นเงินสกุลเข้ารหัส หรือทำการแลกเปลี่ยนเป็นเงินสกุลเข้ารหัส ซึ่งเป็นขั้นตอนการนำเงินสกปรกเข้าสู่ระบบ (Placement Stage) ทั้งนี้เงินสกุลเข้ารหัสดังกล่าวอาจโอนมาจากผู้โอนที่ไม่ระบุตัวตน หรือระบุตัวตนของผู้ใช้งานที่สามารถตรวจพิสูจน์ได้จากฐานข้อมูลสาธารณะหรือไม่ก็ตาม ถือเป็นเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมาย (Tainted Cryptocurrency) (Jacquez, 2016) ทั้งนี้ด้วยระบบฐานข้อมูลสาธารณะของเงินสกุลเข้ารหัสนั้น บุคคลภายนอกสามารถสืบค้นติดตามเส้นทางธุรกรรมการโอนมูลค่าระหว่างผู้ใช้งานในระบบปฏิบัติการบล็อกเชนได้ รวมถึงระบบการพิสูจน์ยืนยันชุดข้อมูลที่ไม่อาจแก้ไขชุดข้มูล จึงไม่อาจเรียกระบบนิเวศเงินสกุลเข้ารหัสเป็นระบบที่สามารถปิดบังผู้ใช้งานอย่างแท้จริง (Anonymity) แต่ควรจะถือเป็นระบบกึ่งเปิดเผย (Pseudonymity) เนื่องจากยังสามารถสืบค้นเส้นทางการโอนมูลค่าได้

เงินสกุลเข้ารหัสของผู้กระทำผิดจึงอาจถูกสืบค้นถึงรหัสที่ตั้งของผู้ทำการโอน หรือรับโอนเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมาย และหากผู้กระทำผิดทำการโอนต่อไปยังบุคคลอื่นต่อไปก็จะถูกบันทึกรายการในระบบฐานข้อมูลสาธารณะ ซึ่งสามารถติดตามเส้นทางการทำธุรกรรมจากรหัสที่ตั้งประจำเครื่องมือสื่อสารของผู้ใช้งานได้อย่างต่อเนื่อง ดังนั้นขั้นตอนที่สอง ผู้กระทำผิดจะดำเนินการกลบเกลื่อนร่องรอย (Layering) โดยมีเป้าหมายที่จะไม่ให้ผู้ใดสามารถติดตามเชื่อมโยงเส้นทางธุรกรรมเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมายกับเงินสกุลเข้ารหัสที่ได้รับปลายทางได้ เช่น การโอนเงินสกุลเข้ารหัสจากกระเป๋าเงินอิเล็กทรอนิกส์ที่ไม่ระบุตัวตน พร้อมทั้งแลกเปลี่ยนกระจายเป็นเงินสกุลเข้ารหัสอื่นหลายสกุลเพื่อโอนไปเข้าหลายกระเป๋าเงิน และการทำการโอนซ้ำไปมาหลาย

รอบเนื่องจากสามารถดำเนินการได้อย่างรวดเร็ว และกระจายข้ามหลายประเทศ เพื่อให้เกิดความซับซ้อนยากต่อการติดตาม (Jacquez, 2016) หรือโดยการโอนเงินสกุลเข้ารหัสดังกล่าวผ่าน **ศูนย์บริการแปรสภาพเงินสกุลเข้ารหัส (Cryptocurrency Mixer or Tumbler)** ซึ่งให้บริการรับแลกเปลี่ยนเป็นเงินตราปกติและเงินสกุลเข้ารหัส เหมือนกับศูนย์บริการแลกเปลี่ยนเงินสกุลเข้ารหัส (Cryptocurrency Exchanger) ทั่วไป แต่มีการให้บริการเสริมโดยให้บริการโอนเงินสกุลเข้ารหัสจากทั้งผู้ใช้บริการทั่วไปและผู้กระทำผิด เพื่อทำการโอนส่งมอบต่อผู้รับโอนตามคำสั่งของผู้กระทำผิดโดยผู้รับโอนจะได้รับเงินสกุลเข้ารหัสที่ไม่สามารถสืบค้น หรือเชื่อมโยงเส้นทางรายการธุรกรรมกลับไปยังผู้โอน และเงินสกุลเข้ารหัสที่ได้รับสามารถระบุตัวตนของผู้โอนที่ชอบด้วยกฎหมาย และสามารถนำไปอ้างอิงต่อได้อย่างถูกต้อง (Jacquez, 2016; Samanta, Mohanta, Pati, & Jena, 2019)

จากนั้น ขั้นตอนสุดท้าย ผู้กระทำผิดก็สามารถนำเงินสกุลเข้ารหัสที่สามารถระบุแหล่งที่มาได้ชัดเจนไปผ่านกระบวนการใช้ประโยชน์จากมูลค่าดังกล่าว ได้ด้วยซื้อทรัพย์สินที่ชอบด้วยกฎหมายด้วยเงินสกุลเข้ารหัสโดยตรง หรือแลกเปลี่ยนเป็นเงินตราที่ชอบด้วยกฎหมายผ่านระบบเครือข่ายที่เชื่อมต่อกับระบบสถาบันการเงิน ซึ่งเรียกขั้นตอนนี้ว่า *“Cash Out Strategy”* (เช่นเดียวกับขั้นตอน Integration ของกระบวนการฟอกเงินปกติ) เช่น เครื่องเบิกถอนเงินอัตโนมัติด้วยเงินสกุลเข้ารหัส (ATM Cryptocurrency) หรือ ศูนย์บริการแลกเปลี่ยนเงินสกุลเข้ารหัส (Cryptocurrency Exchangers) ที่ให้บริการแลกเปลี่ยนเป็นเงินสกุลเข้ารหัสอื่น หรือเป็นทรัพย์สินอื่นเป็นต้น (Choo, 2015)

อาจกล่าวได้ว่า กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสมีรูปแบบการดำเนินงานในลักษณะที่คล้ายกับการฟอกเงินของทรัพย์สินมีรูปร่างทั่วไป แต่จะมีลักษณะซับซ้อนโดยการโอนย้ายมูลค่าผ่านเครือข่ายระบบปฏิบัติการบล็อกเชน ซึ่งมีความรวดเร็วกว่าการเคลื่อนย้ายเงินตราหรือทรัพย์สินอื่นที่จะมีความเสี่ยงต่อการตรวจพิสูจน์เส้นทางการเงินจากหน่วยงานรัฐ แม้ว่าระบบนิเวศเงินสกุลเข้ารหัสจะมีระบบฐานข้อมูลสาธารณะ ที่เปิดเผยให้บุคคลภายนอกสามารถเข้าถึงและตรวจสอบได้โดยง่าย แต่ด้วยระบบไม่มีข้อจำกัดการใช้งาน โดยผู้ใช้งานไม่จำเป็นต้องระบุตัวตน จึงทำให้การตรวจสอบย้อนกลับ เพื่อพิสูจน์ตัวตนผู้กระทำผิดในการถ่ายโอนเงินสกุลเข้ารหัสเป็นไปได้โดยยาก อย่างไรก็ตาม การฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสก็ยังมีข้อจำกัดในขั้นตอนสุดท้าย คือการแปรสภาพเป็นเงินตราปกติ ที่ยังมีข้อจำกัดทางกฎหมายในหลายประเทศซึ่งไม่ยอมรับสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส จึงอาจขาดสภาพคล่องในการแปรสภาพ แต่ก็อยู่ในสถานภาพที่สามารถปกปิดตัวตนของผู้ถือครองได้ ในขณะเดียวกันช่องว่างทางกฎหมายที่แตกต่างกันของแต่ละประเทศ อาจเป็นคุณต่อผู้กระทำผิดที่จะเคลื่อนย้ายเงินสกุลเข้ารหัสไปยังประเทศที่ยอมรับสถานภาพของเงินสกุลเข้ารหัส ทั้งนี้ หากเงินสกุลเข้ารหัสได้รับการยอมรับอย่างเป็นสากลมากขึ้น และสามารถ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ใช้ชำระราคาค่าซื้อขายสินค้าบริการได้โดยตรง ก็จะยิ่งเป็นประเด็นปัญหาต่อการตรวจสอบมากขึ้น เนื่องจากเป็นธุรกรรมที่ไม่ผ่านสถาบันตัวกลางซึ่งอยู่ในบังคับของกฎหมาย

2.2.3 ปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

เนื่องด้วยบริบทของสังคมโลกมีพัฒนาการสู่ระบบการเงินอิเล็กทรอนิกส์ และการค้าพาณิชย์อิเล็กทรอนิกส์มากขึ้น โดยเฉพาะอย่างยิ่งในระหว่างช่วงเวลาวิกฤตการระบาดของเชื้อไวรัสโควิด-19 ที่การค้าระบบปกติหลายธุรกรรมถูกระงับไม่ให้มีการติดต่อกันโดยตรง และคนทั่วไปได้เปลี่ยนพฤติกรรมเป็นการติดต่อบนระบบการสื่อสารแทน ส่งผลต่อบริบทของคนในสังคมที่เกิดการยอมรับระบบการค้าและการชำระเงินทางออนไลน์มากขึ้น เงินสกุลเข้ารหัสก็ถือเป็นส่วนหนึ่งของบริบททางสังคมโลกที่กำลังจะเปลี่ยนไป อีกทั้งคุณลักษณะเฉพาะและกลไกการดำเนินงานของเงินสกุลเข้ารหัส รวมถึงการเปลี่ยนแปลงบริบททางสังคมทำให้เกิดกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสโดยมีปัจจัยที่เอื้อประโยชน์ต่อการกระทำผิด ดังนี้ (HouBen & Snyers, 2018)

(1) **การปิดบังตัวตนผู้ใช้งาน (Anonymity)** เป็นคุณลักษณะเฉพาะที่สำคัญของเงินสกุลเข้ารหัส ทั้งนี้ผู้ใช้งานในระบบนิเวศสามารถใช้นามแฝงโดยไม่ต้องระบุข้อมูลส่วนบุคคล ดังนั้น จึงเป็นปัจจัยทางธรรมชาติของระบบงานที่ป้องกันการตรวจสอบ และการเข้าถึงตัวตนของผู้ใช้งาน (HouBen & Snyers, 2018)

(2) **การทำธุรกรรมได้แบบไร้พรมแดน (Cross-Border Nature)** เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสเป็นการดำเนินการบนระบบอินเตอร์เน็ต ซึ่งปัจจุบันมีโครงข่ายการติดต่อสื่อสารเชื่อมโยงถึงกันทั้งในประเทศและระหว่างประเทศ จึงสามารถทำธุรกรรมการโอนระหว่างกันข้ามเขตประเทศได้อย่างรวดเร็วและเสรี (HouBen & Snyers, 2018)

(3) **การไม่มีหน่วยงานตัวกลางในการกำกับ (No Central Intermediary)** เนื่องจากเป็นระบบการทำธุรกรรมโอนมูลค่าระหว่างผู้โอนและผู้รับโอนกันโดยตรง (Peer-to-Peer) โดยไม่มีกลไกของหน่วยงานตัวกลางใดกำกับดูแลระบบปฏิบัติการ แต่เป็นระบบบริการจัดการฐานข้อมูลแบบกระจายศูนย์ จึงสามารถดำเนินธุรกรรมได้ทันทีโดยไม่ต้องรอการตรวจสอบหรืออนุญาตใด (HouBen & Snyers, 2018)

(4) **ช่องว่างทางกฎหมายระหว่างประเทศ (International Legal Framework)** เงินสกุลเข้ารหัสถือเป็นนวัตกรรมเทคโนโลยีทางการเงินที่ส่งผลกระทบต่อระบบการเงินโลก ซึ่งแต่ละประเทศมีมาตรการภายในของแต่ละประเทศต่อเงินสกุลเข้ารหัสที่แตกต่างกัน ตั้งแต่ยอมรับสถานภาพทางกฎหมายจนไปถึงขั้นต้องห้ามเป็นสิ่งผิดกฎหมาย อีกทั้งยังขาดมาตรการสากลและนโยบายระหว่างประเทศต่อบริบทของเงินสกุลเข้ารหัส จึงถือเป็นโอกาสของผู้ใช้งานที่จะ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

อาศัยช่องว่างทางกฎหมายระหว่างประเทศ ในการถ่ายโอนเพื่อการแปรสภาพเป็นเงินตราในประเทศที่ยอมรับสถานภาพทางกฎหมาย และหลีกเลี่ยงประเทศที่มีกฎหมายบังคับที่เข็มแข็ง (HouBen & Snyers, 2018)

(5) **การปกป้องข้อมูลส่วนบุคคล (Data Protection and Privacy)** กลไกการโอนมูลค่าระหว่างผู้โอนตรงไปยังผู้รับโอน ระบบปฏิบัติการบล็อกเชนจะสร้างรหัสเปิดสาธารณะส่งไปยังผู้รับโอนเพื่อใช้ร่วมกับรหัสเปิดส่วนบุคคลในการเปิดกระเป๋าเงินปลายทาง จึงเป็นการปกป้องข้อมูลส่วนบุคคลโดยธรรมชาติของระบบปฏิบัติการโดยไม่มีกฎระเบียบจากหน่วยงานใดที่จะสามารถใช้อำนาจทางกฎหมายในการเข้าถึงข้อมูลรหัสเปิดส่วนบุคคลสำหรับเปิดกระเป๋าเงิน หรือบังคับใช้อำนาจอายัดเงินสกุลเข้ารหัส (HouBen & Snyers, 2018)

(6) **ต้นทุนการทำธุรกรรมต่ำ (Lower Transaction Cost)** ในกระบวนการฟอกเงินที่ต้องทำการยักย้ายถ่ายโอนเงินระหว่างกันผ่านสถาบันการเงินในขั้นตอนการกลบเกลื่อนร่องรอยจะดำเนินการกระจายรายย่อยเพื่อหลีกเลี่ยงการตรวจสอบ ก่อนจะรวบรวมกลับมาเป็นเงินที่ชอบด้วยกฎหมาย เมื่อเปรียบเทียบกับการโอนเงินสกุลเข้ารหัสสามารถกระจายรายการย่อย หรือทำการโอนกลับไปมาให้ผู้รับโอน (HouBen & Snyers, 2018) ในกลุ่มเครือข่ายได้ด้วยความรวดเร็ว ต้นทุนดำเนินการต่อรายการต่ำกว่ามาก จึงสามารถสร้างความซับซ้อนและก่อภาระการสืบค้นตรวจสอบให้เกิดความยากต่อการเข้าถึงรายการได้มีประสิทธิภาพมากกว่าและต้นทุนดำเนินการรวมต่ำกว่า (Breing et al., 2015)

2.2.4 การปกปิดตัวตนของผู้ใช้งานเงินสกุลเข้ารหัสด้วยระบบปฏิบัติการเฉพาะ

แม้ว่าระบบนิเวศเงินสกุลเข้ารหัสจะเปิดให้ผู้ใช้งานไม่ต้องยืนยันตัวตน แต่ผู้กระทำผิดส่วนหนึ่งที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน อาจเลือกใช้ระบบปฏิบัติการเฉพาะเพื่อปิดบังตัวตนเพิ่มขึ้นอีกชั้นหนึ่ง เนื่องด้วยระบบปฏิบัติการที่กล่าวถึงนี้สามารถป้องกันการสืบค้นจากเครื่องมือตรวจสอบของหน่วยงานรัฐ หรือที่เรียกระบบปฏิบัติการนี้ว่า **The Onion Router (TOR)** ซึ่งเป็นระบบที่พัฒนาขึ้นโดย The U.S. Naval Research Laboratory เพื่อการใช้งานกับเว็บไซต์อาชญกรรมทางเศรษฐกิจ การค้ายาเสพติด และสิ่งผิดกฎหมายที่เรียกว่า Deep Web แต่ปัจจุบันมีผู้ใช้งานหลายกลุ่มที่เลือกใช้งานเครือข่ายระบบปฏิบัติการนี้ เช่น กลุ่มต่อสู้ทางการเมือง บรรณาธิการนักเขียนที่เผยแพร่บทความผิดกฎหมายในระบบปฏิบัติการนี้ เพื่อป้องกันการสืบค้นติดตามจากรัฐบาล รวมถึงอาชญากรและกลุ่มก่อการร้ายที่นิยมใช้ช่องทางระบบปฏิบัติการนี้มากขึ้น ทั้งนี้ผู้ใช้งานในระบบปฏิบัติการนี้จะได้รับการป้องกันการเข้าถึงข้อมูลใช้งานส่วนบุคคล หรือการตรวจสอบสืบค้นรหัสที่ตั้งของผู้ใช้งาน โดยเมื่อผู้ใช้งานเข้าสู่ระบบปฏิบัติการ ระบบจะทำการบริหาร

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

จัดเลือกเส้นทางการติดต่อสื่อสารกับรหัสที่ตั้งหลากหลายจุดในระบบเครือข่ายด้วยวิธีการสุ่มแทนการติดต่อสื่อสารบนรหัสที่ตั้งคงที่ ดังนั้นในขณะใช้งานระบบจะหมุนเวียนรหัสที่ตั้งไปเรื่อยอย่างต่อเนื่อง ทำให้หน่วยงานที่ทำการตรวจสอบเมื่อพบการติดต่อรหัสที่ตั้งแห่งหนึ่ง แต่ในช่วงเวลาถัดไปรหัสที่ตั้งจะเคลื่อนไปยังจุดอื่น นอกจากนี้รหัสที่ตั้งนั้นก็เป็นรหัสที่ตั้งลวงซึ่งระบบสร้างขึ้น พร้อมสร้างเส้นทางการเคลื่อนรหัสที่ตั้งลวงโดยไม่มีผู้ใดทราบข้อมูลที่ชัดเจน และเมื่อเสร็จสิ้นการใช้งานรหัสที่ตั้งจะเคลื่อนกลับไปยังรหัสที่ตั้งตั้งต้น ทำให้หน่วยงานตรวจสอบไม่สามารถสืบค้นประวัติการใช้งานเว็บไซต์ของผู้ใช้งานได้ (Homeland Security Enterprise, 2014) ทั้งนี้นอกจากระบบปฏิบัติการ TOR แล้วยังมีระบบปฏิบัติการอื่นที่มีคุณสมบัติปกปิดผู้ใช้งาน หรืออนุญาตให้ใช้งานได้เฉพาะกลุ่มสมาชิกที่ได้รับอนุญาต เช่น Invisible Internet Project (I2P) หรือ Freenet เป็นต้น (Braga & Luna, 2018)

นอกจากระบบปฏิบัติการที่กล่าวข้างต้นแล้ว ยังมีการใช้ระบบการติดต่อสื่อสารบนเว็บไซต์ที่ไม่สามารถค้นหาด้วยเครื่องมือค้นหาแบบปกติทั่วไป เช่น Google หรือ Bring ได้ แต่ต้องใช้เครื่องมือค้นหาเฉพาะ เช่น Clusty หรือ DuckDuckGo เป็นต้น แม้ว่าเว็บไซต์ดังกล่าวจะอยู่ในระบบฐานข้อมูล World Wide Web เช่นเดียวกัน แต่จะถูกจำกัดการให้ใช้งานเฉพาะสมาชิกที่ได้รับอนุญาตเท่านั้น ซึ่งจะต้องใช้รหัสอนุญาตเข้าระบบ โดยเป็นระบบเครือข่ายที่ไม่สามารถเข้าถึงตัวตนของผู้จัดการเวบไซด์ได้ นอกจากนี้รหัสที่ตั้งเว็บไซต์ยังเป็นรหัสที่ตั้งลวงซึ่งระบบสร้างขึ้น เพื่อปกปิดตัวตนและการใช้งานของเว็บไซต์ ที่เรียกว่า ***"Deep Web"*** ในระยะต่อมาอาชญากรเศรษฐกิจได้พัฒนาระบบการค้ายาเสพติด หรือสิ่งผิดกฎหมายผ่านระบบ Deep Web จนเรียกกันต่อไปว่า ***"Dark Web"*** เช่น Silk Road2.0, Pandora และ Agora เป็นต้น ดังนั้นเงินสกุลเข้ารหัสจึงถูกใช้เป็นสื่อกลางในการค้าธุรกิจผิดกฎหมาย หรืออาชญากรรมอื่น รวมถึงการฟอกเงินบน Dark Web (Homeland Security Enterprise, 2014) นอกจากนี้อาชญากรผู้ใช้งานบน Dark Web อาจใช้โปรแกรมที่มีระบบป้องกันการตรวจสอบข้อความสื่อสาร เพื่อทำการติดต่อกับคู่ค้าในธุรกิจค้าสิ่งผิดกฎหมาย โดยโปรแกรม Telegram หรือ WhatsApp เป็นต้น ซึ่งโปรแกรมดังกล่าวมีกระบวนการแปลงข้อความสื่อสารที่ส่งออกจากผู้ใช้งานต้นทางเป็นรหัสข้อมูลเฉพาะและรหัสข้อมูลเฉพาะดังกล่าวจะถูกถอดรหัสกลับเป็นข้อความสื่อสารเมื่อผู้รับปลายทางเปิดขึ้นด้วยรหัสเปิดที่ถูกต้องเท่านั้น เพื่อป้องกันการเจาะระบบสืบค้นข้อความสื่อสารระหว่างทาง (Hack) จึงเป็นระบบปฏิบัติการทางเลือกอีกระบบหนึ่งในการปกปิดตัวตนและป้องกันการตรวจสืบค้นข้อความที่สื่อสารระหว่างกัน (Chainalysis, 2019)

2.2.5 การกลบเกลื่อนร่องรอยเส้นทางธุรกรรมการโอนเงินสกุลเข้ารหัส

ดังที่กล่าวข้างต้น ระบบนิเวศเงินสกุลเข้ารหัสเป็นระบบฐานข้อมูลสาธารณะ แม้ว่าผู้ใช้งานจะสามารถปิดบังตัวตนได้ แต่ระบบก็ยังจะสามารถเชื่อมโยงเส้นทางการทำธุรกรรมระหว่างผู้ใช้งานได้ ดังนั้นผู้กระทำผิดจึงมีความต้องการที่จะหาวิธีการกลบเกลื่อนร่องรอยระหว่างเส้นทาง

เชื่อมโยงการโอนเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมายไปยังกระเป๋าเงินปลายทางของผู้กระทำผิดที่ไม่สามารถพิสูจน์ย้อนกลับถึงต้นทางได้ (Crawford, 2019) ทั้งนี้ผู้กระทำผิดที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงินผ่านระบบนิเวศมีวิธีดำเนินการ ดังนี้

(1) การดำเนินการผ่านศูนย์บริการแปรสภาพเงินสกุลเข้ารหัส **(Cryptocurrency Mixer or Tumbler)** โดยกลไลการดำเนินการเริ่มจากผู้กระทำผิดโอนเงินสกุลเข้ารหัสเข้ากระเป๋าเงินตามรหัสที่ตั้งซึ่งศูนย์บริการกำหนด จากนั้นระบบงานของศูนย์บริการจะสร้างแผนชุดคำสั่งโอนภายในระบบโครงข่ายตามระยะเวลาโอนที่ตกลงกัน พร้อมทั้งเตรียมกระเป๋าเงินรับโอนปลายทางจำนวนมากรองรับการโอนต่อไปยังรหัสที่ตั้งปลายทางเหล่านั้น รวมถึงอาจทำการโอนไข้วไปมาระหว่างกระเป๋าเงินดังกล่าวในระบบโครงข่าย เพื่อสร้างความซับซ้อนในการสืบค้นเส้นทางธุรกรรม แต่เมื่อเสร็จสิ้นกระบวนการ ผู้กระทำผิดจะได้รับเงินสกุลเข้ารหัสสุทธิหลังจากหักค่าบริการเข้าประเป๋าเงินของตนภายในช่วงเวลาที่ตกลงกัน พร้อมทั้งแผนผังแสดงการโอนในระบบโครงข่ายจากรหัสที่ตั้งต้นทางไปยังจุดต่างๆจนถึงรหัสที่ตั้งปลายทางให้ผู้ใช้บริการทราบ ก่อนจะถูกลบหลักฐานชุดคำสั่งเส้นทางธุรกรรมดังกล่าวโดยอัตโนมัติภายในระยะเวลาที่กำหนด นอกจากนี้ศูนย์บริการยังมีกลยุทธการสร้างความซับซ้อนเพิ่มเติมเพื่อป้องกันการสืบติดตามธุรกรรมการโอน โดยศูนย์บริการจะกำหนดอัตราค่าบริการเป็นช่วง และใช้ระบบทำการสุ่มอัตราค่าบริการในการเรียกเก็บแต่ละรายการไม่เท่ากัน เพื่อป้องกันการประเมินเงินสกุลเข้ารหัสสุทธิที่พึงได้รับในการทำธุรกรรม หรือศูนย์บริการอาจทำการโอนเงินสกุลเข้ารหัสหลายรายการ จากผู้โอนหลายรายเข้าสู่กระเป๋าเงินผู้รับปลายทางจนได้ครบตามจำนวนที่ตกลงกัน หรือศูนย์บริการอาจใช้วิธีการขยายช่วงระยะเวลาดำเนินการโดยระบบจะทำการสุ่มช่วงเวลาดำเนินการ และทยอยทำการโอนตามที่ระบบกำหนดให้แก่ผู้รับปลายทางจนครบตามจำนวนที่ตกลงกัน ดังนั้น ยิ่งระยะเวลาห่างกันมากเท่าไรก็จะยิ่งหาความสัมพันธ์ระหว่างรหัสที่ตั้งต้นทางกับรหัสที่ตั้งปลายทางยากมากยิ่งขึ้นเท่านั้น ซึ่งปกติจะกำหนดไว้ประมาณ 24 ชั่วโมง หรืออาจขยายระยะเวลาเป็น 2-3 วัน หรือถึงสัปดาห์ ขึ้นอยู่กับปริมาณเงินสกุลเข้ารหัสและสถานการณ์ (Crawford, 2019) เช่น Classical Mixer กำหนดค่าบริการอัตราประมาณร้อยละ 1 บวก 0.001 BTC ระยะเวลาดำเนินการ 10 นาที ถึง 1 ชั่วโมงสำหรับรายการขนาด 0.015 BTC ถึง 50 BTC หรือ Mixer& Exchange กำหนดค่าบริการประมาณร้อยละ 3 บวก 0.0015 BTC ระยะเวลาดำเนินการ 1 ถึง 3 ชั่วโมง หรือ Complete Anonymity กำหนดค่าบริการประมาณร้อยละ 5 บวก 0.0015 BTC ระยะเวลาดำเนินการ 2 ถึง 5 ชั่วโมง เป็นต้น (Goriacheva, Jakubenko, Pogodina, & Silnov, 2018)

(2) การดำเนินการผ่านระบบปฏิบัติการแบ่งปันธุรกรรมจากกลุ่มผู้ใช้งานหลายราย **(Multi-party Transactions)** วิธีการนี้ไม่มีวัตถุประสงค์เพื่อกลบเกลื่อนร่องรอยเชิงความสัมพันธ์ระหว่างผู้โอนต้นทางกับผู้รับโอนปลายทาง แต่มีหลักการของระบบปฏิบัติงานด้วยการรวบรวมคำสั่งโอนจากผู้ใช้งานทั้งหลายที่เข้าสู่ระบบงาน จากนั้นระบบจะดำเนินการเลือกและจัดชุดคำสั่งโดยอัตโนมัติเพื่อทำธุรกรรมให้แก่รายการที่มีมูลค่าโอนใกล้เคียงกัน หรือรวบชุดคำสั่งเพื่อให้ได้มูลค่าโอนที่ใกล้เคียงกันซึ่งจะแสดงรายงานธุรกรรมในระบบฐานข้อมูลสาธารณะ ทั้งนี้ผู้รับโอนจะทำธุรกรรมการโอนกับผู้ใช้งานรายอื่นที่มีมูลค่าโอนใกล้เคียงกันแต่ไม่มีความสัมพันธ์ต่อกัน โดยระบบจะแสดงแผนผังโครงข่ายการโอนให้ผู้ทำคำสั่งรับรู้ก่อนที่ข้อมูลจะถูกลบโดยอัตโนมัติ ซึ่งเรียกระบบปฏิบัติการนี้ว่า CoinJoin ซึ่งถูกพัฒนาระบบขึ้นโดย Gregory Maxwell (Goriacheva et al., 2018) อย่างไรก็ตามความเป็นไปได้ในการจัดชุดคำสั่งให้ได้มูลค่าที่เท่ากันเป็นเรื่องยากในทางปฏิบัติ ดังนั้นผู้รับโอนอาจมีโอกาสได้รับมูลค่าน้อยกว่าจำนวนมูลค่าที่สั่งโอน จึงอาจเป็นเหตุแอบแฝงของการฉ้อโกงในระบบปฏิบัติการ อีกประการหนึ่งผู้เข้าสู่ระบบปฏิบัติการอาจส่งคำสั่งมาจากผู้ใช้งานที่กระทำความผิดหรือมาจากระบบงานที่ปกปิดแหล่งที่มาของได้มา อันเป็นการสร้างภาระและความเสี่ยงจากการตรวจสอบแก่ผู้รับโอน ซึ่งอาจถูกจับคู่ทำธุรกรรมโอนเงินสกุลเข้ารหัสจากผู้โอนที่มีลักษณะข้างต้น (Crawford, 2019) ดังนั้นนักพัฒนาระบบปฏิบัติการได้นำเสนอระบบปฏิบัติที่แก้ไขข้อด้อยข้างต้นของ CoinJoin ซึ่งเรียกระบบปฏิบัติการนี้ว่า CoinShuffle โดยกลุ่มผู้ใช้งานจะเข้าสู่ระบบเพื่อแจ้งรหัสที่ตั้งกระเป๋าเงินของตนให้ผู้ใช้งานทุกคนในระบบทราบ แต่ระบบจะสงวนข้อมูลรหัสกระเป๋าเงินปลายทางและมูลค่าของรายการ จากนั้นระบบจะดำเนินการจัดชุดคำสั่งพร้อมแจ้งรหัสเปิดสาธารณะให้ผู้ทำธุรกรรมในชุดคำสั่งทราบ พร้อมสร้างรหัสลับสำหรับเปิดกระเป๋าเงินให้แก่กลุ่มผู้ใช้งานในโครงข่ายเพื่อให้ผู้ใช้งานในโครงข่ายทำการถอดรหัสและยืนยันรายการ ผู้รับโอนจึงจะสามารถรับมูลค่าโอนได้ในขณะเดียวกันผู้ใช้งานที่ร่วมยืนยันรายการ ก็จะเป็นผู้พิสูจน์ยืนยันรายการในระบบปฏิบัติบล็อกเชนไปพร้อมกัน แต่ระบบปฏิบัติการยังมีข้อสงสัยของผู้ใช้งานร่วมอย่างมาก เนื่องจากไม่อาจรับรู้ได้ถึงผู้ใช้งานร่วมในกลุ่มมีแหล่งที่มาหรือถูกจัดการโดยกลุ่มบุคคลใดเป็นหลักหรือไม่ จนอาจก่อให้เกิดความเสี่ยงต่อการฉ้อโกงเงินสกุลเข้ารหัสจากระบบปฏิบัติการ (Goriacheva et al., 2018)

(3) การดำเนินการผ่านผู้ได้รับเงินสกุลเข้ารหัสโดยตรง **(Non-Tainting Mixers)** ด้วยข้อกังวลของผู้กระทำผิดที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน คือ การสืบสวนติดตามเส้นทางธุรกรรมการได้ชัดเจน โดยวิธีการนี้เป็นการติดต่อรับโอนมูลค่าจากกลุ่มผู้ถือครองเงินสกุลเข้ารหัสซึ่งได้รับเป็นค่าตอบแทนจากการพิสูจน์ยืนยันรายการ หรือที่เรียกว่าค่าขุดซึ่งนักขุดได้รับ เนื่องจากค่าขุดเป็นเงินสกุลเข้ารหัสที่ถูกสร้างขึ้นโดยตรงจากระบบนิเวศจึงไม่แสดง

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ความสัมพันธ์ใด จากนั้นผู้ทำรายการจะโอนเงินสกุลเข้ารหัสจากกระเป๋าเงินที่รับค่าขุดให้แก่ผู้รับโอนตามที่ตกลงกัน หรือนักขุดรับโอนเงินสกุลเข้ารหัสจากผู้โอนล่วงหน้า โดยส่งมอบรหัสเปิดส่วนบุคคลของกระเป๋าเงินที่รับค่าขุดของตนให้แก่ผู้โอน ซึ่งจะช่วยกลบเกลื่อนจำนวนมูลค่าโอนที่จะไม่ตรงกันเนื่องจากต้องใช้ระยะเวลาในการได้รับค่าขุดเพิ่มเติม อย่างไรก็ตามวิธีการนี้มีข้อจำกัดค่อนข้างมากเนื่องจากค่าขุดมีจำนวนจำกัด และการค้นหานักขุดที่จะร่วมทำรายการมีจำนวนจำกัดในระบบนิเวศเงินสกุลเข้ารหัส วิธีการนี้จึงไม่ค่อยได้รับความนิยมในการทำธุรกรรม (Goriacheva et al., 2018)

2.3 ทฤษฎีทางสังคมวิทยาที่เกี่ยวข้อง

2.3.1 กระบวนทัศน์การเคลื่อนย้าย (Mobility Paradigm)

Mini Sheller and Urry (2006) ได้นำเสนอผลศึกษาการเคลื่อนย้ายของผู้คนทั่วโลกในช่วงหลายทศวรรษที่ผ่านมา พบว่าในปี 1950 มีผู้เดินทางระหว่างประเทศประมาณ 25 ล้านคนต่อปี ซึ่งได้เพิ่มขึ้นเป็น 700 ล้านคนต่อปีในช่วงปี 2000 ด้วยวัตถุประสงค์การเดินทาง เช่น การศึกษาต่างประเทศ ท่องเที่ยว ธุรกิจ แข่งขันกีฬา อพยพลี้ภัย พักผ่อนหลังเกษียณ ก่อการร้าย หรือการทหาร พร้อมทั้งได้คาดหมายว่าในปี 2010 จะมีผู้เดินทางทั่วโลกสูงถึง 1,000 ล้านคนต่อปี ประกอบด้วยผู้โดยสารทางอากาศ 4 ล้านคนต่อวัน และผู้ลี้ภัยที่ต้องอพยพพลัดถิ่นอีก 31 ล้านคนต่อปี โดยได้นำเสนอความสัมพันธ์ระหว่างเทคโนโลยีการเดินทาง กับอิทธิพลต่อกระบวนการทางสังคม เริ่มต้นจากเทคโนโลยีการเดินโดยทางรถยนต์ที่ทำให้เกิดการเชื่อมโยงระหว่างชนบทกับเมือง ที่ไม่ได้มีผลกระทบเฉพาะการลดช่องว่างระหว่างพื้นที่ความเป็นเมืองกับความเป็นชนบท แต่ได้สร้างโอกาสเกิดขึ้นใหม่ตามมาเป็นเครือข่ายทางสังคม ส่งทอดรสนิยมทันสมัย ส่วนเทคโนโลยีการเดินโดยทางอากาศที่ขยายความเชื่อมโยงประเทศต่อประเทศ ก็ยิ่งช่วย**ลดช่องว่างระหว่างพื้นที่และเวลา** สร้างศักยภาพการติดต่อข้ามประเทศแบบ**ไร้พรมแดน (Globalization)** ทั้งด้านการค้า การท่องเที่ยว และวัฒนธรรม ดังนั้นคนเอเชียจึงได้ลิ้มรสอาหารสดจากยุโรปอย่างสะดวกสบาย นอกจากนี้เทคโนโลยีการสื่อสารได้สร้างจุดเปลี่ยนสำคัญ ที่ทำให้ผู้คนทั่วไปสามารถติดต่อถ่ายทอดพฤติกรรมสังคมได้แบบไร้ข้อจำกัดทั้งด้านเวลาและสถานที่ โดยระบบเครือข่ายอินเตอร์เน็ตบนโลกไซเบอร์ทำให้เกิดปฏิสัมพันธ์เชื่อมโยงผู้คนทั่วโลกเข้าใกล้กันเสมือนอยู่ในพื้นที่เดียวกัน และ ณ เวลาเดียวกัน เช่น การชมการถ่ายทอดสดกีฬาจากต่างประเทศ และโดยเฉพาะอย่างยิ่งพัฒนาการเทคโนโลยีคอมพิวเตอร์ รวมถึงโทรศัพท์เคลื่อนที่ได้สร้างสังคมเสมือนบนเครื่องมือสื่อสาร ทำให้เกิดการเปลี่ยนแปลงทางสังคมในมิติใหม่เป็น **พลเมืองโลก (Cosmopolitan)** และเมื่อความเป็นพลเมืองไม่จำกัดเฉพาะคนเชื้อชาติเดียวกัน หรืออยู่ในอาณาเขตประเทศเดียวกัน แต่ด้วยปฏิสัมพันธ์ต่อบุคคลที่เปิดกว้างผ่านการเรียนรู้ระหว่างกันบนระบบเครือข่ายอินเตอร์เน็ต ทำให้เกิด**กระบวนการสร้างสังคมบนโลกเสมือน**เป็นชุมชนหลากหลาย เช่น ชุมชนผู้ชื่นชอบกีฬาฟุตบอล เป็นต้น (Mini Sheller & Urry, 2006)

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

กระบวนทัศน์การเคลื่อนย้ายด้วยความคล่องตัวก่อให้เกิดอิทธิพลต่อเศรษฐกิจ และการเมืองระหว่างประเทศรวมถึงการพัฒนาชนบทกับการสร้างความเป็นเมือง เนื่องจากการเคลื่อนย้ายอย่างเสรีและรวดเร็วยิ่งตอกย้ำถึงความเหลื่อมล้ำเชิงซ้อนในหลายมิติ ทั้งการใช้ทรัพยากร แรงงาน วัฒนธรรม ท่องเที่ยว และการกระจายสินค้าอุปโภคบริโภค (Mimi Sheller, 2017) ดังนั้น หลายประเทศจึงได้รวมกลุ่มกันจัดทำข้อตกลงเขตการค้าเสรีเพื่อสร้างสมดุลลดความเหลื่อมล้ำระหว่างประเทศในกลุ่มที่ทำความตกลง ยิ่งไปกว่านั้นกลุ่มประเทศผู้ผลิตน้ำมันซึ่งเคยเป็นผู้ทรงอิทธิพลด้านพลังงานของโลกในหลายทศวรรษที่ผ่านมา ซึ่งได้รับอนิสงค์จากวิวัฒนาการเทคโนโลยี่การเดินทางทั้งโดยทางรถยนต์และทางอากาศที่ต้องใช้น้ำมันเป็นเชื้อเพลิงในการขับเคลื่อน ก็ได้รับผลกระทบจากเทคโนโลยี่การสื่อสารที่สร้างบริบททางสังคมใหม่ ซึ่งผู้คนทั่วไปเคลื่อนย้ายตนเองหรือรวมกลุ่มทางสังคมผ่านโลกเสมือนที่ไร้ข้อจำกัดด้านเวลาและสถานที่ ทั้งนี้ สื่อสังคมออนไลน์ (Social Network) ทำให้เกิดสภาวะเสมือนการเคลื่อนย้ายโดยไม่เกิดการเคลื่อนย้ายทางกายภาพ (Mimi Sheller, 2017) ดังนั้น ความจำเป็นของการเดินทางจึงลดลงส่งผลให้ความมั่งคั่งของประเทศดังกล่าวลดลงเช่นกัน ตัวอย่างเช่น พฤติกรรมการท่องเที่ยวผ่านเว็บไซต์ที่ได้รับอรรถรสทางธรรมชาติผ่านจอคอมพิวเตอร์ การประชุมทางไกลผ่านระบบวิดิทัศน์ ทั้งนี้ บทพิสูจน์เชิงประจักษ์สำคัญในช่วงปี 2020 - 2021 เมื่อเกิดวิกฤติการแพร่ระบาดของเชื้อโควิด-19 ระบาดทั่วโลกอย่างรวดเร็ว สาเหตุเริ่มต้นในเดือนธันวาคม 2019 จากผู้ติดเชื้อโคโรน่าไวรัสสายพันธุ์ใหม่ (ซึ่งต่อมาเรียกว่า *“เชื้อไวรัสโควิด-19”*) จำนวนไม่ถึง 10 รายในประเทศจีน แต่บริบทการเคลื่อนย้ายของผู้คนทั่วโลกส่งผลให้เกิดการแพร่ระบาดอย่างต่อเนื่องไปทั่วโลก จนถึงเดือนมีนาคม 2021 มีผู้ติดเชื้อสะสมจำนวนเกินกว่า 128 ล้านคนจากประชากรผู้ติดเชื้อเกือบ 200 ประเทศทั่วโลก ในขณะเดียวกันรัฐบาลหลายประเทศได้กำหนดนโยบายป้องกันการแพร่ระบาดด้วย *“การปิดประเทศ”* มีคำสั่งห้ามการเดินทางระหว่างประเทศในทุกช่องทาง และในบางช่วงเวลายังถึงขั้นสั่งห้ามการเดินทางออกนอกเคหะสถาน และด้วยบทบาทของกระบวนทัศน์การเคลื่อนย้ายในอีกประการหนึ่ง ได้แสดงให้เห็นถึงปฏิสัมพันธ์ทางสังคมออนไลน์ทำให้กิจกรรมทางเศรษฐกิจและชีวิตประจำวันของผู้คนทั่วไปสามารถดำรงอยู่ได้ เช่น การเรียนหรือการทำงานที่บ้านผ่านระบบออนไลน์ (Study/Work From Home) การประชุมธุรกิจหรือการเมืองด้วยระบบวิดิทัศน์ทางไกลข้ามประเทศ รวมถึงภายในประเทศ

ดังนั้น อิทธิพลของเทคโนโลยี่การสื่อสารจึงส่งผลต่อการดำรงชีวิตประจำวันของคนในสังคมปัจจุบัน และ**ปัจจัยชี้นำเศรษฐกิจและสังคมของโลกได้ปรับเปลี่ยนจากอิทธิพลชี้นำด้านพลังงาน มาเป็นปัจจัยการเคลื่อนย้ายเงินทุนระหว่างประเทศ** ระบบการเงินที่สร้างการหมุนเวียนและกระจายการลงทุนไปทั่วโลกได้อย่างรวดเร็วผ่านระบบปฏิบัติการออนไลน์ สร้างธุรกรรมการค้าได้หลายล้านเหรียญสหรัฐภายในเพียงวินาทีเดียว จึงเป็นปัจจัยที่ทรงอิทธิพลต่อกระบวนการทางสังคมที่กว้างและไกล (Mimi Sheller, 2017)

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

เมื่อนำกระบวนทัศน์การเคลื่อนย้าย (Mobility Paradigm) มาศึกษาเปรียบเทียบกับการนำเงินสกุลเข้ารหัสมาใช้เป็นเครื่องมือในการทำธุรกรรมฟอกเงิน จะเห็นได้ว่าระบบนิเวศเงินสกุลเข้ารหัสที่มีกลไกทำงานบนระบบปฏิบัติการบล็อกเชน ซึ่งเชื่อมโยงผ่านระบบอินเตอร์เน็ตที่ผู้ใช้งานทั่วไปทุกเขตประเทศสามารถเข้าร่วมใช้ระบบงานได้อย่างเสรี การทำธุรกรรมโอนมูลค่าระหว่างบุคคลกันโดยตรงด้วยความรวดเร็วและไม่มีการกำกับจากหน่วยงานใด เป็นปรากฏการณ์ทางสังคมที่สอดคล้องกับปัจจัยที่มีอิทธิพลต่อกระบวนการทางสังคม ซึ่งสามารถเคลื่อนย้ายเงินทุนขององค์กรหรือเงินทุนระดับปัจเจกบุคคลระหว่างกันอย่างรวดเร็วและเสรี เนื่องจากกลุ่มผู้ใช้งานรวมถึงนักขุดซึ่งให้ความเชื่อมั่น และยอมรับกลไกการทำงานบนระบบนิเวศที่เชื่อมโยงผู้ใช้งานได้ทุกประเทศทั่วโลกแบบไร้พรมแดน (Globalization) กลุ่มผู้ใช้งานจึงมีลักษณะทางสังคมเข้าข่ายเป็นพลเมืองโลก (Cosmopolitan) ในลักษณะหนึ่งซึ่งเป็นการเปิดทัศนะกว้างที่มีจุดร่วมยอมรับระบบปฏิบัติการเดียวกันแม้ว่าบุคคลดังกล่าวจะอยู่ต่างถิ่น ต่างแดน และต่างสังคม โดยเฉพาะอย่างยิ่งเครือข่ายอาชญากรซึ่งเป็นผู้ใช้งานที่ได้นำเงินจากการกระทำผิดมาดำเนินการผ่านกระบวนฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

2.3.2 ทฤษฎีความซับซ้อน (Complexity Theory)

ระยะเวลาหลายทศวรรษที่ผ่านมา นักปราชญ์หลายท่านได้พัฒนากรอบแนวคิดระเบียบทางสังคมตั้งแต่แนวคิดระบบชนชั้นทางสังคมในช่วงปี 1970 และในช่วงปี 1980 แนวคิดด้านภาษาศาตร์และหลังสมัยใหม่ จนถึงแนวคิดโลกาภิวัตรในช่วงปี 1990 เพื่ออธิบายปรากฏการณ์ระเบียบทางสังคมทั้งด้านวิทยาศาสตร์ สุขภาพ สิ่งแวดล้อม และเศรษฐกิจ บนพื้นฐานการวิเคราะห์พฤติกรรมแบบแยกส่วน (Reductionism) แต่กรอบแนวคิดความซับซ้อนนำเสนอแนวคิดการวิเคราะห์ศึกษาองค์ประกอบย่อย (Nanoscales) แต่ละองค์ประกอบที่มีวิวัฒนาการของการบังเกิดใหม่ตลอดเวลา (Emergent) และมีคุณสมบัติทางกายภาพที่แตกต่างกัน ผ่านกระบวนการจัดระเบียบเข้ามารวมตัวกัน (Self-assembly) เป็นโครงสร้างความซับซ้อนของเครือข่ายองค์ประกอบย่อยรวมกันกลายสภาพเป็นโมเลกุล (Molecules) ซึ่งเป็นพื้นฐานในการสร้างนวัตกรรมสินค้า และอุตสาหกรรม (Urry, 2005) หรือกล่าวอีกนัยหนึ่งว่า *“กรอบแนวคิดความซับซ้อนจะให้ความสนใจทั้งบริบทของป่าไม้และลักษณะเฉพาะของต้นไม้แต่ละต้นที่ก่อให้เกิดความเป็นป่าไม้”* ดังนั้น **ทฤษฎีความซับซ้อน จึงให้ความสำคัญกับความหลากหลายของสาเหตุและผลลัพธ์ที่เกี่ยวข้องในกระบวนการในลักษณะไม่จำกัดเฉพาะเส้นทางสู่เป้าหมายเพียงทางเดียว** จนเกิดเป็นปฏิกริยาลูกโซ่ที่ก่อให้เกิดการเปลี่ยนแปลงเชิงซ้อนในลักษณะที่ไม่ใช่ความสัมพันธ์เชิงเส้นตรง (non-linear) (Zareian, 2019)

“ความซับซ้อน” **จึงเป็นแนวคิดการจัดระเบียบทางสังคมที่รวมความคิดเชิงระบบเข้ากับความคิดเชิงกระบวนการ** ซึ่งเปิดกว้างทางความคิด ความหลากหลายของปัจจัยใน

อนาคต ผลลัพทธ์ที่ไม่อาจคาดหมายได้ในกรอบของเวลาและสถานที่ จึงก่อเกิดความสัมพันธ์เชิงซ้อนที่มีผลต่อการเปลี่ยนแปลงสรรพสิ่งทั้งหลายในธรรมชาติอย่างต่อเนื่อง อีกทั้งยังขยายตัวส่งผลต่อคนและสิ่งแวดล้อมได้ในระยะไกล โดยตามแนวคิดไร้ระเบียบ (Chaos) ซึ่งได้อธิบายปรากฏการณ์ที่เกิดขึ้นจากต้นเหตุย่อย แต่เมื่อเงื่อนไขสภาวะแวดล้อมที่เหมาะสมก็อาจสามารถก่อให้เกิดการเปลี่ยนแปลงขนานใหญ่ได้ (Urry, 2005)

ด้วยความสัมพันธ์ทางสังคมในปัจจุบัน มีประเด็นที่เกี่ยวข้องกับความเหลื่อมล้ำทางสังคมในหลายมิติ ไม่ว่าจะเป็นเพศสภาพ ชนชั้นทางเศรษฐกิจ ชุมชนเชื้อชาติ ดังนั้น การศึกษาระเบียบทางสังคมโดยการแยกส่วนศึกษาปัญหาเฉพาะประเด็น ย่อมเป็นการยากที่จะทำความเข้าใจปรากฏการณ์ทางสังคมทั้งระบบ หากแต่ควรศึกษาความสัมพันธ์ของสรรพสิ่งทั้งหลายไปพร้อมกัน เช่น เพศสภาพที่จะเกี่ยวพันกับสถาบันทางเศรษฐกิจ การเมือง ความรุนแรง ชนชั้นทางสังคม และความสัมพันธ์ระหว่างประเทศ ซึ่งแต่ละชุดปรากฏการณ์ย่อยที่บังเกิดขึ้นก็อาจเป็นสาเหตุต่อความสัมพันธ์กับชุดปรากฏการณ์อื่นต่อเนื่องเป็นเชิงซ้อนจนแสดงผลลัพธ์ขยายเป็นวงกว้าง ดังนั้น การศึกษาจึงไม่ควรจำกัดตีกรอบสังคมเฉพาะระบบใดระบบหนึ่ง หากแต่การศึกษาสังคมควรจะสังเคราะห์กรอบแนวคิดเป็นกระบวนการสร้างความเป็นสังคม (Societalization) โดยการปรับโครงสร้างที่จะสร้างความเปลี่ยนแปลงใหม่ จากปัจจัยแวดล้อมที่เกิดขึ้นด้วยเหตุแห่งความเหลื่อมล้ำเชิงซ้อน (Walby, 2007) โดยคนกลุ่มหนึ่งในสังคมที่อาจประสบภาวะความเหลื่อมล้ำจากหลายมิติพร้อมกัน เช่น เพศสภาพ ความยากจน ชนบทห่างไกล และเป็นกลุ่มชาติพันธุ์ เป็นต้น ยิ่งไปกว่านั้นทฤษฎีความซับซ้อนยังมีความเป็นปัจจุบันตลอดเวลา เนื่องจากกระบวนการสร้างความเป็นสังคมมีพลวัตเปลี่ยนแปลงไปตามปัจจัยแวดล้อมที่วิวัฒนาการขึ้นเป็นลูกโซ่ จนอาจเรียก *“ความซับซ้อน”* นี้ได้เป็นเพียงกรอบแนวคิดที่ไม่ใช่ทฤษฎี (Urry, 2005)

ทั้งนี้ เมื่อวิเคราะห์กรอบแนวคิดของทฤษฎีความซับซ้อนกับการศึกษาวิจัยนี้ เพื่อศึกษาแนวทางป้องกันการใช้เงินสกุลเข้ารหัสมาเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน จึงไม่อาจศึกษาแยกส่วนเฉพาะบริบทคุณสมบัติเฉพาะของเงินสกุลเข้ารหัสที่เสริมแรงจูงใจต่อผู้กระทำผิดในการเลือกใช้เป็นเครื่องมือในการฟอกเงินเท่านั้น ในขณะเดียวกันบริบททางกฎหมายที่มีต่อเงินสกุลเข้ารหัสก็เป็นปัจจัยแวดล้อมที่สำคัญ เนื่องจากนโยบายทางกฎหมายของแต่ละประเทศยังมีความเหลื่อมล้ำ ทั้งระดับยอมรับความชอบด้วยกฎหมาย ต้องห้ามตามกฎหมาย และมีบทบัญญัติกำกับดูแลในบางลักษณะ จนอาจก่อเกิดเป็นช่องว่างและโอกาสแก่ผู้กระทำผิด รวมถึงกลไกการโอนมูลค่าในระบบนิเวศข้ามเขตประเทศได้ด้วยความรวดเร็ว จึงเป็นอีกปัจจัยแวดล้อมที่ส่งผลต่อกระบวนการฟอกเงิน นอกจากผู้กระทำผิดแล้ว ยังมีกลุ่มบุคคลที่เกี่ยวข้องในระบบนิเวศ ซึ่งมีมูลเหตุจูงใจต่อปฏิสัมพันธ์ในระบบที่มีเป้าหมายแตกต่างกัน เช่น นักขุด นักลงทุน ผู้ให้บริการแลกเปลี่ยน และหน่วยงานรัฐที่ไม่สามารถเข้าไปมีส่วนร่วมกำกับกลไกระบบปฏิบัติการบล็อกเชนได้โดยตรง และจากปรากฏการณ์ของ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

เงินสกุลเข้ารหัส อย่างเช่น บิตคอยน์ที่เกิดขึ้นครั้งแรกเมื่อปี 2008 ด้วยมูลค่าตลาดรวมไม่ถึงหลักพันเหรียญสหรัฐ แต่ได้รับการตอบรับเชิงซ้อนจากผู้ที่เกี่ยวข้องจนเดือนมีนาคม 2021 มีขนาดมูลค่าตลาดรวมเกินกว่า 1.0 ล้านล้านเหรียญสหรัฐ

ดังนั้น การศึกษามาตรการป้องกันที่จะมีประสิทธิภาพต่อการป้องกันจึงควรนำปัจจัยแวดล้อมที่เกี่ยวข้องดังกล่าวข้างต้นมาสังเคราะห์ร่วมกัน เพื่อศึกษาองค์ประกอบความสัมพันธ์ของแต่ละชุดปัจจัยแวดล้อมซึ่งส่งผลกระทบทั้งเชิงบวกและเชิงลบที่มีต่อกัน รวมถึงปฏิกริยาลูกโซ่ที่อาจส่งผลต่อเนื่องเป็นเชิงซ้อน ซึ่งจะช่วยให้เกิดกรอบแนวทางการกำกับ การป้องกันและปราปรามในการนำเงินสกุลเข้ารหัสไปใช้เป็นเครื่องมือในการทำธุรกรรมฟอกเงินต่อไปได้อย่างมีประสิทธิภาพ

2.3.3 แนวคิดวัตถุนิยมวิภาษวิธี (Dialectical Materialism)

Karl Marx (1818-1883) นักปรัชญาสังคมที่ให้ความใจปัญหาความสัมพันธ์ระหว่างการผลิตกับสังคม เนื่องจากเป็นช่วงปฏิวัติอุตสาหกรรม ระบบการผลิตมีวิวัฒนาการทางเทคโนโลยี่และระบบการตลาดค้าเสรี หรือที่เรียกว่า *“ระบบทุนนิยม (Capitalism)”* ซึ่งเป็นระบบที่สร้างความเหลื่อมล้ำในสังคม เนื่องจากระบบทุนนิยมสร้างระบบการจัดสรรประโยชน์ตอบแทนอย่างไม่เท่าเทียมให้แก่เจ้าของปัจจัยการผลิต นายทุนซึ่งเป็นชนกลุ่มน้อยแต่เป็นผู้ครอบครองปัจจัยเงินทุน ที่ดิน และโรงงาน จะได้รับจัดสรรผลกำไรจากส่วนเกินปัจจัยการผลิตเพื่อสะสมเงินทุนในการขยายปัจจัยการผลิตต่อไป ในขณะที่ผู้ใช้แรงงานซึ่งเป็นชนกลุ่มใหญ่ในกระบวนการผลิตเพื่อสรรสร้างผลิตภัณฑ์ตามความต้องการของตลาด กลับได้รับผลตอบแทนเป็นเพียงค่าจ้างแรงงานและอาจรวมถึงสวัสดิการเพื่อการดำรงชีพเท่านั้น เมื่อเทคโนโลยี่การผลิตได้รับการพัฒนาศักยภาพการผลิตให้สูงขึ้นทำให้เกิดการขยายตัวทั้งปัจจัยเงินทุน และปัจจัยแรงงาน นายทุนก็จะยิ่งได้รับกำไรสะสมจากส่วนเกินปัจจัยการผลิตมากขึ้น ในขณะที่ผู้ใช้แรงงานก็ยังมีสภาพยากจนต่อไป (Dillion, 2014)

กระบวนการวิเคราะห์ทางสังคมของ Karl Marx ได้นำแนวคิดวิภาษวิธี (Dialectic) ของเฮเกล มาวิเคราะห์ความขัดแย้งทางสังคมในระบบการผลิตทุนนิยมที่มีเกิดขึ้น จากสาเหตุการจัดสรรประโยชน์ตอบแทนการใช้ทรัพยากรอย่างไม่เป็นธรรม ในขณะที่ผู้ใช้แรงงานถูกเอาเปรียบจนมีฐานะยากจน แต่นายทุนมีฐานะทางเศรษฐกิจดีขึ้น โดยเรียกแนววิเคราะห์นี้ว่า *“วัตถุนิยมวิภาษวิธี (Dialectical Materialism)”* อีกทั้งได้นำเสนอแนวคิดโครงสร้างสังคมทุนนิยมประกอบด้วยโครงสร้างส่วนบน (Supper Structure) ที่เกี่ยวข้องกับความคิด อุดมการณ์ และกฎหมาย และโครงสร้างส่วนล่าง (Substructure) เป็นวิถีการผลิตที่ประกอบด้วยพลังการผลิตจากฝ่ายแรงงาน และความสัมพันธ์ในปัจจัยการผลิตจากฝ่ายนายทุน โดยที่ชนชั้นนายทุนใช้ปัจจัยการผลิตเพื่อสร้างกำไร ส่วนชนชั้นแรงงานใช้พลังการผลิตเพื่อการยังชีพ ด้วยเหตุนี้จึงเกิดความขัดแย้งระหว่างชนชั้นจากเป้าหมายที่แตกต่างกัน กล่าวคือ ข้อเสนอ (Thesis) คือ ฝ่ายนายทุนมุ่งสร้างเป้าหมายกำไร จะส่งผล

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ต่อกระบวนการเปลี่ยนแปลงทางสังคม และข้อโต้แย้ง (Anti-Thesis) คือ ฝ่ายแรงงานมีเป้าหมายเพื่อการยังชีพ ทั้งนี้ความขัดแย้งระหว่างฝ่ายนายทุนและฝ่ายแรงงานจะเกิดการต่อรองการจัดสรรผลตอบแทนตลอดเวลาซึ่งขึ้นอยู่กับกลุ่มครอบครองอำนาจในสังคม หากสถานการณ์สะสมข้อขัดแย้งต่อเนื่องโดยไม่สามารถแก้ไขได้ก็อาจเกิดปรากฏการณ์ *"ปฏิวัติ"* ขึ้น ซึ่งกล่าวได้ว่าเป็นข้อสรุป (Synthesis) คือ บังเกิดวิธีการแก้ไขปัญหาแบบถอนรากถอนโคนโดยความขัดแย้งดังกล่าวจะหมดสิ้นไปหลังการปฏิวัติ (สุภางค์ จันทวานิช, 2016)

ในระยะต่อมา กลุ่มนักคิดได้นำแนวคิดของ Marx มาขยายความให้สอดรับกับบริบทสังคมที่เปลี่ยนแปลงในปัจจุบัน ชนชั้นทางสังคมไม่ได้จำกัดเพียงชนชั้นนายทุน และชนชั้นแรงงาน เนื่องจากระบบการผลิตและบริหารจัดการองค์กร ได้พัฒนาศักยภาพของชนชั้นแรงงานส่วนหนึ่งที่เลื่อนสถานะจากผู้ใช้แรงงานไร้ทักษะเป็นผู้ใช้แรงงานทักษะ เช่น หัวหน้างาน ผู้เชี่ยวชาญ ที่ได้รับการกำกับดูแลจากชนชั้นนายทุนที่แตกต่างจากชั้นชนแรงที่จะถูกอำนาจควบคุมโดยสิ้นเชิง ลักษณะการจัดการโครงสร้างทางสังคมจึงปรับเปลี่ยนไป ยอมรับชนชั้นเพิ่มขึ้นเป็นชนชั้นกลาง คือ ผู้ใช้แรงงานทักษะ หรือนักบริหาร รวมถึงเจ้าของที่ครอบครองปัจจัยการผลิตส่วนหนึ่ง และยังต้องอาศัยพึ่งพิงปัจจัยการผลิตส่วนที่เหลือจากชนชั้นนายทุน ดังนั้นโครงสร้างสังคมใหม่จึงมีระดับชั้น เป็นชนชั้นสูงหรือฝ่ายนายทุนเดิมที่ครอบครองปัจจัยการผลิตส่วนใหญ่ ชนชั้นกลางซึ่งเป็นชั้นชนที่เลื่อนระดับขึ้นมา และสุดท้ายชนชั้นล่างหรือฝ่ายแรงงานเดิม นอกจากนี้กลุ่มนักคิดแนวมาร์กซิสใหม่ยังได้ขยายความถึงอำนาจในการครอบครอง ซึ่งไม่ได้หมายถึงเฉพาะเจ้าของปัจจัยการผลิตตามแนวมาร์กซิสเดิมเพียงประการเดียว หากแต่รวมถึงอำนาจในการครอบครองจัดการปัจจัยการผลิตอันอาจได้มาโดยวิธีการอื่นที่ไม่ใช่เจ้าของโดยตรง ในลักษณะอำนาจนอกเหนือโครงสร้าง เช่น อำนาจในการเข้าถึงโดยได้รับอนุญาตให้ใช้ทรัพยากรรวมถึงการเช่า อำนาจในการควบคุมเครื่องมือในการผลิตจากกลไกรัฐ หรืออำนาจในการควบคุมแรงงานจากผู้บริหารองค์กร หรือสหภาพ เป็นต้น (สุภางค์ จันทวานิช, 2016) ดังนั้นในบางกรณีฝ่ายนายทุนอาจอาศัยอำนาจครอบงำของกลไกรัฐในการออกระเบียบ เพื่อการควบคุมฝ่ายแรงงานทางอ้อมแทน

สรุปประเด็นจากแนวคิดวัตถุนิยมวิภาษวิธีแนวมาร์กซิส จะเกิดขึ้นจากข้อขัดแย้งระหว่างกลุ่มผลประโยชน์ 2 ฝ่าย โดยฝ่ายชนชั้นล่างได้รับการจัดสรรผลตอบแทนจากการใช้ทรัพยากรที่ไม่เป็นธรรม สร้างความเหลื่อมล้ำแบ่งชนชั้น รวมถึงฝ่ายชนชั้นบนในระบบทุนนิยมจะอาศัยอำนาจครอบงำผ่านกลไกรัฐในการออกกฎหมาย ระเบียบในการปกป้องผลประโยชน์ และจัดระเบียบการควบคุมฝ่ายชั้นชนล่าง

เมื่อนำแนวคิดนี้มาวิเคราะห์ปรากฏการณ์การเกิดขึ้นของบิตคอยน์เงินสกุลเข้ารหัสสกุลแรก จะพบว่าในช่วงปี 2008 ประเทศสหรัฐอเมริกาประสบปัญหาวิกฤติเศรษฐกิจครั้งสำคัญในอุตสาหกรรมการเงิน โดยสถาบันการเงินรายใหญ่ของสหรัฐและเป็นรายใหญ่ของโลกหลายแห่งอยู่ใน

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

สถานะอาจล้มละลายจากสาเหตุในการปล่อยสินเชื่อที่อยู่อาศัย (Subprime) อย่างไร้ความรับผิดชอบ อีกทั้งได้ใช้เครื่องมือนวัตกรรมการเงินแปรสภาพ (Derivative) สินเชื่อที่มีความเสี่ยงให้แปลงเปลี่ยนเป็นตราสารหนี้ที่มีหลักทรัพย์เป็นประกัน (Collateralized Mortgage Obligation – CMO) เพื่อทำการขายต่อให้นักลงทุนสร้างกำไรในตลาดการเงิน พร้อมทั้งได้สร้างนวัตกรรมทำนองเดียวกันหมุนเวียนในตลาดการเงินอย่างต่อเนื่อง แต่เมื่อผู้กู้เพื่อที่อยู่อาศัยไม่สามารถชำระหนี้ได้จากปัญหาสภาพเศรษฐกิจภายในประเทศของสหรัฐ จึงกลายเป็นชนวนเหตุสำคัญของการสร้างความเสียหายแก่ระบบการเงินและระบบเศรษฐกิจที่ส่งทอดความเสียหายเป็นลูกโซ่อย่างทวีคูณ จนสถานะของสถาบันการเงินขนาดใหญ่หลายแห่งขาดทุนขนาดใหญ่จนถึงขั้นอาจล้มละลาย รัฐบาลกลางสหรัฐจำเป็นต้องออกนโยบายการเงินด้วยมาตรการหลายรูปแบบ รวมถึงการใช้เงินทุนของรัฐเข้าพยุงสถานะของสถาบันการเงินและระบบเศรษฐกิจ (Burniske & Tara, 2017)

ในช่วงเวลาเดียวกันในปี 2008 ซาโตชิได้นำเสนอระบบการโอนเงินอิเล็กทรอนิกส์ระหว่างบุคคลโดยตรง โดยไม่มีหน่วยงานกำกับ แต่ให้ระบบนิเวศตรวจสอบยืนยันกันเอง (Burniske & Tara, 2017) ซึ่งถือเป็นข้อโต้แย้งสำคัญของกลุ่มชนที่รู้สึกต่อความไม่เป็นธรรมจากการที่รัฐบาลใช้เงินทุนมหาศาลของภาครัฐเข้าไปพยุงสถาบันการเงินที่บริหารงานผิดพลาด ซึ่งเกิดจากความโลภในการใช้นวัตกรรมทางการเงิน นอกจากนี้ธุรกิจของสถาบันการเงินก็มีระบบเครือข่ายระหว่างประเทศทั่วโลก ซึ่งเป็นการผูกขาดการเข้าถึงแหล่งเงินทุน และบริการทางการเงิน รวมถึงการโอนเงินระหว่างประเทศที่มีขั้นตอนซับซ้อนใช้ระยะเวลานาน อีกทั้งการเรียกเก็บค่าธรรมเนียมในอัตราสูงเป็นการเอาเปรียบผู้ใช้บริการ ทั้งนี้ หลักฐานสำคัญของวิภาษวิธี คือ เมื่อ**สถาบันการเงินมีข้อเสนอ (Thesis) ในการผูกขาดระบบบริการการเงิน**เพื่อจัดการประโยชน์แก่กลุ่มของตน ในขณะที่กลุ่มซาโตชิ **ผู้คิดค้นนวัตรกรรมเงินสกุลเข้ารหัสมีข้อโต้แย้ง (Anti-Thesis) ในความไม่เป็นธรรมจากการจัดสรรทรัพยากรทางการเงิน** โดยมี**บทสรุปของปรากฏการณ์ (Synthesis) มีลักษณะเป็นการปฏิวัติระบบการโอนเงิน โดยบุคคลสามารถกระทำการโอนมูลค่าระหว่างกันเองได้โดยตรง ไม่ต้องผ่านระบบการกำกับตรวจสอบจากระบบสถาบันการเงิน** อีกทั้งใช้ระยะเวลาดำเนินการรวดเร็ว ไร้ข้อจำกัดด้านขอบเขตประเทศ และค่าใช้จ่ายดำเนินการต่ำ

อย่างไรก็ตามรัฐบาลและระบบการเงินโลกก็มีข้อโต้แย้งหลายประการต่อระบบนิเวศเงินสกุลเข้ารหัส ในประเด็นการกำกับและพิสูจน์ตัวตนผู้ใช้งานระบบการโอนมูลค่า ด้วยข้ออ้างเพื่อการรักษาความสงบเรียบร้อยของสังคม อีกทั้งประเด็นการกำกับการดำเนินงานข้ามอำนาจอธิปไตยนอกอาณาเขตประเทศ แม้แต่ ธรรมรักษ์ หมื่นจักร รัชพร วงศาโรจน์ กษิดิศ ตันสงวน และเกวลี สันตโย (2018) กลุ่มงานยุทธศาตร์องค์กร ธนาคารแห่งประเทศไทย ได้ให้ความเห็นว่า *“คริปโตเคอร์เรนซี (เงินสกุลเข้ารหัส) ได้นำมาซึ่งนวัตกรรมที่เพิ่มประสิทธิภาพของความปลอดภัย ตลอดจนลดต้นทุนทั้งในภาคธุรกิจและภาครัฐ แต่ก็ก่อให้เกิดความเสี่ยงหลายมิติ* ***การกำกับดูแลจึงต้องลดความเสี่ยงโดย***

ไม่ปิดกั้นนวัตกรรม" ทั้งนี้แนวโน้มของบทสรุปประการหนึ่ง คือ รัฐบาลหลายประเทศกำลังศึกษาเตรียมการเสนอเงินสกุลเข้ารหัสของรัฐในระบบเครือข่ายนิเวศซึ่งอยู่ในกำกับ แต่ก็ช่วยอำนวยความสะดวกแก่ผู้ใช้งานให้เข้าถึงระบบการโอนเงินสกุลเข้ารหัสได้ ภายใต้ต้นทุนดำเนินงานที่ลดลง หรืออีกปรากฏการณ์หนึ่งที่แสดงบทสรุป คือ การนำเสนอเงินสกุลเข้ารหัสใหม่ที่ชื่อว่า *"ลิบรา (Libra)"* ซึ่งนำเสนอคู่มือระบบปฏิบัติงานของเงินสกุลเข้ารหัสนี้ (White Paper) โดยเจ้าของเฟซบุ๊ก (Facebook) ซึ่งเป็นเครือข่ายสังคมออนไลน์ขนาดใหญ่ที่มีผู้ใช้งานมากว่า 1 ใน 4 ของประชากรทั่วโลก โดยนำเสนอระบบปฏิบัติแบบกระจายศูนย์ไปยังสมาชิกรับผิดชอบการตรวจสอบ ทั้งนี้ ในระยะแรกเริ่มได้นำเสนอสมาชิกผู้ร่วมก่อตั้งจำนวน 28 ราย ประกอบด้วยกลุ่มผู้ให้บริการชำระเงินรายใหญ่ กลุ่มเทคโนโลยีการตลาดออนไลน์ กลุ่มธุรกิจสื่อสาร กลุ่มนักลงทุน และกลุ่มองค์กรไม่แสวงหากำไร รวมถึงสถาบันการศึกษา โดยมีเป้าหมายที่จะขยายสมาชิกต่อไปจนครบ 100 ราย ซึ่งเป็นบทสรุปที่จะลดความเหลื่อมล้ำแก่ประชากรโลกที่เข้าไม่ถึงบัญชีสถาบันการเงินจำนวน 1,700 ล้านคนทั่วโลก แต่มีระบบการกำกับธุรกรรมข้ามเขตประเทศจากกลุ่มสมาชิกที่มาจากหลากหลายประเทศ (เกาะกระแส, 2019) อย่างไรก็ตาม รัฐบาลสหรัฐอเมริกาในช่วงเวลานั้นโดยประธานาธิบดีโดนัลทรัมป์ได้มีคำสั่งถึงเฟซบุ๊กให้ระงับการดำเนินการโครงการนี้

2.4 ทฤษฎีทางอาชญวิทยาที่เกี่ยวข้อง

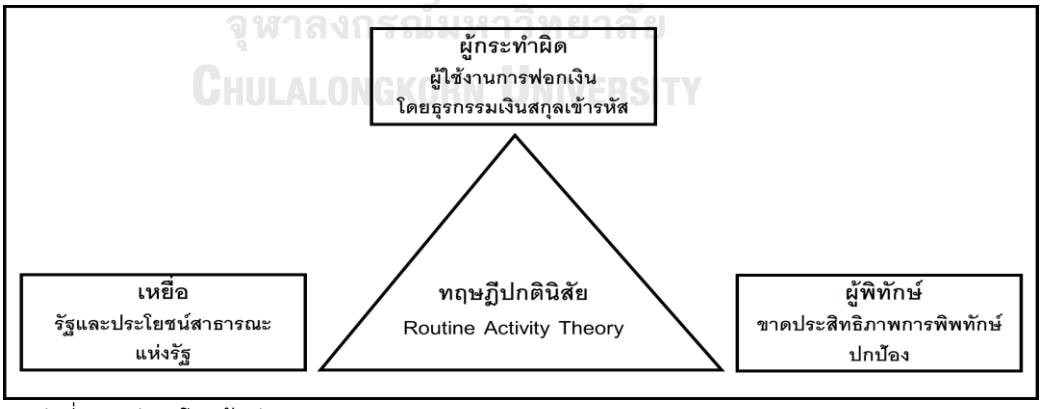
พฤติการณ์โอนย้ายเงินตรา ทรัพย์สิน หรือผลประโยชน์อื่นที่เกิดจากการกระทำผิดเพื่อการปกปิด ยักย้าย กระจายการถือครองทรัพย์สินให้เกิดความยากต่อการติดตามรวบรวมคืนแก่เหยื่อ หรือผู้ที่ได้รับผลกระทบจากการก่อเหตุ ไม่ใช่พฤติกรรมในลักษณะความเลวร้ายโดยตรง หากแต่บทบัญญัติแห่งกฎหมายได้ตราให้ *"การฟอกเงิน"* กระบวนการแปรสภาพเงินที่ได้จากการกระทำผิดให้เป็นเงินที่ชอบด้วยกฎหมายเป็นความผิดทางอาญา (Mala Prohibita) ทั้งนี้การฟอกเงินที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือจะมีลักษณะพฤติการณ์กระทำผิดเช่นเดียวกับการฟอกเงินตราทั่วไป หากแต่มีความแตกต่างกันที่กระบวนการและขั้นตอนในการดำเนินการบนระบบนิเวศออนไลน์ที่มีความซับซ้อนทางเทคนิคการปฏิบัติงาน รวมถึงการดำเนินงานมีความรวดเร็วไร้ขีดจำกัดด้านเขตพรมแดนประเทศ ดังนั้นแนวคิดทฤษฎีทางอาชญาวิทยาที่เกี่ยวข้องซึ่งสามารถอธิบายพฤติกรรมการฟอกเงินโดยเงินสกุลเข้ารหัสพอสรุปได้โดยสังเขป ดังนี้

2.4.1 ทฤษฎีการเลือกกระทำอย่างมีเหตุผล (Rational Choice Theory)

ทฤษฎีนี้นำหลักปรัชญาและแนวคิดเรื่อง *"การประเมินอรรถประโยชน์ Utilitarian Calculus"* ของ เจรามี่ เบนเธม (Jeremy Bentham) (1748-1833) ที่กล่าวว่าบุคคลกระทำการใดขึ้นอยู่บนพื้นฐานของการใช้ตรรกะวิเคราะห์เปรียบเทียบระหว่างต้นทุนกระทำการ เพื่อให้ได้มาซึ่ง

ประโยชน์ที่ต้องการ โดยการตัดสินใจจะเลือกกระทำในสิ่งที่เสริมสร้างความพึงพอใจสูงสุด ในขณะที่สามารถลดการสูญเสียหรือทุกข์ทรมานลงได้ (Siegel, 2013) โดยนักปรัชญาชาวอิตาลี ชื่อ ซีซา แบคคาเรีย (Cesar Beccaria) (1738-1794) ได้นำเสนอทฤษฎีอาชญวิทยาว่าด้วยการเลือกกระทำอย่างมีเหตุผล กล่าวว่าบุคคลมีตรรกะอย่างเสรีในการเลือกกระทำการในทุกสิ่ง รวมถึงการเลือกที่จะกระทำความผิดบนพื้นฐานของเหตุผลในการตัดสินใจเลือกกระทำความผิดกฎหมาย เมื่อบุคคลนั้นประเมินแล้วว่ามีโอกาสได้รับความพึงพอใจจากประโยชน์ที่จะได้รับ มากกว่าบทลงโทษที่อาจได้รับ (Siegel, 2013; พรชัย ขันตรี และคณะ, 2015) ซึ่งขยายความหมายถึงบุคคลจะใช้ตรรกะและเหตุผลของตนอย่างอิสระก่อนตัดสินใจกระทำผิดใด โดยการประเมินผลลัพธ์จากการกระทำนั้นว่ามีความคุ้มค่าทางเศรษฐกิจ หรือสร้างความพึงพอใจแก่ตนมากกว่า เมื่อเปรียบเทียบกับความเสี่ยงที่จะได้รับความเสียหายทางเศรษฐกิจที่จะเกิดขึ้นจากการกระทำผิดนั้น หรือเกิดผลแห่งทุกข์ทรมานใจแก่ตน ไม่ว่าจะเป็นความเสี่ยงที่อาจถูกจับกุม อัตราโทษที่จะได้รับหลังจากถูกจับกุม ตลอดจนการประเมินเปรียบเทียบกับการดำเนินการตามทางเลือกอื่น รวมถึงการปฏิบัติให้ถูกต้องตามกฎหมาย

กล่าวอีกนัยหนึ่งว่า บุคคลที่คิดจะกระทำความผิดย่อมมีเหตุแห่งแรงจูงใจที่ชัดเจนเพียงพอไม่ว่าจะเป็นการเลือกลักษณะการก่อเหตุและเหยื่อเป้าหมายที่จะถูกกระทำ นอกจากนี้มูลเหตุจูงใจอาจไม่ได้ก่อขึ้นจากสาเหตุหลักเพียงประการเดียว แต่อาจมีเหตุปัจจัยแวดล้อมอื่นเสริมอีกหลายประการ ทั้งนี้ผู้ที่จะก่อเหตุย่อมมีศักยภาพในการควบคุมพฤติกรรมตนเองอย่างเพียงพอที่จะเลือกอย่างเสรีว่าสมควรกระทำหรือไม่ รวมถึงประเมินถึงโอกาสความสำเร็จในการก่อเหตุ ผลลัพธ์ที่ได้ซึ่งอาจเป็นความพึงพอใจหรือผลประโยชน์ทางเศรษฐกิจที่มากพอต่อความเสี่ยงจากการได้รับผลร้าย การลงโทษ หรือการสูญเสีย (Lilly, Cullen, & Ball, 2015)



แหล่งที่มา : จัดทำโดยผู้วิจัย

ดังนั้น เมื่อนำทฤษฎีการเลือกกระทำอย่างมีเหตุผลมาอธิบายพฤติกรรมของผู้กระทำผิดที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงินนั้น ดังที่กล่าวข้างต้นกระบวนการฟอกเงินเป็นกระบวนการในการแปรสภาพเงินที่ได้จากการกระทำผิดเป็นเงินที่ชอบด้วยกฎหมาย ซึ่งเป็น

อรรถประโยชน์ที่ผู้กระทำผิดคาดหวังจะได้รับจากการกระทำความผิด ซึ่งเป็นประโยชน์ทางเศรษฐกิจที่จะได้รับเมื่อกระบวนการฟอกเงินสำเร็จ เช่น ผู้ค้ายาเสพติด หรือผู้กระทำการฉ้อโกง เมื่อได้เงินจากการกระทำผิดแล้วยังไม่สามารถนำไปใช้ประโยชน์ได้ ดังนั้นประโยชน์จากการก่อเหตุจึงยังไม่สมบูรณ์จนกว่าจะได้ฟอกเป็นเงินที่ชอบด้วยกฎหมายสำเร็จ จึงคิดที่จะเลือกกระทำการฟอกเงินเพื่อประโยชน์ที่ได้รับ เมื่อเปรียบเทียบกับความเสี่ยงที่อาจถูกจับกุมหรือยึดอายัดเงินในระหว่างกระบวนการฟอกเงิน นอกจากนี้ด้วยบริบทของเงินสกุลเข้ารหัสมีปัจจัยเสริมหลายประการที่อาจลดความเสี่ยงจากการตรวจสอบสืบค้น และในขณะเดียวกันด้วยคุณสมบัติเฉพาะของเงินสกุลเข้ารหัสที่สามารถกระทำการได้อย่างรวดเร็วแบบไร้เขตพรมแดนประเทศ จึงเป็นการเพิ่มโอกาสความสำเร็จของการฟอกเงิน

2.4.2 ทฤษฎีปกตินิสัย (Routine Activity Theory)

ทฤษฎีอาชญาวิทยานี้อธิบายถึงปัจจัยสำคัญที่เป็นสาเหตุให้เกิดการก่ออาชญากรรมขึ้น เมื่อองค์ประกอบหลัก 3 ปัจจัยได้มีโอกาสเกิดขึ้นครบทั้งสามปัจจัยพร้อมกัน ณ สถานการณ์หนึ่ง อันเป็นสถานการณ์ที่จะก่อให้เกิดเหตุอาชญากรรมได้ หรือที่ ลอร์เรน โคเฮน และ มาร์คัส เฟลสัน (Lawrence Cohen and Marcus Felson) (1979) เรียกสถานการณ์นี้ว่า *“Chemistry for Crime”* โดยปัจจัยแรกคือ ผู้กระทำผิด ซึ่งมีแรงจูงใจหรือแรงกระตุ้นที่เป็นโอกาสสร้างความโน้มเอียงให้ก่อเหตุกระทำผิด ปัจจัยที่สองคือ เหยื่อหรือเป้าหมาย ซึ่งหมายรวมถึงบุคคลและทรัพย์สินที่เหมาะสมแก่โอกาสการก่อเหตุและได้รับความคุ้มค่าจากผลในการกระทำผิด และปัจจัยสุดท้ายคือ การขาดศักยภาพของการพิทักษ์ปกป้องอย่างมีประสิทธิผล ณ บริเวณพื้นที่ก่อเหตุ หรือในจังหวะเวลาที่ไม่มีดูแลพิทักษ์ปกป้องที่มีความสามารถอย่างเพียงพอในการรักษาความปลอดภัยต่อร่างกายและทรัพย์สิน ทั้งนี้การพิทักษ์ปกป้องหมายรวมถึง บุคคลและเครื่องมืออุปกรณ์ที่มีศักยภาพในการปกป้องช่วยเหลือ (Lilly et al., 2015; พรชัย ขันตรี และคณะ, 2015) ทั้งนี้ พรชัย ขันตรี และคณะ (2015) ได้อธิบายพฤติกรรมของผู้กระทำผิดตามหลักการของทฤษฎีนี้ โดยผู้กระทำผิดจะมีขั้นตอนการเฝ้าติดตามกิจกรรมของเหยื่อเป้าหมายที่กระทำเป็นกิจวัตรประจำ หรือการกระทำใดที่เกิดขึ้นบ่อยครั้งจนสามารถนำมาประเมินศักยภาพการป้องกันพิทักษ์ตนเองได้ ซึ่งผู้กระทำผิดจะประเมินพื้นที่และจังหวะเวลาที่เหมาะสมในขณะที่ขาดการพิทักษ์ปกป้องอย่างเพียงพอ และมีโอกาสการก่อเหตุสำเร็จ เช่น เหยื่อเป้าหมายออกไปทำงานนอกบ้านในช่วงเวลาเดียวกันเสมอ และเป็นช่วงเวลาที่ปลอดจากการตรวจตราของเจ้าหน้าที่ จึงเป็นการสบโอกาสที่เหมาะสมต่อผู้กระทำผิดทำการก่อเหตุเป็นผลสำเร็จ (พรชัย ขันตรี และคณะ, 2015)อย่างไรก็ตาม ลอร์เรน โคเฮน และ มาร์คัส เฟลสัน (1979) ได้ขยายความถึงปัจจัยสำคัญที่จะก่อให้เกิดอาชญากรรม คือ โอกาสที่เอื้อประโยชน์ต่อผู้กระทำผิดให้สามารถก่อเหตุกระทำผิดได้สำเร็จ ทั้งนี้โอกาสหมายถึงช่วงเวลาหรือจังหวะเวลาที่เหมาะสมซึ่งจะให้ประโยชน์แก่ผู้กระทำผิดสูงสุด และเป็นขณะเวลาที่การพิทักษ์ปกป้องขาดประสิทธิภาพ หรืออยู่ในวิสัยที่

CHULALONGKORN UNIVERSITY

ผู้กระทำผิดจะจัดการได้ นอกจากจังหวะเวลาแล้ว พื้นที่ก็เป็นการสร้างโอกาสให้แก่ผู้กระทำผิด ว่าจะเป็นพื้นที่ที่เหมาะสมต่อการก่อเหตุให้สำเร็จ หรือขาดการเฝ้าดูแลของผู้พิทักษ์ ซึ่งอาจหมายรวมถึงบางพื้นที่ที่ขาดการบังคับใช้กฎหมายอย่างมีประสิทธภาพ (Lilly et al., 2015)

แหล่งที่มา: จัดทำโดยผู้วิจัย

ดังนั้น เมื่อนำทฤษฎีปกตินิสัย มาอธิบายพฤติกรรมของ**ผู้กระทำผิด**ที่เลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน เนื่องจากผลประโยชน์จากการก่อเหตุอาชญากรรมส่วนหนึ่งอาจอยู่ในรูปแบบอาชญากรรมทางไซเบอร์ จึงมีโอกาสที่จะนำผลประโยชน์นั้นแลกเปลี่ยนจากเงินตราปกติเป็นเงินสกุลเข้ารหัส หรือนำผลประโยชน์ในรูปเงินสกุลเข้ารหัสเข้าสู่ระบบนิเวศโดยตรง ภายใต้บริบททางกฎหมายกับสภาพบังคับต่อเงินสกุลเข้ารหัสในปัจจุบันที่หลายประเทศบัญญัติสถานสภาพทางกฎหมายของเงินสกุลเข้ารหัสแตกต่างกัน ตั้งแต่ขั้นรับรองความชอบด้วยกฎหมาย จนถึงขั้นต้องห้ามเป็นสิ่งผิดกฎหมาย และด้วยคุณลักษณะเฉพาะสำคัญของเงินสกุลเข้ารหัสที่สามารถโอนมูลค่าข้ามเขตพรมแดนประเทศด้วยความรวดเร็วและไร้การกำกับควบคุมด้วยหน่วยงานใด จึงเข้าข่ายลักษณะเป็น**การขาดประสิทธิภาพของการพิทักษ์ปกป้อง**ที่เหมาะสม อันเป็นอีกปัจจัยสำคัญต่อการก่ออาชญากรรมตามทฤษฎีนี้ โดยเฉพาะอย่างยิ่งหากการกระทำผิดขยายไปถึงพื้นที่ในเขตประเทศที่มีสภาพบังคับกฎหมายที่แตกต่างกัน และช่วงเวลาการก่อเหตุที่สามารถดำเนินการข้ามเขตเวลาระหว่างประเทศได้อย่างเสรี ก็จะส่งกระทบต่อความมั่นคงของระบบเศรษฐกิจการเงิน และประโยชน์สาธารณะแห่งรัฐ อีกทั้งการนำผลประโยชน์จากกระบวนการฟอกเงิน ไปเป็นทุนสนับสนุนการก่ออาชญกรรมต่อไปได้อีกอย่างต่อเนื่อง ยิ่งเป็นการสร้างภาระที่ยากแก่การปราบปรามรวมถึงเป็นต้นทุนต่อรัฐในการรักษาความสงบเรียบร้อยให้แก่สังคม ดังเช่นความผิดมูลฐานซึ่งเป็นลักษณะความผิดที่ผู้กระทำผิดก่อเหตุขึ้นและนำประโยชน์ที่ได้รับจากการก่อเหตุ ไปทำธุรกรรมการฟอกเงินซึ่งถูกบัญญัติขึ้นในกฎหมายป้องกันและปราบปรามการฟอกเงิน อันได้แก่ การค้ายาเสพติด การค้ามนุษย์ การฉ้อโกงสถาบันการเงิน การหลีกเลี่ยงภาษีอากรและภาษีศุลกากร การพนันทางอิเล็กทรอนิกส์ การแสวงหาประโยชน์จากทรัพยากรธรรมชาติโดยมิชอบ การมีส่วนร่วมในองค์กรอาชญากรรมรวมถึงองค์กรอาชญากรรมข้ามชาติ และการสนับสนุนการค้าอาวุธร้ายแรง เป็นต้น ดังนั้น**รัฐและประโยชน์สาธารณะแห่งรัฐจึงเข้าลักษณะเป็นเหยื่อ** ที่ได้รับผลร้ายจากกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

2.4.3 ทฤษฎีป้องกันอาชญากรรม (Situational Crime Prevention Theory)

ทฤษฎีนี้พัฒนาขึ้นจากแนวคิดการป้องกันอาชญากรรมมาจากหลักการของทฤษฎีการเลือกกระทำอย่างมีเหตุผล (Rational Choice Theory) ประกอบทฤษฎีปกตินิสัย (Routine

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

Activity Theory) โดยหลักการสำคัญ คือ การป้องปรามเพื่อลดโอกาสการก่อเหตุกระทำผิดได้สำเร็จอย่างมีประสิทธิภาพมากขึ้นเท่าไรก็จะส่งผลในทิศทางให้การเกิดอาชญากรรมลดลงยิ่งขึ้นเช่นเดียวกัน (Lilly et al., 2015) และหลักการลดทอนประโยชน์ที่พึงได้รับจากการกระทำผิด หรือก่อภาระเพิ่มแก่ต้นทุนการสูญเสียจากการก่อเหตุ ทั้งนี้ไม่จำกัดเฉพาะโอกาสที่พึงได้รับประโยชน์หรือภาระการสูญเสียทางเศรษฐกิจ แต่ยังหมายรวมถึงโอกาสการสร้างสะสมประสบการณ์ และการเรียนรู้กระบวนการกระทำผิด รวมถึงการพัฒนาองค์ความรู้เทคนิคการก่อเหตุอาชญากรรมอย่างเป็นระเบียบแบบแผน (Siegel, 2013)

เดริค คอร์นิส และ โรนัล คราค (Derek Cornish and Ronald Clarke) (1980) ได้นำเสนอกลยุทธเพื่อการป้องกันอาชญากรรมตามแนวคิดของทฤษฎีนี้ ด้วยการกำหนดและบริหารจัดการมาตรการเพื่อการตัด ลดทอนโอกาสที่อาจก่อให้เกิดสถานการณ์พร้อมแก่การก่อเหตุกระทำผิดได้ ในขณะเดียวกันก็เป็นมาตรการในการสร้างภาระเพิ่มอันมากเกินแก่เหตุที่เหมาะสมต่อการกระทำผิด ซึ่งประกอบด้วยแนวทางดังนี้ (Lilly et al., 2015; Siegel, 2013)

(1) **การเพิ่มภาระความยากลำบากแก่ผู้กระทำผิด**ในการก่อเหตุ (Increase the effort needed to commit crime) เป็นมาตรการที่ก่อให้เกิดภาระการดำเนินการที่มากเกินกว่าประโยชน์ที่พึงได้รับ หรือเพิ่มมาตรการป้องกันโดยบุคคล เครื่องมือ หรือเทคโนโลยี่ที่จะสร้างภาระเพิ่มแก่ผู้กระทำผิดหากจะการดำเนินการก่อเหตุจนสำเร็จ เช่น การเพิ่มการตรวจอัตลักษณ์บุคคลบนบัตรเครดิต หรือการพัฒนาระบบกันขโมยรถยนต์ทั้งระบบกุญแจสองชั้นพร้อมเสียงสัญญาน เป็นต้น

(2) **การเพิ่มความเสี่ยงต่อการถูกตรวจพบ**การกระทำผิดหรือถูกจับกุม (Increase the risks of committing crime) ทั้งนี้อาจเพิ่มมาตรการทางกฎหมายในการบัญญัติเพิ่มลักษณะการกระทำความผิดทางอาญา หรือเพิ่มบุคคลากรผู้บังคับใช้กฎหมาย ซึ่งอาจรวมถึงการเพิ่มเครื่องมืออุปกรณ์ในการตรวจสอบสืบค้น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

(3) **การลดผลตอบแทนหรือประโยชน์ที่ได้รับ**จากการก่อเหตุ (Reduce the rewards of committing crime) มาตรการในการจำกัดช่องทางการจำหน่าย จ่าย โอน หรือการแปลงสภาพผลประโยชน์ที่ผู้กระทำผิดได้รับจากการก่อเหตุ เพื่อลดมูลค่าของผลตอบแทนสุทธิที่ผู้กระทำผิดจะได้รับ เช่น การควบคุมตลาดรถยนต์มือสองป้องกันการถ่ายโอนรถยนต์จากการถูกโจรกรรม ลดจำนวนวงเงินทอนที่เก็บไว้ในเครื่องคิดเงิน

(4) **การลดแรงกระตุ้นและสร้างสำนึกผิด** เพื่อหลีกเลี่ยงจากเหตุกระทำผิด (Reduce provocation/ induce guilt or shame for committing crime) มาตรการสื่อสารสร้างความเข้าใจถึงความร้ายแรงของเหตุอาชญากรรม แนวทางการหลีกเลี่ยงและป้องกันตนเองต่อสาธารณชน เพื่อลดโอกาสการตกเป็นเหยื่อ

(5) **การลดเหตุและข้ออ้าง**ที่ผู้กระทำผิดจะใช้แก้ตัวเมื่อก่อเหตุขึ้น (Reduce excuses for committing crime) การประชาสัมพันธ์เสริมสร้างความเข็มแข็งของชุมชนต่อต้านสิ่งเร้าที่อาจก่อให้เกิดเหตุกระทำผิด รวมถึงสร้างองค์ความรู้ถึงกระบวนการก่อเกิดอาชญากรรมต่อสาธารณะ เพื่อหลีกเลี่ยงการกล่าวอ้างแก้ตัวเนื่องจากไม่รับรู้ถึงความผิดที่ก่อขึ้น เช่น การขับรถเร็วบนทางด่วนเกินความเร็วควบคุม

นอกจากนี้ มาร์คัส เฟลสัน ได้เสนอแนวทางป้องกันการก่ออาญชากรรมโดยความร่วมมือของผู้รับผิดชอบ 3 กลุ่ม เพื่อให้กำกับดูแลปัจจัยสำคัญที่เป็นสาเหตุให้เกิดการก่ออาชญากรรมขึ้นจากทั้ง 3 ปัจจัยตามทฤษฎีปกตินิสัย กล่าวคือ (1) ผู้พิทักษ์ *“Guardians”* รับผิดชอบหน้าที่ในการตรวจตราดูแลให้ความปลอดภัยป้องกันการตกเป็นเหยื่อ (2) ผู้ดูแล *“Handler”* รับผิดชอบหน้าที่ดูแลบุคคลที่มีโอกาสเกิดพฤติกรรมเบี่ยงเบนหรือเป็นผู้กระทำผิด ซึ่งส่วนใหญ่จะเป็นบุคคคใกล้ชิดและแวดล้อมบุคคลดังกล่าว เช่น บิดามารดา พี่น้อง ญาติ และเพื่อน เพื่ออบรมขัดเกลาลดทอนความเบี่ยงเบน และ (3) ผู้จัดการ *“Manager”* รับผิดชอบหน้าที่ดูแลเฝ้าระวังพื้นที่เสี่ยงที่มีโอกาสต่อการเกิดเหตุ (Lilly et al., 2015; Siegel, 2013)

ทั้งนี้ทฤษฎีป้องกันอาชญากรรมตามสถานการณ์ เป็นกรอบแนวคิดสำคัญต่อการวางมาตรการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ไม่จำกัดเฉพาะการเพิ่มมาตรการทางกฎหมาย และการบังคับใช้ในการตรวจสอบข้อมูลส่วนบุคคลและความเป็นตัวตนของผู้ใช้งานระบบนิเวศเงินสกุลเข้ารหัส การเพิ่มโทษทางกฎหมาย รวมถึงการพัฒนาระบบความร่วมมือระหว่างประเทศในการบังคับยึดอายัดเงินสกุลเข้ารหัสนั้น ยังควรประกอบด้วยการประชาสัมพันธ์สร้างความเข้าใจต่อองค์ความรู้ที่ถูกต้องเกี่ยวกับเงินสกุลเข้ารหัส และการประชาสัมพันธ์ความเสี่ยงต่อการตกเป็นเหยื่อในกระบวนการฟอกเงินโดยเงินสกุลเข้ารหัส เป็นต้น

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

2.4.4 อาชญากรรมเศรษฐกิจ (Economic Crime)

เอ็ดวิน เฮช ซัตเธอร์แลนด์ (Edwin H. Sutherland) เป็นนักอาชญาวิทยาที่ให้ความสนใจศึกษาพฤติกรรมการก่ออาชญากรรมของคนชนชั้นสูงของสังคม และเป็นบุคคลแรกที่นิยาม ***“อาชญากรรมคอปกขาว (White Collar Crime)”*** ทั้งนี้ ในระยะต่อมาได้มีการขยายแนวคิดของซัตเธอร์แลนด์เป็น อาชญากรรมธุรกิจ อาชญากรรมการเงิน และอาชญากรรมเศรษฐกิจ โดยองค์ประกอบของอาชญากรรมประเภทนี้ ประกอบด้วย (1) ผู้กระทำผิดหรืออาชญากรเป็นนักธุรกิจ ผู้บริหารองค์กร รวมถึงบุคคลชนชั้นสูงของสังคมที่มีฐานะทางเศรษฐกิจมั่งคั่ง หรือมีความสัมพันธ์เชิงธุรกิจวิชาชีพที่มีอำนาจสั่งการอันทรงอิทธิพลโดยอาศัยตำแหน่งหน้าที่ ใช้อำนาจสั่งการเพื่อการกระทำผิดเชิงเศรษฐกิจและการสร้างเสริมต่อยอดฐานอำนาจ และ (2) รูปแบบของการก่ออาชญกรรมที่ส่งผลกระทบร้ายแรงต่อระบบเศรษฐกิจ เช่น การฉ้อโกงผลประโยชน์ขององค์กร หรือคอรัปชั่นที่เกิดขึ้นกับ

ทั้งองค์กรภาคเอกชนและภาคราชการที่เรียกว่า *"ฉ้อราษฎรบังหลวง"* การสร้างอำนาจเหนือตลาดด้วยความได้เปรียบเชิงการค้า การสร้างความไม่เป็นธรรมในการซื้อขายหลักทรัพย์ การฉ้อโกงสถาบันการเงิน การติดสินบนทั้งระบบราชการและเอกชน การก่อมลพิษต่อสิ่งแวดล้อม การบุกรุกเพื่อใช้ทรัพยากรธรรมชาติ รวมถึงการหลบเลี่ยงภาษีอากร เป็นต้น (Lilly et al., 2015) ดังนั้นอาจกล่าวได้ว่าเหยื่อของอาชญากรรมเศรษฐกิจ คือ ประโยชน์สาธารณะของภาครัฐหรือองค์กรเอกชนซึ่งผู้กระทำผิดส่วนใหญ่เป็นเจ้าหน้าที่ประจำหรือสมาชิกขององค์กรนั้น หรืออาจเป็นสมาชิกขององค์กรคู่แข่งขัน (Siegel, 2013)

ทั้งนี้จากการศึกษาของซัตเธอร์แลนด์ได้นำทฤษฎีทางอาชญาวิทยาอธิบายพฤติกรรมอาชญากรรมทางเศรษฐกิจ โดยทฤษฎีการคบค้าสมาคมที่แตกต่าง (Differential Association Theory) อธิบายลักษณะของผู้กระทำผิดเกิดการยอมรับพฤติกรรมเบี่ยงเบน และการเรียนรู้การกระทำผิดของกลุ่มนักธุรกิจ ผู้บริหาร หรือผู้มีอำนาจ จนกลายเป็นการสร้างการยอมรับบรรทัดฐานสังคมและวัฒนธรรมองค์กรที่ขาดจริยธรรม ไม่เคารพระเบียบหรือกฎหมาย แต่เพียงมุ่งหวังให้ได้ผลประโยชน์สูงสุดแก่ตนหรือกลุ่มของตน โดยไม่จำกัดรูปแบบของการกระทำแม้ว่าจะเป็นการปฏิบัติที่ขัดต่อกฎหมายหมายหรือจริยธรรม ประกอบกับทฤษฎีการควบคุมตนเอง (Self-control Theory) อธิบายถึงการขาดการควบคุมตนเองที่เพียงพอต่อการเผชิญหน้ากับการสบโอกาสก่อเหตุ หรือความคาดหวังต่อผลประโยชน์เฉพาะหน้า ถึงแม้ว่าผู้กระทำผิดจะเป็นบุคคลที่มีระดับการศึกษาสูง หรือผู้บริหารที่มีทักษะการบริหารจัดการองค์กรก็ตาม รวมถึงทฤษฎีการเลือกกระทำอย่างมีเหตุผล (Rational Choice Theory) และ ทฤษฎีแก้ตัว (Neutralization Theory) เนื่องจากผู้กระทำผิดอยู่ในฐานะทางสังคมชั้นสูงและมีอำนาจในการสั่งการ จึงมีความเชื่อว่าโอกาสการถูกตรวจสอบ หรือถูกจับกุมมีโอกาสเกิดขึ้นได้โดยยาก เมื่อเปรียบกับผลประโยชน์ตอบแทนเฉพาะหน้าที่คาดว่าจะได้รับอยากมากเพียงพอ ในขณะเดียวกันก็มีทัศนคติต่อการกระทำผิดว่าเป็นเรื่องปกติธรรมดาที่ผู้มีอำนาจพึงกระทำการได้ โดยปราศจากความละอายต่อการกระทำผิดกฎระเบียบ หรือขัดต่อจริยธรรมวิชาชีพและองค์กร (Lilly et al., 2015)

อีกทั้งอาชญากรรมเศรษฐกิจได้ขยายพฤติกรรมการกระทำผิดไปในหลายลักษณะซึ่งอยู่บนพื้นฐานปัจจัยผู้กระทำผิดที่มีฐานะทางเศรษฐกิจ และมีอำนาจอิทธิพลต่อการสั่งการให้ผู้อื่นกระทำ ร่วมกระทำ หรือกระทำความผิดด้วยตนเอง รวมถึงมีความเชื่อมั่นที่จะสามารถปิดกั้นการตรวจสอบจับกุมของเจ้าหน้าที่ได้ โดยเฉพาะอย่างยิ่งพัฒนาการทางเทคโนโลยีเพื่อการบริหารงานองค์กรก็เป็นการเปิดช่องทางโอกาสการก่อเหตุกระทำผิดมากยิ่งขึ้น และการตรวจสอบสืบค้นร่องรอยการกระทำผิดก็ยากขึ้นเช่นกัน ด้วยเหตุแห่งความซับซ้อนของระบบคอมพิวเตอร์ การสื่อสารสังคมออนไลน์ เช่น การฉ้อโกงเศษทศนิยมด้วยเงินจำนวนน้อยต่อรายการแต่ปริมาณรายการผ่านระบบคอมพิวเตอร์จำนวนมหาศาลต่อวัน การหลอกลวงในระบบการค้าพาณิชย์อิเล็กทรอนิกส์ผ่านการ

สื่อสารในสังคมออนไลน์ การคอรัปชั่นด้วยการเรียกเก็บค่านายหน้าหรือค่าที่ปรึกษาจำนวนมากโดยเรียกเก็บจากกิจการต่างประเทศ เป็นต้น

ทั้งนี้รูปแบบของอาชญากรรมทางเศรษฐกิจมีความหลากหลายลักษณะ ตัวอย่างเช่น

(1) อาชญากรรมที่เกี่ยวข้องกับสถาบันการเงิน โดยอาศัยอำนาจหน้าที่ปฏิบัติงานโดยมิชอบของทั้งเจ้าหน้าที่ระดับปฏิบัติการและเจ้าหน้าที่ระดับบริหาร เช่น การสมคบกับลูกค้าในการอนุมัติวงเงินกู้ให้แก่ลูกค้าสูงเกินกว่ามูลค่าหลักประกันหรือไม่มีหลักประกัน โดยได้รับผลประโยชน์จากการใช้อำนาจอนุมัติเป็นการตอบแทน การอนุมัติสินเชื่อให้แก่ลูกค้าที่ไม่มีตัวตน การจัดเตรียมแผนธุรกิจของลูกค้าสูงเกินจริงหรือปรับลดปัจจัยความเสี่ยง เพื่อให้สามารถอนุมัติวงเงินสินเชื่อที่เกินความสามารถการจ่ายชำระคืน การใช้ข้อมูลส่วนบุคคลของลูกค้าเพื่อนำไปใช้ประโยชน์แก่ตน การหลอกขายตราสารการเงินที่มีความเสี่ยงสูงให้แก่ลูกค้า การทยอยเบิกถอนเงินจำนวนน้อยจากบัญชีเงินฝากของลูกค้า เป็นต้น

(2) อาชญากรรมที่เกี่ยวข้องกับการซื้อขายหลักทรัพย์ เช่น ผู้บริหารบริษัทจดทะเบียนใช้ประโยชน์จากข้อมูลภายในกิจการก่อนการเผยแพร่ต่อประชาชนทั่วไป เพื่อสร้างกำไรจากการซื้อขายหลักทรัพย์ หรือที่เรียกว่า *“Inside Trading”* นายหน้าซื้อขายหลักทรัพย์ลักลอบนำหุ้นหรือหลักทรัพย์ในบัญชีของลูกค้าไปทำการซื้อขาย เพื่อสร้างกำไรระยะสั้นแก่ตนเอง เป็นต้น

(3) อาชญากรรมภายในองค์กร โดยอาศัยอำนาจสั่งการในตำแหน่งหน้าที่เกินกว่าขอบเขตอำนาจ หรือบิดเบือนอำนาจเพื่อหาประโยชน์แก่ตนโดยมิชอบ เช่น การสั่งซื้อวัสดุอุปกรณ์หรือว่าจ้างบริการในมูลค่าที่สูงกว่าราคาตลาดทั่วไป หรือในปริมาณสูงเกินความจำเป็น เพื่อรับประโยชน์เป็นสินบนตอบแทนในรูปตัวเงินหรือสิ่งของจากคู่ค้า รวมถึงการตรวจรับวัสดุอุปกรณ์หรือตรวจรับงานบริการที่มีคุณภาพด้อยกว่าข้อตกลงทางการค้า การสั่งจ่ายค่าล่วงเวลาการทำงานเกินกว่าความเป็นจริงเพื่อแบ่งประโยชน์คืนจากพนักงานภายหลัง หรือสร้างอิทธิพลต่อพนักงานเพื่อให้ความร่วมมือกระทำการอื่นตามที่จะสั่งการต่อไป การใช้ทรัพย์สินขององค์กรเพื่อประโยชน์ส่วนตน การสร้างรายจ่ายหรือกำหนดผลประโยชน์ของผู้บริหารเกินสมควร เพื่อผู้บริหารได้รับประโยชน์ก่อนที่จะเหลือจัดสรรกำไรให้แก่ผู้ถือหุ้น การตกแต่งรายการบัญชีทั้งด้านการสร้างรายได้และด้านการลดรายจ่ายเพื่อให้งบการเงินแสดงมูลค่ากิจการสูงเกินความเป็นจริง เป็นต้น

(4) อาชญากรรมหลอกลวงลักษณะแชร์ลูกโซ่ โดยอาศัยภาพลักษณ์ของบุคคลที่สังคมเชื่อถือ เช่น ดารา แพทย์ นักวิชาการ ผู้บริหาร เน็ตไอดอล เป็นผู้นำเสนอโครงการแก่กลุ่มเป้าหมายเพื่อเชิญชวนให้ร่วมลงทุน เป็นตัวแทนขายสินค้า ด้วยการหลอกลวงให้นำเงินมาลงทุน

และได้รับผลตอบแทนสูงเกินกว่าอัตราผลตอบแทนทั่วไป เพื่อขยายฐานเหยื่อเป้าหมายรวมถึงเพิ่มวงเงินหมุนเวียนจากการหลอกลวง และจะหยุดกิจการในที่สุด เช่น การซื้อขายสินค้าเกษตรล่วงหน้า การซื้อขายเงินตราต่างประเทศ การขายสินค้าสุขภาพหรือเครื่องสำอางค์ การเช่าเครื่องมือขุดเงินสกุลเข้ารหัส การซื้อขายคาร์บอนเครดิต เป็นต้น

(5) อาชญากรรมหลอกลวงผ่านระบบพาณิชย์อิเล็กทรอนิกส์ ด้วยการส่งมอบสินค้าด้อยคุณภาพกว่าที่ประชาสัมพันธ์ในเว็บไซต์ให้แก่ลูกค้า ไม่ทำการส่งมอบสินค้าหลังได้รับเงินล่วงหน้าค่าสินค้าแล้ว การหลอกลวงเพื่อการขอรับบริจาคหรือการทำกุศล การหลอกลวงให้ลงทุนซื้อขายเงินสกุลเข้ารหัส เป็นต้น

(6) อาชญากรรมที่ส่งผลกระทบต่อประโยชน์สาธารณะ เช่น การบุกรุกแหล่งทรัพยากรธรรมชาติเพื่อหาประโยชน์เข้าตนโดยมิชอบ ด้วยการใช้ประโยชน์บนที่ดินเขตป่าไม้เป็นโรงแรมหรือรีสอร์ทเพื่อการพาณิชย์ การทำเหมืองแร่บนที่ดินของตนโดยไม่ได้รับอนุญาต การปล่อยมลพิษอุตสาหกรรมสู่แหล่งน้ำธรรมชาติหรือสู่อากาศ รวมถึงการควบรวมธุรกิจประเภทเดียวกันเพื่อการผูกขาดอุตสาหกรรมและเพิ่มอำนาจควบคุมกลไกตลาดที่อาจสร้างภาระแก่ผู้บริโภค เป็นต้น

อย่างไรก็ตาม รูปแบบอาชญากรรมเศรษฐกิจยังมีอีกหลายลักษณะ รวมถึงลักษณะการกระทำอาชญากรรมบนระบบนิเวศออนไลน์ ซึ่งมีโอกาสที่อาจได้รับผลประโยชน์จากการกระทำผิดที่มีมูลค่าสูงในรูปแบบของแหล่งเงินในประเทศ หรือในต่างประเทศ และอาจเป็นแหล่งเงินในรูปแบบอิเล็กทรอนิกส์โดยเฉพาะอย่างยิ่งเงินสกุลเข้ารหัส ดังนั้นกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ซึ่งเป็นกระบวนการยักย้ายทรัพย์สินแบบไร้พรมแดน การถ่ายเทมูลค่าโดยเทคโนโลยีขั้นสูง รวมถึงการหลีกเลี่ยงการตรวจสอบสืบค้นและการยึดอายัดทรัพย์สินบนระบบเครือข่ายออนไลน์ จึงอาจเป็นทางเลือกให้แก่ผู้กระทำผิดจากอาชญากรรมเศรษฐกิจ ในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

2.4.5 อาชญากรรมไซเบอร์ (Cybercrime) และอาชญากรรมองค์กรข้ามชาติ (Transnational Organized Crime)

การพัฒนานวัตกรรมทางเทคโนโลยีคอมพิวเตอร์และการสื่อสารซึ่งสร้างศักยภาพการดำเนินงานด้วยความรวดเร็ว และสามารถเชื่อมต่อระบบเครือข่ายการสื่อสารออนไลน์ข้ามเขตประเทศในระบบงานที่เรียกว่า *“อินเตอร์เน็ต (Internet)”* นอกจากจะเป็นการสร้างโอกาสทางธุรกิจทั้งด้านการค้าออนไลน์ที่สามารถขยายตลาดการค้าได้ทั่วโลก และด้านการสื่อสารบริหารกิจกรรมทางเศรษฐกิจได้อย่างรวดเร็ว ในขณะเดียวกันก็เป็นการสร้างโอกาสแก่ผู้กระทำผิดที่ใช้เทคโนโลยีเป็นเครื่องมือในก่ออาชญากรรมได้หลายรูปแบบ รวมถึงระบบเครือข่ายอินเตอร์เน็ตได้สร้างความเชื่อมโยงผู้กระทำผิดหรืออาชญากรระดับท้องถิ่น สามารถติดต่อร่วมมือกันเป็นเครือข่ายกับกลุ่มอาชญากร

ข้ามชาติ ซึ่งสามารถสมคบคิดวางแผนเตรียมการระหว่างผู้กระทำผิดต่างรัฐ เพื่อกระทำสิ่งผิดกฎหมายในอีกรัฐโดยไร้ข้อจำกัดด้านขอบเขตประเทศ เข้าลักษณะกระทำการเป็นองค์กรอาชญากรรมข้ามชาติ (Siegel, 2013)

ทั้งนี้ องค์ประกอบของการก่ออาชญากรรมไซเบอร์อยู่บนพื้นฐานแนวคิดทฤษฎีอาชญาวิทยาเช่นเดียวกับทฤษฎีสามเหลี่ยมอาชญากรรม กล่าวคือประกอบด้วย (1) เหยื่อซึ่งอาจเป็นทั้งผู้ใช้งานระบบ อุปกรณ์เครื่องคอมพิวเตอร์ หรือระบบปฏิบัติการ (2) ระบบงานของผู้กระทำผิดซึ่งสามารถเชื่อมต่อเข้าสู่ระบบงานเป้าหมายเพื่อการโจรกรรม การแจ้งเตือน การเปลี่ยนแปลงแก้ไข การถ่ายโอน รวมถึงการทำลายข้อมูลอิเล็กทรอนิกส์ และ (3) ระบบการสื่อสารและเครื่องมืออุปกรณ์สร้างโอกาสการเชื่อมต่อเข้าสู่ระบบงานเป้าหมาย ดังนั้นอาชญากรรมไซเบอร์ หมายถึง การกระทำผิดกฎหมายโดยใช้อุปกรณ์คอมพิวเตอร์ เครื่องมือสื่อสาร ระบบข้อมูลสารสนเทศ รวมถึงระบบอินเตอร์เน็ตเป็นเครื่องมือในการก่ออาชญากรรมโดยบุคคล กลุ่มบุคคล หรือองค์กรอาชญากรรม (McQuade, 2006) ทั้งนี้อาชญากรรมไซเบอร์ถือเป็นอาชญากรรมเศรษฐกิจลักษณะหนึ่ง เนื่องจากผู้กระทำผิดมีวัตถุประสงค์เพื่อคาดหวังได้รับประโยชน์จากเป้าหมายที่เป็นทั้งปัจเจกบุคคล หรือผลประโยชน์ขององค์กรเอกชน รวมถึงประโยชน์สาธารณะของภาครัฐ (Siegel, 2013) โดยมีรูปแบบการก่ออาชญากรรม ดังนี้

(1) การโจรกรรมทางไซเบอร์ (Cybertheft) เป็นการใช้ระบบงานคอมพิวเตอร์เพื่อการฉ้อโกงผลประโยชน์ของประชาชนหรือองค์กรด้วยความรวดเร็ว หรือการใช้เป็นช่องทางในการค้าหรือให้บริการสิ่งผิดกฎหมาย เช่น การโจรกรรมข้อมูล การฉ้อโกงเงินจำนวนน้อยจากบัญชีของลูกค้า (Salami fraud) การค้ายาเสพติดหรือสิ่งผิดกฎหมายทางออนไลน์ การหลอกลวงทางออนไลน์ในลักษณะแชร์ลูกโซ่ (Ponzi) การขโมยรหัสข้อมูลแสดงตัวตนผู้ใช้งาน (Phishing)

(2) การทำลายระบบงานไซเบอร์ (Cybervandalism) เป็นการใช้ระบบงานคอมพิวเตอร์เพื่อการตอบโต้และการมุ่งหมายสู่การทำลายล้างระบบปฏิบัติการ หรือระบบฐานข้อมูลของเป้าหมาย เช่น ไวรัสคอมพิวเตอร์ (Viruses) ที่มุ่งหมายขัดขวางหรือทำลายระบบปฏิบัติการคอมพิวเตอร์ หรือการเข้าสู่ระบบเพื่อผลิตซ้ำข้อมูลให้ขยายตัวในระบบการทำงาน (Worms) การส่งชุดรหัสข้อมูลเข้าสู่ระบบเพื่อรอการกระจายตัวเมื่อมีผู้เปิดใช้งาน หรือเพื่อทำลายระบบงาน (Trojan House) การส่งชุดรหัสข้อมูลเข้าสู่ระบบเพื่อรอเวลาที่ตั้งค่าล่วงหน้าหรือรอเวลารหัสลับทำงาน เพื่อทำลายระบบงาน (Logic Bomb) การส่งรหัสชุดข้อมูลเพื่อการทำลายระบบผ่านทางจดหมายอิเล็กทรอนิกส์ (Spam) การใช้ข้อมูลเชิงลบและทำการผลิตซ้ำในลักษณะการประจานบุคคลหรือองค์กรจัดส่งเข้าสู่ระบบสื่อสารสังคมออนไลน์ (Cyberbullying) รวมถึงการใช้ระบบคอมพิเตอร์เพื่อการสะกดรอยบุคคลหรือองค์กร รวมถึงการเข้าถึงข้อมูลความลับหรือข้อมูลส่วนบุคคลโดยไม่ชอบด้วย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

กฎหมาย (Cyberspying) ทั้งนี้การกระทำการข้างต้นมีวัตถุประสงค์เพื่อเรียกร้องผลประโยชน์จากเหยื่อเป็นการตอบแทนในการบรรเทาความเสียหายของระบบงานเป้าหมายในลักษณะการเรียกค่าไถ่ (Ransom)

(3) การสงครามทางไซเบอร์ (Cyberwarfare) เป็นการใช้ระบบงานเพื่อการต่อต้านฝ่ายปฏิปักษ์ เพื่อการทำลายล้างระบบโครงสร้างเครือข่ายการสื่อสารพื้นฐาน หรือเพื่อการทำลายล้างระบบปฏิบัติการหรือระบบฐานข้อมูลของประเทศศัตรู เช่น การก่อการร้ายทางไซเบอร์ (Cyberterrorism) ใช้ระบบปฏิบัติการคอมพิวเตอร์สร้างเครือข่ายเชื่อมต่อระบบเพื่อการทำลายเป้าหมายในโลกความเป็นจริง ตัวอย่างเช่น ระบบท่อส่งน้ำมัน อาคารภาคราชการสำคัญ เป็นต้น

ทั้งนี้การโจรกรรมทางไซเบอร์ประเภทการค้าสิ่งผิดกฎหมายบนระบบออนไลน์ เช่น การค้ายาเสพติด การค้าอาวุธร้ายแรง การค้ามนุษย์ และอาจรวมถึงการเรียกค่าไถ่ โดยผู้กระทำผิดมักดำเนินการบนระบบ Deep Web ซึ่งเป็นเว็บไซต์ที่ไม่สามารถสืบค้นด้วยเครื่องมือการค้นหาบนเว็บไซต์ทั่วไปได้ อย่างเช่น Google, Yahoo, Bring, Ask.com และ AOL Search เป็นต้น โดยสามารถเชื่อมโยงฐานข้อมูล และ Matadata ซึ่งเป็นข้อมูลที่ใช้อ้างอิงถึงข้อมูลอื่นๆบนอีกหลายมิติ เพื่อการสืบค้นข้อมูลบนเว็บไซต์และแสดงผลลัพธ์ตามต้องการ ทั้งนี้เนื่องจาก Deep Web มีลักษณะการปฏิบัติงานแบบพลวัต สามารถเคลื่อนย้ายในระบบเครือข่ายได้ หรือเป็นเว็บไซต์ที่ถูกจำกัดการใช้งานเฉพาะกลุ่มผู้ใช้งานที่ได้รับอนุญาตด้วยรหัสเฉพาะในการเข้าถึงระบบเท่านั้น ดังนั้นเว็บไซต์ลักษณะนี้จึงถูกนำมาใช้เป็นเครื่องมือในการค้าสิ่งผิดกฎหมายบนระบบออนไลน์ เรียกว่า Dark Web ซึ่งนอกจากการจำกัดกลุ่มผู้ใช้งานบนเว็บไซต์นี้แล้ว ยังมีการดำเนินงานบนระบบปฏิบัติการเฉพาะที่สามารถปิดบังตัวตนผู้ใช้งาน โดยการเคลื่อนย้ายรหัสที่ตั้งของผู้ใช้งานตลอดเวลาระหว่างการเปิดใช้งาน เช่น TOR, I2P (Invisible Internet Project) หรือ Freenet เป็นต้น เพื่อสร้างความซับซ้อนปกปิดตำแหน่งรหัสที่ตั้งระหว่างการติดต่อสื่อสาร ลดความเสี่ยงต่อการตรวจติดตามสืบค้น ซึ่งเป็นอาชญากรรมทางไซเบอร์ที่มีโอกาสได้รับผลตอบแทนทางการค้าสิ่งผิดกฎหมาย เป็นเงินสกุลเข้ารหัสบนระบบการชำระราคาทางออนไลน์ และสามารถนำเข้าสู่กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้โดยสะดวกและรวดเร็ว เนื่องจากธุรกรรมทั้งหมดดำเนินการบนระบบนิเวศออนไลน์ทั้งสิ้น (Braga & Luna, 2018)

การดำเนินการอาชญากรรมไซเบอร์ส่วนใหญ่ มีลักษณะเข้าข่ายการร่วมมือวางแผนและปฏิบัติการเป็นกลุ่มบุคคล องค์กร รวมถึงอาจเป็นการสมคบกระทำความผิดร่วมกันของกลุ่มบุคคลจากหลายประเทศเพื่อดำเนินการก่อเหตุอาชญากรรมในต่างประเทศ หรือปฏิบัติการในระบบนิเวศอินเตอร์เน็ต ซึ่งเข้าลักษณะองค์ประกอบขององค์กรอาชญากรรมข้ามชาติ คือ การสบคบกันของบุคคลหรือองค์กรจากหลายประเทศร่วมมือกระทำผิด หรือการจัดเตรียมวางแผนก่อเหตุ ณ ประเทศหนึ่งแต่

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ไปปฏิบัติการก่อเหตุ ณ อีกประเทศหนึ่ง หรือกระทำความผิดในรัฐหนึ่งแต่มีความร่วมมือจากบุคคลหรือองค์กรหลายประเทศ หรือกระทำความผิดในประเทศหนึ่งแต่ส่งผลกระทบสร้างความเสียหายเป็นวงกว้างในหลายประเทศ โดยอนุสัญญาสหประชาชาติเพื่อการต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร (United Nation Convention Against Transnational Organized Crime (UNTOC) ได้แบ่งลักษณะอาชญากรรมองค์กรเป็น 10 ลักษณะ ได้แก่ (สุมนทิพย์ จิตสว่าง, 2019)

(1) การลักลอบค้ายาเสพติด (Illicit Trafficking in Drugs)

(2) การลักลอบนำคนเข้าเมือง (Smuggling of Illegal Migrants)

(3) การค้าอาวุธ (Arms Trafficking)

(4) การลักลอบค้าอาวุธนิวเคลียร์ (Trafficking in Nuclear Material)

(5) กลุ่มองค์กรอาชญากรรมข้ามชาติและการก่อการร้าย (Transnational Criminal Organization and Terrorism)

(6) การค้าหญิงและเด็ก (Trafficking in Women and Children)

(7) การลักลอบค้าชิ้นส่วนมนุษย์ (Trafficking in Body Parts)

(8) การโจรกรรมและลักลอบค้ายานพาหนะ (Theft and Smuggling of Vehicles)

(9) การฟอกเงิน (Money Laundering)

(10) การกระทำอื่น (Other Activities) เช่น การโจรกรรมศิลปวัตถุ การให้สินบนเจ้าหน้าที่ราชการ เป็นต้น

ดังนั้นการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสเป็นการกระทำความผิดที่อาจเข้าข่ายเป็นการกระทำอันมีส่วนร่วมในการกระทำผิดลักษณะบุคคลต่อบุคคล กลุ่มบุคคล หรือองค์กรรวมถึงองค์กรอาชญากรรมข้ามชาติ เนื่องจากการทำธุรกรรมบนระบบนิเวศเงินสกุลเข้ารหัสเป็นระบบปฏิบัติการที่เชื่อมโยงข้ามเขตแดนหลายประเทศ โดยเฉพาะอย่างยิ่งการดำเนินการของศูนย์บริการแปรสภาพเงินสกุลเข้ารหัส ที่มีโครงข่ายความร่วมมือของบุคคลและกลุ่มบุคคลเจ้าของรหัสที่ตั้งและกระเป๋าเงินอิเล็กทรอนิกส์ ในการถ่ายโอนเงินสกุลเข้ารหัสไข้วไปมาระหว่างกันในกลุ่มโครงข่าย เพื่อปกปิดความเชื่อมโยงระหว่างรหัสที่ตั้งต้นทางของผู้โอนกับรหัสที่ตั้งปลายทางของผู้รับโอน รวมถึงการกลบเกลื่อนร่องรอยเส้นทางธุรกรรมระหว่างกันเพื่อให้ผู้รับโอนปลายทางได้รับเงินสกุลเข้ารหัสที่ไม่ปนเปื้อนกับเงินสกุลเข้ารหัสต้นทาง นอกจากนี้อนุสัญญาสหประชาชาติเพื่อการต่อต้านองค์กรอาชญากรรมข้ามชาติ ได้ให้ความสำคัญกับการต่อต้านลักษณะอาชญากรรมการฟอกเงิน ทั้งนี้มาตรการต่อต้านการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส มีความจำเป็นอย่างยิ่งที่ต้องได้รับความร่วมมือระหว่างประเทศให้ดำเนินนโยบายไปในทิศทางเดียวกัน เนื่องจากการโอนมูลค่าในระบบนิเวศ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

เงินสกุลเข้ารหัสสามารถเคลื่อนย้ายถ่ายเทโดยอาศัยช่องว่างทางกฎหมายไปดำเนินการยังประเทศที่มีมาตรการต่อต้านเบาบางได้

ในขณะเดียวกัน เงินสกุลเข้ารหัสเป็นชุดรหัสข้อมูลที่สามารถแสดงมูลค่าและดำเนินการในระบบปฏิบัติการอินเตอร์เน็ต เช่นเดียวกับการกระทำความผิดของอาชญากรรมไซเบอร์ ดังนั้นผู้กระทำผิดที่มีมูลเหตุจูงใจในการฉ้อโกงหรือการขโมยเงินสกุลเข้ารหัส สามารถมุ่งเป้าหมายกระทำการก่อเหตุกับกระเป๋าเงินอิเล็กทรอนิกส์ เส้นทางธุรกรรม หรือรหัสเปิดส่วนบุคคลของเหยื่อบนระบบนิเวศอินเตอร์เน็ต โดยสามารถโอนย้ายผลประโยชน์จากการกระทำผิดในรูปเงินสกุลเข้ารหัสได้อย่างรวดเร็ว รวมถึงการเรียกร้องผลประโยชน์ตอบแทนเป็นค่าไถ่แบบเฉียบพลันจากเหยื่อด้วยกลไกการทำงานของเงินสกุลเข้ารหัส

2.5 กฎหมายและข้อบัญญัติขององค์กรระหว่างประเทศที่เกี่ยวข้องกับกำกับดูแล

2.5.1 Financial Action Task Force on Money Laundering (FATF)

เนื่องจากองค์การสหประชาชาติ (The United Nations) ได้ประเมินความเสี่ยงภัยจากการเงินทุนหมุนเวียนในระบบการเงิน ที่มีแหล่งเงินมาจากธุรกิจค้ายาเสพติดและอาชญากรรมทั่วโลกในปี 1987 มีจำนวนสูงถึง 300,000 ล้านเหรียญสหรัฐ หรือประมาณร้อยละ 2 ถึง 5 ของผลิตภัณฑ์มวลรวมของทุกประเทศรวมกัน (Global GDP) ดังนั้นในปี 1989 ที่ประชุมกลุ่มประเทศเศรษฐกิจขนาดใหญ่ G7 Summit ซึ่งจัดขึ้น ณ กรุงปารีส ได้มีมติจัดตั้งคณะทำงานเพื่อทำหน้าที่กำหนดมาตรฐานและแนวทางในการป้องกันและปราบรามการฟอกเงิน (Financial Action Task Force on Money Laundering) หรือเรียกคำย่อว่า FATF โดยในระยะเริ่มต้นคณะทำงานประกอบด้วยสมาชิก 16 ประเทศและประเทศร่วมอีก 8 ประเทศ เพื่อมุ่งศึกษากลไกการฟอกเงินด้วยการใช้เครื่องมือการเงินระหว่างประเทศรวมถึงมาตรการปราบปรามในขณะนั้น เพื่อจัดทำแนวปฏิบัติเพื่อปรับปรุงมาตรการปราบปรามการฟอกเงิน โดยในปี 1990 FATF ได้นำเสนอแนวปฏิบัติในการป้องกันและปราบปรามการฟอกเงินขึ้นเป็นครั้งแรกจำนวน 40 ข้อแนะนำ หรือที่เรียกว่า The 40 Recommendations ประกอบด้วยข้อแนะนำเกี่ยวกับหลักกฎหมาย กฎระเบียบ และมาตราการเพื่อให้แต่ละประเทศวางเป็นแนวปฏิบัติในการป้องกัน ปราบปราม และการลงโทษในกระบวนการฟอกเงิน อย่างไรก็ตาม FATF ได้ทบทวนและปรับปรุงข้อแนะนำตามบริบทของอาชญากรรมที่มีพลวัตอย่างต่อเนื่อง และได้มีประเทศเข้าร่วมเครือข่ายเพิ่มขึ้นจากคณะทำงานประเทศสมาชิก 16 ประเทศเป็น 38 ประเทศและประเทศเครือข่ายอีก 205 ประเทศรวมถึงประเทศไทย อย่างไรก็ตามจากเหตุการณ์ครั้งสำคัญในปี 2011 ซึ่งกลุ่มผู้ก่อการร้ายสากลได้ทำลายอาคารเวิลด์เทรดศูนย์กลางธุรกิจของสหรัฐอเมริกา ที่เรียกว่า เหตุการณ์ 9-11 คณะทำงาน FATF จึงได้นำเสนอมาตการป้องกันการ

สนับสนุนการก่อการร้ายเพิ่มเติมอีก 9 ข้อแนะนำ จึงมักเรียกมาตรการของ FATF ว่า 40+9 Recommendations (FATF, 2019)

ทั้งนี้ FATF ได้ให้ความสนใจระบบนิเวศของระบบปฏิบัติการแบบกระจายศูนย์ (Distributed Ledger Technology – DLT) และบริบทของเงินสกุลเข้ารหัสในระบบการเงิน ตั้งแต่ปี 2014 ที่ได้นำเสนอแนวปฏิบัติในการกำกับดูแลเงินเสมือน และในช่วงครึ่งแรกของปี 2018 FATF พบว่า มีผู้เสนอขายเงินสกุลเข้ารหัสรายใหม่บนเกาะเคย์แมน (Cayman ซึ่งเป็นประเทศปลอดภาษี และไม่ได้เป็นสมาชิกของ FATF) มากกว่าร้อยละ 40 ของปริมาณที่นำเสนอเข้าสู่ระบบการเงินโลก (Frick, 2019) จึงได้พัฒนาแนวคิดเพื่อปรับปรุงข้อแนะนำโดยมติที่ประชุมประเทศ G20 ในปี 2018 ได้เสนอเพิ่มเติมนิยาม *"สินทรัพย์เสมือน (Virtual Assets) หมายถึงมูลค่าของหน่วยข้อมูลดิจิทัลที่สามารถใช้เพื่อการค้า การโอนมูลค่า การชำระเงิน และการลงทุนบนระบบเครือข่ายดิจิทัล"* (Federico Paesano, 2019) พร้อมทั้งปรับปรุงข้อแนะนำที่ 15 (Recommendation 15 – New Technologies) เพื่อการจัดการลดความเสี่ยงจากสินทรัพย์เสมือน (Virtual Assets) โดยแนะนำให้รัฐควรจะให้ความเชื่อมั่นได้ว่า ผู้ให้บริการที่เกี่ยวข้องกับสินทรัพย์เสมือน (Virtual Assets Service Providers - VASP) จะต้องอยู่ภายใต้กฎระเบียบ การกำกับ การอนุญาตเพื่อให้ระบบการติดตามและสร้างความมั่นใจด้วยมาตรการป้องกันและปราบปรามการฟอกเงินอย่างเหมาะสม โดยหมายรวมถึงระบบการตรวจสอบข้อมูลตัวตนผู้ใช้งาน และการรายงานธุรกรรมต้องสงสัย เป็นต้น (Federico Paesano, 2019; Frick, 2019)

ดังนั้น รัฐจึงควรปรับมาตรการให้สอดคล้องกับข้อแนะนำที่ 15 (ปรับปรุง) โดยมุ่งให้ความสำคัญต่อผู้ให้บริการที่เกี่ยวข้องกับสินทรัพย์เสมือน (VASP) โดยรัฐต้องวางมาตรการให้ผู้ให้บริการจะต้องมีระบบการจัดเก็บข้อมูลที่เกี่ยวข้องกับตัวตนผู้ใช้บริการและรายการธุรกรรม เพื่อพร้อมให้หน่วยงานรัฐตรวจสอบ รวมถึงมาตรการกำกับติดตามระบบปฏิบัติงาน การระงับธุรกรรมหรือการอายัดบางธุรกรรมที่ต้องสังสัย โดยมีการกำหนดขั้นตอนการดำเนินงานที่ชัดเจน นอกจากนี้ควรวางมาตรการป้องกันการโอนมูลค่าระหว่างบุคคลโดยตรง ซึ่งเป็นช่องว่างทางเทคโนโลยีในการตรวจสอบระบบนิเวศ โดยอนุญาตให้ทำธุรกรรมเงินสกุลเข้ารหัสกับผู้ให้บริการที่ได้รับอนุญาตเท่านั้น (Federico Paesano, 2019)

ดังจะเห็นได้ว่า องค์กรกำกับดูแลระหว่างประเทศอย่างเช่น FATF ให้ความสำคัญกับการป้องกันเงินสกุลเข้ารหัสในการใช้เป็นเครื่องมือในการทำธุรกรรมฟอกเงิน ด้วยการวางมาตรการกำกับดูแล และการอนุญาตกับผู้ให้บริการซึ่งจะถือเป็นกลุ่มบุคคลสำคัญในระบบนิเวศ โดยการวางกรอบให้ผู้ใช้บริการทำธุรกรรมเฉพาะผู้ให้บริการที่ได้รับอนุญาตเท่านั้น อย่างไรก็ตามระบบปฏิบัติการของกลไกการทำงานของเงินสกุลเข้ารหัส สนับสนุนการทำธุรกรรมโอนมูลค่าระหว่างผู้ใช้งานโดยตรง

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ซึ่งเป็นข้อด้อยสำคัญในการป้องกันธุรกรรมต้องสงสัย อีกทั้งระบบปฏิบัติการก็ไม่มีข้อจำกัดให้ผู้ใช้งานต้องแสดงตัวตนก่อนใช้งาน

2.5.2 European Union Anti-Money Laundering Directives

European Union Anti-Money Laundering Directives หรือเรียกคำย่อว่า EU AMLD เป็นมาตรการทางกฎหมายที่ออกบังคับใช้โดยสภาสหภาพยุโรป (The European Parliament and of The Council) เพื่อป้องกันการใช้สถาบันการเงินในสหภาพยุโรปเป็นเครื่องในการฟอกเงินหรือสนับสนุนทางการเงินแก่ผู้ก่อการร้าย โดยได้ประกาศใช้บังคับมาตรการนี้ครั้งในแรกในปี 1991 โดยกรอบการปฏิบัติงานให้ความสำคัญต่อการกำกับดูแลธุรกรรมของสถาบันสินเชื่อ และสถาบันการเงินที่อาจเข้าข่ายการฟอกเงินจากความผิดมูลฐานเฉพาะธุรกิจค้ายาเสพติดและในปี 2001 ได้ออกมาตรการฉบับที่ 2 ขยายขอบเขตบังคับใช้กับความผิดมูลฐานที่เกิดจากอาชญากรรม และวิชาชีพเฉพาะอื่น จากนั้นในปี 2005 ได้ออกมาตราฉบับที่ 3 โดยนำกรอบแนวคิดตามข้อแนะนำการป้องกันการฟอกเงินของ FATF มาปรับหลักการกำกับด้วยการมุ่งเน้นการพิสูจน์ตัวตนของลูกค้าสถาบันการเงิน รวมถึงการวิเคราะห์ธุรกรรมบนพื้นฐานความเสี่ยง (Risk Base Approach) ทั้งนี้ได้มีการพัฒนากรอบมาตรการฉบับที่ 4 ตามข้อแนะนำฉบับปรับปรุงของ FATF ได้ขยายเป้าหมายวิเคราะห์ธุรกรรมบนความเสี่ยงรวม (Consolidated Risk Base Approach) ที่กำหนดให้สถาบันการเงินมีหน้าที่ตรวจสอบสถานภาพและความสัมพันธ์ทางธุรกิจของคู่ค้า (KYC) รวมถึงธุรกรรมทางการเงินที่มีข้อสงสัยว่าจะเข้าข่ายการฟอกเงิน เพื่อรายงานให้หน่วยงานรัฐได้ทราบตามวิธีปฏิบัติที่กำหนด (Vandezande, 2017) รวมถึงได้พิจารณาปรากฏการณ์ของเงินสกุลเข้ารหัสด้วยการปรับแนวปฏิบัติเทียบเคียงกับมาตรการกำกับเงินอิเล็กทรอนิกส์ชนิดปกปิดตัวตน (Anonymous E-Money) แต่ในทางปฏิบัติ คุณลักษณะเฉพาะของเงินสกุลเข้ารหัสมีความแตกต่างจากเงินอิเล็กทรอนิกส์ ซึ่งได้บัญญัติไว้ตั้งแต่มาตรการฉบับที่ 2 สหภาพยุโรปจึงได้มีการทบทวนและแก้ไขเพิ่มเติมมาตรการป้องกันการฟอกเงินอย่างต่อเนื่อง จนถึงปัจจุบันประกาศบังคับใช้เป็นมาตรการฉบับที่ 5 ตั้งแต่ปี 2018 โดยได้ขยายฐานความรับผิดเพิ่มเติมกับธุรกิจที่เกี่ยวข้องกับระบบนิเวศเงินสกุลเข้ารหัส ที่ต้องปฏิบัติตามมาตรการฉบับนี้ คือ ผู้ให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัสเป็นเงินตราปกติ (Exchanger) และผู้ให้บริการดูแลกระเป๋าเงินอิเล็กทรอนิกส์ (Custodian Wallet Providers) จะต้องได้รับอนุญาต และมีหน้าที่ตรวจสอบผู้ใช้บริการในลักษณะเดียวกับมาตรการของสถาบันการเงิน

ทั้งนี้ หลักปฏิบัติการป้องกันการฟอกเงินของสหภาพยุโรปเริ่มด้วยกรอบแนวคิดในการกำกับดูแลในระบบสถาบันการเงินเป็นสำคัญ ดังนั้นมาตรการจึงมุ่งเฝ้าระวังผู้ใช้บริการสถาบันการเงิน แม้ว่าระบบการเงินโลกจะได้มีการพัฒนาเงินสกุลเข้ารหัสที่มีคุณลักษณะเฉพาะเอื้อต่อการใช้

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

เป็นเครื่องมือในการทำธุรกรรมฟอกเงิน แนวปฏิบัติของมาตรการก็ยังคงมุ่งจุดเฝ้าระวัง ณ สถาบันการเงินซึ่งจะเป็นจุดแลกเปลี่ยนเงินสกุลเข้ารหัสเป็นเงินตราปกติ

2.6 กฎหมายไทยที่เกี่ยวข้อง

2.6.1 พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน

ตามเจตนารมณ์ของพระราชบัญญัติป้องกันและปราบปรามการฟอกเงินฉบับนี้ ซึ่งตราขึ้นและมีผลบังคับใช้ตั้งแต่วันที่ 19 สิงหาคม 1999 เป็นต้นไป (พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542, 2017) ด้วยสาเหตุจากผู้กระทำผิดได้นำเงินหรือทรัพย์สินที่เกี่ยวข้องกับการกระทำผิดไปทำการฟอกเงิน เพื่อนำเงินและทรัพย์สินนั้นไปใช้กระทำผิดต่อไปอีก ทำให้ยากแก่ปราบปรามอาชญากรรม ดังนั้นเพื่อเป็นการตัดวงจรการประกอบอาชญากรรมจึงจำเป็นต้องตรากฎหมายเฉพาะขึ้นในการจัดการกับอาชญากร และเงินหรือทรัพย์สินที่ได้จากการกระทำผิด รวมถึงการดำเนินมาตรการป้องกันและปราบปรามการฟอกเงินได้อย่างมีประสิทธิภาพ (สำนักงานป้องกันและปราบปรามการฟอกเงิน, 2017)

องค์ประกอบฐานความผิดการฟอกเงิน ตามมาตรา 5 แห่งพระราชบัญญัตินี้ ประกอบด้วย (1) ผู้ใด ซึ่งหมายถึงบุคคล นิติบุคคล รวมถึงผู้กระทำความผิดฐานฟอกเงิน แม้จะกระทำนอกราชอาณาจักรผู้นั้นจะต้องรับโทษในราชอาณาจักรตามมาตรา 6 แห่งพระราชบัญญัตินี้ (2) การกระทำ ในการโอน รับโอน หรือแปลงสภาพทรัพย์สินที่เกี่ยวข้องกับการกระทำผิดหรือกระทำด้วยประการใดๆ (3) มีเจตนาพิเศษ เพื่อการซุกซ่อน หรือปกปิดอำพรางแหล่งที่มา หรือช่วยเหลือผู้อื่นให้มิต้องให้ได้รับโทษหรือได้รับโทษน้อยลง และ (4) วัตถุที่กระทำ อันหมายถึงเงินหรือทรัพย์สินที่เกี่ยวกับการกระทำความผิด (สำนักงานป้องกันและปราบปรามการฟอกเงิน, 2017) ทั้งนี้ภายใต้ความผิดมูลฐานตามมาตรา 3 แห่งพระราชบัญญัตินี้ ซึ่งปัจจุบันประกอบด้วยลักษณะความผิด 29 รูปแบบ กล่าวคือ (1) การค้ายาเสพติด, (2) การค้ามนุษย์ ผู้หญิงและเด็ก, (3) การฉ้อโกงประชาชน, (4) การยักยอกฉ้อโกงสถาบันการเงิน, (5) ความผิดต่อตำแหน่งหน้าที่ราชการ, (6) การกรรโชก รีดเอาทรัพย์ลักษณะช่องโจร, (7) การลักลอบหนีภาษีศุลกากร, (8) การก่อการร้าย, (9) การจัดการให้มีการเล่นพนันรวมถึงการพนันทางสื่ออิเล็กทรอนิกส์, (10) การเป็นสมาชิกอั้งยี่ การมีส่วนร่วมในองค์กรอาชญากรรม, (11) การรับของโจรลักษณะเป็นการค้า, (12) การปลอมแปลงเงินตรา ดวงตราลักษณะเป็นการค้า, (13) การละเมิดทรัพย์สินทางปัญญา, (14) การปลอมแปลงบัตรอิเล็กทรอนิกส์ หนังสือเดินทาง, (15) การแสวงหาประโยชน์จากทรัพย์กรธรรมชาติโดยมิชอบ, (16) การประทุษร้ายต่อชีวิตหรือร่างกายจนสาหัสเพื่อให้ได้ประโยชน์ซึ่งทรัพย์สิน, (17) การหน่วงเหนี่ยวหรือกักขังผู้อื่นเพื่อต่อรองรับผลประโยชน์, (18) การกรรโชก รีดเอาทรัพย์อันมีลักษณะเป็นปกติธุระ, (19) การกระทำอันเป็นโจรสลัด, (20) การกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์, (21) การค้าอาวุธ

เครื่องกระสุนปืน และวัตถุระเบิด, (22) การกระทำการเพื่อจูงใจให้ผู้มีสิทธิเลือกตั้งลงคะแนนให้แก่ตนเองหรือผู้สมัครอื่น, (23) การกระทำการเพื่อจูงใจให้ผู้อื่นสมัครเข้ารับเลือกเป็นสมาชิกวุฒิสภา, (24) การมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ, (25) การสนับสนุนทางการเงินแก่การก่อการร้าย, (26) การสนับสนุนทางการเงินแก่การแพร่ขยายอาวุธทำลายล้างสูง, (27) การหลีกเลี่ยงหรือฉ้อโกงภาษีตามประมวลรัษฎากร, (28) การบังคับใช้แรงงานหรือบริการที่อันตรายสาหัสหรือถึงแก่ชีวิต, และ (29) การกระทำการเพื่อจูงใจให้ผู้มีสิทธิเลือกตั้งสมาชิกสภาหรือผู้บริหารท้องถิ่น

ทั้งนี้มาตรการทางอาญากับผู้กระทำผิดฐานฟอกเงิน ต้องระวางโทษจำคุกตั้งแต่ 1 ถึง 10 ปี หรือปรับตั้งแต่ 20,000 บาทถึง 200,000 บาท หรือทั้งจำทั้งปรับ ในขณะที่มาตรการทางแพ่ง คือ การดำเนินการขอให้ทรัพย์สินที่เกี่ยวกับการกระทำผิดตกเป็นของแผ่นดิน ทั้งนี้การพิสูจน์ที่มาของทรัพย์สินเพื่อขอเพิกถอนการยึดหรืออายัดเป็นหน้าที่ของผู้ทำธุรกรรม โดยกระบวนการป้องกันและปราบปรามการฟอกเงินได้บัญญัติมาตรการตามหมวด 2 การรายงานธุรกรรมการเงินและการแสดงตนผู้ทำธุรกรรม ซึ่งกำหนดให้สถาบันการเงิน สำนักงานที่ดิน ศุลกากร และผู้ประกอบวิชาชีพตามมาตรา 16 เป็นผู้มีหน้าที่รายงานธุรกรรม อันได้แก่ ธุรกรรมเงินสดหรือธุรกรรมเกี่ยวกับทรัพย์สินที่มีจำนวนหรือมูลค่าเกินกว่ากำหนดในกฎกระทรวง รวมถึงธุรกรรมที่มีเหตุอันควรสังสัยซึ่งเชื่อได้ว่ากระทำขึ้นเพื่อการหลีกเลี่ยงไม่ให้ตกอยู่ในบังคับแห่งพระราชบัญญัตินี้ นอกจากนี้ได้บัญญัติมาตรการตามหมวด 6 การดำเนินการเกี่ยวกับทรัพย์ที่กระทำผิดเพื่อการตรวจสอบ ติดตาม ยึด อายัดทรัพย์สินอันมีเหตุควรเชื่อได้ว่าอาจได้มาจากการโอน จำหน่าย ยักย้าย ปกปิด หรือซ่อนเร้นทรัพย์สินเกี่ยวกับการกระทำผิด

เมื่อวิเคราะห์ มาตราการป้องกันและปราบปรามการฟอกเงินตามพระราชบัญญัตินี้โดยอาศัยกลไกการรายงานธุรกรรมการเงิน และรายงานแสดงตัวตนผู้ทำธุรกรรมซึ่งเป็นฐานข้อมูลจากผู้มีหน้าที่รายงาน โดยเฉพาะอย่างยิ่งสถาบันการเงินซึ่งประกอบกิจการเกี่ยวกับกิจกรรมทางการเงินเป็นปกติธุระและทำหน้าที่เป็นสื่อกลางในการทำธุรกรรมทางการเงินระหว่างบุคคล ดังนั้นผู้มีหน้าที่รายงานจึงถือเป็นด่านหน้าอันสำคัญต่อกลไกการป้องกันและปราบปรามการฟอกเงิน แต่เมื่อวิเคราะห์เปรียบเทียบกับคุณลักษณะเฉพาะของเงินสกุลเข้ารหัส ที่ไม่มีข้อจำกัดในการระบุตัวตนผู้ใช้งาน อีกทั้งระบบนิเวศที่ดำเนินการบนระบบฐานข้อมูลสาธารณะแบบกระจายศูนย์ ไม่มีหน่วยงานใดกำกับดูแล จึงเป็นช่องว่างทางกฎหมายที่สำคัญในการเข้าถึงตัวตนของผู้ใช้งาน ในการทำธุรกรรมเงินสกุลเข้ารหัส ซึ่งหมายรวมถึงฐานข้อมูลของเส้นทางการทำธุรกรรม จึงเป็นประเด็นมาตรการทางกฎหมายที่พึงศึกษาค้นหาแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อไป

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

2.6.2 พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล

กฎหมายฉบับนี้ถูกตราขึ้นในลักษณะพระราชกำหนดในปี 2018 (พ.ศ. 2561) จึงเป็นการแสดงถึงความจำเป็นเร่งด่วนในการตรากฎหมาย เพื่อกำหนดให้มีกลไกในการกำกับดูแลรักษาเสถียรภาพทางการเงินและระบบเศรษฐกิจโดยรวมของประเทศ จากการนำสินทรัพย์ดิจิทัลมาใช้เป็นเครื่องมือในการระดมทุนต่อประชาชน เป็นสื่อกลางในการแลกเปลี่ยน รวมถึงนำมาซื้อขายแลกเปลี่ยนในศูนย์ซื้อขายสินทรัพย์ดิจิทัล แต่ยังไม่มีกฎหมายที่กำกับดูแลการดำเนินกิจกรรมดังกล่าว ทั้งนี้เจตนารมณ์ของพระราชกำหนดฉบับนี้ เพื่อกำกับดูแลการระดมทุนผ่านสินทรัพย์ดิจิทัล การประกอบธุรกิจและการดำเนินกิจการเกี่ยวกับสินทรัพย์ดิจิทัล ส่งเสริมการนำเทคโนโลยีมาพัฒนาเศรษฐกิจและสังคมอย่างหยั่งยืน คุ้มครองผู้ลงทุนมิให้ถูกฉ้อโกงหรือถูกหลอกลวงจากผู้ไม่สุจริต การป้องกันการนำสินทรัพย์ดิจิทัลไปใช้สนับสนุนธุรกรรมที่ผิดกฎหมาย รวมถึงดูแลการซื้อขายในศูนย์ซื้อขายสินทรัพย์ดิจิทัลให้มีความเป็นธรรม โปร่งใส และตรวจสอบได้ (วสันต์ เทียนหอม, 2018)

พระราชกำหนดได้บัญญัติประเภทสินทรัพย์ดิจิทัล ประกอบด้วย (1) คริปโตเคอเรนซี หมายถึง หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะเป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และ (2) โทเคนดิจิทัล หมายถึง หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีวัตถุประสงค์เพื่อการกำหนดสิทธิของบุคคลในการเข้าร่วมลงทุนในโครงการหรือกิจการใด หรือกำหนดสิทธิในการได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใดที่เฉพาะเจาะจงตามที่กำหนดในข้อตกลงระหว่างผู้ออกและผู้ถือ ทั้งนี้เพื่อป้องกันมิให้เกิดความซ้ำซ้อนของกฎหมาย จึงบัญญัติมิให้หลักทรัพย์ตามพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ที่อยู่ในรูปของหน่วยข้อมูลอิเล็กทรอนิกส์ ไม่เป็นสินทรัพย์ดิจิทัลตามพระราชกำหนดนี้ (พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561, 2018)

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ในฐานะหน่วยงานที่มีอำนาจในการกำกับและควบคุมเกี่ยวกับการประกอบธุรกิจสินทรัพย์ดิจิทัล อันได้แก่ (1) ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (2) นายหน้าซื้อขายสินทรัพย์ดิจิทัล และ (3) ผู้ค้าสินทรัพย์ดิจิทัล รวมถึงการเสนอขายสินทรัพย์ดิจิทัลใหม่ต่อประชาชน การป้องกันการนำคริปโตเคอเรนซีที่ไม่มีแหล่งที่มาอย่างชัดเจนมาใช้ในการทำธุรกรรม โดยกำหนดให้ผู้ประกอบธุรกิจเกี่ยวกับสินทรัพย์ดิจิทัลมีหน้าที่ลักษณะเช่นเดียวกับสถาบันการเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน รวมถึงการป้องกันการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายสินทรัพย์ดิจิทัล ในทำนองเดียวกับการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์

ดังนั้น จึงอาจกล่าวได้ว่าระบบกฎหมายไทยได้กำหนดสถานภาพของเงินสกุลเข้ารหัสหรือสินทรัพย์ดิจิทัลเทียบเคียงในทำนองเดียวกับหลักทรัพย์เพื่อการลงทุน เนื่องจากโครงสร้างของ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

กฎหมายมีบทบัญญัติในการกำกับและควบคุม ตามแนวปฏิบัติของสำนักงานกำกับหลักทรัพย์และตลาดหลักทรัพย์ซึ่งเป็นผู้มีหน้าที่และอำนาจดูแลตามกฎหมาย เช่น คริปโตเคอเรนซีเปรียบเทียบเสมือนหลักทรัพย์ และโทเคนดิจิทัลเปรียบเสมือนใบสำคัญแสดงสิทธิที่จะซื้อหุ้นสามัญ (warrant) รวมถึงการเสนอขายโทเคนดิจิทัลที่ออกใหม่ต่อประชาชน (Initial coin offering – ICO) ก็มีแนวปฏิบัติทำนองเดียวกับการเสนอขายหุ้นใหม่ต่อประชาชน (Initial public offering – IPO) ทั้งนี้ประเด็นที่แสดงความชัดเจนในแนวปฏิบัติทำนองเดียวกัน คือการป้องกันการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขาย และการกำหนดให้ผู้ประกอบธุรกิจเกี่ยวกับสินทรัพย์ดิจิทัล เป็นสถาบันการเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน นอกจากนี้พระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19) พ.ศ.2561 ได้บัญญัติเพิ่มเติม มาตรา 40(4) ซึ่งเป็นมาตราเกี่ยวประเภทเงินได้พึงประเมินที่มีแหล่งที่มาจากเงินทุน โดยเพิ่มเติมมาตรา 40(4)(ช) เงินส่วนแบ่งกำไรหรือผลประโยชน์อื่นใดในลักษณะเดียวกันที่ได้จากการถือหรือครอบครองโทเคนดิจิทัล และมาตรา 40(4)(ฌ) ผลประโยชน์ที่ได้รับจากการโอนคริปดตเคอเรนซีหรือโทเคนดิจิทัล ทั้งนี้เฉพาะซึ่งตีราคาเป็นเงินได้เกินกว่าที่ลงทุน จึงมีลักษณะเงินได้เข้าข่ายผลประโยชน์ทำนองเดียวกับหลักทรัพย์หรือเงินลงทุน ในรูปแบบของเงินส่วนแบ่งกำไรหรือเงินปันผล และเงินส่วนเกินกว่าเงินลงทุน (พระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19) พ.ศ.2561, 2018)

2.6.3 พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ

เนื่องจากปัญหาการขาดเครื่องมือทางกฎหมายที่ใช้บังคับ เพื่อดำเนินคดีกับการกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติได้อย่างมีประสิทธิภาพ ประกอบกับประเทศไทยได้ลงนามในอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร จึงได้ตราพระราชบัญญัตินี้เพื่ออนุวัติตามอนุสัญญาดังกล่าวในการกำหนดลักษณะความผิดให้ครอบคลุมการประกอบอาชญากรรมที่มีลักษณะเป็นองค์กรอาชญากรรมข้ามชาติ รวมทั้งกำหนดวิธีการสืบสวน สอบสวนการกระทำความผิดซึ่งมีลักษณะเฉพาะ (สุทธมาศ จันทร์แดง, 2013)

กฎหมายได้บัญญัติ การกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ โดยอนุวัติให้สอดคล้องกับอนุสัญญาสหประชาชาติเพื่อต่อต้านอาชญากรรมข้ามชาติที่จัดตั้งในลักษณะองค์กร ปี 2000 โดย *“องค์กรอาชญากรรม”* หมายถึง คณะบุคคลตั้งแต่สามคนขึ้นไปที่รวมตัวกันช่วงระยะเวลาหนึ่งและร่วมกันกระทำการใด โดยมีวัตถุประสงค์เพื่อกระทำความผิดร้ายแรงและเพื่อได้มาซึ่งผลประโยชน์ทางการเงิน ทรัพย์สิน หรือผลประโยชน์ทางวัตถุอย่างอื่นไม่ว่าโดยทางตรงหรือทางอ้อม และ *“องค์กรอาชญากรรมข้ามชาติ”* หมายถึง องค์กรอาชญากรรมที่มีการกระทำความผิดในเขตแดนของรัฐมากกว่าหนึ่งรัฐ หรือกระทำความผิดในรัฐหนึ่งแต่กระทำการ

ตระเตรียม การวางแผน การสั่งการ การสนับสนุนหรือการควบคุมการกระทำความผิดได้กระทำในอีกรัฐหนึ่ง หรือกระทำความผิดในรัฐหนึ่งแต่เกี่ยวข้องกับองค์กรอาชญากรรมที่มีการกระทำความผิดมากกว่าหนึ่งรัฐ หรือกระทำความผิดในรัฐหนึ่งแต่ผลของการกระทำที่สำคัญเกิดขึ้นในอีกรัฐหนึ่ง โดยการกระทำผิดดังกล่าวเป็น *“ความผิดร้ายแรง”* ซึ่งเป็นความผิดอาญาที่กฎหมายกำหนดโทษจำคุกขั้นสูงตั้งแต่สี่ปีขึ้นไปหรือโทษสถานที่หนักกว่านั้น ทั้งนี้ผู้ที่เข้าข่ายกระทำความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ เมื่อผู้นั้นเป็นสมาชิกหรือเป็นเครือข่ายขององค์กรอาชญากรรมข้ามชาติหรือสบคบกันตั้งแต่สองคนขึ้นไป เพื่อกระทำความผิดร้ายแรงอันเกี่ยวข้องกับองค์อาชญากรรมข้ามชาติ หรือมีส่วนร่วมกระทำการใดๆไม่ว่าโดยทางตรงหรือทางอ้อมในการดำเนินกิจกรรม โดยรู้ถึงเจตนาที่จะกระทำผิดร้ายแรงขององค์อาชญากรรมข้ามชาติ หรือจัดการ สั่งการ ช่วยเหลือ ให้คำปรึกษาโดยรู้ถึงเจตนาที่จะกระทำผิดร้ายแรงขององค์อาชญากรรมข้ามชาติ (สุพัตรา แผนวิชิต, 2019)

ทั้งนี้ กลไกการป้องกันและปราบปราบความผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ โดยการใช้เทคนิควิธีการสืบสวนสอบสวนพิเศษซึ่งถือว่าเป็นการกระทำที่ชอบด้วยกฎหมายเพื่อให้การบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพและสามารถนำผู้กระทำผิด หรือผู้บงการมาลงโทษได้ เช่น (1) การเข้าถึงและได้มาซึ่งข้อมูลข่าวสารอันเป็นการกระทบสิทธิส่วนบุคคลหรือสิทธิอื่นใด ในกรณีมีที่เหตุอันควรเชื่อว่าข้อมูลข่าวสารเหล่านั้นถูกจัดส่ง หรือสื่อสารโดยวิธีการใดรวมถึงสื่อสารทางอิเล็กทรอนิกส์เพื่อประโยชน์จากการกระทำผิด (2) การปฏิบัติการอำพราง (Undercover) โดยการดำเนินการเพื่อปิดบังสถานะ หรือวัตถุประสงค์ของการดำเนินการโดยลวงผู้อื่นให้เข้าใจไปในทางอื่นหรือเพื่อมิให้รู้ความจริงเกี่ยวกับการปฏิบัติหน้าที่ของเจ้าพนักงาน (3) การเคลื่อนย้ายภายใต้การควบคุม (Controlled delivery) โดยวิธีการอนุญาตให้ของผิดกฎหมายหรือต้องสงสัยผ่านออกไป หรือเข้าไปสู่เขตแดนของอีกรัฐหนึ่ง โดยรับรู้และอยู่ภายใต้การติดตามดูแลของเจ้าพนักงานเพื่อการสืบสวนสอบสวนความผิดและเพื่อระบุตัวตนบุคคลที่เกี่ยวข้องกับการกระทำผิดนั้น และ (4) การสะกดรอย (Electronic surveillance) โดยเจ้าพนักงานอาจใช้เครื่องมือสื่อสารอิเล็กทรอนิกส์ หรือด้วยวิธีการอื่นใดเฉพาะในการสะกดรอยผู้ต้องสงสัยเพื่อสืบสวน จับกุม แสวงหาและรวบรวมพยานหลักฐาน เป็นต้น (พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556, 2013)

ดังนั้น ผู้กระทำผิดที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน มีลักษณะกระทำการเข้าข่ายการมีส่วนร่วมในการกระทำผิดขององค์กรอาชญากรรมข้ามชาติ โดยคุณสมบัติเฉพาะของเงินสกุลเข้ารหัส สามารถดำเนินการโอนมูลค่าข้ามเขตประเทศแบบไร้พรมแดนและการดำเนินการ เพื่อกลบเกลื่อนร่องรอยเส้นทางธุรกรรมผ่านศูนย์บริการแปรสภาพเงินสกุลเข้ารหัส ซึ่งมีลักษณะเข้าองค์ประกอบผู้กระทำผิดฐานมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ

เนื่องจากการสบคบกันตั้งแต่สองคนขึ้นไป เพื่อกระทำการหรือมีส่วนร่วมกระทำการฟอกเงินซึ่งเป็นถือความผิดร้ายแรงตามพระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน จึงถือเป็นอีกหนึ่งช่องทางในการบังคับใช้วิธีการสืบสวนสอบสวนพิเศษเพื่อเพิ่มประสิทธิภาพการสืบวน จับกุม แสวหารวบรวมพยานหลักฐาน รวมถึงการเข้าถึงตัวบุคคลผู้กระทำผิด อย่างไรก็ตามประเด็นการเพิ่มอำนาจการสอบสวนพิเศษทางกฎหมาย ก็ยังไม่มีหลักประกันที่เพียงพอต่อการสืบสวนสอบสวนที่ต้องอาศัยเทคโนโลยี่ขั้นสูงในการตรวจสอบสืบค้นระบบนิเวศเงินสกุลเข้ารหัส

2.7 งานวิจัยที่เกี่ยวข้อง

2.7.1 งานวิจัยเกี่ยวกับมาตรการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

2.7.1.1 Frick (2019) หัวเรื่อง *"Virtual and Cryptocurrencies-Regulatory and Anti-money Laundering Approaches in the European Union and in Switzerland"* มีวัตถุประสงค์การศึกษา กฎระเบียบเกี่ยวกับมาตรการป้องกันการฟอกเงินกับพลวัตของบริบทของเงินสกุลเข้ารหัส โดยวิธีการวิจัยเชิงเอกสาร (Documentary Research) จากมาตรการกฎหมายยุโรปในแนวปฏิบัติการป้องกันการฟอกเงินฉบับที่ 5 (EU-AMLD5) ซึ่งเพิ่มบทบัญญัติการกำกับ *"เงินเสมือน (Virtual Currency)"* และกฎระเบียบของสำนักงานกำกับหลักทรัพย์และตลาดหลักทรัพย์แห่งยุโรป (European Securities and Markets Authority) ธนาคารกลางยุโรป (European Banking Authority) รวมถึงกฎหมายของประเทศสวิตเซอร์แลนด์

ทั้งนี้ AMLD5 ได้นิยาม *"เงินเสมือน (Virtual Currency)"* หมายถึงมูลค่าของหน่วยข้อมูลดิจิทัลซึ่งไม่ได้ออกหรือรับรองโดยธนาคารกลางหรือหน่วยงานรัฐ และไม่มีสถานะเป็นเงินตราตามกฎหมาย แต่สามารถเป็นสื่อกลางในการแลกเปลี่ยน โอนมูลค่า สะสมมูลค่า และซื้อขายทางระบบออนไลน์ได้ ในขณะที่สำนักงานกำกับตลาดเงินของประเทศสวิตเซอร์แลนด์ (Swiss Financial Markets Authority – FINMA) ได้ให้นิยามแยกเป็น 2 ลักษณะ คือ Tokens เป็นสินทรัพย์ดิจิทัลที่มีวัตถุประสงค์เพื่อการชำระเงินค่าสินค้าและบริการ รวมถึงการสื่อกลางแลกเปลี่ยนและโอนมูลค่าทั้งขณะปัจจุบันหรือในอนาคต สำหรับเงินสกุลเข้ารหัส (Cryptocurrency) ถูกระบุลักษณะสำคัญคือเป็นหน่วยมูลค่าที่ไม่สามารถเรียกชดเชยความเสียหายจากผู้ใดได้ ในขณะที่ Tokens สามารถจะเรียกชดเชยจากผู้นำเสนอขายได้ จึงเป็นประเด็นความแตกต่างในสถานภาพทางกฎหมายที่สำคัญ ซึ่งเป็นกรอบแนวคิดเดียวกับธนาคารเพื่อการชำระเงินระหว่างประเทศ (Bank for International Settlements – BIS) ได้ให้คุณลักษณะสำคัญของเงินสกุลเข้ารหัส คือ เป็นรูปแบบดิจิทัลที่จัดทำขึ้นโดยเอกชนและไม่มีผู้รับประกันความเสียหาย

นอกจากนี้ AMLD5 ได้ขยายความแตกต่างระหว่างเงินสกุลเข้ารหัสกับเงินอิเล็กทรอนิกส์ (Electronic Money) ซึ่งนิยามตามแนวปฏิบัติ Directive 2009/110/EC ที่มี

วัตถุประสงค์เพื่อการใช้หมุนเวียนเฉพาะกลุ่มจำกัดหรือกลุ่มผู้ใช้บริการเกมส์ออนไลน์เท่านั้น ทั้งนี้ AMLD5 ได้กำหนดมาตรการป้องกันการฟอกเงิน โดยเพิ่มการกำกับให้ถือเป็นหน่วยงานที่ต้องถูกควบคุมตามแนวปฏิบัติ ซึ่งหมายถึงผู้ให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัส (Cryptocurrency Exchanger) กับเงินสกุลเข้ารหัสอื่นและเงินตราทั่วไป รวมถึงผู้ให้บริการดูแลกระเป๋าเงิน (Custodian Wallet Provider) ซึ่งเป็นผู้ดูแลรหัสเปิดกระเป๋าส่วนบุคคลแทนบุคคลอื่น เพื่อการทำธุรกรรมการโอนมูลค่าการถือครองและส่งมอบตามคำสั่งแทนลูกค้า อย่างไรก็ตามสหภาพยุโรปยังยึดถือกรอบแนวปฏิบัติการป้องกันการฟอกเงินในลักษณะ *“ผู้เฝ้าประตู (Gate Keeper)”* กล่าวคือจะมุ่งกำกับดูแลการหมุนเวียนเงินเฉพาะเมื่อทำธุรกรรมแปลงเงินสกุลเข้ารหัสเป็นเงินตราทั่วไป หรือการแปลงเป็นสินทรัพย์ที่มีตัวตนเป็นสำคัญ

ในขณะที่รัฐบาลสวิตมีกรอบแนวปฏิบัติการป้องกันการฟอกเงินที่หลากหลาย ขึ้นอยู่กับระเบียบการกำกับดูแลของแต่ละองค์กร (Self-Regulatory Organization) โดยมีหลักการกำกับดูแลบนพื้นฐานความเป็นกลางทางเทคโนโลยี่ (Technology Neutral) ด้วยการไม่แบ่งแยกการกำกับตามรูปแบบของเทคโนโลยี่ แต่ให้ความสำคัญต่อผลิตภัณฑ์ประยุกต์ทางการเงินของเทคโนโลยี่นั้น โดยหากผลิตภัณฑ์ทางการเงินเข้าข่ายเป็นสื่อกลางในการชำระเงิน ก็จะอยู่ในบังคับมาตรการป้องกันการฟอกเงินของตราสารการเงิน เช่น ผู้เสนอขายเงินสกุลเข้ารหัสรายใหม่ ผู้ให้บริการแลกเปลี่ยน ผู้ดูแลกระเป๋าเงิน ยกเว้น นักขุดซึ่งเป็นผู้ได้รับเงินสกุลเข้ารหัสจากระบบโดยตรงไม่ถือเป็นการชำระเงิน ดังนั้น หากผลิตภัณฑ์ประยุต์จากเทคโนโลยี่บนระบบปฏิบัติการบล็อกเชนเช่นเดียวกันแต่ผลิตภัณฑ์ประยุกต์เข้าข่ายเป็นสินทรัพย์ (Asset Token) หรือเป็นสิทธิประโยชน์ (Utility Token) ก็จะอยู่ภายใต้แนวปฏิบัติขององค์กรที่เกี่ยวข้อง เว้นแต่จะได้มีการตรากฎหมายเฉพาะขึ้นและยกเว้นหลักการความเป็นกลางทางเทคโนโลยี่

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

2.7.1.2 Campbell-Verduyn (2018) หัวเรื่อง *“Crypto-coins and Global Anti-money Laundering Governance”* มีวัตถุประสงค์การศึกษา มาตรการสากลในการป้องกันการฟอกเงินโดยเงินสกุลเข้ารหัสที่สมดุลอย่างเหมาะสม ระหว่างการป้องกันความเสี่ยงในระดับสากลจากการใช้ระบบเงินสกุลเข้ารหัสเพื่อธุรกรรมผิดกฎหมาย กับการสร้างโอกาสทางธุรกิจของระบบการเงินโลก แต่ด้วยคุณลักษณะเฉพาะของเงินสกุลเข้ารหัสที่สามารถทำธุรกรรมปิดบังตัวตนข้ามพรมแดนด้วยความรวดเร็ว ก่อให้เกิดความเสี่ยงจากการใช้เงินสกุลเข้ารหัสที่ยิ่งกว่าระบบเงินตราทั่วไป อีกทั้ง มาตรการทางกฎหมายของแต่ละประเทศมีการกำกับดูแลเงินสกุลเข้ารหัสที่แตกต่างกันก่อให้เกิดช่องว่างของการบังคับใช้มาตรการทางกฎหมาย ต่อเงินสกุลเข้ารหัสที่สามารถโอนข้ามเขตแดนประเทศได้อย่างรวดเร็ว

จากการศึกษามาตรการป้องกันการฟอกเงินของระบบเงิน ซึ่งมีแนวปฏิบัติมุ่งตรวจสอบกระแสเงินหมุนเวียนของธุรกรรมการเงินจากแหล่งกระทำผิดกฎหมาย ด้วยการกำกับดูแลรายการธุรกรรมการเงินภายใต้กรอบของกฎระเบียบ เพื่อป้องกันผลกระทบต่อระบบสถาบันการเงิน โดยแนวปฏิบัติในการแสดงตัวตนของผู้ใช้บริการสถาบันการเงิน ซึ่งจะต้องระบุข้อมูลส่วนบุคคลที่เพียงพอต่อการพิสูจน์ (Know Your Customer – KYC) และการรายงานผลการตรวจประเมินรายการธุรกรรมการเงินที่ต้องสังสัย เมื่อพบเงินสกุลเข้ารหัสมีพื้นฐานการทำธุรกรรมเป็นไปในทิศทางผิดปกติ กล่าวคือ มาตรการปัจจุบันมุ่งกำกับข้อมูลผู้ใช้บริการเพื่อนำไปสู่การตรวจสอบสืบค้นธุรกรรมต้องสงสัยหรือเส้นทางการเงินต้องสงสัยต่อไป ในขณะที่เงินสกุลเข้ารหัสอยู่บนระบบฐานข้อมูลสาธารณะแบบกระจายศูนย์ จึงสามารถเข้าถึงการตรวจสอบเส้นทางธุรกรรมการได้อย่างชัดเจนโดยไม่ต้องพิสูจน์เพียงแต่ต้องดำเนินตรวจสอบสืบค้นหาตัวตนของผู้ใช้งานที่แท้จริงต่อไป อย่างไรก็ตามด้วยปริมาณธุรกรรมจำนวนมากในระบบนิเวศเงินสกุลเข้ารหัส ซึ่งข้ามเขตแดนประเทศและมีความเคลื่อนไหวอย่างรวดเร็วต่อเนื่อง ดังนั้นธุรกรรมที่ถูกบันทึกอย่างชัดเจนในฐานข้อมูลสาธารณะจำนวนมาก จึงไม่เป็นการเอื้อต่อมาตรการป้องกันการฟอกเงิน ถ้าไม่ทราบตัวตนผู้ใช้งานหรือรหัสที่ตั้งในระบบนิเวศเช่นกัน

ประเด็นปัญหาต่อการกำกับดูแลพิสูจน์ความมีตัวตนของผู้ใช้งานเงินสกุลเข้ารหัสในกระบวนการฟอกเงิน ตั้งแต่ผู้กระทำผิดสามารถนำเงินที่ได้จากการกระทำผิดเข้าสู่ระบบเงินสกุลเข้ารหัสได้โดยไม่ต้องแสดงตัวตน และในขั้นตอนการกลบเกลื่อนร่องรอยเส้นทางธุรกรรมดังกล่าวจะถูกกระจายแยกย่อยออกไปยังผู้รับโอนอีกหลายรายที่ไม่สามารถระบุตัวตน หรือแสดงสัณญาณเตือนธุรกรรมต้องสังสัยได้ รวมถึงขั้นตอนการแปลงเป็นเงินตราปกติยังมีช่องทางการให้บริการที่เชื่อมโยงกับระบบนิเวศเงินสกุลเข้ารหัสโดยไม่ต้องแสดงตัวตนเช่นกัน นอกจากนี้ปัญหาความรวดเร็วของการทำธุรกรรม ส่งผลให้ผู้กระทำผิดสามารถโอนเงินสกุลเข้ารหัสข้ามเขตประเทศจากประเทศที่ก่อฐานความผิดไปยังประเทศอื่น และในขั้นตอนการกลบเกลื่อนร่องรอยก็มีเวลาเพียงระยะสั้นในการดำเนินหยุดยั้งรายการธุรกรรมต้องสงสัย สุดท้ายการแปลงเงินสกุลเข้ารหัสเป็นเงินตราปกติก็สามารถเคลื่อนย้ายในระบบการเงินสากลไปยังประเทศที่มีมาตรการกำกับที่เบาบางได้

ดังนั้น ประเด็นปัญหาสำคัญอีกประการคือ ความแตกต่างระหว่างมาตรการกำกับเงินสกุลเข้ารหัสของแต่ละประเทศ ก่อให้เกิดช่องว่างทางกฎหมายและการบังคับใช้กฎหมายระหว่างประเทศ หรือกล่าวอีกนัยหนึ่งว่ามาตรการกำกับดูแลเงินสกุลเข้ารหัสระหว่างประเทศที่มีประสิทธิภาพจะเกิดขึ้นไม่เลย หากปราศจากซึ่งความร่วมมือของแต่ละประเทศในการนำไปสู่ภาคปฏิบัติ ดังเช่นบทบาทหน้าที่ขององค์กรระหว่างประเทศ FATF ได้พัฒนาข้อแนะนำเพื่อการป้องกันและปราบปรามการฟอกเงิน 40+9 ประการ โดยในปี 2003 ได้ทบทวนปรับเปลี่ยนกรอบแนวคิดในการป้องกันการฟอกเงินจากการมุ่งปฏิบัติตามกฎระเบียบ (Rules Based Approach) เป็นกรอบแนวคิดการกำกับ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ดูแลตามระดับความเสี่ยง (Risk Based Approach) ส่งผลให้เกิดความยืดหยุ่นในการวางมาตรการป้องกันสอดคล้องกับบริบทความเสี่ยงของแต่ละประเทศ ลักษณะของการกระทำผิด รวมถึงทรัพย์สินที่ถูกนำมาเป็นเครื่องในกระบวนการฟอกเงิน และในปี 2013 ได้ทำการศึกษาบริบทของเงินสกุลเข้ารหัส และแสดงทัศนะว่าเงินสกุลเข้ารหัสมีรูปแบบเสมือนเงินอิเล็กทรอนิกส์ที่โอนย้ายบนระบบอินเตอร์เน็ต แต่มีความซับซ้อนทางเทคนิคบนระบบนิเวศที่เกี่ยวข้องกับบุคคลผู้เกี่ยวข้องข้ามเขตอำนาจต่างรัฐ ซึ่งมาตรการที่ดำเนินการอยู่ไม่เพียงพอต่อการป้องกันการฟอกเงินโดยเงินสกุลเข้ารหัส จนกระทั่งในปี 2015 FATF ได้นำประเด็นบริบทของเงินสกุลเข้ารหัสร่วมทบทวนและปรับปรุงข้อแนะนำ 40+9 ประการฉบับใหม่ขึ้น โดยขยายขอบเขตการกำกับดูแลเสริมมาตรการควบคุมไปถึงบุคคลที่เกี่ยวข้องกับบริบทในระบบนิเวศเงินสกุลเข้ารหัส พร้อมทั้งให้คำแนะนำแก่รัฐสมาชิกเพื่อพัฒนาการตรากฎหมายและกฎระเบียบที่เกี่ยวข้องกับเงินสกุลเข้ารหัสให้สอดคล้องและสนับสนุนการป้องกันการฟอกเงินโดยเงินสกุลเข้ารหัสในระดับสากล อันประกอบด้วยแนะนำให้รัฐสมาชิดจัดตั้งหน่วยประสานงาน เพื่อเป็นกลไกในการแบ่งปันสารสนเทศพฤติกรรมความเสี่ยงที่อาจเกิดขึ้นจากระบบนิเวศเงินสกุลเข้ารหัสและแนะนำให้หน่วยงานกำกับของรัฐสามาชิกได้เฝ้าติดตามวิเคราะห์ระดับความเสี่ยงของผู้ใช้งานเงินสกุลเข้ารหัสที่อาจเข้าข่ายต้องสงสัย โดยเฉพาะผู้ใช้งานที่อาจเชื่อมโยงกับการใช้บริการทางการเงินกับระบบสถาบันการเงิน

ในการศึกษา ได้นำเสนอสรุปความเห็นต่อการประเมินประสิทธิผลของข้อแนะนำ FATF ฉบับปรับปรุงปี 2015 เนื่องจากกรอบแนวคิดเป็นเพียงข้อแนะนำไม่มีสภาพบังคับให้ดำเนินการตามมาตรการกำกับป้องกันการฟอกเงิน แต่ในขณะเดียวกันก็ยอมรับหลักการระบบการเงินเสรีที่จะเคลื่อนย้ายเงินทุนในทำนองเดียวกับข้อแนะนำการกำกับเงินสกุลเข้ารหัส ที่มีข้อแนะนำให้ดำเนินมาตรการลดความเสี่ยงจากการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ที่ยังคำนึงถึงโอกาสที่จะได้รับประโยชน์จากการประยุกต์ใช้งานระบบปฏิบัติการบล็อกเชน รวมถึงข้อแนะนำให้รัฐสมาชิกนำมาตรการป้องกันการฟอกเงินสกุลเข้ารหัสไปปรับใช้ แม้ว่ารัฐดังกล่าวจะมีมาตรการต้องห้ามทางกฎหมายกับธุรกรรมเงินสกุลเข้ารหัสในประเทศก็ตาม แต่เนื่องจากต้นทุนการดำเนินการตามมาตรการป้องกันการฟอกเงินโดยเงินสกุลเข้ารหัสก่อภาระต้นทุนค่อนข้างสูง เมื่อเปรียบเทียบกับประโยชน์ที่จะได้รับ ข้อแนะนำจึงยังไม่สัมฤทธิผล

นอกจากนี้ข้อแนะนำได้เสนอให้สถาบันการเงิน และหน่วยงานที่ไม่ใช่สถาบันการเงินทำการประเมินความเสี่ยงต่อการฟอกเงินเมื่อทำธุรกิจเกี่ยวข้องกับเงินสกุลเข้ารหัส โดยแนะนำให้หน่วยงานที่เกี่ยวข้อง ร่วมกันจัดทำนโยบายและแนวปฏิบัติในการประเมินความเสี่ยงของธุรกรรม รวมถึงกระบวนการติดตามธุรกรรมดังกล่าวอย่างเหมาะสม ที่เรียกว่า Customer Due Diligence – CDD ซึ่งยังมีประเด็นปัญหาเกี่ยวกับการจัดการฐานข้อมูล และกฎระเบียบเพื่อการเข้าถึงข้อมูลส่วนบุคคล รวมถึงให้ข้อแนะนำแก่หน่วยงานกำกับของรัฐได้มีส่วนร่วมในการลดภาระและส่งเสริมการ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ปฏิบัติงานของกิจการที่เกี่ยวข้องกับเงินสกุลเข้ารหัส โดยใช้มาตรการขออนุญาตและให้อนุญาตแต่ผู้ประสงค์จะประกอบกิจการที่เกี่ยวข้องกับเงินสกุลเข้ารหัส เพื่อรับผิดชอบหน้าที่ในการระบุตัวตนของลูกค้ารวมถึงการเก็บรวบรวมข้อมูลธุรกรรมต้องสังสัย ซึ่งยังมีประเด็นข้อสงสัยถึงความพร้อมของผู้ประกอบกิจการ

และอีกข้อแนะนำให้พัฒนาเทคโนโลยี่นวัตกรรมระบบปฏิบัติการ เพื่อการตรวจสอบข้อมูลยืนยันตัวตนของผู้ใช้งานในลักษณะโปรแกรมประยุกต์เชื่อมต่อ (Application Programming Interfaces – API) กับระบบนิเวศเงินสกุลเข้ารหัส เพื่อใช้เทคโนโลยี่เป็นเครื่องมือเชื่อมโยงผู้ใช้งานกับหน่วยงานกำกับของรัฐ ซึ่งเป็นประเด็นข้อโต้แย้งที่ขัดต่อหลักการพื้นฐานของเงินสกุลเข้ารหัสที่กลไกการปฏิบัติงานในรูปแบบไม่มีศูนย์กลางการควบคุม

สำหรับข้อแนะนำ ในการขยายขอบเขตการกำกับตามาตรการป้องกันการฟอกเงินไปสู่บุคคลที่เกี่ยวข้องกับระบบนิเวศเงินสกุลเข้ารหัส โดยให้ความสำคัญมุ่งกำกับผู้ใช้งานในระบบ และเส้นทางธุรกรรมระหว่างผู้ใช้งาน ส่งผลให้เกิดช่องว่างทางกฎหมายต่อนักขุดซึ่งเป็นผู้ใช้งานในระบบเช่นกัน แต่จะได้รับเงินสกุลเข้ารหัสจากระบบโดยตรงและไม่มีเส้นทางธุรกรรมในระบบ แต่นักขุดถือเป็นบุคคลที่มีความเสี่ยงต่อกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสเช่นกัน

2.7.1.3 จากงานวิจัยเกี่ยวกับมาตรการป้องกันการฟอกเงินโดยเงินสกุลเข้ารหัสที่ได้ทำการศึกษา ผู้วิจัยสามารถสรุปเป็นประเด็นข้อพิจารณาเพื่อเพิ่มประสิทธิภาพแนวทางการป้องกันการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในกระบวนการฟอกเงิน ดังนี้

(1) เนื่องด้วยคุณลักษณะเฉพาะของเงินสกุลเข้ารหัส ที่สามารถทำธุรกรรมบนระบบนิเวศโดยไร้พรมแดน หรือข้ามขอบเขตประเทศได้โดยสะดวก ดังนั้นมาตรการสำคัญจึงขึ้นอยู่กับความร่วมมือของนานาประเทศ ในการแลกเปลี่ยนประสบการณ์กรณีศึกษาการต่อต้านการฟอกเงินในรูปแบบของแต่ละประเทศ และความร่วมมือจัดทำแนวปฏิบัติที่เหมาะสมเพื่อการปฏิบัติงานที่สามารถรู้เท่าทันพัฒนาการของผู้กระทำผิด ที่จะดำเนินการฟอกเงินโดยอาศัยช่องว่างทางกฎระเบียบ (Carlisle, 2017; Jacquez, 2016) รวมถึงความร่วมมือในการออกกฎระเบียบและการบังคับกำกับธุรกรรมเงินสกุลเข้ารหัสในลักษณะที่เทียบเท่ากันระหว่างประเทศ (Campbell-Verduyn, 2018)

(2) การปรับกรอบแนวคิดในการวิเคราะห์ระดับความเสี่ยงของธุรกรรม พร้อมออกมาตรการกำกับที่เหมาะสม สามารถรักษาสมดุลระหว่างการจัดการความเสี่ยงกับประโยชน์ที่จะได้รับจากธุรกรรมเงินสกุลเข้ารหัสซึ่งอำนวยความสะดวกต่อการโอนมูลค่า ต้นทุนการดำเนินงานต่ำ รวมถึงสามารถขยายขอบข่ายการให้บริการแก่ผู้ที่เข้าไม่ถึงบริการทางการเงินของสถาบันการเงิน แทนการ

ปฏิเสธหรือต้องห้ามธุรกรรมที่ไม่สามารถพิสูจน์ตัวตนผู้ใช้งานได้ โดยเป็นการเพิ่มมาตรการกำกับผู้ใช้งานที่จะเข้าถึงระบบนิเวศเงินสกุลเข้ารหัส (Campbell-Verduyn, 2018; Carlisle, 2017)

(3) มาตรการอนุญาตให้เข้าถึงข้อมูลส่วนบุคคลของผู้ใช้งานต้องสงสัย ในระบบอินเตอร์เน็ตหรือสื่อสังคมออนไลน์ เมื่อระบบปฏิบัติการตรวจสอบคืบค้นเปรียบเทียบรหัสที่ตั้งของผู้ใช้งานเงินสกุลเข้ารหัสต้องสงสัยซึ่งไม่ระบุตัวตน เปรียบเทียบกับรหัสที่ตั้งของผู้ใช้งานในระบบงานอื่น (Hazar, 2019)

(4) การพัฒนาศักยภาพของผู้ทำหน้าที่รับผิดชอบ ในการกำกับดูแลป้องกันกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เนื่องจากเป็นนวัตกรรมทางเทคโนโลยี่การเงินซึ่งมีกลไกการทำงานในระบบนิเวศที่มีความซับซ้อนต้องอาศัยความรู้และความชี่ยวชาญในการใช้เครื่องมือโปรแกรมประยุกต์เพื่อการตรวจสอบสืบค้นฐานข้อมูลสาธารณะและการวิเคราะห์รหัสที่ตั้ง รวมถึงเส้นทางธุรกรรมต้องสงสัย (Campbell-Verduyn, 2018)

(5) การสร้างเครือข่ายความร่วมมือ ของกลุ่มกิจการที่เกี่ยวข้องในอุตสาหกรรมธุรกิจเงินสกุลเข้ารหัส เพื่อสร้างความร่วมมือในการเฝ้าระวัง แลกเปลี่ยนข้อมูลข่าวสารภายในกลุ่มอุตสาหกรรม รวมถึงให้ช่วยเหลือในการพัฒนาระบบจัดการความเสี่ยงที่เท่าทันสถานการณ์ (Carlisle, 2017)

2.7.1.4 กิจชัยยะ สุรารักษ์ (2020) หัวข้อ *“แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินสกุลเข้ารหัสในประเทศไทย: กรณีศึกษาบิตคอยน์”* มีวัตถุประสงค์ในการศึกษารูปแบบ สภาพปัญหาและสาเหตุของอาชญากรรมที่ใช้บิตคอยน์ แนวนโยบายทางกฎหมายที่เกี่ยวกับสกุลเงินสกุลเข้ารหัสที่มีอยู่ในประเทศไทยและต่างประเทศ รวมถึงมาตรการในการป้องกันอาชญากรรมที่ใช้บิตคอยน์ในฐานะสกุลเงินสกุลเข้ารหัสเป็นเครื่องมือในประเทศไทย โดยวิธีการค้นคว้าวิจัยเชิงเอกสารและการสัมภาษณ์เชิงลึก ทั้งนี้ผลการศึกษาพบว่า คุณสมบัติของบิตคอยน์ในการไม่เปิดเผยตัวตนผู้ใช้งานที่แท้จริง ความเป็นส่วนตัวและความรวดเร็วสอดคล้องกับสภาพสังคมและเทคโนโลยี่ในปัจจุบัน แต่กลับเป็นเครื่องมือชั้นดีที่อาชญากรนำไปใช้ในการก่ออาชญากรรมในรูปแบบต่างๆ ได้แก่ การใช้บิตคอยน์เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการที่ผิดกฎหมาย เช่น การค้ายาเสพติด การค้าอาวุธ การค้าอวัยวะ และบริการเอกสารราชการปลอม เป็นต้น การเรียกค่าไถ่จากการลักพาตัวเป็นบิตคอยน์ การระดมทุนของกลุ่มผู้ก่อการร้ายผ่านบิตคอยน์ การฟอกเงินด้วยบิตคอยน์ และการหลอกหลวงให้เหยื่อร่วมลงทุนในกิจการเกี่ยวกับบิตคอยน์ นอกจากนี้รูปแบบในการนำบิตคอยน์ไปใช้ในการก่ออาชญากรรม โดยมีลักษณะการดำเนินงานในก่ออาชญากรรมโดยตรงที่

ใช้บิตคอยน์เป็นเครื่องมือ และการใช้บิตคอยน์เป็นเครื่องมือในการก่ออาชญากรรมทางอ้อม เช่น การหลอกหลวงเหยื่อให้ร่วมลงทุนธุรกิจเกี่ยวกับบิตคอยน์

ดังนั้นด้วยคุณลักษณะเฉพาะของบิตคอยน์ซึ่งเป็นเงินสกุลเข้ารหัสแรก ในการปิดบังตัวตนผู้ใช้งานและความรวดเร็วในการโอนมูลค่า จึงกลายเป็นหนึ่งในเครื่องมือการก่ออาชญากรรมทั้งในลักษณะของอาชญากรรมทั่วไปและอาชญากรรมไซเบอร์ หรืออาชญากรรมที่ใช้ระบบนิเวศอินเตอร์เน็ตเป็นเครื่องมือในการกระทำความผิด ซึ่งจากรายงานผลการศึกษาดังกล่าวควรแก่การขยายผลการศึกษา ถึงรูปแบบอาชญากรรมที่นำผลประโยชน์จากการกระทำผิดไปสู่การใช้เงินสกุลเข้ารหัสเป็นเครื่องมือการฟอกเงินต่อไป

2.7.2 งานวิจัยเกี่ยวกับเทคนิคการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

2.7.2.1 Moser, Bohme, and Breuker (2013) หัวเรื่อง *"An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem"* มีวัตถุประสงค์การศึกษากระบวนการใช้บิตคอยน์เป็นเครื่องมือในการทำธุรกรรมฟอกเงิน และประเมินศักยภาพการกลบเกลื่อนร่องรอยธุรกรรมของผู้ให้บริการแปรสภาพบิตคอยน์ ทั้งนี้กระบวนการแปรสภาพเงินสกุลเข้ารหัสจะมีวัตถุประสงค์สำคัญ คือ การกลบเกลื่อนร่องรอยหรือตัดตอนความสัมพันธ์ของเส้นทางธุรกรรมระหว่างผู้โอนต้นทางกับผู้รับปลายทาง เนื่องจากระบบนิเวศบนระบบปฏิบัติการบล็อกเชนซึ่งเป็นฐานข้อมูลสาธารณะ จึงทำให้ผู้ใช้งานทุกรายสามารถเข้าทำการตรวจสอบข้อมูลการโอนระหว่างบุคคลจากรหัสที่ตั้งในรายการบันทึกข้อมูลแบบกระจายศูนย์ได้ อย่างไรก็ตามผู้ใช้บริการรายเดียวสามารถสร้างรหัสที่ตั้ง และกระเป๋าเงินอิเล็กทรอนิกส์ได้ไม่จำกัดจำนวน ผู้ใช้งานจึงสามารถสร้างโครงข่ายระบบการโอนมูลค่าของตนเองอย่างซับซ้อนได้ซึ่งเป็นการเพิ่มความยุ่งยากในการตรวจสอบขึ้นไปอีกชั้นหนึ่ง ในกรณีที่ผู้ใช้งานซึ่งมีโครงข่ายรหัสที่ตั้งของตนเอง สร้างกลุ่มพันธมิตรร่วมมือกันในการทำธุรกรรมโอนไขว้มูลค่าระหว่างกันในระบบนิเวศจะเพิ่มโอกาสการกลบเกลื่อนร่องรอยได้มากขึ้น โดยเฉพาะอย่างยิ่งถ้ากลุ่มพันธมิตรมีขนาดโครงข่ายรหัสที่ตั้งจำนวนมากขึ้นเท่าไร โอกาสการตัดตอนความสัมพันธ์ของเส้นทางธุรกรรมระหว่างต้นทางกับปลายทางก็ยิ่งมีประสิทธิภาพมากขึ้นเท่านั้น

ทั้งนี้ การวิจัยนี้ได้ออกแบบการศึกษาด้วยวิธีการทดลอง (Experiment) การฟอกเงินบิตคอยน์ผ่านผู้ให้บริการแปรสภาพบิตคอยน์กรณีศึกษา 3 ราย คือ Bitcoin Fog, BitLaundry และ Blockchain.info โดยการวิเคราะห์เส้นทางธุรกรรมที่แสดงรายการใน Blockchain.info ด้วยการติดตั้งโปรแกรมประยุกต์ที่เรียกว่า Gephi เชื่อมต่อกับระบบปฏิบัติการบล็อกเชนและฐานข้อมูลสาธารณะซึ่งจะแสดงผลเป็นกราฟระหว่างจุดโอนและเส้นทางการโอนระหว่างจุดโอน

Bitcoin Fog ให้บริการเฉพาะผู้ใช้บริการบนระบบ TOR และอนุญาตให้ผู้ใช้บริการใช้รหัสที่ตั้งโอนบิตคอยน์ฝากเข้ากระเป๋าเงินของผู้ให้บริการครั้งละไม่เกิน 5 รหัสที่ตั้ง และสามารถขอ

ระบุรหัสที่ตั้งรับโอนบิตคอยน์ได้สูงสุดไม่เกิน 20 รหัสที่ตั้ง ด้วยค่าบริการแบบซุ่มอัตราไม่คงที่อยู่ระหว่างร้อยละ 1 ถึง 3 ด้วยระยะเวลาดำเนินการ 6 ถึง 96 ชั่วโมง จากการวิเคราะห์กราฟเส้นทางธุรกรรมแสดงผลสรุปการทดลอง พบว่า ผู้ให้บริการใช้กลยุทธดำเนินการด้วยวิธีการกระจายธุรกรรมเป็นรายการย่อยจากหลายแหล่งแล้วรวบรวมเป็นธุรกรรมรายการใหญ่ เพื่อเตรียมการโอนให้ผู้รับปลายทาง ซึ่งรูปแบบการให้บริการนี้สามารถหลีกเลี่ยงการสืบค้นความสัมพันธ์ของเส้นทางการโอนระหว่างต้นทางกับปลายทางได้

BitLaundry มีลักษณะการให้บริการที่แตกต่างจาก Bitcoin Fog กล่าวคือไม่อนุญาตให้ผู้ใช้บริการโอนบิตคอนย์เข้ากระเป๋าเงินของผู้ให้บริการโดยตรง แต่ใช้วิธีการให้ผู้ใช้บริการโอนบิตคอยน์ไปยังรหัสที่ตั้งที่กำหนด จากนั้นระบบจะทำการกระจายโอนบิตคอยน์ออกจากรหัสที่ตั้งนั้นต่อออกไปเป็นลูกโซ่ในโครงข่าย โดยกำหนดอัตราค่าบริการคงที่ร้อยละ 2.49 และค่าบริการต่อรายการของรหัสที่ตั้งผู้รับปลายทางอีก 0.00249 BTC ภายในระยะเวลาดำเนินการที่กำหนดไว้ล่วงหน้าแน่นอน จากการวิเคราะห์กราฟเส้นทางธุรกรรมแสดงผลสรุปการทดลองได้ว่า สามารถตรวจสืบค้นความสัมพันธ์บางรายการระหว่างเส้นทางโอนต้นทางกับปลายทาง ซึ่งอาจเกิดจากขนาดตัวอย่างของรายการมีมูลค่าไม่สูงทำให้การกระจายรายการไม่มีประสิทธิภาพ ดังนั้นวิธีการนี้จึงมีแนวโน้มขาดความน่าเชื่อถือต่อการกลบเกลื่อนร่องรอย

Blockchain.info มีลักษณะการให้บริการเป็นฟังชั่นหนึ่งในเว็บไซต์เพื่อใช้บริการกระบวนการแบ่งปันบิตคอยน์ เมื่อผู้ใช้บริการโอนบิตคอยน์เข้ากระเป๋าเงินตนเองแล้วใช้ฟังชั่นแบ่งปันบิตคอยน์ กระเป๋าเงินดังกล่าวจะเข้าไปร่วมเป็นโครงข่ายพันธมิตรกระเป๋าเงินขนาดใหญ่ จากนั้นระบบจะทำการรวบรวมรายการย่อยเป็นรายการขนาดใหญ่แล้วกระจายการโอนกลับไปยังแต่ละกระเป๋าเงินปลายทางที่ระบุ โดยอัตราค่าบริการคงที่ร้อยละ 0.5 ของมูลค่าเท่านั้น จากการวิเคราะห์กราฟเส้นทางธุรกรรมแสดงผลสรุปการทดลองได้ว่า สามารถตรวจสืบค้นความสัมพันธ์ระหว่างเส้นทางโอนต้นทางและปลายทาง แต่เป็นการยากที่จะระบุตัวตนของบิตคอย์ต้นทางได้ เนื่องจากระบบทำการรวบรวมรายการบิตคอยน์ย่อยจากผู้ใช้งานหลายรายไปรวมกันเป็นรายการขนาดใหญ่ก่อนที่จะทำการกระจายเป็นรายการย่อยอีกครั้งเพื่อทำการโอนไปสู่ผู้รับปลายทางต่อไป

กล่าวโดยสรุป ผลการศึกษา Bitcoin Fog เป็นผู้ให้บริการที่มีระบบโครงสร้างการกลบเกลื่อนรายการได้อย่างมีประสิทธิภาพ ส่วน Blockchain.info แม้ว่าจะสามารถตรวจสอบสืบค้นความสัมพันธ์ของเส้นทางระหว่างต้นทางและปลายทางได้ แต่การพิจสูจน์ความเป็นตัวตนของบิตคอยน์ต้นทางกับปลายทางอาจเป็นเรื่องยาก โดยเฉพาะอย่างยิ่งหากเครือข่ายของผู้ร่วมใช้งานมีขนาดใหญ่มากขึ้น ประสิทธิภาพการกลบเกลื่อนก็จะสูงขึ้นในทำนองเดียวกัน สำหรับ BitLaundery ไม่สามารถกลบเกลื่อยรายการได้อย่างมีประสิทธิภาพ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

2.7.2.2 Andrew and Douglas (2018) หัวเรื่อง *"Bitcoin Investigations: Evolving Methodologies and Case Studies"* มีวัตถุประสงค์การศึกษาและพัฒนาเครื่องมือการตรวจสอบสืบค้นเครือข่ายการทำธุรกรรมบิตคอยน์ที่มีประสิทธิภาพ โดยการศึกษาวิจัยด้วยวิธีการวิเคราะห์อภิทาน (Meta-Analysis) และใช้โปรแกรมประยุกต์ CoinSeer ซึ่งเป็นเครื่องมือในจัดทำระบบฐานข้อมูลขนาดใหญ่รวบรวมข้อมูลเส้นทางธุรกรรม ข้อมูลรหัสที่ตั้งทั้งผู้ส่งและผู้รับ รวมถึงเวลาที่โอน และทำการวิเคราะห์ฐานข้อมูลที่รวบรวมจากระบบนิเวศเพื่อศึกษาความสัมพันธ์ของเส้นทางธุรกรรมกับผู้ใช้งานในการวิเคราะห์ตัวต้นของผู้ใช้งาน

ทั้งนี้ ในการศึกษาใช้ระยะเวลาการเก็บข้อมูลจากระบบนิเวศ 5 เดือน ระหว่าง วันที่ 24 กรกฎาคม 2012 ถึงวันที่ 2 มกราคม 2013 โดยโปรแกรม CoinSeer ทำการสุ่มรวบรวมข้อมูลทุกสัปดาห์จากระบบนิเวศขนาดข้อมูล 60 GB จากผู้ใช้งาน 2,678 ราย และผลการวิเคราะห์แสดงเส้นทางการเชื่อมโยงธุรกรรมเกิดขึ้นจากรหัสที่ตั้งผู้ใช้งานจำนวน 252 ถึง 1,162 รหัสที่ตั้งซึ่งมีแนวโน้มเป็นธุรกรรมในกลุ่มโครงข่ายเดียวกัน นอกจากนี้ได้วิเคราะห์รหัสที่ตั้งในการทำธุรกรรมซึ่งเชื่อมโยงไปยังผู้ใช้งานเดียวกันจะถือเป็นธุรกรรมในกลุ่มของผู้ใช้งานคนเดียวกัน (Cluster) จากวิเคราะห์ 140,000 ชุดรหัสข้อมูล (blocks) พบว่าร้อยละ 58 ของรหัสที่ตั้งแสดงการใช้งานเป็นกลุ่มโครงข่าย โดยเฉลี่ยผู้ใช้งานแต่ละรายจะมีรหัสที่ตั้งประมาณ 11.55 รหัสที่ตั้งต่อกลุ่ม ดังนั้นเพื่อการสืบค้นหาตัวตนผู้ใช้งานให้นำกลุ่มรหัสที่ตั้งของผู้ใช้งานรายนั้น ไปสืบหาเปรียบเทียบรหัสที่ตั้งกับฐานข้อมูลสาธารณะนอกระบบนิเวศเงินสกุลเข้ารหัส เพื่อระบุหาตัวตนผู้ใช้งานที่เคยแสดงตัวตนไว้ในระบบงานดังกล่าว เช่น Twitter

2.7.2.3 Van Wegberg, Oerlemans, van Deventer, and Futter (2018) หัวเรื่อง *"Bitcoin Money Laundering Mixed Result?: An Explorative Study on Money Laundering of Cybercrime Proceeds Using Bitcoin"* มีวัตถุประสงค์การศึกษา วิธีการคัดเลือกผู้ให้บริการแปรสภาพบิตคอยน์ที่เหมาะสม และการประเมินประสิทธิภาพการให้บริการ โดยได้ออกแบบการศึกษาวิจัยด้วยวิธีการทดลอง (Experiment) การฟอกเงินด้วยบิตคอยน์ ทั้งนี้การศึกษาได้ใช้เครื่องมือ TNO Dark Web Monitor เป็นเครื่องมือในการสำรวจและกรองข้อมูลเว็บไซต์เป้าหมายบนระบบอินเตอร์เน็ตในช่วงระยะเวลาที่กำหนด (Exploratory and Longitudinal Research) ปรากฏว่าค้นพบเว็บไซต์ผู้ให้บริการแปรสภาพบิตคอยน์ซึ่งซ่อนตัวอยู่ใน Dark Web ไม่น้อยกว่า 25,000 ราย ในการทดลองได้กำหนดเกณฑ์การเลือกตัวแทนผู้ให้บริการแปรสภาพบิตคอยน์จากอัตราสัดส่วนการให้บริการแปรสภาพเทียบกับการให้บริการแลกเปลี่ยนบิตคอยน์ปกติ ข้อปฏิบัติในการลงทะเบียนผู้ใช้งาน ประวัติความเห็นของผู้เคยใช้บริการ และระยะเวลาในการดำเนินการโอน

ทั้งนี้ในการศึกษาวิจัยได้จัดทำสถานการณ์จำลองการฟอกเงินด้วยบิตคอยน์ โดยได้ใช้เกณฑ์ข้างต้นเลือกตัวแทนผู้ให้บริการแปรสภาพบิตคอยน์ 5 ราย เพื่อจำลองสถานการณ์โอนบิตคอยน์เข้าระบบงานของผู้ให้บริการแปรสภาพและติดตามผลการโอนบิตคอยน์สู่ปลายทาง จากนั้นเข้าสู่ขั้นตอนการแลกเปลี่ยนบิตคอยน์เป็นเงินตราปกติ

เมื่อเริ่มสถานการณ์จำลอง ได้ทำการโอนบิตคอยน์ให้แก่ผู้ให้บริการแปรสภาพพร้อมกันทั้ง 5 ราย ผลปรากฏว่าได้รับการโอนบิตคอยน์ไปยังกระเป๋าเงินปลายทางเพียง 2 ราย โดยใช้ระยะเวลาดำเนินการโอน 3 ชั่วโมง และ 17 ชั่วโมงตามลำดับ จากนั้นได้ทดลองนำบิตคอยน์ที่ได้รับหลังแปรสภาพไปโอนต่อแลกเปลี่ยนเป็นเงินตราปกติผ่านผู้ให้บริการแลกเปลี่ยน PayPal, Perfect Money, Western Union และ Bitonic ปรากฏว่า PayPal มีระบบในการปิดบังตัวตนที่มีศักยภาพมากกว่า Western Union เนื่องจากระบบ PayPal เปิดรับการโอนบิตคอยน์จากผู้ใช้งานที่ไม่เปิดเผยตัวตน ในขณะที่ Western Union มีข้อปฏิบัติการลงทะเบียนข้อมูลผู้ใช้งานและระบุแหล่งที่มาของบิตคอยน์ นอกจากนี้ได้ศึกษาแนวทางการปิดบังตัวตนในการทำธุรกรรมเพื่อป้องกันการตรวจสอบสืบค้นผู้ใช้งาน ควรดำเนินการบน TOR Browser หรือควรสร้างรหัสที่ตั้งเป็นการเฉพาะกิจในการโอนเพื่อป้องกันการเชื่อมโยงรหัสที่ตั้งในการใช้งานโอนกับรหัสที่ตั้งผู้ใช้งาน ซึ่งอาจได้มีการระบุข้อมูลส่วนบุคคลในระบบงานอื่น เช่น Facebook, Twitter เป็นต้น รวมถึงไม่ควรใช้ Email ประจำตัวทำรายการโอนบิตคอยน์

และผลการศึกษา พบว่า ต้นทุนการฟอกเงินจากสถานการณ์จำลองมีอัตราสูงเกินกว่าร้อยละ 50 เนื่องจากบิตคอยน์ส่วนหนึ่งถูกฉ้อโกงจากผู้ให้บริการที่ขาดความน่าเชื่อถือ รวมกับค่าบริการโอนปกติจากผู้ให้บริการที่มีระดับน่าเชื่อถือ โดยความน่าเชื่อถือของผู้ให้บริการแปรสภาพที่ถูกคัดเลือกเป็นตัวแทนในสถานการณ์จำลอง มีความสอดคล้องกับระดับความเห็นจากประวัติผู้เคยใช้บริการการฟอกเงินผ่านระบบ Dark Web กล่าวคือ ระดับสีแดง หรือสีส้ม เป็นระดับที่ผู้ใช้งานมีความเสี่ยงถูกขโมย หรือถูกฉ้อโกงจากผู้ให้บริการ ในขณะที่ระดับสีเขียว เป็นระดับที่ผู้ให้บริการมีความเสี่ยงต่ำจากอาชญากรรมคอมพิวเตอร์ แต่เมื่อประเมินต้นทุนการฟอกเงินในสถานการณ์จำลองเฉพาะรายการที่ผ่านผู้ให้บริการที่น่าเชื่อถือ ปรากฏว่า มีต้นทุนประมาณร้อยละ 15 ของมูลค่า สอดคล้องกับประมาณการณ์ระดับต้นทุนการฟอกเงินตามแผนดำเนินการที่ยอมรับได้โดยไม่ควรเกินร้อยละ 15 ของมูลค่า

2.7.2.4 Seo, Park, Oh, and Lee (2018) หัวเรื่อง *"Money Laundering in the Bitcoin Network: Perspective of Mixing Services"* มีวัตถุประสงค์การศึกษา กระบวนการฟอกเงินด้วยบิตคอยน์ผ่านผู้ให้บริการแปรสภาพบิตคอยน์ โดยการศึกษาวิจัยด้วยวิธีการทดลองทำธุรกรรมโอนบิตคอยน์ผ่านผู้ให้บริการแปรสภาพบิตคอยน์ ทั้งนี้การให้บริการแปรสถาพบิตคอยน์มี

เป้าหมายเพื่อหลีกเลี่ยงการสืบค้น หรือสร้างความยุ่งยากในการติดตามมูลค่า รวมถึงเพิ่มขั้นตอนการปกปิดตัวตนด้วยการฟอกเงินบนระบบ TOR browser เพื่อเสริมความมั่นใจในปกปิดตัวตนบนระบบปฏิบัติการ อย่างไรก็ตามผู้ให้บริการแต่ละรายมีข้อปฏิบัติที่เกี่ยวกับข้อมูลจำเป็นที่แตกต่างกัน เช่น รหัสที่ตั้งผู้โอนหรือผู้รับโอน ระยะเวลาดำเนินการ หรือจำนวนธุรกรรมขั้นต่ำในการโอนไข้วรายการ เป็นต้น

จากการศึกษาเปรียบเทียบผู้ให้บริการแปรสภาพบิตคอยน์ พบว่า

(1) Bitcoin Fog (foggerddriztrcar2.onion) ให้บริการเฉพาะบนระบบปฏิบัติการ TOR ด้วยอัตราค่าบริการร้อยละ 1 ถึง 3 โดยผู้ใช้งานสามารถกำหนดกรอบระยะเวลาดำเนินการได้ถึง 48 ชั่วโมง และสามารถกำหนดรหัสที่ตั้งผู้รับโอนได้สูงสุด 20 รหัสที่ตั้ง

(2) Coin Mixer (coinmixibh45abn7.onion) ให้บริการบนระบบปฏิบัติการทั่วไปรวมถึง TOR ด้วยอัตราค่าบริการร้อยละ 1 ถึง 3 โดยผู้ใช้งานสามารถกำหนดกรอบระยะเวลาดำเนินการเองได้ และสามารถกำหนดรหัสที่ตั้งผู้รับโอนได้สูงสุด 5 รหัสที่ตั้ง

(3) Crypto Mixer (cryptomixns23scr.onion) ให้บริการบนระบบปฏิบัติการทั่วไป ด้วยอัตราค่าบริการร้อยละ 0.5 ถึง 3 โดยผู้ใช้งานสามารถกำหนดกรอบระยะเวลาดำเนินการได้ถึง 48 ชั่วโมง และสามารถกำหนดรหัสที่ตั้งผู้รับโอนได้สูงสุด 10 รหัสที่ตั้ง

(4) Bitcoinmix (bitcoinmix.org) ให้บริการบนระบบปฏิบัติการทั่วไป ยกเว้น TOR ด้วยอัตราค่าบริการร้อยละ 1 ถึง 5 โดยผู้ใช้งานสามารถกำหนดกรอบระยะเวลาดำเนินการได้ถึง 24 ชั่วโมง และสามารถกำหนดรหัสที่ตั้งผู้รับโอนได้สูงสุด 5 รหัสที่ตั้ง

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

2.7.2.5 กล่าวโดยสรุป จากงานวิจัยเกี่ยวกับเทคนิคการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสดังกล่าวข้างต้นนั้น งานวิจัยส่วนใหญ่ทำการศึกษาบิตคอยน์ซึ่งเป็นตัวแทนของเงินสกุลเข้ารหัส เนื่องจากบิตคอยน์เป็นเงินสกุลเข้ารหัสแรกและเป็นที่ยอมรับของระบบตลาดเงินสกุลเข้ารหัสซึ่งมีมูลค่าหมุนเวียนเกินกว่าร้อยละ 50 ของมูลค่าทางการตลาด ทั้งนี้ด้วยคุณลักษณะเฉพาะของเงินสกุลเข้ารหัสที่ไม่มีข้อกำหนดให้ระบุตัวตนผู้ใช้งาน จึงเป็นปัจจัยส่งเสริมต่อการฟอกเงินแต่ในขณะเดียวกัน ระบบปฏิบัติการบล็อกเชนก็มีกลไกการทำงานบนฐานข้อมูลสาธารณะแบบกระจายศูนย์ที่ผู้ใช้งานสามารถเข้าถึงเส้นทางธุรกรรมระหว่างบุคคลได้ จึงเป็นความเสี่ยงต่อการสืบค้นหลักฐานของธุรกรรม ดังนั้นการวิจัยจึงให้ความสนใจต่อกลไกการกลบเกลื่อนร่องรอย หรือหลีกเลี่ยงการตรวจสืบค้นเชื่อมโยงความสัมพันธ์ระหว่างผู้โอนต้นทางกับผู้รับปลายทางผ่านผู้ให้บริการแปรสภาพ โดยผู้วิจัยได้สรุปผลการศึกษาเป็นประเด็นสำคัญ ดังนี้

(1) ผู้ใช้งานสามารถสร้างรหัสที่ตั้งที่ไม่ต้องระบุตัวตน เพื่อการทำธุรกรรมโอนในระบบนิเวศได้ไม่จำกัดจำนวน (Moser et al, 2013) และส่วนใหญ่ผู้ใช้งานมักจะทำธุรกรรมด้วยการใช้รหัสที่ตั้งดำเนินการเป็นกลุ่มโดยเฉลี่ยประมาณ 11 ถึง 12 รหัสที่ตั้งต่อผู้ใช้งานหนึ่งราย (Andrew & Douglas, 2018; Van Wegberg et al., 2018)

(2) การเพิ่มประสิทธิภาพการปกปิดตัวตนโดยการทำธุรกรรมบนระบบปฏิบัติที่สามารถกลบเกลื่อนร่องรอยรหัสที่ตั้งหรือปกปิดรหัสที่ตั้ง เช่น TOR Browser (Andrew & Douglas, 2018; Hazar, 2019; Hu, Seneviratne, Thilakaratha, Fukuda, & Seneviratne, 2019; Moser et al., 2013; Van Wegberg et al., 2018)

(3) ผู้ให้บริการแปรสภาพบางรายมีระดับความเสี่ยงต่อการถูกขโมย หรือฉ้อโกงเงินสกุลเข้ารหัสของผู้ใช้งานจากอาชญากรรมทางไซเบอร์ ดังนั้นผู้ใช้งานส่วนใหญ่จึงเลือกใช้ผู้ให้บริการแปรสภาพที่มีประวัติการให้บริการที่น่าเชื่อถือ (Van Wegberg et al., 2018)

(4) การตรวจพิสูจน์ตัวตนผู้ใช้งาน โดยการวิเคราะห์เปรียบเทียบกลุ่มรหัสที่ตั้งของผู้ใช้งาน (Cluster) กับรหัสที่ตั้งในฐานข้อมูลนอกระบบนิเวศเงินสกุลเข้ารหัส (Andrew & Douglas, 2018) หรือกล่าวอีกนัยหนึ่งคือการนำรหัสที่ตั้งของผู้ใช้งานต้องสงสัย สืบค้นเปรียบเทียบกับธุรกรรมประจำวันบนระบบอินเตอร์เน็ต ไม่ว่าจะเป็นตรวจเปรียบเทียบกับการใช้ Email, Facebook, Twitter รวมถึงสื่อสังคมออนไลน์อื่นๆ เพื่อการสืบค้นและเข้าถึงตัวบุคคลของผู้ใช้งานต้องสังสัย (Hazar, 2019) การใช้บริการโอนเงินสกุลเข้ารหัสผ่านผู้ให้บริการแปรสภาพ ซึ่งอนุญาตให้ผู้ใช้งานทำการโอนเข้าสู่ระบบจากรหัสที่ตั้งต้นทางหลายบัญชี และกำหนดรหัสที่ตั้งของผู้รับปลายทางหลายบัญชีได้เช่นกัน จึงเป็นการสร้างรายการธุรกรรมย่อยเข้าสู่ระบบ อันอาจถือได้ว่าเป็นการร่วมกระบวนการสร้างโครงข่ายของผู้ร่วมใช้งานขนาดใหญ่ในระบบนิเวศของเงินสกุลเข้ารัหส โดยการบริการจัดการของผู้ให้บริการแปรสภาพ (Moser et al., 2013; Seo et al., 2018) เพื่อให้ความเชื่อมั่นแก่ผู้ใช้งานได้ว่าผู้รับโอนจะได้รับเงินสกุลเข้ารหัสทุกรายการจากผู้ใช้งานรายอื่น ดังนั้นจึงเป็นการตัดตอนความเชื่อมโยงระหว่างผู้โอนต้นทางกับผู้รับปลายทาง

(5) การกำหนดอัตราค่าบริการแบบช่วง และกลไกการคำนวณค่าบริการแบบสุ่มของผู้ให้บริการแปรสภาพ เป็นกลไลการกลบเกลื่อนร่อยรอยของเส้นทางการทำธุรกรรมอีกแนวทางหนึ่ง โดยระบบปฏิบัติงานผู้ให้บริการแปรสภาพจะทำการสุ่มอัตราค่าบริการโดยอัตโนมัติ และคำนวณหักค่าบริการจากการโอนแต่ละรายการย่อยของผู้ใช้งานในอัตราที่ไม่เท่ากัน (Moser et al., 2013; Seo et al., 2018) แต่เมื่อเสร็จสิ้นกระบวนการผู้รับโอนปลายทางจะได้รับเงินสกุลเข้ารหัสสุทธิหลัง

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

หักค่าบริการตามเงื่อนไขข้อตกลง ดังนั้นการตรวจสอบสืบค้นรายการจากฐานข้อมูลสาธารณะแบบกระจายศูนย์จึงไม่สามารถกระทบจับคู่รายการอย่างตรงไปตรงมาได้

(6) นอกจากกลไกการสร้างโครงข่ายผู้ร่วมใช้งานขนาดใหญ่ และกลไกการคิดค่าบริการแบบสุ่มในอัตราที่ไม่เท่ากันของแต่ละรายการย่อยแล้ว ผู้ให้บริการแปรสภาพยังดำเนินการกลบเกลื่อนร่องรอยของเส้นทางธุรกรรมด้วยวิธีการหน่วงเวลาระยะเวลาดำเนินการภายใต้ข้อตกลงที่กำหนด (Moser et al., 2013; Seo et al., 2018) ดังนั้นการตรวจติดตามเพื่อสืบค้นหาความสัมพันธ์ของเส้นทางธุรกรรมจึงอาจเกิดขึ้นได้ยาก เนื่องจากการทอดระยะเวลาดำเนินการเพื่อทยอยทำการโอนรายการย่อยแต่ละรายการต่างช่วงเวลากัน และการโอนย้ายเงินสกุลเข้ารหัสหลายทอดภายใต้โครงข่ายขนาดใหญ่ของผู้ให้บริการแปรสภาพ จึงเป็นสร้างอุปสรรคต่อการรวบรวมข้อมูลเส้นทางธุรกรรมที่เชื่อมโยงกับผู้โอนต้นทางไปยังผู้รับโอนปลาย โดยเฉพาะอย่างยิ่งหากผู้โอนและผู้รับโอนทำธุรกรรมหลายรายการพร้อมกันจะยิ่งเป็นอุปสรรคต่อการพิสูจน์แหล่งที่มาของเงินสกุลเข้ารหัส

(7) เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสดำเนินการบนระบบอินเตอร์เน็ต ที่เชื่อมโยงครอบคลุมผู้ใช้งานแบบไร้พรมแดน และมีปริมาณธุรกรรมจำนวนมหาศาล รวมถึงธุรกรรมดำเนินการด้วยความรวดเร็ว ดังนั้นการตรวจสอบสืบค้นจึงจำเป็นต้องใช้โปรแกรมประยุกต์เชื่อมต่อกับระบบงานแบบเปิดของระบบปฏิบัติการบล็อกเชน เพื่อการวิเคราะห์พฤติกรรมของกลุ่มรหัสที่ตั้งต้องสงสัย หรือเส้นทางธุรกรรมต้องสงสัย รวมถึงการนำรหัสที่ตั้งต้องสงสัยมาวิเคราะห์เปรียบเทียบกับรหัสที่ตั้งประจำตัวที่แสดงตัวตนไว้ในระบบปฏิบัติอื่น ทั้งนี้การปฏิบัติการดังกล่าวจำเป็นต้องใช้ทรัพยากรในระบบคอมพิวเตอร์ขนาดใหญ่ และโปรแกรมประยุกต์ที่เหมาะสม เช่น Elliptic หรือ Chainalysis ซึ่งเป็นโปรแกรมประยุกต์ที่ถูกพัฒนาขึ้นโดยผู้เชี่ยวชาญด้านการตรวจสอบสืบค้นธุรกรรมเงินสกุลเข้ารหัส (Dyson, Buchanan, & Bell, 2018) หรือ Graph Convolutional Networks (GCN) ซึ่งเป็นโปรแกรมประยุกต์ในการวิเคราะห์ข้อมูลความสัมพันธ์ของเส้นทางธุรกรรมในระบบนิเวศ (Hu et al., 2019) นอกจากโปรแกรมประยุกต์ที่เหมาะสมซึ่งเป็นเครื่องมือสำคัญในการตรวจสอบสืบค้นความสัมพันธ์ของผู้ใช้งานต้องสงสัยกับเส้นทางธุรกรรมต้องสงสัยแล้ว ผู้ทำหน้าที่และผู้ปฏิบัติงานที่ใช้งานระบบตรวจสอบนี้ก็เป็นปัจจัยสำคัญไม่น้อยไปกว่าเครื่องมือ คือ บุคคลากรควรมีความรู้และความเชี่ยวชาญ ทั้งระดับบริบทของความเป็นเงินสกุลเข้ารหัสและระดับเทคนิคปฏิบัติการประยุกต์โปรแกรมตรวจสอบ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

2.8 กรอบแนวคิดการวิจัย

จากการทบทวนวรรณกรรม ศึกษาแนวคิด ทฤษฎี งานวิจัย และเอกสารที่เกี่ยวข้องกับบริบทของเงินสกุลเข้ารหัส กระบวนการฟอกเงิน และกระบวนการฟอกเงินโดยเงินสกุลเข้ารหัส จึงนำมาสู่การพัฒนากรอบแนวคิดการวิจัย *"แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส"* ดังนี้

โดยการนำทฤษฎีปกตินิสัย ประกอบกับทฤษฎีการเลือกกระทำผิดอย่างมีเหตุผลมาร่วมสังเคราะห์กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส จะพบว่า ผู้กระทำผิด เป็นบุคคลที่ได้รับประโยชน์จากการก่อเหตุอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และอาศัยโอกาสทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เพื่อการหลีกเลี่ยงการตรวจจับกุมและสามารถแปลงสภาพเป็นเงินสกุลเข้ารหัสหรือเงินตราปกติที่ชอบด้วยกฎหมาย ซึ่งเงินสกุลเข้ารหัสมีปัจจัยที่มีอิทธิพลต่อผู้กระทำผิดในการเลือกทำธุรกรรมการฟอกเงินโดยเงินสกุลเข้ารหัส อันประกอบด้วยปัจจัยเชิงบวกที่ส่งเสริมประโยชน์แก่ผู้กระทำผิด ได้แก่

(1) ระบบนิเวศเอื้อต่อการปิดบังตัวตนผู้ใช้งาน

(2) ศักยภาพในการทำธุรกรรมข้ามประเทศแบบไร้พรมแดน

(3) ไม่มีหน่วยงานกลางใดกำกับดูแลหรือจัดการระบบงาน

(4) การทำธุรกรรมโอนมูลค่าในระบบนิเวศเป็นไปด้วยความรวดเร็ว

(5) ต้นทุนในการทำธุรกรรมโอนมูลค่ามีค่าใช้จ่ายต่ำ

(6) มีระบบปฏิบัติการที่สนับสนุนการกลบเกลื่อนร่องรอยในการทำธุรกรรม

(7) มีระบบปฏิบัติการเฉพาะสนับสนุนการปิดบังรหัสที่ตั้งผู้ใช้งาน

(8) ระบบนิเวศมีการปกป้องการเข้าถึงรหัสเปิดส่วนบุคคลและข้อมูลส่วนบุคคล

อย่างไรก็ตามระบบนิเวศเงินสกุลเข้ารหัสมีปัจจัยเชิงลบที่อาจก่อภาระ หรือเป็นการเพิ่มความเสี่ยงต่อผู้กระทำผิดในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ได้แก่

(1) ระบบนิเวศเป็นระบบฐานข้อมูลสาธารณะแบบกระจายศูนย์ซึ่งเปิดให้บุคคลทั่วไป หรือผู้ใช้งานสามารถเข้าถึงระบบงานได้ รวมถึงสามารถนำโปรแกรมประยุกต์ของตนเข้าเชื่อมต่อระบบงานได้ด้วยเช่นกัน

(2) ความเสี่ยงจากการถูกโจรกรรมทางไซเบอร์ในระหว่างดำเนินการโอนมูลค่าในระบบนิเวศ

ในขณะที่การพิทักษ์ปกป้องเพื่อยับยั้งเหตุการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสนั้น มีลักษณะขาดศักยภาพในการกำกับดูแล โดยมีปัจจัยที่มีผลต่อการดำเนินการ ได้แก่

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

(1) ขาดมาตรการทางกฎหมายภายในประเทศที่เกี่ยวข้องกับการกำกับดูแล การป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่ชัดเจน

(2) ขาดการออกมาตรการทางกฎหมายระหว่างประเทศในการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัสอย่างเป็นสากล

(3) หน่วยงานในประเทศที่มีหน้าที่รับผิดชอบต่อการกำกับดูแล การป้องกันและปราบปรามยังขาดศักยภาพในการปฏิบัติงาน

(4) ขาดความร่วมมือระหว่างหน่วยงาน หรือองค์กรระหว่างประเทศที่เกี่ยวข้องกับการกำกับดูแล การป้องกันและปราบปราม ในการเสริมสร้างศักยภาพการดำเนินงานร่วมกัน

(5) ผู้มีหน้าที่รับผิดชอบกำกับดูแล การป้องกันและปราบปราม ยังขาดองค์ความรู้เกี่ยวกับเงินสกุลเข้ารหัส และขาดทักษะในการปฏิบัติหน้าที่ป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

(6) หน่วยงานและผู้มีหน้าที่รับผิดชอบกำกับดูแล การป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ขาดเครื่องมือและอุปกรณ์ที่มีศักยภาพในการดำเนินการ

องค์ประกอบสุดท้ายคือ เหยื่อ อันหมายถึง รัฐและประโยชน์สาธารณะแห่งรัฐ ซึ่งเป็นผู้ที่ได้รับผลเสียหายจากกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยมีปัจจัยที่สร้างความเสียหายแก่รัฐและประโยชน์สาธารณะแห่งรัฐ ได้แก่

(1) ก่อให้เกิดแหล่งเงินทุนสนับสนุนการก่ออาชญกรรม โดยนำมาเงินจากการกระทำผิดไปเป็นเงินทุนในการขยายการกระทำผิดต่อไปเป็นเครือข่ายอย่างต่อเนื่อง เช่น ผลประโยชน์จากการค้ายาเสพติด การค้ามนุษย์ หรือการพนันทางอิเล็กทรอนิกส์

(2) ขาดประโยชน์สาธารณะที่พึงได้รับ เนื่องจากการหลีกเลี่ยงภาษีอากรและศุลกากร

(3) สูญเสียประโยชน์สาธารณะจากการแสวงหาประโยชน์ในทรัพยากรธรรมชาติโดยมิชอบ หรือการฉ้อโกงสถาบันการเงิน ซึ่งรัฐต้องนำประโยชน์สาธารณะเข้าไปช่วยเหลือดูแลสร้างความมั่นคง แก่ระบบสถาบันการเงิน

(4) สร้างภาระและเป็นต้นทุนการรักษาความสงบเรียบร้อยให้แก่สังคม จากการร่วมกระทำผิดที่มีเครือข่ายเชื่อมโยง เป็นองค์กรอาชญากรรมรวมถึงองค์กรข้ามชาติ และการสนับสนุนการค้าอาวุธร้ายแรง เป็นต้น

ทั้งนี้ โดยทฤษฎีการป้องกันอาชญากรรมตามสถานการณ์ เมื่อนำมาสังเคราะห์ปัจจัยที่ส่งผลต่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสของผู้กระทำผิด ได้แก่

(1) การเพิ่มภาระหน้าที่ความรับผิดในการทำธุรกรรม รวมถึงการเพิ่มบทลงโทษ

(2) การเพิ่มกลไกการทำงาน เพื่อเพิ่มโอกาสการตรวจสอบสืบค้นธุรกรรมในระบบนิเวศ และก่อให้เกิดความเสี่ยงแก่ผู้กระทำผิดเพิ่มมากขึ้น

(3) การลดผลประโยชน์ที่ผู้กระทำผิดได้รับจากการทำธุรกรรม

(4) การเผยแพร่ประชาสัมพันธ์เพื่อสร้างองค์ความรู้ที่ถูกต้องแก่สาธารณะ

(5) การสร้างความร่วมมือของกลุ่มบุคคล หน่วยงาน องค์กรที่เกี่ยวข้องกับการทำธุรกรรม ในลักษณะการสร้างเครือข่ายองค์กรต่อต้านการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

กรอบแนวคิดการวิจัย: แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

ผู้กระทำผิด

- การปิดบังตัวตนผู้ใช้งาน
- ธุรกรรมไร้พรมแดน
- ไม่มีหน่วยงานกลางกำกับ
- ธุรกรรมรวดเร็ว
- ต้นทุนธุรกรรมต่ำ
- กลบเกลื่อนร่องรอยธุรกรรม
- ระบบปฏิบัติการปิดบังผู้ใช้งาน
- การปกป้องข้อมูลส่วนบุคคล
- ระบบฐานข้อมูลสาธารณะ
- ความเสี่ยงการถูกโจรกรรมทางคอมพิวเตอร์

รูปแบบอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และใช้การฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

การฟอกเงินโดย
ธุรกรรมเงินสกุลเข้ารหัส

เหยื่อ
(รัฐและประโยชน์สาธารณะ)

- ก่อให้เกิดเงินทุนสนับสนุนการก่ออาชญากรรมต่อไปอีก
- ขาดประโยชน์สาธารณะที่พึงได้รับ
- สูญเสียประโยชน์สาธารณะ
- สร้างภาระและเป็นต้นทุนการรักษาความสงบเรียบร้อยให้แก่สังคม

การขาดผู้พิทักษ์ปกป้อง

- กฎหมายในประเทศ
- กฎหมายระหว่างประเทศ
- หน่วยงานกำกับดูแลในประเทศ
- หน่วยงานกำกับดูแลระหว่างประเทศ
- ผู้ปฏิบัติหน้าที่กำกับดูแล
- เครื่องมือในการกำกับดูแล

การป้องกันอาชญากรรม

- เพิ่มภาระความรับผิดในการทำธุรกรรม
- เพิ่มความเสี่ยงต่อการถูกสืบค้นตรวจพบธุรกรรม
- ลดผลประโยชน์ที่จะได้รับจากการทำธุรกรรม
- สร้างองค์ความรู้แก่สาธารณะ
- สร้างความร่วมมือลักษณะองค์กรต่อต้าน

แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

บทที่ 3
ระเบียบวิธีการวิจัย

การศึกษาวิจัยเรื่อง *"แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส"* ใช้ระเบียบวิธีการวิจัยในรูปแบบของการวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งประกอบด้วยเทคนิคการวิจัยในขั้นตอนการดำเนินการวิจัย ดังนี้ (1) การวิจัยเชิงเอกสาร เพื่อทำความเข้าใจบริบทของประเด็นที่ทำการศึกษา และการสร้างกรอบแนวคิดการวิจัย (2) การสัมภาษณ์เชิงลึก เพื่อรวบรวมข้อมูลและวิเคราะห์ผลการศึกษาตามวัตถุประสงค์การวิจัย (3) เทคนิควิธีเดลฟาย เพื่อสำรวจความเห็นอิสระเชิงเสนอแนะ ต่อประเด็นการศึกษาแนวทางการป้องกันและปราบปรามการฟอกเงินธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมสำหรับบริบทในประเทศไทยและสากล ซึ่งมีระเบียบวิธีการวิจัยเป็นลำดับขั้นตอน ดังนี้

3.1 วิธีการดำเนินการวิจัย
3.2 ผู้เชี่ยวชาญ และผู้ให้ข้อมูลสำคัญ
3.3 เครื่องมือที่ใช้ในการวิจัย
3.4 การเก็บรวบรวมข้อมูล
3.5 การวิเคราะห์ข้อมูล
3.6 ระยะเวลาการวิจัย
3.7 จริยธรรมการวิจัย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

3.1 วิธีการดำเนินการวิจัย

3.1.1 การวิจัยเชิงเอกสาร (Documentary Research)

โดยผู้วิจัยได้ศึกษาหนังสือ วารสาร เอกสาร บทบัญญัติของกฎหมาย และงานวิจัยที่เกี่ยวข้อง รวมถึงข้อมูลวารสารอิเล็กทรอนิกส์ เพื่อศึกษาทำความเข้าใจถึงบริบทของเงินสกุลเข้ารหัส อันประกอบด้วยคุณลักษณะเฉพาะและกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัส สถานภาพและมาตรการทางกฎหมายที่มีต่อเงินสกุลเข้ารหัส รวมถึงทำความเข้าใจพฤติกรรมการกระทำผิดในบริบทของกระบวนการฟอกเงินและการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส อันได้แก่ ปัจจัยส่งเสริมให้ผู้กระทำผิดใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน กลไกการปกปิดตัวตนในระบบนิเวศและระบบปฏิบัติการบล็อกเชน การกลบเกลื่อนร่องรอยธุรกรรมการโอนเงินสกุลเข้ารหัส และการประเมินมาตรการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส อีกทั้งทำการวิจัยเชิงวิเคราะห์เนื้อหา (Content Analysis) จากฐานข้อมูลที่ค้นคว้าตามขอบเขตการวิจัย พร้อมทั้งนำแนวคิดและทฤษฎีอาชญาวิทยาที่เกี่ยวข้องร่วมสังเคราะห์ประเด็น เพื่อนำไปสู่การสร้างกรอบแนวคิด

การวิจัย อันได้แก่ ปัจจัยที่มีอิทธิพลต่อการกระทำผิดในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ภายใต้แนวคิดทฤษฎีปกตินิสัยประกอบกับทฤษฎีการเลือกกระทำอย่างมีเหตุผล อันประกอบด้วย บริบทของเงินสกุลเข้ารหัสที่สร้างแรงจูงใจ ต่อการตัดสินใจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือกระทำผิด และโอกาสที่เอื้อประโยชน์ให้แก่ผู้กระทำผิดมากกว่าความเสี่ยงที่อาจเกิดขึ้น รวมถึงช่องว่างของการพิทักษ์ป้องกันการกระทำผิด ทั้งบทบัญญัติแห่งกฎหมาย ผู้บังคับใช้กฎหมาย และเครื่องมือในการตรวจสอบสืบค้นให้สามารถบังคับใช้กฎหมายได้อย่างมีประสิทธิภาพ กอรปกับปัจจัยที่มีอิทธิพลต่อการป้องกันการกระทำผิด ภายใต้แนวคิดทฤษฎีการป้องกันอาชญากรรมตามสถานการณ์ ประกอบด้วยปัจจัยเชิงลบต่อผู้กระทำผิด ด้วยการสร้างภาระความรับผิดและความเสี่ยงต่อการถูกตรวจจับซึ่งจะไม่คุ้มประโยชน์ต่อการก่อเหตุ และปัจจัยเชิงบวกส่งเสริมความเข้าใจที่ถูกต้องต่อสาธารณะ และสร้างความเข็มแข็งขององค์กรต่อต้านการกระทำผิด

3.1.2 การสัมภาษณ์เชิงลึก (In-depth Interviews)

ดำเนินการเก็บรวบรวมข้อมูลจากการสัมภาษณ์ผู้ให้ข้อมูลสำคัญ (Key Informants) ซึ่งเป็นบุคคลากรหรือผู้เชี่ยวชาญประจำหน่วยงานที่ถูกเลือกแบบเฉพาะเจาะจงจากผู้เชี่ยวชาญประจำหน่วยงานที่จัดแบ่งเป็นกลุ่มตามหน้าที่ความรับผิดชอบ อันประกอบด้วย กลุ่มหน่วยงานหลักของภาครัฐมีหน้าที่รับผิดชอบโดยตรง ต่อการป้องกันและปราบปรามอาชญากรรมทางเศรษฐกิจ และการฟอกเงิน และการกำกับดูแลการดำเนินกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม กลุ่มหน่วยงานองค์สถาบันการเงินทั้งภาครัฐและภาคเอกชน กลุ่มหน่วยงานในกระบวนการยุติธรรม และกลุ่มหน่วยงานผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงิน โดยเทคนิควิธีการสัมภาษณ์เชิงลึก (In-depth interviews) ด้วยกรอบแนวคำถามปลายเปิดแบบกึ่งโครงสร้าง (Semi-structure Interview) เพื่อครอบคลุมประเด็นการศึกษาตามวัตถุประสงค์การวิจัย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

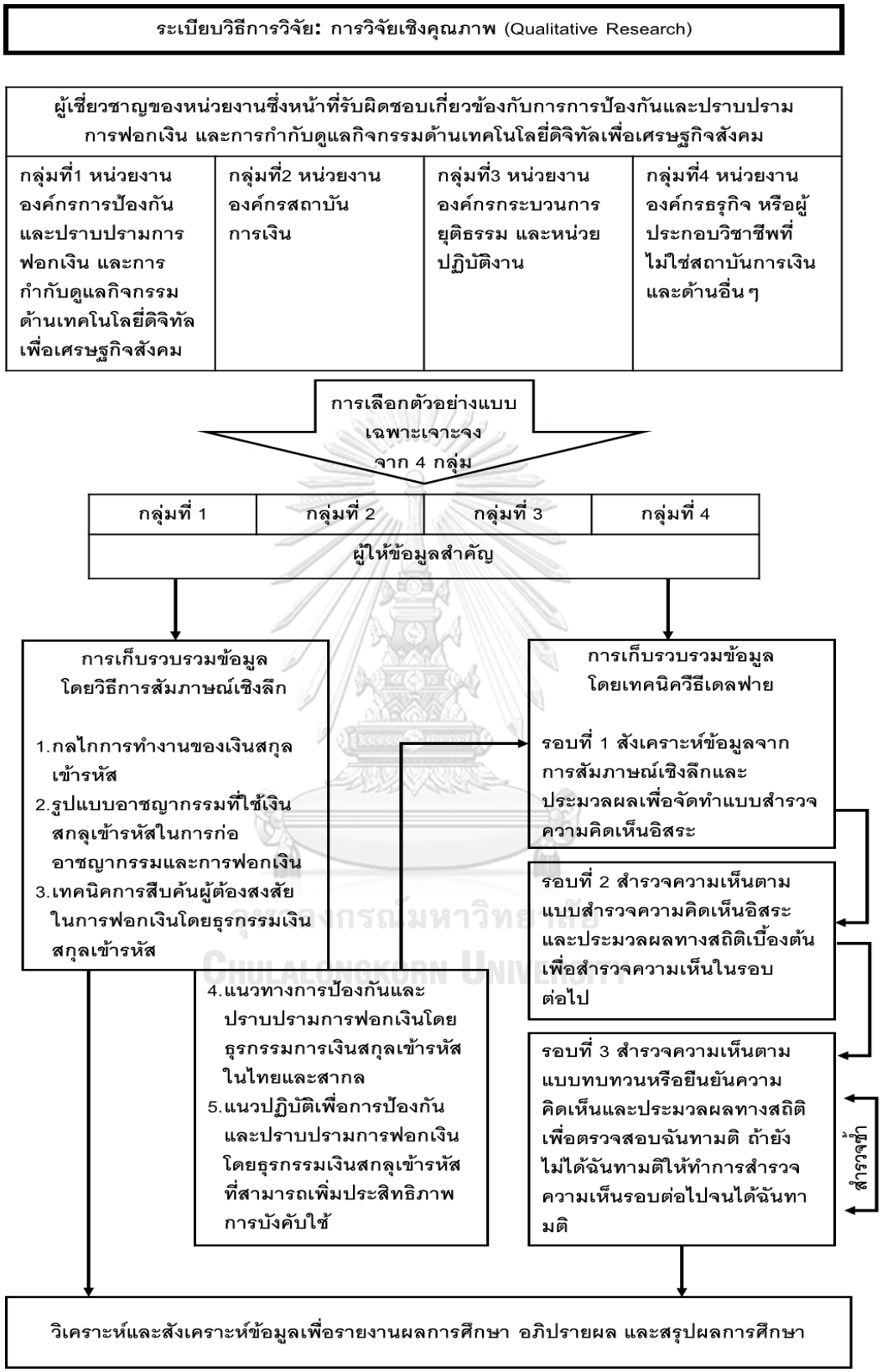
3.1.3 การใช้เทคนิควิธีเดลฟาย (Delphi Technique)

การวิจัยนี้ได้ใช้เทคนิควิธีเดลฟายรูปแบบปรับปรุง (Modified Delphi Technique) ในส่วนของการเก็บรวมข้อมูลรอบแรกด้วยการสัมภาษณ์เชิงลึกกับผู้เชี่ยวชาญแทนการเก็บรวบรวมข้อมูลแบบดั่งเดิม ที่ใช้วิธีการส่งแบบสอบถามนำเข้าสู่ประเด็นที่ศึกษาในรูปแบบคำถามปลายเปิดไปยังผู้เชี่ยวชาญ เพื่อขอให้ผู้เชี่ยวชาญแสดงความเห็นให้ข้อมูลที่เกี่ยวข้องได้อย่างอิสระ ซึ่งมีโอกาสได้รับข้อมูลที่หลากหลายแบบไม่มีข้อจำกัด แต่ต้องใช้ระยะเวลาในการรอคอยการตอบกลับความเห็นจากผู้เชี่ยวชาญนานกว่าจะครบจำนวน และมักประสบปัญหาในการรวบรวมและวิเคราะห์ข้อมูลเพื่อการจัดทำแบบสำรวจความเห็นในรอบต่อไป อีกทั้งข้อมูลที่จัดเก็บได้มักมีการกระจายตัวสูง

จึงมักส่งผลต่อกระบวนการวิจัยที่ต้องจัดทำแบบสำรวจความเห็นจำนวนหลายรอบมากขึ้น จนกว่าจะได้รับความเห็นที่มีแนวโน้นระดับความคงที่เข้าสู่ศูนย์กลางเป็นฉันทามติ

ดังนั้นการวิจัยนี้จึงเริ่มกระบวนการด้วยการเก็บรวบรวมข้อมูลโดยเทคนิควิธีเดลฟายกับผู้เชี่ยวชาญหรือบุคคลากรประจำหน่วยงานจากผู้ให้ข้อมูลชุดเดียวกัน กับการรวบรวมข้อมูลโดยเทคนิควิธีการสัมภาษณ์เชิงลึกตามข้อ 3.1.2 เป็นผู้ให้ข้อมูลสำคัญเพื่อการศึกษาตามวัตถุประสงค์การวิจัยในประเด็น แนวทางการป้องกันและปราบปรามการการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสด้วยการสำรวจความเห็นอย่างเป็นอิสระเชิงเสนอแนะจากผู้ให้ข้อมูลสำคัญแต่ละคน และในลำดับถัดไปเป็นกระบวนการสอบทานความเห็นของผู้ให้ข้อมูลสำคัญอย่างเป็นอิสระหลายรอบ จนมีแนวโน้มที่ได้ฉันทามติต่อผลการวิจัยในประเด็นที่ศึกษา ทั้งนี้การเริ่มต้นรอบแรกโดยคำถามปลายเปิดถึงแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม ควรเป็นอย่างไรต่อบริบทในประเทศไทยและสากล รวมถึงแนวการบังคับใช้เชิงปฏิบัติการเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม ต่อจากนั้นได้ทำการประมวลผลทางสถิติสำหรับข้อมูลความเห็นที่สำรวจจากผู้ให้ข้อมูลสำคัญทุกคน และทำการจัดอันดับแนวทางการป้องกันและปราบปราม รวมถึงแนวการบังคับใช้เชิงปฏิบัติการ ตามความเห็นของผู้ให้ข้อมูลสำคัญพร้อมผลวิเคราะห์ทางสถิติ จากนั้นทำการส่งผลการวิเคราะห์กลับไปยังผู้ให้ข้อมูลสำคัญแต่ละคนเพื่อแสดงความเห็นทบทวนหรือยืนยันอีกรอบ แล้วทำการวิเคราะห์ผลทางสถิติต่อเพื่อดำเนินกระบวนการเช่นนี้ในการสำรรวจซ้ำวนเวียนจนได้รับความเห็นจากผู้ให้ข้อมูลสำคัญเป็นฉันทามติ ต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส รวมถึงแนวการบังคับใช้เชิงปฏิบัติการเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ซึ่งโดยปกติจะดำเนินกระบวนการอย่างน้อย 3 รอบ หรือจนกว่าจะได้รับฉันทามติ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY


ระเบียบวิธีการวิจัย: การวิจัยเชิงคุณภาพ (Qualitative Research)
ผู้เชี่ยวชาญของหน่วยงานซึ่งหน้าที่รับผิดชอบเกี่ยวข้องกับการการป้องกันและปราบปรามการฟอกเงิน และการกำกับดูแลกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจสังคม
กลุ่มที่1 หน่วยงานองค์กรการป้องกันและปราบปรามการฟอกเงิน และการกำกับดูแลกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจสังคม
กลุ่มที่2 หน่วยงานองค์กรสถาบันการเงิน
กลุ่มที่3 หน่วยงานองค์กรกระบวนการยุติธรรม และหน่วยปฏิบัติงาน
กลุ่มที่4 หน่วยงานองค์กรธุรกิจ หรือผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงินและด้านอื่นๆ
การเลือกตัวอย่างแบบเฉพาะเจาะจงจาก 4 กลุ่ม
กลุ่มที่ 1
กลุ่มที่ 2
กลุ่มที่ 3
กลุ่มที่ 4
ผู้ให้ข้อมูลสำคัญ
การเก็บรวบรวมข้อมูลโดยวิธีการสัมภาษณ์เชิงลึก
1.กลไกการทำงานของเงินสกุลเข้ารหัส
2.รูปแบบอาชญากรรมที่ใช้เงินสกลุเข้ารหัสในการก่ออาชญากรรมและการฟอกเงิน
3.เทคนิคการสืบค้นผู้ต้องสงสัยในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส
4.แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมการเงินสกุลเข้ารหัสในไทยและสากล
5.แนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกลุเข้ารหัสที่สามารถเพิ่มประสิทธิภาพการบังคับใช้
การเก็บรวบรวมข้อมูลโดยเทคนิควิธีเดลฟาย
รอบที่ 1 สังเคราะห์ข้อมูลจากการสัมภาษณ์เชิงลึกและประมวลผลเพื่อจัดทำแบบสำรวจความคิดเห็นอิสระ
รอบที่ 2 สำรวจความเห็นตามแบบสำรวจความคิดเห็นอิสระและประมวลผลทางสถิติเบื้องต้นเพื่อสำรวจความเห็นในรอบต่อไป
รอบที่ 3 สำรวจความเห็นตามแบบทบทวนหรือยืนยันความคิดเห็นและประมวลผลทางสถิติเพื่อตรวจสอบฉันทามติ ถ้ายังไม่ได้ฉันทามติให้ทำการสำรวจความเห็นรอบต่อไปจนได้ฉันทามติ
สำรวจซ้ำ
วิเคราะห์และสังเคราะห์ข้อมูลเพื่อรายงานผลการศึกษา อภิปรายผล และสรุปผลการศึกษา

3.2 ผู้เชี่ยวชาญ และผู้ให้ข้อมูลสำคัญ

3.2.1 ผู้เชี่ยวชาญ

ในการศึกษาวิจัยนี้ได้กำหนดขอบเขตผู้เชี่ยวชาญซึ่งเป็นบุคคลากรประจำหน่วยงานซึ่งมีหน้าที่รับผิดชอบเกี่ยวข้องกับ การปฏิบัติตามมาตรการสากลว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย รวมถึงการกำกับดูแลการดำเนินกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม โดยได้จัดกลุ่มผู้เชี่ยวชาญตามภารกิจของหน่วยงานที่มีลักษณะหน้าที่รับผิดชอบออกเป็น 4 กลุ่ม ได้แก่ กลุ่มที่ 1 หน่วยงานราชการกระทรวง คณะกรรมการ หรือหน่วยงานหลักตามมาตรการสากลว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการกำกับดูแลการดำเนินกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม, กลุ่มที่ 2 หน่วยงานองค์กรสถาบันการเงิน, กลุ่มที่ 3 หน่วยงานองค์กรในกระบวนการยุติธรรม และหน่วยปฏิบัติงาน, และกลุ่มที่ 4 หน่วยงานด้านหน่วยงานองค์กรธุรกิจ หรือผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงินและด้านอื่นๆ

หน่วยงานกระทรวง คณะกรรมการ หรือหน่วยงานหลัก	**หน่วยงานด้านองค์กรสถาบันการเงิน**
(1) สำนักงานป้องกันและปราบปรามการฟอกเงิน	(1) ธนาคารแห่งประเทศไทย
(2) สำนักงานคณะกรรมการป้องกันและปราบปรามการทุจริตแห่งชาติ	(2) สมาคมธนาคารไทย
(3) สำนักงานป้องกันและปราบปรามยาเสพติด	(3) สมาคมธนาคารต่างชาติ
(4) กรมการประกันภัย	(4) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์
(5) กรมเศรษฐกิจระหว่างประเทศ	(5) สมาคมบริษัทหลักทรัพย์
(6) กรมสิทธิสัญญาและกฎหมาย	(6) สมาคมบริษัทจัดการลงทุน
(7) กรมตรวจบัญชีสหกรณ์	(7) บรรษัทบริหารสินทรัพย์สถาบันการเงิน
(8) สันติบาตสหกรณ์แห่งประเทศไทย	(8) บรรษัทตลาดรองสินเชื่อที่อยู่อาศัย
(9) กรมส่งเสริมสหกรณ์	(9) สมาคมประกันวินาศภัย
(10) กรมศุลกากร	(10) สมาคมประกันชีวิตไทย
(11) กรมสรรพสามิต	(11) ธนาคารออมสิน
(12) กรมสรรพากร	(12) ธนาคารอาคารสงเคราะห์
(13) สำนักงานคณะกรรมการกำกับการซื้อขายสินค้าเกษตรล่วงหน้า	(13) ธนาคารอิสลามแห่งประเทศไทย
(14) กรมการจัดหางาน	(14) ธนาคารเพื่อการส่งออกและนำเข้าแห่งประเทศไทย
(15) กรมการปกครอง	(15) ธนาคารพัฒนาวิสาหกิจขนาดกลางและขนาดย่อมแห่งประเทศไทย
(16) กรมที่ดิน	

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

(17) กระทรวงพัฒนาสังคมและความมั่นคงของมนุษย์ (18) สำนักงานคณะกรรมการวัฒนธรรมแห่งชาติ (19) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม (20) สำนักงานคณะกรรมการดิจิทัลเพื่อเศรษฐกิจและสังคมแห่งชาติ	(16) ธนาคารเพื่อการเกษตรและสหกรณ์การเกษตร (17) สำนักงานปลัดกระทรวงการคลัง (18) สำนักงานเศรษฐกิจการคลัง
ส่วนด้านองค์กรในกระบวนการยุติธรรมและหน่วยปฏิบัติงาน	**ส่วนงานด้านหน่วยธรุกิจ หรือผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงิน และด้านอื่นๆ**
(1) ศาลยุติธรรม (2) ศาลปกครอง (3) สำนักงานอัยการสูงสุด (4) กรมสอบสวนคดีพิเศษ (5) สำนักงานตำรวจแห่งชาติ (6) สำนักงานสภาความมั่นคงแห่งชาติ (7) สำนักข่าวกรองแห่งชาติ (8) สำนักคุ้มครองพยาน (9) กองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเทคโนโลยี	(1) สมาคมธุรกิจเช่าซื้อ (2) สมาคมค้าทองคำ (3) สมาคมผู้ค้าอัญมณีไทยและเครื่องประดับ (4) สมาคมเพชรพลอยเงินทอง (5) สมาคมผู้ผลิตอัญมณี (6) สมาคมการขายและตลาดอสังหาริมทรัพย์ (7) สภาทนายความ (8) สภาวิชาชีพการบัญชี (9) สมาคมฟินเทคประเทศไทย (10) สมาคมสินทรัพย์ดิจิทัลไทย (11) สมาคมไทยบล็อคเชน (12) สมาคมผู้ประกอบการพาณิชย์อิเล็กทรอนิกส์ไทย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

3.2.2 ผู้ให้ข้อมูลสำคัญ

การเลือกผู้ให้ข้อมูลสำคัญจากผู้เชี่ยวชาญประจำหน่วยงาน ตามกลุ่มภารกิจหน้าที่รับผิดชอบ ประกอบด้วยกลุ่มที่ 1 กลุ่มหน่วยงานหลักของภาครัฐมีหน้าที่รับผิดชอบโดยตรงต่อการป้องกันและปราบปรามการฟอกเงิน ซึ่งรวมถึงหน่วยงานรัฐที่มีหน้าที่รับผิดชอบกิจกรรมด้านเทคโนโลยี่ดิจิทัลเพื่อเศรษฐกิจและสังคม, กลุ่มที่ 2 หน่วยงานองค์กรสถาบันการเงินทั้งภาครัฐและภาคเอกชน, กลุ่มที่ 3 หน่วยงานในกระบวนการยุติธรรม และกลุ่มที่ 4 หน่วยงานผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงิน ซึ่งหมายรวมถึงผู้ประกอบการที่เกี่ยวข้องกับกิจกรรมเทคโนโลยี่ดิจิทัลเพื่อเศรษฐกิจและสังคม

ต่อจากนั้นทำการเลือกผู้ให้ข้อมูลสำคัญจากผู้เชี่ยวชาญประจำหน่วยงานจากแต่ละกลุ่ม โดยวิธีการเลือกแบบเฉพาะเจาะจง (Purposive Sampling) กล่าวคือ ทำการเลือกผู้ให้ข้อมูลสำคัญจากหน่วยงาน ที่มีหน้าที่ความรับผิดชอบเกี่ยวข้องกับการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัส

และการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยขอความร่วมมือจากหน่วยงานดังกล่าวเพื่อขอเข้าสัมภาษณ์ผู้ให้ข้อมูลสำคัญ ซึ่งเป็นบุคคลากรหรือผู้เชี่ยวชาญประจำหน่วยงานข้างต้นประมาณ 1 ถึง 3 คนต่อหน่วยงานขึ้นอยู่กับความสัมพันธ์ทางตรงกับวัตถุประสงค์การศึกษาวิจัย และความพร้อมของหน่วยงาน ทั้งนี้แผนการคัดเลือกผู้ให้ข้อมูลสำคัญแบบเฉพาะเจาะจงจำนวนประมาณ 17 ถึง 25 คน ดังนี้

กลุ่มหน่วยงานหลักของภาครัฐ (1) สำนักงานป้องกันและปราบปรามการฟอกเงิน (2) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม	3 – 5 คน
กลุ่มหน่วยงานองค์สถาบันการเงิน (1) สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (2) ธนาคารแห่งประเทศไทย (3) ธนาคารพาณิชย์ (4) ตลาดหลักทรัพย์แห่งประเทศไทย	4 – 6 คน
กลุ่มหน่วยงานในกระบวนการยุติธรรม (1) สำนักงานศาลยุติธรรม (2) สำนักงานอัยการสูงสุด (3) กรมสอบสวนคดีพิเศษ (4) สำนักงานตำรวจแห่งชาติ	5 - 7 คน
กลุ่มหน่วยงานผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงิน (1) ธุรกิจให้บริการที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล (2) สมาคมเกี่ยวข้องกับสินทรัพย์ดิจิทัล	5 - 7 คน

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

3.2.3 การคัดผู้ให้ข้อมูลสำคัญเข้า

ผู้วิจัยได้ศึกษาข้อมูลเบื้องต้นเกี่ยวกับบุคคลซึ่งจะคัดเข้าให้มีส่วนร่วมในการวิจัย จากผลงานและประสบการณ์ความเชี่ยวชาญของบุคคล ซึ่งคัดเลือกให้เป็นผู้ให้ข้อมูลสำคัญจากข้อมูลสาธารณะ ประกอบกับการศึกษาโครงสร้างหน้าที่ของหน่วยงานที่กำลังศึกษา รวมถึงคำแนะนำที่ได้รับจากผู้เชี่ยวชาญที่เกี่ยวข้องถึงบุคคลที่มีคุณสมบัติเหมาะสมต่อหัวข้อการวิจัย นอกจากนี้ได้ทำการติดต่อหน่วยงานของผู้ให้ข้อมูลสำคัญโดยตรง เพื่อขอคำแนะนำในการติดต่อบุคคลในหน่วยงานที่มีหน้าที่รับผิดชอบเกี่ยวข้องกับหัวข้อการวิจัยเพื่อขอโอกาสเข้าสัมภาษณ์ ทั้งนี้วิธีการติดต่อเริ่มต้นโดยการส่งข้อความแนะนำตัวผู้วิจัย หัวข้อการวิจัย ข้อมูลเบื้องต้นเกี่ยวกับการวิจัย รวมถึงแนวคำถามเบื้องต้นในการสัมภาษณ์ และขอความอนุเคราะห์กำหนดเวลาที่สะดวกเพื่อโทรเรียนชี้แจงรายละเอียด

เพิ่มเติมโดยตรง หรืออาจชี้แจงประเด็นสอบถามทาง SMS หรือ Line หรือ Email ตามวิธีการสื่อสารที่ผู้ให้ข้อมูลสำคัญสะดวก

เมื่อได้ทำการชี้แจงประเด็นข้อซักถามจากผู้เชี่ยวชาญ และบุคคลดังกล่าวให้ความยินยอมทางวาจาเป็นการเบื้องต้นที่จะมีส่วนร่วมในการวิจัยเป็นผู้ให้ข้อมูลสำคัญแล้ว ผู้วิจัยจะดำเนินการจัดทำหนังสือยินยอมของผู้ส่วนร่วมในการวิจัย เพื่อแจ้งให้ผู้มีส่วนร่วมในการวิจัยทำการตอบรับเป็นเอกสาร หรือการตอบรับทางวาจาในวันสัมภาษณ์ ทั้งนี้การติดต่อประสานงานโดยอาจใช้วิธีการสื่อสารอิเล็กทรอนิกส์ Email หรือ Line พร้อมทั้งขอนัดหมายวันเวลา และวิธีการให้สัมภาษณ์ล่วงหน้าไม่น้อยกว่า 10 วันตามช่วงเวลา และวิธีการที่ผู้ให้ข้อมูลสำคัญสะดวก รวมถึงการสัมภาษณ์ด้วยระบบออนไลน์

3.2.4 การคัดผู้ให้ข้อมูลสำคัญออก

ในกรณีที่ได้ทำการคัดเลือกผู้ให้ข้อมูลสำคัญแล้ว และผู้ให้ข้อมูลสำคัญได้เข้าร่วมการวิจัยในการให้ข้อมูลการสัมภาษณ์แล้ว แต่ไม่สามารถให้ข้อมูลได้ครบถ้วนในทุกประเด็นตามแนวคำถามการสัมภาษณ์เบื้องต้นแบบกึ่งโครงสร้าง ผู้วิจัยจะประเมินความพอเพียงเบื้องต้นของข้อมูลที่ได้รับก่อน หากข้อมูลที่ไม่สมบูรณ์เป็นประเด็นที่ไม่ส่งผลต่อคุณภาพข้อมูลอย่างมีนัยสำคัญ ผู้วิจัยจะนำข้อมูลส่วนที่สมบูรณ์ไปทำการวิเคราะห์ แต่หากผู้ให้ข้อมูลสำคัญไม่สามารถให้ข้อมูลได้เกินกว่าครึ่งหนึ่งของแนวคำถามการสัมภาษณ์เบื้องต้น ผู้วิจัยจะคัดข้อมูลจากผู้ให้ข้อมูลสำคัญบุคคลดังกล่าวออก และทำการพิจารณาต่อไปว่าบุคคลดังกล่าวอยู่ในกลุ่มผู้เชี่ยวชาญใด หากจำนวนผู้ให้ข้อมูลสำคัญยังอยู่ในเกณฑ์ตามแผนการคัดเลือกแบบเฉพาะเจาะจงข้างต้นก็จะไม่สรรหาบุคคลทดแทน อย่างไรก็ตามผู้จัยได้มีแนวปฏิบัติเพื่อป้องกันปัญหาดังกล่าวไว้ล่วงหน้า โดยผู้วิจัยได้ติดต่อและชี้แจงรายละเอียดเบื้องต้นของการวิจัย รวมถึงแนวคำถามการสัมภาษณ์ เพื่อให้บุคคลซึ่งจะถูกคัดเข้าเป็นผู้ให้ข้อมูลสำคัญได้พิจารณาล่วงหน้าก่อนการตัดสินใจตอบรับทางวาจา หากบุคคลดังกล่าวไม่พร้อมให้สัมภาษณ์ ผู้วิจัยก็จะดำเนินการสรรหาบุคคลอื่นทดแทนก่อนการเริ่มขั้นตอนการเก็บรวบรวมข้อมูล

3.2.5 การพิทักษ์สิทธิ ป้องกันความเสี่ยง และรักษาความลับของผู้ให้ข้อมูลสำคัญ

วิธีปฏิบัติเพื่อการพิทักษ์สิทธิของผู้ให้ข้อมูลสำคัญ โดยผู้วิจัยได้ชี้แจงสิทธิของผู้ให้ข้อมูลสำคัญ ซึ่งเป็นผู้มีส่วนร่วมในการวิจัยมีสิทธิที่จะไม่ตอบคำถามระหว่างการสัมภาษณ์และ/หรือการตอบแบบสำรวจความคิดเห็นได้ในทุกกรณีหากรู้สึกอึดอัด หรืออาจรู้สึกไม่สบายใจอยู่บ้างกับบางคำถาม และมีสิทธิถอนตัวออกเมื่อใดก็ได้ โดยไม่ต้องแจ้งให้ทราบล่วงหน้า และการไม่เข้าร่วมวิจัยหรือถอนตัวออกจะไม่มีผลกระทบต่อผู้ให้ข้อมูลสำคัญแต่อย่างใด

นอกจากนี้ผู้วิจัยได้ชี้แจงต่อผู้ให้ข้อมูลสำคัญ ถึงระบบการรักษาความปลอดภัยข้อมูลส่วนบุคคลของผู้ให้ข้อมูลสำคัญนั้นจะถูกเก็บรักษาไว้ โดยการอธิปรายผลการศึกษาต่อสาธารณะจะเป็นการรายงานลักษณะภาพรวม แต่หากมีความจำเป็นในการรายงานความเห็นรายบุคคลก็จะใช้นามแฝงแทน ซึ่งผู้ที่มีสิทธิเข้าถึงข้อมูลที่จัดเก็บจากการวิจัยจะมีเฉพาะผู้ที่เกี่ยวข้องกับการวิจัยนี้เท่านั้นทั้งนี้ผู้วิจัยจะทำลายข้อมูลที่จัดเก็บจากการวิจัยภายหลังเสร็จสิ้นกระบวนการวิจัย โดยข้อมูลประเภทเอกสารจะทำลายด้วยวิธีการย่อยเอกสาร ส่วนข้อมูลประเภทอิเล็กทรอนิกส์จะถูกลบล้างอย่างถาวรออกจากฐานข้อมูลและระบบสื่อสารจดหมายอิเล็กทรอนิกส์ของผู้วิจัย

3.3 เครื่องมือที่ใช้ในการวิจัย

3.3.1 ขั้นตอนการศึกษาวิจัยโดยเทคนิควิธีการสัมภาษณ์เชิงลึก

การศึกษาวิจัยนี้ใช้ระเบียบวิจัยเชิงคุณภาพด้วยการดำเนินการเป็น 3 ขั้นตอน เริ่มขั้นตอนการศึกษาวิจัย โดยเทคนิควิธีการสัมภาษณ์เชิงลึกกับผู้ให้ข้อมูลสำคัญจากหน่วยงานที่คัดเลือกทั้งนี้เพื่อให้สามารถรวบรวมข้อมูลได้ครบถ้วนตามวัตถุประสงค์การวิจัย จึงได้ทำการออกแบบกรอบการสัมภาษณ์แบบกึ่งโครงสร้าง โดยวางแนวหัวข้อการสัมภาษณ์เบื้องต้น ดังนี้ (ภาคผนวก ข)

(1) ปัจจัยสำคัญอะไรบ้าง ในกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสที่อาจมีอิทธิพลต่ออาชญากรในการตัดสินใจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน

(2) รูปแบบของอาชญากรรมประเภทใดบ้าง ที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการประกอบอาชญากรรมและในการทำธุรกรรมฟอกเงิน เพราะอะไร

(3) เทคนิควิธีการติดตามสืบค้นหาผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัสที่ใช้เป็นเครื่องมือในการฟอกเงิน ควรมีลักษณะการดำเนินการอย่างไร

(4) แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน ควรเป็นอย่างไร

(5) แนวทางปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงิน โดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะและสามารถเพิ่มประสิทธิภาพการบังคับใช้เชิงปฏิบัติการ ควรเป็นอย่างไร

ทั้งนี้หัวข้อการสัมภาษณ์เบื้องต้นใช้เป็นกรอบการศึกษาวิจัยโดยการสัมภาษณ์เชิงลึกกับผู้ให้ข้อมูลสำคัญทุกกลุ่มด้วยชุดคำถามเดียวกัน เพื่อให้ได้รับข้อมูลเชิงทัศนะจากผู้ให้ข้อมูลสำคัญต่างกลุ่มต่อประเด็นคำถามเดียวกัน ซึ่งอาจทำให้ได้รับข้อมูลอย่างรอบด้านจากบุคคลที่มีหน้าที่ความรับผิดชอบเกี่ยวข้องกับการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัส และการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส อย่างไรก็ตามในขณะสัมภาษณ์ได้ปิดกว้างในการรับฟังข้อมูลจากผู้ให้ข้อมูลสำคัญสำหรับประเด็นอื่นซึ่งเกี่ยวข้องกับขอบเขตการวิจัย

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

3.3.2 ขั้นตอนการศึกษาวิจัยโดยเทคนิควิธีเดลฟาย

ทั้งนี้เพื่อการศึกษาในประเด็นแนวทางการป้องกันและปราบปรามการฟอกเงิน โดยธุรกรรมเงินสกุลเข้ารหัส รวมถึงแนวการบังคับใช้เชิงปฏิบัติการเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม โดยเทคนิควิธีเดลฟายรูปแบบปรับปรุงด้วยการสำรวจความเห็นอิสระเชิงแนะนำจากผู้ให้ข้อมูลสำคัญ ด้วยเครื่องมือการสำรวจความเห็น ดังนี้

(1) การสำรวจความเห็นรอบที่ 1 เป็นการสำรวจความเห็นอิสระแบบคำถามปลายเปิดจากผู้ให้ข้อมูลสำคัญทุกคน ในประเด็นแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส รวมถึงแนวทางการบังคับใช้เชิงปฏิบัติการเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม โดยทำการสำรวจความเห็นจากผู้ให้ข้อมูลสำคัญในขณะทำการสัมภาษณ์เชิงลึก

(2) การสำรวจความเห็นรอบที่ 2 เป็นการสำรวจความเห็นอิสระจากผู้ให้ข้อมูลสำคัญโดยใช้แบบสำรวจความเห็น ซึ่งเป็นข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุล รวมถึงข้อเสนอแนวทางการบังคับใช้เชิงปฏิบัติการเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมที่ได้จากการเก็บรวมรวมข้อมูลโดยการสัมภาษณ์เชิงลึก พร้อมข้อมูลสถิติประกอบที่ได้จากการวิเคราะห์ทางสถิติต่อผลการสำรวจความเห็นรอบที่ 1

(3) การสำรวจความเห็นรอบที่ 3 เป็นการสำรวจความเห็นอิสระจากผู้ให้ข้อมูลสำคัญชุดเดิมโดยใช้แบบสำรวจความเห็น ซึ่งแสดงผลสรุปความเห็นประกอบการวิเคราะห์ทางสถิติต่อผลการสำรวจความเห็นรอบที่ 2 ในประเด็นข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส รวมถึงข้อเสนอแนวทางการบังคับใช้เชิงปฏิบัติการเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม เพื่อผู้ให้ข้อมูลสำคัญได้ทบทวนหรือยืนยันความเห็น จากนั้นจะทำการวิเคราะห์ทางสถิติต่อผลสำรวจความเห็นรอบที่ 3 ว่าได้รับฉันทามติจากผู้ให้ข้อมูลสำคัญหรือไม่ หากยังไม่ได้ฉันทามติจากผลสำรวจความเห็นของผู้ให้ข้อมูลสำคัญก็จะดำเนินกระบวนการเช่นนี้ต่อไปจนได้รับความเห็นที่มีระดับความคงที่เป็นฉันทามติ จึงถือเป็นการสิ้นสุดกระบวนการวิจัยในขั้นตอนนี้

3.4 การเก็บรวบรวมข้อมูล

3.4.1 ศึกษาค้นคว้าและรวบรวมข้อมูล จากหนังสือ วารสาร เอกสาร บทบัญญัติของกฎหมาย และงานวิจัยที่เกี่ยวข้อง รวมถึงข้อมูลวารสารอิเล็กทรอนิกส์ เพื่อศึกษาทำความเข้าใจถึงบริบทของเงินสกุลเข้ารหัส พฤติกรรมการกระทำผิดในบริบทของกระบวนการฟอกเงินโดยธุรกรรม

เงินสกุลเข้ารหัส และกรอบแนวคิดเชิงทฤษฎีอาชญาวิทยา รวมถึงมาตรการกำกับทางกฎหมายที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและการป้องกันการฟอกเงิน

3.4.2 วิเคราะห์ข้อมูลจากการค้นคว้า เพื่อค้นหาประเด็นสำหรับการออกแบบคำถามการสัมภาษณ์เบื้องต้นแบบกึ่งโครงสร้าง สำหรับการสัมภาษณ์เชิงลึกกับผู้ให้ข้อมูลสำคัญซึ่งถูกเลือกแบบเฉพาะเจาะจงดังกล่าวข้างต้นนั้น โดยผู้วิจัยเตรียมคำถามเพื่อการสัมภาษณ์ล่วงหน้าตามกรอบแนวหัวข้อคำถามเบื้องต้น แต่อาจปรับเปลี่ยนหัวข้อคำถามตามความเหมาะสมกับหน้าที่ความรับผิดชอบของผู้ให้ข้อมูลสำคัญ และเปิดรับฟังข้อมูลในประเด็นเพิ่มเติมตามความเห็นของผู้ให้ข้อมูลสำคัญ พร้อมทั้งกำกับการสัมภาษณ์ให้อยู่ภายในขอบเขตของการวิจัย

3.4.3 การรวบรวมผลการสำรวจความเห็นอิสระของผู้ให้ข้อมูลสำคัญ ในประเด็นแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส รวมถึงแนวทางการบังคับใช้เชิงปฏิบัติการเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ด้วยเทคนิควิธีเดลฟาย ซึ่งทำการรวบรวมข้อมูลสำรวจความเห็นอิสระของผู้ให้ข้อมูลสำคัญแต่ละรอบ พร้อมทั้งทำการวิเคราะห์ผลสำรวจทางสถิติ เพื่อนำรายงานสรุปผลสำรวจย้อนกลับไปสำรวจความเห็นจากผู้ให้ข้อมูลสำคัญอีกรอบ จนกว่าจะได้ผลสรุปความเห็นที่มีระดับความคงที่อย่างเป็นฉันทามติของผู้ให้ข้อมูลสำคัญ ทั้งนี้ด้วยข้อจำกัดด้านระยะเวลาการวิจัยและโดยสถานการณ์ จึงอาจใช้วิธีการรวบรวมข้อมูลสำรวจความเห็น โดยจดหมายอิเล็กทรอนิกส์แทนการสัมภาษณ์รายบุคคลโดยตรงในแต่ละรอบของการสำรวจ รวมถึงการทบทวนหรือยืนยันความเห็น

ในกรณีการเก็บข้อมูลตอบกลับการสำรวจความเห็นอิสระจากผู้ให้ข้อมูลสำคัญด้วยวิธีเทคนิคเดลฟายในแต่ละรอบ หากปรากฏว่าได้รับข้อมูลตอบกลับไม่ครบจำนวนที่ได้จัดส่งไปสำรวจ โดยมีจำนวนผู้ตอบกลับตั้งแต่ 17 รายขึ้นไป ผู้วิจัยจะดำเนินการสำรวจความเห็นต่อเนื่องในรอบต่อไป แต่ถ้าผู้ตอบกลับมีจำนวนอยู่ระหว่าง 13 - 17 ราย ผู้วิจัยจะยังดำเนินการสำรวจความเห็นต่อเนื่องในรอบต่อไป โดยจะระบุเป็นประเด็นข้อสังเกตุในการรายงานผลการศึกษา แต่ถ้าผู้ตอบกลับมีจำนวนต่ำกว่า 13 ราย ผู้วิจัยอาจใช้ดุลยพินิจยุติการสำรวจความเห็นในรอบต่อไปทันที ทั้งนี้ขึ้นอยู่กับจำนวนผู้ตอบกลับด้วยเช่นกัน พร้อมทั้งจะได้ระบุเป็นประเด็นสาเหตุในการยุติการสำรวจความเห็นในการรายงานผลการศึกษาต่อไป

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

3.5 การวิเคราะห์ข้อมูล

การวิเคราะห์ข้อมูลจะนำข้อมูลที่ได้รับจากการศึกษาทางเอกสาร วิเคราะห์ร่วมกับการสัมภาษณ์เชิงลึก โดยวิธีการวิเคราะห์แนวอุปนัย (Analytic Induction) ด้วยการตรวจสอบ

ประเมินคุณค่าของข้อมูลที่ได้รวบรวมและความเพียงพอของข้อมูล เพื่อการวิเคราะห์หาคำตอบ จัดแยกหมวดหมู่ของข้อมูล เพื่อประกอบการวิเคราะห์หาคำตอบแต่ละประเด็นปัญหาให้ครอบคลุมวัตถุประสงค์การวิจัย ตรวจสอบความครบถ้วนของคำตอบของแต่ละประเด็นปัญหา จากนั้นรวบรวมผลการวิเคราะห์เพื่อการพรรณาปรากฏการณ์ พร้อมการตีความผลการวิเคราะห์เพื่อนำไปสู่การรายงานสรุปผลการศึกษาถึงสิ่งที่ค้นพบจากการวิจัย

นอกจากนี้ ได้ทำการวิเคราะห์ผลสำรวจความเห็นอิสระเชิงเสนอแนะที่รวบรวมได้จากเทคนิควิธีเดลฟาย เพื่อการตีความผลสำรวจความเห็น วิเคราะห์อภิปรายความเห็น และสังเคราะห์สิ่งที่ค้นพบ สรุปเป็นข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อบริบทของประเทศไทยและสากลในปัจจุบัน รวมถึงข้อเสนอแนวปฏิบัติเพื่อการบังคับใช้เชิงปฏิบัติการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะ และสามารถเพิ่มประสิทธิภาพการดำเนินงาน โดยอาศัยค่าสถิติประกอบการวิเคราะห์ตามแนวเทคนิควิธีเดลฟายด้วยการวัดระดับความเห็น 5 ระดับ ดังนี้

การวิเคราะห์ระดับความคงที่ของความเห็น (Stability) ซึ่งเป็นการวัดระดับการเปลี่ยนแปลงทางความเห็นเปรียบเทียบกับการสำรวจรอบที่ผ่านมา ถ้าระดับการเปลี่ยนแปลงทางความเห็นระหว่างการสำรวจทั้ง 2 รอบยังคงมีความแตกต่างกันมาก ก็จะดำเนินการสำรวจความเห็นในรอบต่อไป แต่ถ้าระดับการเปลี่ยนแปลงทางความเห็นอยู่ในระดับคงที่ก็จะยุติการสำรวจความเห็นและทำการวิเคราะห์ข้อมูลเพื่อรายงานผลต่อไป โดยใช้ค่าสถิติ อัตราร้อยละเป็นเกณฑ์วัดระดับความคงที่ของความเห็นจากความแตกต่างของผลสำรวจรอบที่ผ่านมาเปรียบเทียบกับผลสำรวจรอบปัจจุบันต้องมีค่าไม่เกินร้อยละ 15.0 และค่าสถิติ F-Test เป็นเกณฑ์วัดค่าความแปรปรวนเปรียบเทียบของระดับความเห็นจากการสำรวจทั้งสองรอบ โดยต้องมีค่าสถิติที่ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ

การวิเคราะห์ความเป็นฉันทามติ (Consensus) ทั้งนี้การตรวจสอบความเป็นฉันทามติ จะดำเนินการก็ต่อเมื่อความเห็นมีระดับความคงที่และยุติการสำรวจความเห็นรอบต่อไปแล้ว โดยการวัดระดับการยอมรับความเห็นพ้องกันอย่างเพียงพอ ต่อการสรุปผลเป็นความเห็นร่วมกันของผู้ให้ข้อมูลสำคัญ โดยใช้ค่าสถิติ ค่าสัมประสิทธิ์การกระจาย (coefficient of variation) ที่มีค่าการกระจายของความเห็นไม่เกิน 0.5 และค่าสัมบูรณ์ของผลต่างระหว่างค่ามัธยฐาน (Median) และค่าฐานนิยม (Mode) ของความเห็นมีค่าไม่เกิน 1.00 รวมถึงค่าพิสัยระหว่างควอไทล์ (Interquartile Range) ของความเห็นมีค่าไม่เกิน 1.50 ทั้งนี้ในกรณีที่ผลทดสอบค่าสถิติเข้าเกณฑ์ครบทั้งสามกรณี ก็จะถือว่าความเห็นดังกล่าวได้รับฉันทามติจากผู้ให้ข้อมูลสำคัญ

การวิเคราะห์ความเป็นฉันทามติเสียงข้างมาก (Majority of Consensus) ซึ่งเป็นการวัดระดับการยอมรับความเห็นร่วมกันด้วยเสียงข้างมากระดับสูงของผู้ให้ข้อมูลสำคัญ โดยใช้ค่าสถิติ ค่าเฉลี่ย (Mean) ของระดับความเห็นตั้งแต่ 4.00 ขึ้นไป และค่ามัธยฐาน (Median) ของระดับ

ความเห็นตั้งแต่ 4.00 ขึ้นไป และอัตราร้อยละของผลรวมความเห็นระดับ 5 (“มากที่สุด”) และระดับ 4 (“มาก”) มีค่าตั้งแต่ร้อยละ 75.00 ขึ้นไป

3.6 ระยะเวลาการวิจัย

การวิจัยนี้มีการดำเนินกิจกรรมการวิจัยทุกขั้นตอนตลอดโครงการ เป็นระยะเวลาประมาณ 1 ปี ตั้งแต่เดือนกรกฎาคม 2563 ถึงเดือนมิถุนายน 2564

3.7 จริยธรรมการวิจัย

ผู้วิจัยได้เสนอโครงการวิจัยเพื่อขอรับการพิจารณาจริยธรรมการวิจัยในคน โดยได้รับการพิจารณาแบบลดขั้นตอน (Expedited Review) และได้รับการอนุมัติรับรองเป็นโครงการวิจัยที่ 027/64 เรื่อง แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส (PREVENTION AND SUPPRESSION OF MONEY LAUNDERINGBY CRYPTOCURENCY TRANSACTION) จากคณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย (ภาคผนวก ก)

ทั้งนี้ ผู้วัจัยได้ให้ความสำคัญต่อความยินยอมเข้ามีส่วนร่วมในการวิจัยโดยความสมัครใจจากผู้ให้ข้อมูลสำคัญ โดยก่อนการตัดสินใจเข้าร่วมการวิจัยตามคำเชิญ ผู้วิจัยได้นำเสนอเอกสารข้อมูลสำหรับผู้มีส่วนร่วมในการวิจัยตามแบบ AF04-07 ให้ผู้ให้ข้อมูลสำคัญได้พิจารณาพร้อมทั้งชี้แจงรายละเอียดและตอบข้อซักถาม ในประเด็นเกี่ยวกับโครงการวิจัยรวมถึงภาระหน้าที่และผลกระทบที่อาจมีต่อผู้ให้ข้อมูลสำคัญเพื่อขอความยินยอม โดยผู้ให้ข้อมูลสำคัญสามารถตอบรับเป็นเอกสารตามแบบ AF05-07 หนังสือยินยอมเข้าร่วมในการวิจัย หรือตอบรับทางวาจาในวันกำหนดนัดสัมภาษณ์เพื่อเก็บรวบรวมข้อมูล และผู้ให้ข้อมูลสำคัญสามารถถอนตัวออกจากการวิจัยเมื่อใดก็ได้ตามความประสงค์โดยไม่ต้องแจ้งเหตุผลซึ่งการถอนตัวออกจากการวิจัย และจะไม่มีผลกระทบทางลบใดๆต่อผู้ให้ข้อมูลสำคัญ นอกจากนี้ผู้วิจัยได้คำนึงถึงความเป็นส่วนตัวในการเก็บรักษาความลับโดยจะไม่ทำการเปิดเผยข้อมูลใดในรายงานที่จะนำไปสู่การระบุถึงผู้ให้ข้อมูลำคัญต่อสาธารณะเป็นรายบุคคล โดยจะนำเสนอรายงานผลการวิจัยเป็นภาพรวมเท่านั้น ทั้งนี้ผู้ที่มีสิทธิเข้าถึงข้อมูลรายบุคคลจะมีเฉพาะผู้ที่เกี่ยวข้องกับการวิจัยนี้ และคณะกรรมการจริยธรรมการวิจัยในคนเท่านั้น อีกทั้งข้อมูลที่ได้จากการสัมภาษณ์ผู้วิจัยจะดำเนินการทำลายข้อมูลที่ได้รับจากการสัมภาษณ์ และข้อมูลจากการตอบแบบสำรวจความคิดเห็นตลอดจนข้อมูลอื่นๆ ทั้งหมดที่เกี่ยวข้องกับผู้ให้ข้อมูลสำคัญ ภายหลังเสร็จสิ้นการวิจัยและได้นำเสนอรายงานต่อคณะกรรมการสอบโครงการวิทยานิพนธ์เป็นที่เรียบร้อย โดยการทำลายข้อมูล

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ประเภทเอกสารจะดำเนินการด้วยวิธีการย่อยเอกสาร สำหรับข้อมูลประเภทอิเล็กทรอนิกส์จะลบล้างอย่างถาวรออกจากฐานข้อมูล และระบบสื่อสารจดหมายอิเล็กทรอนิกส์

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

บทที่ 4
ผลการศึกษาแลการอภิปรายผลการศึกษา

การศึกษาวิจัยเรื่อง “แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส” มีวัตถุประสงค์เพื่อศึกษาคุณลักษณะเฉพาะ กลไกการทำงาน และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส ซึ่งเป็นปัจจัยที่มีอิทธิพลต่ออาชญากรในการตัดสินใจใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน รวมถึงรูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและใช้กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส สำหรับผลประโยชน์ที่ได้รับจากการกระทำผิด และแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากลในปัจจุบัน

ในการนำเสนอผลการศึกษานี้ ผู้วิจัยได้วิเคราะห์ข้อมูลโดยอาศัยข้อมูลเชิงคุณภาพจากการสมัภาษณ์เชิงลึก เพื่อวิเคราะห์เนื้อหาในส่วนที่เกี่ยวกับกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัส และปัจจัยที่อาจมีอิทธิพลต่ออาชญากรในการเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมการฟอกเงิน รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และมีโอกาสทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส และเทคนิควิธีการในกระบวนการติดตามสืบสวนหาผู้ต้องสังสัยในระบบนิเวศที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน นอกจากนี้ผู้วิจัยได้วิเคราะห์ข้อมูลโดยอาศัยข้อมูลเชิงคุณภาพจากการสมัภาษณ์เชิงลึก ร่วมกับเทคนิควิธีเดลฟายเพื่อวิเคราะห์เนื้อหา และประมวลข้อมูลทัศนะเชิงเสนอแนะ ในส่วนที่เกี่ยวกับแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม ต่อการปรับใช้กับบริบทของประเทศไทยและสากลในปัจจุบัน และแนวทางปฏิบัติเพื่อการบังคับใช้เชิงปฏิบัติต่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะ และสามารถเพิ่มประสิทธิภาพการดำเนินงาน อันนำมาสู่การสร้างข้อสรุปตลอดจนการตีความข้อค้นพบที่ได้จากการศึกษา อย่างไรก็ตามการนำเสนอผลการศึกษาอาศัยกระบวนการสังเคราะห์ข้อมูล จากการถ่ายทอดเรื่องราว ประสบการณ์ รวมถึงการแสดงความเห็นเชิงทัศนะของผู้ให้ข้อมูลสำคัญซึ่งเป็นบุคคลากรผู้เชี่ยวชาญประจำหน่วยงานทั้งภาครัฐและภาคเอกชนที่มีหน้าที่รับผิดชอบเกี่ยวข้องกับ การปฏิบัติตามมาตรการสากลว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่ การก่อการร้าย รวมถึงการกำกับดูแลการดำเนินกิจกรรมด้านเทคโนโลยี่ดิจิทัลเพื่อเศรษฐกิจและสังคม จำนวนรวม 19 ราย ได้แก่

ผู้ให้ข้อมูลสำคัญ	จำนวนผู้ให้ข้อมูลสำคัญ		
1. กลุ่มหน่วยงานหลักของภาครัฐ	**3**		**รหัสนามแฝง**
1.1 สำนักงานป้องกันและปราบปรามการฟอกเงิน		3	#111, #112, #113
2. กลุ่มหน่วยงานองค์กรสถาบันการเงิน	**7**		
2.1 สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์		2	#211, #212
2.2 ธนาคารแห่งประเทศไทย		1	#221
2.3 ธนาคารพาณิชย์		2	#231, #232
2.4 ตลาดหลักทรัพย์แห่งประเทศไทย		2	#241, #242
3. กลุ่มหน่วยงานในกระบวนการยุติธรรม	**5**		
3.1 สำนักงานศาลยุติธรรม		1	#311
3.2 สำนักงานอัยการสูงสุด		1	#321
3.3 กรมสอบสวนคดีพิเศษ		2	#331, #332
3.4 สำนักงานตำรวจแห่งชาติ		1	#341
4. กลุ่มหน่วยงานผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงิน	**4**		
4.1 ธุรกิจที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล		3	#411, #412, #413
4.2 สมาคมที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล		1	#421
รวมจำนวนผู้ให้ข้อมูลสำคัญ	**19**	**19**	

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ทั้งนี้ การสังเคราะห์ดังกล่าว ได้อาศัยข้อมูลเพิ่มเติมจากแหล่งข้อมูลจากหน่วยงานภาครัฐและภาคประชาชน รวมถึงเอกสารสำคัญของทางราชการประกอบการวิเคราะห์ข้อมูล และการคัดกรองความจริงทั้งหมด เพื่อให้ได้มาซึ่งข้อเสนอแนะต่อการพัฒนากระบวนการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินลกุลเข้ารหัสได้ทันต่อการเปลี่ยนแปลงทางเทคโนโลยี่ และพัฒนาการทางพฤติกรรมของอาชญากร โดยผู้วิจัยขอนำเสนอผลการศึกษาตามลำดับ ดังนี้

4.1 ปัจจัยสำคัญในกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสที่อาจมีอิทธิพลต่ออาชญากรในการตัดสินใจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องในการทำธุรกรรมฟอกเงิน

4.1.1 ปัจจัยกลไกการทำงานแบบกระจายศูนย์ไร้การควบคุมจากหน่วยงานใด

4.1.2 ปัจจัยการอำพรางตัวตน และความยากต่อการสืบค้นเส้นทางธุรกรรม

4.1.3 ปัจจัยด้านความสะดวก รวดเร็ว และสามารถทำธุรกรรมข้ามประเทศ

4.1.4 ปัจจัยการรักษามูลค่าทรัพย์สินด้วยต้นทุนการดูแลต่ำ

4.1.5 ปัจจัยด้านมาตรการทางกฎหมายและการบังคับใช้เชิงปฏิบัติ

4.1.6 สรุปบริบทของเงินสกุลเข้ารหัสที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

4.2 รูปแบบของอาชญากรรมที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการประกอบอาชญากรรม และในการทำธุรกรรมฟอกเงิน

4.2.1 การหลอกลวงฉ้อโกงประชาชนในลักษณะแชร์ลูกโซ่ (Ponzi Scheme)

4.2.2 การค้ายาเสพติด รวมถึงการค้าบนระบบออนไลน์

4.2.3 การเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิวเตอร์เข้าทำลายระบบงาน

4.2.4 การพนันรวมถึงการพนันบนระบบออนไลน์

4.2.5 สรุปรูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและใช้เป็นเครื่องมือในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

4.3 เทคนิควิธีการติดตามสืบค้นหาผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัสที่ใช้เป็นเครื่องมือในการฟอกเงิน

4.3.1 การสืบค้นผู้ต้องสงสัยผ่านทางผู้ให้บริการรับอนุญาต

4.3.2 การใช้โปรแกรมการตรวจสอบ Digital Forensic Program ช่วยสืบค้น

4.3.3 การวิเคราะห์พฤติกรรมและเชื่อมโยงความมีตัวตนกับระบบงานอื่น

4.3.4 สรุปเทคนิควิธีการติดตามสืบค้นหาตัวผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส

4.4 แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน และแนวทางปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะและสามารถเพิ่มประสิทธิภาพการบังคับใช้เชิงปฏิบัติการ

4.4.1 ข้อเสนอต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

4.4.2 ข้อเสนอต่อแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

4.4.3 การสำรวจความเห็นอิสระและการวิเคราะห์โดยเทคนิควิธีเดลฟาย

4.4.4 สรุปผลการศึกษาข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม รวมถึงข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินที่เหมาะสมและเพิ่มประสิทธิภาพในการบังคับใช้เชิงปฏิบัติการ

4.5 การอภิปรายผลการศึกษา

4.5.1 กระบวนทัศน์ต่อมุมมองเงินสกุลเข้ารหัสกับความเป็นเงินตรา และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัสที่เหมาะสมต่อบริบทของประเทศไทย

4.5.2 ปัจจัยปัจจัยสำคัญในกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสที่อาจมีอิทธิพลต่ออาชญากรในการตัดสินใจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องในการทำธุรกรรมฟอกเงิน

4.5.3 รูปแบบของอาชญากรรมที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการประกอบอาชญากรรม และในการทำธุรกรรมฟอกเงิน

4.5.4 แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน และแนวทางปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะ และสามารถเพิ่มประสิทธิภาพการบังคับใช้เชิงปฏิบัติการ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

4.1 ปัจจัยสำคัญในกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสที่อาจมีอิทธิพลต่ออาชญากรในการตัดสินใจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องในการทำธุรกรรมฟอกเงิน

จากการศึกษาโดยการสัมภาษณ์เชิงลึก เพื่อรวบรวมข้อมูลเชิงทัศนะจากผู้ให้ข้อมูลสำคัญ ซึ่งเป็นผู้เชี่ยวชาญที่มีหน้าที่รับผิดชอบเกี่ยวข้องกับการปฏิบัติตามมาตรการสากลว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย รวมถึงการกำกับดูแลการดำเนินกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม พบว่า ผู้ให้ข้อมูลสำคัญส่วนใหญ่มีความเห็นตรงกัน ถึงปัจจัยที่เป็นแรงจูงใจและมีอิทธิพลต่ออาชญากรในการเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน ประกอบด้วยปัจจัยด้านเทคโนโลยีซึ่งเป็นคุณลักษณะเฉพาะของเงินสกุลเข้ารหัส และกลไกการทำงานของเงินสกุลเข้ารหัสบนระบบปฏิบัติการ

บล็อกเชนซึ่งเป็นระบบนิเวศแบบกระจายศูนย์ที่ไม่มีตัวกลาง หรือหน่วยงานใดทำหน้าที่กำกับดูแลจัดการธุรกรรม ปัจจัยด้านเศรษฐศาสตร์ และปัจจัยด้านกฎระเบียบในการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัส ทั้งนี้ประกอบด้วยปัจจัยย่อยที่สำคัญหลายประการ ดังนี้

4.1.1 ปัจจัยกลไกการทำงานแบบกระจายศูนย์ไร้การควบคุมจากหน่วยงานใด

ระบบนิเวศเงินสกุลเข้ารหัสเป็นระบบปฏิบัติการบล็อกเชน เพื่อการติดต่อโอนมูลค่าด้วยรหัสข้อมูลกันโดยตรงระหว่างผู้ใช้งาน (Peer-to-Peer หรือ P2P) ในลักษณะไม่มีหน่วยงานกลางตัวแทน หรือผู้ดูแลระบบเป็นผู้กำกับจัดการควบคุมระบบการทำงาน (Nakamoto, 2008) แต่มีกลไกในการสร้างความน่าเชื่อถือ ต่อรายการโอนมูลค่าระหว่างผู้โอนและผู้รับโอนที่อาจไม่มีประวัติความสัมพันธ์ต่อกันมาก่อน ด้วยระบบการตรวจพิสูจน์ยืนยันรายการ (Proof of Work -Pow) ที่สร้างแรงจูงใจให้ผู้ใช้งานซึ่งกระจายอยู่ทั่วไป เชื่อมต่อเข้าสู่ระบบนิเวศเพื่อแข่งขันเป็นผู้ตรวจพิสูจน์ยืนยันรายการด้วยการแก้โจทย์รหัสทางคณิตาสตร์ประจำชุดข้อมูล (Block) โดยการยืนยันด้วยฉันทามติของผู้ร่วมดำเนินการ (หรือเรียกทางเทคนิคว่า 51% Attack) นอกจากนี้ผู้ใช้งานทั่วไปยังสามารถเข้าถึงฐานข้อมูล ที่ถูกบันทึกในสมุดบัญชีอิเล็กทรอนิกส์ของระบบนิเวศเงินสกุลเข้ารหัสได้อย่างไม่มีข้อจำกัด รวมถึงสามารถติดตามความเคลื่อนไหวของรายการระหว่างผู้ใช้งานต่างๆในระบบนิเวศได้ ที่เรียกว่า Distributed Ledger Technology – DLT (Burniske & Tara, 2017) ดังนั้นกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสที่ไม่หน่วยงานกลาง หรือผู้กำกับดูแลจัดการธุรกรรมการโอนมูลค่าระหว่างกันจึงเป็นโอกาสแก่อาชญากรที่จะเลือกใช้เป็นเครื่องมือในการฟอกเงิน เนื่องจากแนวทางการป้องกันและปราบปรามการฟอกเงินโดยทั่วไป มักจะมุ่งกำหนดมาตรการกำกับธุรกรรมการเงินผ่านทางสถาบันการเงินซึ่งเป็นหน่วยงานผู้ให้บริการแก่ผู้ประสงค์ทำธุรกรรมการเงินทั้งภายในประเทศ และระหว่างประเทศ โดยสถาบันการเงินจะทำหน้าที่เป็นตัวกลางในการดำเนินการโอนมูลค่าและบันทึกรายการที่เกี่ยวข้องกับมูลค่าของเงินจากผู้โอน ผ่านระบบงานเครือข่ายของระบบสถาบันการเงินไปยังสถาบันการเงินปลายทางและผู้รับโอนในที่สุด ดังเช่น สหภาพยุโรปที่ยึดถือกรอบแนวปฏิบัติการป้องกันการฟอกเงินลักษณะ “ผู้เฝ้าประตู (Gate Keeper)” โดยมุ่งกำกับดูแลการหมุนเวียนเงินเฉพาะเมื่อทำธุรกรรมแปลงเงินสกุลเข้ารหัสเป็นเงินตราทั่วไป หรือการแปลงเป็นสินทรัพย์ที่มีตัวตนเป็นสำคัญ (Frick, 2019) และประกอบความเห็นของผู้ให้ข้อมูลสำคัญ ได้แก่

ความเห็นของผู้ให้ข้อมูลสำคัญ #113

“เสน่ห์สำคัญของเงินสกุลเข้ารหัสเป็นเทคนิคในการปกปิดอำพรางตัวตน โดยมีหลักการทำงานที่สำคัญคือการแปลงระบบงาน Centralized ไปเป็น Decentralized ทำให้ปลอดจากการติดตามหรือกำกับดูแลของหน่วยงานรัฐ”

ความเห็นของผู้ให้ข้อมูลสำคัญ #241

“หากจะเปรียบเทียบธนบัตรเป็นรูปแบบโทเคน (Token) ของเงินตราที่ใช้เป็นสื่อกลางในการแลกเปลี่ยนมูลค่า หรือเหมือนกับตั๋วโดยสารก็เป็นโทเคนลักษณะหนึ่งที่สามารถโอนเปลี่ยนมือกันได้โดยไม่จำเป็นต้องมีตัวกลางมาดำเนินการ หรือแม้แต่หุ้นในตลาดหลักทรัพย์ก็เป็นโทเคนลักษณะหนึ่งเช่นกัน แต่มีหน่วยงานกลางหรือตัวกลางในการกำกับและดำเนินธุรกรรม ส่วนเงินสกุลเข้ารหัสก็เป็นโทเคนเหมือนกันแต่มีรูปแบบเป็นดิจิทัล ซึ่งสามารถโอนจากคนหนึ่งไปให้อีกคนหนึ่งได้โดยไม่ต้องมีตัวกลางมากำกับการดำเนินงาน ซึ่งระบบสามารถทำงานได้เอง เช่น บิตคอยน์ อีเทอเรียม เพียงแต่ผู้ใช้งานเข้าระบบเพื่อขอเปิดบัญชีกระเป๋าเงินอิเล็กทรอนิกส์ และส่งรหัสข้อมูลไปยังกระเป๋าเงินของผู้รับ ผู้รับปลายทางก็ใช้รหัสเปิดส่วนบุคคลเป็นเทคโนโลยีในการเข้ารหัส และถอดรหัสข้อมูลที่จัดเก็บไว้เพื่อรับเงินสกุลเข้ารหัสที่โอนมา โดยไม่จำเป็นต้องทำกระบวนการรู้จักตัวตนของคู่ค้า จึงเป็นช่องว่างสำคัญที่อาชญากรใช้เป็นเครื่องมือในการฟอกเงินเนื่องจากไม่มีตัวกลางหรือหน่วยงานกลางใดมากำกับ

อีกตัวอย่างคือ ในประเทศสวิตเซอร์แลนด์มีตู้บริการเงินสกุลเข้ารหัสคล้ายตู้เอทีเอ็มตั้งอยู่ตามข้างทางเดิน เมื่อเอาธนบัตรเงินฟรังก์ใส่เข้าไปก็จะได้รับกระดาษแผ่นเล็กๆที่ปรากฏข้อมูลเป็น QR Code แสดงรหัสเปิดสาธารณะและรหัสเปิดส่วนบุคคลอยู่บนกระดาษแผ่นนั้น เมื่อนำเอากระดาษ QR Code แผ่นดังกล่าวไปลองใส่ในตู้บริการเงินสกุลเข้ารหัสอีกแห่งหนึ่ง ระบบก็จะส่งเงินธนบัตรฟรังก์ออกมาจากตู้ให้ ถือว่าครบกระบวนการโดยไม่ต้องมีการยืนยันตัวตนผู้ฝาก และผู้ถอนเงิน ในเมืองไทยก็เคยมีตู้บริการเงินสกุลเข้ารหัสประมาณ 1 - 2 ตู้ ตั้งอยู่ในศูนย์การค้าสักพักหนึ่ง แต่ปัจจุบันนี้ไม่มีแล้ว[11]”

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[11] Cryptonew (2019) รายงานว่าในปี 2014 ทีมงานของคุณ Nicknet_CZ ได้ออกมาเผยแพร่เรื่องราวของการกดเงินผ่านตู้ ATM Bitcoin ครั้งแรก ที่ติดตั้งอยู่ที่หน้าร้าน KIDO สาขา 2 บนถนน RCA พระราม 9 ผ่านช่อง Youtube Muimui Gadget โดยมีวิธีการใช้งานโดยไม่ใช้บัตร ATM แต่ใช้ Scan QR Code เพื่อถอนเงินสดออกมาจากสกุล Bitcoin ที่ทางเครื่องจะแปลงออกมาเป็นเงินอัตโนมัติ (แต่ปัจจุบันเครื่องนี้ไม่ได้ติดตั้งที่หน้าร้านแล้ว) และในปี 2018 ได้มีการเผยแพร่ภาพเครื่องกดเงินสดจากตู้ BitCoin อีกครั้ง ในชื่อว่าเครื่อง Cryptocurrency ATM Bitcoin ที่นำมาจัดแสดงในงาน CLMVT Forum 2018 เมื่อวันที่ 16–17 ตุลาคม 2018 แต่เป็นการแสดงวิธีการใช้งานให้แก่ผู้สนใจได้รับชมเท่านั้น และในช่วงต้นปี 2018 มีการนำเสนอ ATM Bitcoin อีกเครื่องในไทย ตั้งอยู่ ณ ร้านกาแฟ สุดชิค Cube no.7 เชียงใหม่ ก่อนที่ช่วงกลางปีจะมีปัญหาภายใน และถอดถอนการติดตั้งออกไปแล้ว และสุดท้ายในช่วงปลายปี 2018 เหมืองขุดคนไทย Hashbx ได้เผยแพร่วีดีโอตู้ Atm bitcoin บน facebook fanpage ของพวกเขาในวันที่ 6 ธันวาคม 2018 โดยมีเนื้อหาเชิญชวนให้มาทดลองศึกษาใช้บริการเทคโนโลยี ATM Bitcoin ได้ที่ออฟฟิตของทาง Hashbx ผู้ใดที่สนใจสามารถติดต่อสอบถามข้อมูลเพิ่มเติมได้ทาง facepage https://www.facebook.com/cubeno7/https://cryptonews.in.th/%E0%B8%95%E0%B8%B9%E0%B9%89-atm-bitcoin-%E0%B9%83%E0%B8%99%E0%B9%84%E0%B8%97%E0%B8%A2-2019-

ความเห็นของผู้ให้ข้อมูลสำคัญ #242

“ความน่าเชื่อถือได้ของระบบ DLT การบันทึกบัญชีแบบกระจายศูนย์ ทำให้ลดความเสี่ยงจากอาชญากรที่ติดต่อกันโดยไม่รู้จักกันมาก่อน แต่สามารถให้ความไว้วางใจต่อระบบนิเวศเงินสกุลเข้ารหัสที่จะทำการส่งมอบมูลค่าตามที่กำหนดไว้ ดังนั้นการใช้เงินสกุลเข้ารหัสจึงถือเป็นระบบที่น่าเชื่อถือได้มากกว่าการส่งมอบด้วยเงินสด ทรัพย์สิน ที่อาจมีการผิดพริ้ว และมีความเสี่ยงในการดำเนินการส่งมอบและรับมอบ”

คามเห็นของผู้ให้ข้อมูลสำคัญ #332

“ระบบปฏิบัติการบล็อกเชนที่ใช้เป็นแกนหลักของเงินสกุลเข้ารหัสทุกสกุล จะมีลักษณะเป็นการกระจายศูนย์ โดยการกระจายข้อมูลไปเก็บข้อมูลยังแต่ละ Node (เครื่องคอมพิวเตอร์หรือเครื่องมือสื่อสารที่เข้ามาเชื่อมต่อในระบบนิเวศเงินสกุลเข้ารหัส) ที่เข้ามาเชื่อมต่อเพื่อการยืนยันรายการธุรกรรม หรือที่เรียกว่า Mining ไม่ว่าจะเป็นระบบ Proof of Work หรือ Proof of Stake ก็ไม่ได้จัดเก็บข้อมูลอยู่ในฐานข้อมูลเพียงจุดเดียว แต่กระจายการเก็บไปตาม Node ต่างๆที่เข้ามายืนยันและการใช้งานไม่ต้องแสดงตัวตน เนื่องจากการติดต่อเป็นรหัสตัวเลขตัวอักษรประมาณ 20 - 30 ตัว ทั้งผู้ส่งและผู้รับเพื่อการเปิดกล่องข้อมูลที่เรียกว่า Block โดยไม่มีตัวกลางในการกำกับ จึงเป็นช่องโอกาสที่อาชญากรเล็งเห็นในการปกปิดตัวตนในการทำธุรกรรม และการเข้าตรวจสอบไม่ได้ ซึ่งแตกต่างจากสถาบันการเงินที่เป็นตัวกลางในการดูแลธุรกรรม ซึ่งรัฐเข้าไปกำกับที่ตัวกลางได้”

ความเห็นของผู้ให้ข้อมูลสำคัญ #412

“เงินสกุลเข้ารหัสดำเนินงานในรูปแบบการทำงานแบบกระจายศูนย์ ทำให้ธุรกิจที่เกี่ยวกับเงินสกุลเข้ารหัส หรือผู้ใช้บริการทั้งหลายสามารถทำการซื้อขายโดยไม่จำเป็นต้องทำการลงทะเบียนเพื่อการตรวจสอบตัวตนก่อนเริ่มใช้งาน (KYC Onboarding) เนื่องจากระบบไม่อยู่ในกำกับของใครหรือประเทศใด เช่น Binance หรือ Exchangers ต่างๆ สามารถไปขอเปิดระบบทำธุรกรรมในหมู่เกาะเคย์แมน หมู่เกาะบริติชเวอร์จิน หรือประเทศปานามา ซึ่งไม่มีมาตราการทางกฎหมายในการกำกับธุรกรรมเงินสกุลเข้ารหัส การทำธุรกรรมจึงเป็นเสรีไม่มีการเปิดเผยตัวตนของผู้โอนและผู้รับโอนเพียงแต่ใช่รหัสเปิดข้อมูลเท่านั้น จึงน่าจะเป็นปัจจัยสำคัญที่อาชญากรเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน”

ความเห็นของผู้ให้ข้อมูลสำคัญ #421

“หากจะเทียบเคียงลักษณะของเงินสกุลเข้ารหัสกับเงินสดมีความเหมือนกัน คือไม่ต้องเปิดเผยตัวตนของเจ้าของ สามารถโอนย้ายส่งมอบให้ใครก็ได้จำนวนเท่าใดก็ได้โดยไม่จำเป็นต้อง

%E0%B8%A1%E0%B8%B5%E0%B8%97%E0%B8%B5%E0%B9%88%E0%B9%84%E0%B8%AB%E0%B8%99%E0%B8%9A%E0%B9%89%E0%B8%B2%E0%B8%87/

ไปขออนุญาตใครก่อน และการเคลื่อนย้านเงินสดก็ไม่อาจสืบค้นได้ แต่หากเป็นเงินสดจำนวนมากก็อาจถูกตั้งข้อสังเกตุเป็นรายการต้องสงสัยของสถาบันการเงินได้ ในขณะที่เงินสกุลเข้ารหัสจะโอนมูลค่าด้วยรหัสจำนวนเท่าใดก็ได้อย่างเสรี โดยไม่จำเป็นต้องไปขออนุญาตใครก่อนการส่งมอบ แต่ในความเป็นจริงแล้วเงินสกุลเข้ารหัสก็มีระบบปฏิบัติการบล็อกเชนที่บันทึกเส้นทางธุรกรรมไว้"

ดังนั้น การปลอดจากตัวกลางในการกำกับดูแลกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัส และระบบได้เปิดกว้างต่อผู้ใช้งานสามารถติดต่อเข้าสู่ระบบได้อย่างไม่มีเงื่อนไข ผู้ใช้งานจึงไม่จำเป็นต้องลงทะเบียนอัตลักษณ์ตัวตนแท้จริงของผู้ใช้งานก่อนเข้าสู่ระบบ กล่าวคือ ผู้ใช้งานสามารถเลือกใช้นามแฝงเพื่อปิดบังตัวตนได้ ซึ่งถือเป็นคุณลักษณะเฉพาะที่สำคัญ ที่เป็นปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส (Girasa, 2018)

4.1.2 ปัจจัยการอำพรางตัวตน และความยากต่อการสืบค้นเส้นทางธุรกรรม

แม้ว่าระบบนิเวศเงินสกุลเข้ารหัสจะดำเนินการบนระบบปฏิบัติการบล็อกเชนที่ไม่มีข้อจำกัดให้ผู้ใช้งานต้องแสดงตน แต่ระบบจะมีการบันทึกรายการธุรกรรมการโอนมูลค่าหรือการติดต่อระหว่างผู้ใช้งาน หรือผู้โอนและผู้รับโอน หลังจากรายการธุรกรรมนั้นได้ผ่านการตรวจพิสูจน์ยืนยันรายการแล้ว และจะไม่สามารถแก้ไขเปลี่ยนแปลงได้ (Immutable) เนื่องจากรหัสที่ได้รับการพิสูจน์ในส่วนท้ายของชุดข้อมูลจะมีความสัมพันธ์ทางคณิตศาสตร์กับรหัสส่วนต้นของชุดข้อมูลถัดไป จึงเป็นการให้ความเชื่อมั่นแก่ผู้ใช้งานในระบบได้โดยเสมือนว่า *"ได้มีการทิ้งร่องรอยอันถาวรเหมือนกับการสลักลงบนแผ่นหินแกรนิต ทันทีข้อมูลได้รับการพิสูจน์ยืนยันในชุดข้อมูลแล้ว ข้อมูลนั้นจะติดแน่นถาวรไม่อาจเปลี่ยนแปลงได้"* (Burniske & Tara, 2017)

อย่างไรก็ตาม เมื่อระบบนิเวศเงินสกุลเข้ารหัสได้บันทึกรายการในฐานข้อมูลแบบเปิด ผู้ใช้งานทั่วไปสามารถต่อเชื่อมเข้าสู่ระบบบล็อกเชน เพื่อทำการตรวจสอบเส้นทางธุรกรรมระหว่างผู้ใช้งานได้ตลอดเวลา เช่น Blockchain.info โดยผู้พัฒนาระบบงานสามารถสร้างโปรแกรมประยุกต์ (API - Application Programing Interface) เพื่อนำข้อมูลจากฐานข้อมูลแบบเปิดในระบบปฏิบัติการบล็อกเชนมาทำการวิเคราะห์สร้างความสัมพันธ์ระหว่างกลุ่มผู้ใช้งาน และศึกษาพฤติกรรมการใช้งานหรือพฤติกรรมต้องสงสัยของผู้ใช้งานที่อาจเข้าข่ายการฟอกเงิน ดังนั้นอาชญากรอาจเลือกเครื่องมือสนับสนุนในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส และการเพิ่มศักยภาพในการกลบเกลื่อร่องรอยของการทำธุกรรมเพื่อให้เกิดความยากต่อการสืบค้นเส้นทางธุรกรรม

ดังที่ Crawford (2019) ได้กล่าวไว้ว่า ระบบนิเวศเงินสกุลเข้ารหัสเป็นระบบฐานข้อมูลสาธารณะ แม้ว่าผู้ใช้งานจะสามารถปิดบังตัวตนได้แต่ระบบก็ยังจะสามารถเชื่อมโยงเส้นทางการทำธุรกรรมระหว่างผู้ใช้งานได้ ดังนั้นผู้กระทำผิดจึงมีความต้องการที่จะหาวิธีการกลบเกลื่อนร่องรอยระหว่างเส้นทางเชื่อมโยงการโอนเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมาย ไปยังกระเป๋าเงิน

ปลายทางของผู้กระทำผิดเองที่ไม่สามารถพิสูจน์ย้อนกลับถึงต้นทางได้ และประกอบความเห็นของผู้ให้ข้อมูลสำคัญ ดังนี้

ความเห็นของผู้ให้ข้อมูล #111

“แม้ว่าโดยเทคโนโลยี่ของเงินสกุลเข้ารหัสจะสามารถสืบค้นเส้นทางการทำธุรกรรมระหว่างผู้โอนกับผู้รับโอนได้ แต่ไม่สามารถทราบตัวตนของเจ้าของกระเป๋า และถ้ามีการทำธุรกรรมกับผู้ให้บริการที่ไม่อยู่ในกำกับของกฎหมาย หรือผู้ให้บริการต่างประเทศก็จะยิ่งเพิ่มความยากในการสืบค้นตัวตนของผู้ใช้งาน หรืออาชญากรที่ทำการซื้อขายสิ่งผิดกฎหมายบน Dark Web ซึ่งดำเนินงานโดยองค์กรอาชญากรรม ซึ่งทำธุรกรรมลักษณะเดียวกันหลายพันเว็บไซต์เหมือนกับการใช้งานอินเตอร์เน็ตปกติ ที่สามารถทำการติดต่อซื้อขายสิ่งผิดกฎหมายผ่านกระทู้ และมีการตรวจสอบความน่าเชื่อถือของคู่ค้าจากความเห็นของผู้เคยใช้บริการ ก่อนที่จะเลือกชำระค่าสินค้าด้วยวิธีการอะไรก็ได้ ซึ่งเงินสกุลเข้ารหัสก็เป็นหนึ่งในวิธีการชำระ ตัวอย่างเช่น Silk Road, Alphabay ที่ถูกดำเนินงานปิดไป ก็เป็นเพียงส่วนหนึ่งใน Dark Web ซึ่งจะทำให้การติดตามยากขึ้น เนื่องจากผู้ใช้งานใน Dark Web จะถูกจำกัดเฉพาะสมาชิกที่ได้รับอนุญาตจากผู้บริหารเว็บไซต์เท่านั้น โดย Dark Web จะดำเนินการชำระเงินให้แก่คู่ค้าในลักษณะ Escrow Wallet ซึ่งเป็นกระเป๋าเงินกลางขององค์กรอาชญากรรม และความยากในการติดตามสืบค้นจะเพิ่มมากขึ้นหากอาชญากรทำธุรกรรมบน Mixer, CoinJoin ซึ่งเป็นผู้ให้บริการในการปิดบังเส้นทางธุรกรรมจากผู้โอนและผู้รับโอนตัวจริง โดยจะผ่านการปนเงินสกุลเข้ารหัสของผู้ใช้งานรายอื่น หรือกระจายรายการย่อย สลับรายการกับผู้ใช้รายอื่น เพื่อเพิ่มความยากในการตรวจสอบย้อนกลับไปยังต้นทาง

และการปกปิดเจ้าของเงินที่แท้จริงโดยเทคโนโลยี่ที่ไม่ต้องระบุตัวตน อาชญากรก็จะได้ประโยชน์จากกรณีนี้ แต่ถ้าเป็นผู้ใช้งานสุจริตก็ยินยอมเปิดเผยข้อมูลเพื่อการตรวจสอบอยู่แล้ว และเมื่ออาชญากรใช้ประโยชน์มักจะทำการโอนถ่ายเทไปหลายทอดข้ามประเทศอย่างรวดเร็ว อีกทั้งผู้รับโอนปลายทางก็ไม่ใช่บัญชีของเจ้าของที่แท้จริง ยิ่งไปกว่านั้นอาชญากรอาจเลือกใช้เงินสกุลเข้ารหัสที่มีลักษณะเฉพาะซึ่งถูกออกแบบโดยเทคโนโลยี่ในการปกปิดตัวตน และเส้นทางธุรกรรมที่เรียกว่า Privacy Coin[12] มากกว่าการใช้บิตคอยน์ หรือเงินสกุลเข้ารหัสอื่นที่ผ่านผู้ให้บริการจด

[12] Privacy Coins เป็นคริปโทเคอร์เรนซีประเภทหนึ่งที่สามารถปกปิดข้อมูล การทำธุรกรรม โดยอนุญาตให้ users ควบคุมสิทธิการไม่เปิดเผยข้อมูล wallet ของผู้โอนหรือผู้รับโอน หรือธุรกรรมที่ทำระหว่างกันได้ จึงทำให้การติดตามตรวจสอบธุรกรรมของผู้ที่ถือ privacy coins เป็นไปได้ยาก และมีความเสี่ยงต่อ AML/CFT ตัวอย่าง privacy coins เช่น Monero เป็นเหรียญที่สามารถปกปิดข้อมูลผู้โอน ผู้รับหรือจำนวนที่ต้องการโอนได้ สามารถใช้ได้หลายเทคโนโลยีในการปกปิดข้อมูล เช่น ใช้เทคโนโลยี Ring Signature ซึ่งเป็นการ sign digital signature ที่ให้ sign ร่วมกับธุรกรรมของผู้อื่น ทำให้สามารถปิดข้อมูลตัวตนผู้โอนได้ หรือใช้เทคโนโลยี RingCT ที่ใช้ encryption ต่อยอดจาก Ring Signature เพื่อปกปิดข้อมูลจำนวนที่ต้องการโอน เป็นต้น และ Zcash4 เป็นเหรียญที่สามารถปกปิด

ทะเบียนตามกฎหมาย โดยอาจใช้บริการกับผู้ให้บริการในต่างประเทศแม้ว่าอาชญากรรมนั้นจะเกิดขึ้นในเมืองไทย”

ความเห็นของผู้ให้ข้อมูลสำคัญ #212

“โดยลำพังระบบนิเวศเงินสกุลเข้ารหัสบนระบบปฏิบัติการบล็อกเชน แม้จะสามารถทราบเส้นทางธุรกรรมก็มีความยากที่จะติดตามตัวตนของผู้ใช้งานแล้ว ยังมีผู้ให้บริการบางรายมีกลไกส่งเสริมช่วยในการปกปิดตัวตนเพิ่มขึ้นไปอีกที่เรียกว่า Privacy Coin ซึ่งเป็นเงินสกุลเข้ารหัสเหมือนกันแต่มีฟังชั่นในการเลือกบริการที่จะไม่เปิดเผยรหัสที่ตั้ง (IP Address) ของผู้โอนและผู้รับโอนหรือเส้นทางธุรกรรม รวมถึงข้อมูลจำนวนมูลค่าในกระเป๋าเงินอีกด้วย นอกจากนี้ยังมีระบบงานอีกรูปแบบหนึ่งที่เข้าเสริมในการช่วยปกปิดตัวตนอีก เช่น Mixer, Tumbler ที่นำเงินสกุลเข้ารหัสของผู้ใช้บริการหลายรายมาปน และจัดลำดับการส่งให้ใหม่ทำให้ตรวจสอบย้อนกลับไปหาแหล่งที่มาไม่ได้ หรือ Chain Hopping ที่จะช่วยทำการเคลื่อนย้ายรหัสที่ตั้งไปเรื่อยๆ ในระหว่างการทำธุรกรรมทำให้ยากต่อการติดตามอีกเช่นกัน ด้วยตัวของเทคโนโลยี่เองเป็นส่วนที่ช่วยเสริมให้อาชญากรเลือกใช้เนื่องจากเป็นระบบที่ไม่เปิดเผยตัวตนอยู่แล้ว”

ความเห็นผู้ให้ข้อมูลสำคัญ #232

“เงินสกุลเข้ารหัสทั่วไปก็จะมีความโปร่งใสในตัวเองระดับหนึ่ง เนื่องจากสามารถเข้าไปตรวจสอบเส้นทางธุรกรรมในฐานข้อมูลแบบเปิดได้ เพียงแต่ไม่ทราบว่าใครคือเจ้าของกระเป๋าเงิน แต่ถ้าอาชญากรใช้ Privacy Coin ซึ่งเป็นเงินสกุลเข้ารหัสที่ช่วยให้ไม่สามารถตรวจสอบได้แม้กระทั่งรหัสที่ตั้งของกระเป๋าเงิน หรือเส้นทางธุรกรรม เช่น Manero เป็นระบบที่สามารถปกปิดเส้นทางธุรกรรมในระบบปฏิบัติการได้ ทำให้ไม่สามารถตรวจสอบความเชื่อมโยงระหว่างต้นทางกับปลายทาง

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ข้อมูลผู้โอน ผู้รับโอนและจำนวนที่โอนจะใช้เทคโนโลยี zk-SNARKs กับ cryptographic hash เพื่อให้การยืนยันธุรกรรมสามารถทำได้โดยผู้ยืนยันไม่ต้องทราบข้อมูล ดังนั้น จึงปกปิดข้อมูลผู้โอน ผู้รับโอนและจำนวนที่โอนได้ และ DASH5 เป็นเหรียญที่ปกปิดข้อมูลผู้โอนจะใช้เทคโนโลยี CoinJoin ในขั้นตอนการ mining ทำให้ธุรกรรมการโอนไปยังผู้รับสามารถถูกทำร่วมกับ ธุรกรรมผู้อื่นได้ ส่งผลให้สามารถปกปิดข้อมูลผู้โอนได้ (เอกสารรับฟังความคิดเห็น เลขที่ อกต. 4/2564 เรื่อง แนวทางการกำกับดูแลเพื่อป้องกันการใช้สินทรัพย์ดิจิทัลเป็นเครื่องมือ กระทำความผิดและแนวทางการกำกับดูแลผู้ให้บริการกระเป๋าสินทรัพย์ดิจิทัลที่รับฝากสินทรัพย์ดิจิทัล (custodial wallet provider) เผยแพร่เมื่อวันที่27 มกราคม 2564
https://www.sec.or.th/Documents/PHS/Main/690/hearing042564.pdf) และ Firo ซึ่งเป็น privacy coin ของคนไทยที่ถูกเปิดตัวในนามเรียกขนานว่า Zcoin ในปี 2016 โดยนายปรมินทร์ อินโสม ถือเป็นเหรียญที่ให้ความเป็นส่วนตัวในการทำธุรกรรม กล่าวคือไม่ว่าใครก็จะไม่มีวันรู้ข้อมูลการทำธุรกรรมของคุณบน Blockchain เลยโดยใช้โปรโตคอลที่ชื่อว่า ZecoCoin หรือระบบ zero-knowledge proof ที่ทำให้ผู้ใช้งานสามารถทำลายเหรียญและ redeem เหรียญเหล่านั้นเป็นเหรียญใหม่ได้ โดยที่จะไม่มีการทิ้งประวัติการทำธุรกรรมใด ๆ ไว้ (คุณจิรบูลย์, 2021) https://siamblockchain.com/2021/01/16/firo-activates-latest-privacy-upgrade-lelantus/

ได้ โดยระบบจะทำการแตกย่อยรายการโอนไปสู่ปลายทางจำนวนมาก ซึ่งเป็นของผู้รับโอนตัวจริงในลักษณะที่ไม่ใช่รายการโอนตรงแบบ One-to-One ทั้งนี้เข้าใจว่าสำนักงาน กลต น่าจะกำลังพิจารณาออกคำสั่งห้ามผู้ให้บริการ Exchanger นำ Privacy Coin เข้ามาทำการซื้อขายในกระดาน”

ความเห็นผู้ให้ข้อมูลสำคัญ #242

“เงินสกุลเข้ารหัสเกิดขึ้นมาด้วยแนวคิดระบบการทำงานเพื่อหลีกหนีจากการควบคุมอยู่แล้ว แต่สามารถเข้าถึงได้ง่ายจากระบบอินเตอร์เน็ต แม้จะไม่ต้องยืนยันตัวของผู้ใช้งานก็ไม่น่าจะถือเป็น Anonymity ควรจะถือเป็น Pseudo-anonymity ที่ยังสามารถติดตามเส้นทางธุรกรรมได้ จึงอาจเป็นความเข้าใจที่ไม่ชัดเจนของอาชญากรที่ใช้เงินสกุลเข้ารหัสในการฟอกเงิน แต่ถ้าต้องจะปิดบังตัวตนที่แท้จริงต้องใช้เป็นเงินสกุลเข้ารหัสประเภท Privacy Coin เป็นระบบที่สร้างขึ้นเพื่อความเป็น Anonymity ที่แท้จริง เช่น Manero หรือ ZCash”

ความเห็นของผู้ให้ข้อมูลสำคัญ #331

“ในช่วงแรกของการเริ่มใช้บิตคอยน์ คนทั่วไปมักเข้าใจว่าเงินสกุลเข้ารหัสเป็น Anonymity เต็มตัว แต่ตั้งแต่กรณีของ Alphabay ถูกหน่วยงานของ FBI ใช้โปรแกรมเข้าไปตรวจจับความเคลื่อนไหวของการทำธุรกรรมในระบบบปฏิบัติการบล็อกเชน จนสามารถติดตามถึงตัวอาชญากรได้ และทำการค้นหารหัสเปิดส่วบุคคลของกระเป๋าเงินที่อายัดได้จากการตรวจพิสูจน์หลักฐานในเครื่องคอมพิเวอตร์ของอาชญากร ดังนั้นอาชญากรจึงต้องพัฒนาตนเองหลีกหนีการแกะร่องรอย โดยทำธุรกรรมบน TOR Browser เพื่อทำการติดต่อซื้อขายสิ่งผิดกฎหมายกับ Dark Web ซึ่งมักจะใช้ระบบจัดส่งโอนมูลค่าผ่านระบบ Mixer หรือ Tumbler ในการให้บริการปนเงินสกุลข้ารหัสจากหลายแหล่งเงินและกระจายออกเพื่อให้สามารถตัดความเชื่อมโยงจากผู้ส่งต้นและผู้รับปลายทางได้ และเมื่อต้องการจะแปลงเงินสกุลเข้ารหัสไปสู่ระบบการเงินตรา ก็จะผ่านทางผู้ให้บริการนอกระบบกฎหมายหรือผู้ให้บริการเอกชนอิสระ เช่น Paypal ที่สามารถแปลงค่าและรับเงินตราโดยไม่ต้องระบุตัวตนของผู้รับเงิน”

โดยความเห็นของผู้ให้ข้อมูลสำคัญข้างต้น จึงอาจกล่าวได้ว่าเทคโนโลยีทางการเงินมีพัฒนาการอย่างรวดเร็วภายใต้แนวคิดความเป็นอิสระเพื่อหลีกหนีจากการควบคุม จึงเกิดนวัตรกรรมบนระบบนิเวศเงินสกุลเข้ารหัสในการช่วยสนับสนุนการปิดบังตัวตนที่แท้จริงของผู้ใช้งาน กระบวนการกลบเกลื่อนร่องรอยการทำธุรกรรม ไม่ว่าจะเป็นการใช้ TOR Browser ในการทำธุรกรรมเพื่อลวงรหัสที่ตั้งในขณะทำงาน และการใช้บริการ Crypto Mixer หรือ Tumbler ในการตัดความเชื่อมโยงระหว่างผู้ใช้งานต้นทางและปลายทาง จนกระทั่งถึงขั้นไม่ปรากฏร่องรอยในการทำธุรกรรมทางเทคโนโลยีจากการใช้ Privacy Coin บางสกุล ซึ่งขัดกับความเชื่อพื้นฐานของนักอาชญาวิทยา ที่ว่า *“อาชญากรย่อมทิ้งร่องรอยไว้เสมอ”* ดังนั้นปัจจัยด้านศักยภาพทางเทคโนโลยีในการช่วยอำพรางตัวตนของผู้ใช้งาน และสร้างอุปสรรคด้วยความซับซ้อนของเส้นทางธุรกรรมส่งผลให้เกิดความยากต่อ

การสืบค้นเชื่อมโยงเส้นทางธุรกรรมถึงตัวผู้ใช้งานที่แท้จริงได้ จึงเป็นอีกปัจจัยหนึ่งที่เป็นมูลเหตุจูงใจให้อาชญากรเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน

4.1.3 ปัจจัยด้านความสะดวก รวดเร็ว และสามารถทำธุรกรรมข้ามประเทศ

ระบบปฏิบัติการบล็อกเชน ซึ่งเป็นระบบงานที่รองรับการทำธุกรรมของเงินสกุลเข้ารหัสโดยดำเนินงานอยู่บนระบบอินเตอร์เน็ตที่ใช้งานกันอยู่ทั่วไปในปัจจุบัน และด้วยพัฒนาการทางเทคโนโลยี่การสื่อสารมีความก้าวหน้าอย่างรวดเร็วและต่อเนื่อง จากเทคโนโลยี่การสื่อสารยุค 2G ที่เริ่มมีการส่งข้อความระบบดิจิทัลเมื่อประมาณกว่า 10 ปีที่ผ่านมา เป็นเทคโนโลยี่การสื่อสารยุค 4G อย่างเช่นที่กำลังใช้งานปัจจุบันในประเทศไทยที่เป็นระบบการสื่อสารอินเตอร์เน็ตความเร็วสูง โดยมีความเร็วสูงกว่ายุค 3G หลาย 10 เท่า และประเทศไทยกำลังจะก้าวสู่เทคโนโลยี่การสื่อสารยุค 5G ในไม่ช้า ดังนั้นขอบข่ายการให้บริการอินเตอร์เน็ตความเร็วสูงของผู้ให้บริการในประเทศไทยสามารถครอบคลุมพื้นที่การให้บริการเกือบทั้งประเทศ และยังสามารถเชื่อมต่อระบบโครงข่ายกับผู้ให้บริการอินเตอร์เย็ตระหว่างประเทศได้อย่างกว้างขว้าง ส่งผลให้การติดต่อสื่อสารภายในประเทศและระหว่างประเทศมีประสิทธิภาพสูงในระดับเศษของวินาที ในขณะที่ธุรกรรมเงินสกุลเข้ารหัสถือเป็นการทำธุรกรรมแบบไร้พรมแดน (Cross-Border Nature) เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสเป็นการดำเนินการบนระบบอินเตอร์เน็ตแบบออนไลน์ ซึ่งปัจจุบันมีโครงข่ายการติดต่อสื่อสารออนไลน์เชื่อมโยงถึงกันทั้งในประเทศและระหว่างประเทศ จึงสามารถทำธุรกรรมการโอนระหว่างกันข้ามขอบเขตประเทศได้อย่างรวดเร็วและเสรี (HouBen & Snyers, 2018) หรือ กล่าวอีกนัยหนึ่ง คือ พื้นที่ใดมีโครงข่ายอินเตอร์เน็ตให้บริการ พื้นที่นั้นก็สามารถเป็นแหล่งกำเนิดของการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้ และประกอบความเห็นของผู้ให้ข้อมูลสำคัญ ดังนี้

ความเห็นของผู้ให้ข้อมูลสำคัญ #113

“มีความสะดวกในการจัดการสามารถทำธุรกรรมโอนเงินสกุลเข้ารหัสข้ามประเทศได้โดยตรงแบบไม่จำกัดมูลค่า เมื่อเปรียบเทียบวิธีการอื่นที่จะต้องทำการแปลงทรัพย์เป็นหลายชั้นหลายขั้นตอนแยกย่อย หรือการผ่านระบบสถาบันการเงินในประเทศและต่างประเทศที่จะมีตัวกรองรายการอีกหลายชั้นเช่นกัน การฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสจึงทำได้โดยง่ายและรวดเร็ว

ความเห็นของผู้ให้ข้อมูลสำคัญ #221

“การทำธุรกรรมเงินสกุลเข้ารหัสสามารถโอนมูลค่าข้ามประเทศได้สะดวกโดยตรงแบบออนไลน์ ไม่เหมือนกับการโอนเงินหรือส่งเงินสดข้ามประเทศที่ต้องมีขั้นตอนการดำเนินงานหลายขั้นตอนกว่าจะรวบรวมเงินกลับมาได้ครบตามจำนวนที่อาชญากรต้องการ”

ความเห็นของผู้ให้ข้อมูลสำคัญ #411

“เป็นเทคโนโลยี่ที่เข้ามาทำลายพรมแดน เนื่องจากการทำธุรกรรมโอนเงินสกุลเข้ารหัสเกิดจากการเชื่อมต่อเครือข่ายคอมพิวเตอร์ หรืออุปกรณ์สื่อสารที่ใดในโลกสามารถเข้าถึงกันโดยตรงไม่ต้องมีตัวกลางในการกำกับการดำเนินการ จึงสามารถสื่อสารข้ามประเทศได้เหมือนการติดต่อทางโซเชียลมีเดียทั่วไป ที่สามารถติดต่อกันได้ตลอดเวลาแบบไร้พรมแดนและข้อจำกัดด้านเวลาไม่มีวันหยุดทำการหรือต้องรอเวลาทำการ อีกประการคือจำนวนมูลค่าในการโอนนั้นแต่ละประเทศมักจำกัดจำนวนการโอนเงินระหว่างประเทศ แต่เงินสกุลเข้ารหัสเป็นสินทรัพย์ไร้ตัวตนที่มีมูลค่าเทียบเคียงกับทองคำ เป็นสื่อกลางที่เกิดการยอมรับของกลุ่มบุคคลในการแลกเปลี่ยนมูลค่าระหว่างกันจึงสามารถโอนย้ายข้ามประเทศโดยไม่จำกัดปริมาณ แต่ขึ้นอยู่กับการยอมรับและความเชื่อถือของผู้ใช้งานเท่านั้น”

ความเห็นของผู้ให้ข้อมูลสำคัญ #413

“การทำธุรกรรมโอนเงินสกุลเข้ารหัสสามารถทำการชำระราคาค่าซื้อขายในมูลค่าสูงได้ง่าย ในคราวเดียวอย่างรวดเร็ว และสามารถโอนข้ามประเทศได้อย่างสะดวกโดยไม่มีข้อจำกัดจากหน่วยงานกำกับของแต่ละประเทศ เพื่อการหลีกเลี่ยงการตรวจสอบระหว่างทาง เพราะหากจะมีการชำระค่าซื้อขายหลักร้อยล้านพันล้านด้วยเงินสดจะมีความยุ่งยากมาก แต่เงินสกุลเข้ารหัสสามารถทำได้ในธุรกรรมเดียว”

ความเห็นของผู้ให้ข้อมูลสำคัญ #421

“หากจะให้ความเห็นเปรียบเทียบเงินสดกับเงินสกุลเข้ารหัสแบบหมัดต่อหมัด คิดว่าอาชญากรน่าจะเลือกเงินสดมากกว่า แต่เนื่องจากเงินสกุลเข้ารหัสเป็นสิ่งใหม่ที่คนรู้จักน้อย และคิดว่าเป็นเครื่องมือที่จะใช้ปกปิดตัวตน สามารถเคลื่อนย้ายโอนมูลค่าได้อย่างรวดเร็ว รวมถึงข้ามประเทศและทำรายการมูลค่าสูงได้โดยง่าย สะดวกกว่าการส่งมอบเงินสดในจำนวนสูงที่ต้องผ่านขั้นตอนการกระจายโยกย้ายเงินหลายขั้นตอน อีกประการหนึ่งอาชญากรสามารถกระจายรายการธุรกรรมเงินสกุลเข้ารหัสเป็นรายการย่อยจำนวนมากได้อย่างรวดเร็ว และรวบรวมกลับไปยังเป้าหมายได้สะดวกสร้างภาระความยากในการติดตามให้แก่เจ้าหน้าที่”

ดังนั้นปัจจัยด้านความสะดวก รวดเร็ว และสามารถทำธุรกรรมข้ามประเทศได้ของธุรกรรมเงินสกุลเข้ารหัส จึงเป็นมูลเหตุจูงใจอันดับแรกๆที่อาชญากรอาจเลือกใช้เป็นเครื่องมือในการฟอกเงิน โดยเฉพาะอย่างยิ่งการทำธุรกรรมในจำนวนมูลค่าสูง หากเลือกใช้เครื่องมืออื่น เช่น เงินสด รถยนต์หรู ที่ดิน หรือหลักทรัพย์ ก็ต้องอาศัยความร่วมมือของตัวแทนร่วมดำเนินการจำนวนมาก เพื่อดำเนินการแปลงสภาพทรัพย์หลายขั้นตอน และใช้ระยะเวลาดำเนินการมากพอสมควร ทั้งนี้ขึ้นอยู่กับ

ศักยภาพของเครือข่ายของอาชญากร แต่การดำเนินการโดยธุรกรรมเงินสกุลเข้ารหัสสามารถกระทำการได้เพียงคราวเดียวครอบคลุมมูลค่าทั้งจำนวน ลดความเสี่ยงจากการแปลงสภาพทรัพย์หลายขั้นตอนที่อาจก่อให้เกิดภาระความผิดทางกฎหมายหลายกรรม อีกทั้งยังมีความเสี่ยงจากความโลภของตัวแทนร่วมดำเนินการที่อาจยักยอกทรัพย์เป็นของตนเองระหว่างกระบวนการด้วยเช่นกัน

4.1.4 ปัจจัยการรักษามูลค่าทรัพย์สินด้วยต้นทุนการดูแลต่ำ

ปัจจัยนี้เป็นปัจจัยเชิงเศรษฐศาสตร์ของหนึ่งในหน้าที่ความเป็นเงินตรา คือการดำรงรักษาและสะสมความมั่งคั่งทางเศรษฐกิจ (A Store of Value) ผู้ถือครองเงินสกุลเข้ารหัสย่อมประสงค์ที่จะสะสมความมั่งคั่งเพื่อใช้ประโยชน์ทางเศรษฐกิจในอนาคต และมูลค่าที่ดำรงรักษาไว้ควรจะมีเสถียรภาพภายใต้สภาพเศรษฐกิจ แต่ด้วยระบบนิเวศเงินสกุลเข้ารหัสที่ผู้ถือครองจะเก็บเงินดังกล่าวไว้ในกระเป๋าเงินอิเล็กทรอนิกส์ก็อาจจะมีค่าใช้จ่ายเพื่อการดูแลรักษาของผู้ให้บริการกระเป๋าเงิน (Wallet Provider) ซึ่งเป็นต้นทุนที่ลดทอนมูลค่า ในขณะเดียวกันราคาของเงินสกุลเข้ารหัสมีความผันผันเปลี่ยนแปลงระหว่างปีและปีต่อปีอย่างมีนัยสำคัญ ทั้งทิศทางที่มีราคาสูงค่าขึ้นหรือลดค่าลง จึงเป็นความเสี่ยงในลักษณะที่เข้าข่ายการถือครองเพื่อการเก็งกำไรมากกว่า (Yermack, 2015) อย่างไรก็ตามปัจจุบันความต้องการลงทุนในเงินสกุลเข้ารหัสมีสูง โดยเฉพาะอย่างยิ่งบิตคอยน์จึงส่งผลให้ราคาของบิตคอยน์ต่อเหรียญสหรัฐปรับตัวสูงขึ้นต่อเนื่องจากเดือนมิถุนายน 2020 อยู่ที่ระดับประมาณ 9,100 เหรียญสหรัฐอเมริกา และปรับตัวขึ้นเป็นระดับราคาประมาณ 28,000 เหรียญสหรัฐอเมริกา ณ สิ้นปี 2020 กระทั่งถึงเดือนมีนาคม 2021 ราคาปรับขึ้นมาอยู่ที่ระดับประมาณ 59,000 เหรียญสหรัฐอเมริกา[13] และอยู่ในระดับที่มีแนวโน้มปรับตัวขึ้น เนื่องจากความต้องการบิตคอยน์เพื่อการลงทุนของกองทุนการเงินขนาดใหญ่เพิ่มมากขึ้น ในขณะเดียวกันธุรกิจขนาดใหญ่เริ่มตอบรับบิตคอยน์เป็นสื่อกลางในการชำระค่าสินค้า ดังนั้น จึงเป็นอีกปัจจัยที่มีอิทธิพลต่อทางเลือกในการเก็บรักษาเงินสกุลเข้ารหัสจากการฟอกเงินไว้ในกระเป๋าเงินเพื่อรอระยะเวลาที่เหมาะ ทั้งนี้ผู้ให้ข้อมูลสำคัญได้แสดงความเห็นต่อประเด็นนี้ ดังนี้

ความเห็นของผู้ให้ข้อมูลสำคัญ #241

“เงินสกุลเข้ารหัสมีลักษณะที่สามารถเข้าข่าย เป็นการรักษามูลค่าของทรัพย์สิน Store of Value และมีราคาตลาดอ้างอิงได้ เนื่องจากเงินสกุลเข้ารหัสเป็นที่ยอมรับในระบบตลาดจากกลุ่มคนระดับหนึ่งจึงมีราคาซื้อขายที่อ้างอิงได้ แม้ว่าจะมีความผันผวนไปตามความต้องการของผู้ใช้งานหรือไปตามกลไกตลาด Demand-Supply แต่ค่าความผันผวนนั้นอาชญากรที่ต้องการฟอก

[13] https://coinmarketcap.com/currencies/bitcoin/

เงินก็น่าจะยอมรับได้ มากกว่าการแปลงไปเป็นของเก่าเครื่องลายครามที่มีการตีราคาตามความพอใจ และไม่มีสภาพคล่อง โดยเฉพาะอย่างยิ่งประเทศที่มีอัตราเงินเฟ้อสูง เช่น ประเทศเวเนซูเอล่า อาจเป็นตัวเร่งให้อาชญากรเลือกใช้เงินสกุลเข้ารหัส เนื่องจากมีความผันผวนของค่าเงินในระดับที่ใกล้เคียงกัน อีกทั้งความไม่เสื่อมค่าในตัวเองจากการเก็บรักษาและมีต้นทุนการดูแลต่ำเมื่อเปรียบเทียบการฟอกเงินโดยทรัพย์สินอื่นไม่ว่าจะเป็น รถยนต์หรู นาฬิกา เครื่องลายคราม หรือทองคำ ที่ต้องมีสถานที่จัดเก็บและดูแลรักษารวมถึงขาดสภาพคล่องทางการตลาด จึงขึ้นอยู่กับความพอใจและสถานการณ์ของผู้ซื้อ”

ความเห็นของผู้ให้ข้อมูลสำคัญ #411

“น่าจะเป็นด้านเศรษฐศาสตร์ เนื่องจากเงินสกุลเข้ารหัสมีขนาดทางการตลาดใหญ่ที่น่าจะอยู่ราวไม่น้อยกว่า 30 ล้านล้านบาท ซึ่งมากกว่า GDP ของไทยทั้งประเทศ และเกิดการยอมรับของคนในวงกว้างมากขึ้นส่งผลให้เกิดสภาพคล่องทางการเงิน ดังนั้นการฟอกเงินและเก็บรักษาทรัพย์สินโดยผ่านสินทรัพย์อื่นไม่ว่าจะเป็น ของเก่าลายคราม รถยนต์หรู หรือแม้แต่เพชร ก็จะขาดสภาพคล่องเนื่องจากจะหมุนเวียนอยู่กับคนในวงจำกัด ซึ่งในอดีตมักจะปรากฏข่าวการฟอกเงินโดยรถยนต์หรูที่ส่งมาจากต่างประเทศ นำเข้ามาฟอกเงินในประเทศไทยด้วยเงินจำนวนหนึ่งแถมยังได้กำไรจากการขายอีกต่อ แต่ก็มีข้อจำกัดเฉพาะกลุ่มคนที่ชอบและมีกำลังเงินพอ ในขณะที่เงินสกุลเข้ารหัสมีตลาดรองที่ซื้อขายสภาพคล่อง และมีราคาตลาดชัดเจน อีกทั้งมีผู้ให้บริการแปลงค่าได้สะดวก”

ความเห็นของผู้ให้ข้อมูลสำคัญ #412

“การขยายศักยภาพตลาดการเงินของเงินสกุลเข้ารหัสมีขนาดครอบคลุมสภาพคล่องเพื่อใช้หมุนเวียนไปได้ทั่วโลก โดยเฉพาะอย่างยิ่งเงินสกุลเข้ารหัสขนาดใหญ่ ไม่ว่าจะเป็น บิตคอยน์ อีเธอเรียม USDT[14] ที่ไม่มีข้อจำกัดในการโอนมูลค่าข้ามประเทศ เช่น สามารถโอนบิตคอยน์ในมูลค่าหลายร้อยล้าน พันล้าน หรือแม้แต่หมื่นล้านก็ไม่มีหน่วยงานใดเข้ามากำกับ ในขณะที่เงินบาทไทยเองหากต้องการโอนเงินบาทระหว่างประเทศก็อาจมีข้อจำกัดตามปริมาณเงินบาทในตลาดโลก โดยมีหน่วยงานระหว่างประเทศในการกำกับทำธุรกรรม เช่น SWIFT[15] และ IBAN[16] เป็นต้น เพื่อสร้าง

[14] USDT เป็นเงินสกุลเข้ารหัสประเภท Stable Coin ที่มีมูลค่าและทรัพย์สินอ้างอิงเป็นเงินสกุลเหรียญสหรัฐ

[15] SWIFT เป็นองค์การที่ย่อมาจาก Society for Worldwide Interbank Financial Telecommunication เป็นองค์กรความร่วมมือระหว่างประเทศสมาชิก ในการดูแลรักษาความปลอดภัยรายการธุรกรรมทางการเงินระหว่างสมาชิก โดยระบบงานที่รูปแบบมาตรฐานในการติดต่อกับสถาบันการเงิน เพื่อการโอนเงิน และการชำระราคาซื้อขายระหว่างประเทศ https://www.investopedia.com/terms/s/swift.asp

[16] IBAN เป็นระบบสารสนเทศที่ย่อมาจาก International Bank Account Number ซึ่งมีรูปแบบของรหัสข้อมูลมาตรฐานในการทำธุรกรรมการเงินเพื่อนโอนหรือชำระค่าสินค้าระหว่างประเทศ โดยรหัสประกอบไปด้วยรหัสประเทศและรหัสที่จำเป็นเพื่อการตรวจพิสูจน์รายการ https://www.investopedia.com/terms/i/iban.asp

เสถียรภาพและความปลอดภัยของตลาดการเงินโลก อีกประการหนึ่งด้วยความสะดวกทางเทคโนโลยี่จึงสามารถทำธุรกรรมได้ในทุกที่ และมีค่าธรรมเนียมต่ำครั้งละ 10 บาท ไม่ว่าจะเป็นจำนวนเงินเท่าไร 100 บาทก็เสีย 10 บาท หรือ 100 ล้านบาทก็เสีย 10 บาทเช่นกัน ทั้งระบบโทรศัพท์มือถือหรือคอมพิวเตอร์ก็สามารถเชื่อมต่อทำธุรกรรมได้ตลอดเวลา”

ความเห็นของผู้ให้ข้อมูลสำคัญ #413

“ด้วยระบบนิเวศเงินสกุลเข้ารหัสที่ไม่สามารถตรวจพิสูจน์ตัวตนของเจ้าของกระเป๋าเงิน ดังนั้นอาชญากรอาจเลือกกระเป๋าเงินที่ปลอดจากความเชื่อมโยงในการตรวจสอบย้อนกลับเป็นแหล่งในการเก็บรักษามูลค่าของทรัพย์ (Store of Value) ในรูปเงินสกุลเข้ารหัสในกระเป๋าเงิน และคงสภาพอยู่ในระบบนิเวศเงินสกุลเข้ารหัสตลอดเวลา จนกว่าจะมีความปลอดภัยเพียงพอจากการตรวจสอบ หรือยึดอายัดจากหน่วยงานใดๆ ค่อยทำการเคลื่อนย้ายต่อไป”

ความเห็นของผู้ให้ข้อมูลสำคัญ #421

“อันที่จริงถ้าอาชญากรมีความรู้เชิงเทคโนโลยี่มากหน่อย การจัดเก็บรักษาผลประโยชน์ในรูปเงินสกุลเข้ารหัสจะมีความปลอดภัยสูงสุด โดยต้องไม่มีความเคลื่อนไหวให้ทางเจ้าหน้าที่ตรวจสอบธุรกรรมต้องสงสัยได้ นั่นคือ นำไปจัดเก็บเงินสกุลเข้ารหัสแบบแช่แข็งในกระเป๋าเงินก็เหมือนกับการจัดเก็บรหัสข้อมูลที่ไม่เชื่อมโยงกับระบบอินเตอร์เน็ต ทำให้เจ้าหน้าที่ไม่สามารถเข้าถึงได้”

จากการสังเคราะห์ความเห็นของผู้ให้ข้อมูลสำคัญ และสำรวจข้อเท็จจริงในปัจจุบันพบว่าในเดือนมีนาคม 2021 มีเงินสกุลเข้ารหัสหมุนเวียนอยู่ในระบบตลาดเงินสกุลรหัสเข้ารหัสทั่วโลกไม่น้อยกว่า 8,900 สกุลเงิน ด้วยขนาดตลาดมูลค่ารวมประมาณ 1.8 ล้านล้านเหรียญสหรัฐ[17] หรือคิดเป็น 54 ล้านล้านบาท ในขณะที่บิตคอยน์ก็ยังเป็นเงินสกุลเข้ารหัสที่ได้รับการยอมรับในอันดับแรกด้วยขนาดตลาดมูลค่าประมาณ 1.0 ล้านล้านเหรียญสหรัฐ หรือคิดเป็นร้อยละ 59.6 ของมูลค่าทางการตลาดรวม และอันดับสองได้แก่ อีเทอเรียม มีสัดส่วนทางการตลาดประมาณร้อยละ 11.4 จึงถือได้ว่าเงินสกุลเข้ารหัสเป็นทรัพย์สินทางการเงินที่มีมูลค่าทางการตลาด และมีสภาพคล่องทั่วโลกเพียงพอที่จะรักษาและสะสมความมั่งคั่ง เพื่อประโยชน์ในทางเศรษฐกิจในอนาคตได้ แม้ว่าระดับราคาของเงินสกุลเข้ารหัสจะมีความผันผวนแปรไปตามระบบตลาดขึ้นอยู่ความต้องการในแต่ละขณะ ก็ถือเป็นทรัพย์สินที่มีอัตราการเสื่อมราคาน้อยกว่าการถือครองทรัพย์สินประเภท รถยนต์หรู และมีขนาดตลาดสภาพคล่องมากกว่าการถือครองทรัพย์ประเภท ของเก่าลายคราม ที่ดิน หรือเพชร ที่มีความจำกัดเฉพาะกลุ่มบุคคลที่สนใจเท่านั้น นอกจากนี้ต้นทุนในการดูแลรักษาสภาพของเงินสกุลเข้ารหัส

[17] ข้อมูลจากเว็บไซต์ CoinMarketCap.com ณ Last updated: Sat, 20 Mar 2021 15:10:17 UTC

เกือบจะไม่ค่าใช้จ่าย ในขณะที่ทรัพย์สินประเภทอื่นไม่ว่าจะเป็น รถยนต์หรู ของเก่าลายคราม ที่ดิน หรือเพชร ก็มีต้นทุนในการหาสถานที่จัดเก็บและมีค่าใช้จ่ายประจำในการดูแลรักษาให้อยู่ในสภาพปกติ โดยเฉพาะอย่างยิ่งศักยภาพในการซ่อนเร้นต่อการตรวจสอบสืบค้นเงินสกุลเข้ารหัสมีสูงมาก เมื่อจัดเก็บในการเป๋าเงินประเภท Cold Wallet ที่อยู่ในอุปกรณ์ที่ไม่เชื่อมต่อกับระบบอินเตอร์เน็ต เช่น Trump Drive, Handy Drive, Flash Drive หรือ USB Drive ซึ่งเป็นอุปกรณ์ขนาดเล็กที่สามารถพกพา หรือหลบซ่อนในพื้นที่ขนาดเล็ก ในกรณีที่ถูกตรวจพบอาชญากรก็เป็นผู้เก็บรหัสเปิดส่วนบุคคล ซึ่งจะไม่มีผู้ใดสามารถเปิดกระเป๋าเงินเพื่อยึดอายัดเงินสกุลเข้ารหัสได้ เมื่อเปรียบเทียบกับ รถยนต์หรูที่ต้องมีอาคารจัดเก็บ ของเก่าลายครามต้องมีห้องจัดเก็บ ที่ดินต้องมีการดูแลพื้นที่ และเพชรต้องมีตู้นิรภัยในการจัดเก็บ ซึ่งกลายเป็นจุดสนใจสำคัญที่เจ้าหน้าที่รัฐสามารถตรวจสอบสืบค้นและเข้าถึงทรัพย์สินในการยึดอายัดได้ ดังนั้นด้วยปัจจัยเชิงเศรษฐศาสตร์ในการรักษามูลค่าทรัพย์สินด้วยความปลอดภัย และต้นทุนการดูแลต่ำของเงินสกุลเข้ารหัส จึงอาจเป็นอีกปัจจัยหนึ่งที่เป็นมูลเหตุจูงใจให้อาชญกรเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน

4.1.5 ปัจจัยด้านมาตรการทางกฎหมายและการบังคับใช้เชิงปฏิบัติ

ระบบนิเวศเงินสกุลเข้ารหัส เป็นนวัตกรรมทางการเงินอิเล็กทรอนิกส์ในลักษณะโลกาภิวัตรที่มีความเป็นหนึ่งเดียวของบริบท และคุณลักษณะเฉพาะของแต่ละสกุลเงินโดยเฉพาะอย่างยิ่งบิตคอยน์ที่เป็นเงินสกุลเข้ารหัสอันดับหนึ่ง ซึ่งมีขนาดมูลค่าทางการตลาดมากกว่า 1.0 ล้านล้านเหรียญสหรัฐ หรือไม่น้อยกว่า 30 ล้านล้านบาท โดยมีมูลค่าใกล้เคียงกับ GDP ของประเทศอินโดนิเซียซึ่งมีเศรษฐกิจขนาดใหญ่เป็นอันดับที่ 16 ของโลก ในขณะที่ประเทศไทยมีขนาดเศรษฐกิจประมาณ 5.47 แสนล้านเหรียญสหรัฐเท่านั้น[18] ดังนั้นมาตรการทางกฎหมายจึงมีความสำคัญต่อการรักษาเสถียรภาพความมั่นคงของระบบการเงินระดับสากล เนื่องจากปัจจัยทางเทคโนโลยีของเงินสกุลเข้ารหัสสามารถเชื่อมโยงติดต่อข้ามพรมแดนประเทศ และไร้การกำกับความคุมของหน่วยงานใด ดังนั้นในปี 2018 The Law Library of Congress (2018) ได้ทำการสำรวจมาตรการทางกฎหมายที่เกี่ยวกับการกำกับดูแลเงินสกุลเข้ารหัสทั่วโลกจำนวน 130 ประเทศ เนื่องจากเงินสกุลเข้ารหัสมีอัตราเติบโตในมูลค่าทางเศรษฐกิจอย่างรวดเร็ว และการให้ความหมายของแต่ละประเทศแตกต่างกันโดยยังไม่มีข้อสรุปอย่างเป็นสากล รวมถึงมีระดับการบังคับใช้กฎหมายที่แตกต่างกันตามบริบทของแต่ละประเทศ ได้แก่ กลุ่มแรก เป็นประเทศที่มีมาตรการทางกฎหมายรองรับสถานภาพเงินสกุลเข้ารหัส และยินยอม

[18] ประเทศอินโดนีเซียมี GPD ในปี 2019 เท่ากับ 1.21 ล้านล้านเหรียญสหรัฐ นับเป็นประเทศที่มีขนาดเศรษฐใหญ่เป็นอันดับที่ 16 และประเทศไทยมี GDP เท่ากับ 5.47 แสนล้านเหรียญสหรัฐ เป็นอันดับที่ 25 ตามการจัดลำดับของ IMF, https://worldpopulationreview.com/countries/countries-by-gdp

ให้สามารถทำธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสได้อย่างชอบด้วยกฎหมาย โดยประเทศญี่ปุ่นเป็นประเทศแรกที่ยอมรับสถานภาพทางกฎหมายของบิตคอยน์ตั้งแต่ปี 2017 จนกลายเป็นตลาดธุรกรรมเงินสกุลเข้ารหัสที่มีขนาดใหญ่ระดับโลกในปัจจุบัน และประเทศออสเตรียที่ให้การยอมรับบิตคอยน์ในปีเดียว จากนั้นมีหลายประเทศได้ประกาศมาตรการทางกฎหมายให้การยอมรับเงินสกุลเข้ารหัสมากขึ้น เช่น ประเทศมอร์ต้าที่เป็นศูนย์กลางแลกเปลี่ยนเงินสกุลเข้ารหัสที่สำคัญของโลก และประเทศเยอรมัน บลาซิล เป็นต้น (Kethineni & Cao, 2019) สำหรับกลุ่มที่สอง เป็นประเทศที่มีมาตรการต้องห้ามและไม่ยอมรับสภานภาพเงินสกุลเข้ารหัสถือเป็นสิ่งที่ไม่ชอบด้วยกฎหมาย ต้องห้ามสถาบันการเงินดำเนินธุรกรรมใดๆ ที่เกี่ยวข้องรวมถึงการเสนอขายเงินสกุลเข้ารหัสสุกลใหม่ภายในขอบเขตประเทศของตน เช่น ประเทศแอลจิเรีย โบลีเวีย โมรอคโค เนปาล ปากีสถาน และเวียดนาม เป็นต้น ส่วนประเทศการ์ตา และบาเรน จะยกเว้นไม่ต้องห้ามสำหรับธุรกรรมเงินสกุลเข้ารหัสที่ดำเนินการในต่างประเทศ (The Law Library of Congress, 2018) รวมถึงประเทศที่มีเศรษฐกิจขนาดใหญ่ คือ ประเทศจีน เกาหลีใต้ และรัสเซีย เป็นต้น (Kethineni & Cao, 2019) และ กลุ่มประเทศสุดท้าย เป็นประเทศที่มีมาตรการทางกฎหมายยอมรับสถานภาพเงินสกุลเข้ารหัสในบางลักษณะ และอนุญาตให้ดำเนินธุรกรรมที่เกี่ยวข้องบางลักษณะที่อยู่ภายใต้กรอบมาตรการกำกับดูแลที่เคร่งครัด รวมถึงการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ที่มีลักษณะเข้าข่ายหลักทรัพย์ หรือตราสารหนี้ เช่น ประเทศนิวซีแลนด์ และเนเธอร์แลนด์ นอกจากนี้บางประเทศไม่ต้องห้ามประชาชนในกรณีการถือครองเงินสกุลเข้ารหัสเพื่อการลงทุน แต่อาจมีข้อกำหนดในการกำกับการทำธุรกรรมของสถาบันการเงินที่เกี่ยวข้องกับเงินสกุลเข้ารหัส เช่น ประเทศบังคลาเทศ อิหร่าน ลิตเธอร์เนีย กัมพูชา และไทย เป็นต้น (The Law Library of Congress, 2018)

ดังนั้นเมื่อบริบทมาตราการทางกฎหมายทางมีต่อเงินสกุลเข้ารหัสมีความแตกต่างกันตั้งแต่กลุ่มประเทศที่ยอมรับเงินสกุลเข้ารหัสเป็นสิ่งที่ชอบด้วยกฎหมาย ธุรกรรมเงินสกุลเข้ารหัสและธุรกิจที่เกี่ยวข้องได้รับการรับรอง จนถึงไปถึงขั้นกลุ่มประเทศที่ปฏิเสธต้องห้ามเงินสกุลเข้ารหัสเป็นสิ่งที่ไม่ชอบด้วยกฎหมาย ธุรกรรมเงินสกุลเข้ารหัสและธุรกิจที่เกี่ยวข้องถือเป็นการกระทำที่ผิดกฎหมาย จึงเกิดเป็นช่องว่างของมาตรการทางกฎหมายระหว่างประเทศ อาชญากรจึงสามารถเลือกแหล่งการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้สะดวก เพราะเทคโนโลยี่บนระบบปฏิบัติการบล็อกเชนสามารถทำธุรกรรมโอนเงินสกุลเข้ารหัสข้ามประเทศได้ด้วยความสะดวก รวดเร็ว และต้นทุนดำเนินการต่ำ อีกทั้งสามารถเลือกสถานที่แปลงมูลค่าเป็นเงินตราปกติในเขตประเทศที่มีมาตราทางกฎหมายรองรับ ดังนั้น ปัจจัยด้านมาตรการทางกฎหมายจึงเป็นอีกมูลเหตุจูงใจหนึ่งต่ออาชญากรในการเลือกฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ทั้งนี้ผู้ให้ข้อมูลสำคัญได้แสดงความเห็นในประเด็นนี้ดังนี้

ความเห็นของผู้ให้ข้อมูล #112

“เชื่อว่ากฎหมายป้องกันและปราบปรามการฟอกเงินในปัจจุบันของไทยมีความเข็มแข็งรัดกุมเพียงพอ และหากมีการกระทำผิดที่เชื่อมโยงไปต่างประเทศ รัฐบาลไทยก็มีระบบความสัมพันธ์ที่จะได้รับการสนับสนุนจากรัฐภาคี แต่ประเด็นปัญหาสำคัญ คือการบังคับใช้กฎหมายไม่ทันต่อการเคลื่อนย้ายเงินสกุลเข้ารหัส ตัวอย่างเช่น การจับกุมเว็บไซต์พนันออนไลน์ที่เพิ่งเกิดขึ้น ผู้กระทำผิดได้นำเงินไปซ่อนไว้ในรูปของบิตคอยน์ที่ Exchanger รับอนุญาตแห่งหนึ่ง โดยในทางการสืบสวนสามารถเข้าถึงเป้าหมายได้แล้ว แต่กว่าจะเสร็จสิ้นขั้นตอนเสนอขออนุมัติต่อคณะกรรมการธุรกรรม ผู้กระทำผิดก็โอนบิตคอยน์ออกจากกระเป๋าเงินไปหมดแล้วไม่ทันต่อการยึดอายัด เพราะความล่าช้าเพียงวินาทีเดียวเงินสกุลเข้ารหัสก็สามารถถูกโยกย้ายไปไกลนอกเขตอำนาจแล้ว”

ความเห็นของผู้ให้ข้อมูลสำคัญ #211

“โดยกลไกปกติของเงินสกุลเข้ารหัสเป็นเทคโนโลยีที่สืบหาตัวตนได้ยาก เนื่องจากไม่ต้องแสดงตัวตนก่อนใช้งาน แต่ในปัจจุบันประเทศไทยมีกฎหมายที่ให้อำนาจสำนักงาน กลต เข้ามากำกับผู้ให้บริการเกี่ยวกับเงินสกุลเข้ารหัสต้องปฏิบัติตามกฎหมายเกี่ยวกับการป้องกันและปราบปรามการฟอกเงิน โดยสำนักงาน กลต เข้ามากำกับผู้ให้บริหารรับอนุญาตมีหน้าที่ในการตรวจสอบตัวตนของผู้ขอใช้งานซึ่งเป็นระบบที่เข้าช่วยให้สามารถรู้ตัวตนผู้ใช้งาน และสามารถตรวจสอบธุรกรรมรายการต้องสงสัยได้ แต่ถ้าเป็นการทำธุรกรรมระหว่างผู้ใช้งานโดยตรงส่งมอบระหว่างกันเป็นนอกขอบข่ายการกำกับ ก็เสมือนบุคคลส่งมอบเงินสดระหว่างกันที่จะไม่สามารถเข้าไปตรวจสอบได้ หรือธุรกรรมข้ามประเทศก็ยังไม่มีกฎหมายระหว่างประเทศเข้ามากำกับเช่นกัน คงต้องอาศัยความร่วมมือระหว่างประเทศแทน”

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ความเห็นของผู้ให้ข้อมูลสำคัญ #212

“ปัจจุบันมาตรการทางการกฎหมายที่มีต่อเงินสกุลเข้ารหัสมีความแตกต่างกัน มีทั้งประเทศที่ไม่มีระบบการกำกับ และประเทศที่มีระบบการกำกับ สำหรับประเทศที่มีระบบการกำกับก็ยังแยกเป็นประเทศที่มีระบบการกำกับการแสดงตัวตนของผู้ใช้งาน KYC และระเบียบการกำกับธุรกรรมเงินสกุลเข้ารหัสอย่างเคร่งครัดตามมาตรฐานสากล กับบางประเทศที่มีระบบการกำกับแบบอ่อนไม่เคร่งครัดต่อการแสดงตัวตนผู้ใช้งาน ทำให้เป็นจุดอ่อนของมาตรการทางกฎหมายที่อาชญากรสามารถเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงินในประเทศที่ไม่มีระบบกำกับ หรือประเทศที่ไม่เคร่งครัดในการกำกับ”

ความเห็นของผู้ให้ข้อมูลสำคัญ #221

“ระเบียบในการกำกับดูแลเงินสกุลเข้ารหัสยังไม่สามารถดำเนินการได้ชัดเจนเต็มที่ และมาตรการกำกับทางกฎหมายของแต่ละประเทศยังมีความไม่เท่าเทียบกัน จึงเป็นช่องว่างทางกฎระเบียบที่อาชญากรได้รับประโยชน์สามารถก้าวข้าม หรือลอดผ่านกฎระเบียบได้”

ความเห็นของผู้ให้ข้อมูลสำคัญ #241

“จากการที่ได้มีโอกาสร่วมประชุม กับหน่วยงานบังคับใช้กฎหมายระดับนานาชาติ เกี่ยวกับประเด็นการกำกับดูแลเงินสกุลเข้ารหัส ก็มีความเห็นร่วมกันว่ากฎระเบียบที่กับข้องกับการต่อต้านการฟอกเงินสกุลเข้ารหัสของหลายประเทศยังไม่มีความพร้อม รวมถึงประเทศไทยด้วย จึงยังไม่สามารถเข้าไปควบคุมดูแลการดำเนินการของผู้กระทำผิดได้ และความไม่พร้อมในไทย เป็นทั้งด้านกฎระเบียบและการบังคับใช้”

ความเห็นของผู้ให้ข้อมูลสำคัญ #441

“กลไกการกำกับดูแลของรัฐในบางประเทศไม่มีการกำกับดูแล หรือดูแลอย่างไม่เคร่งครัด ทำให้เจ้าหน้าที่ของรัฐที่พึ่งมีหน้าที่ในการกำกับดูแล เช่น ตำรวจ หรือหน่วยงานต่อต้านการฟอกเงินของในประเทศนั้น ไม่มีองค์ความรู้เกี่ยวกับบริบทของเงินสกุลเข้ารหัส ขาดความเข้าใจในการป้องกันและปราบปรามการกระทำผิด จึงเป็นช่องว่างที่เปิดให้อาชญากรเข้าไปทำการฟอกเงินผ่านประเทศเหล่านั้นได้โดยง่าย”

ความแตกต่างของมาตรทางกฎหมายในการกำกับดูแลบริบท ของเงินสกุลเข้ารหัสในแต่ละประเทศ จึงเป็นช่องโอกาสที่มีนัยสำคัญต่ออาชญากรในการตัดสินเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน เนื่องจากอาชญากรสามารถบริหารจัดการแผนการฟอกเงินโดยทำธุรกรรมข้ามประเทศโดยเทคโนโลยีได้สะดวก รวมถึงการบริหารเครือข่ายกระบวนการฟอกเงินก็มีแนวโน้มที่จะสามารถลดจำนวนบุคคลที่เข้ามาเกี่ยวข้องกับการโยกย้ายถ่ายเทเงินสกุลเข้ารหัส เมื่อเปรียบเทียบกับการบริหารจัดการทรัพย์สินอื่น ซึ่งก็เป็นปัจจัยหนึ่งที่จะลดปริมาณกิจกรรมเสี่ยงต่อกฎหมายต่อต้านการฟอกเงิน หากมีการเคลื่อนย้ายเงินสกุลเข้ารหัสในระบบนิเวศโดยคำสั่งอัตโนมัติ และไปดำเนินการแปลงค่าเป็นเงินตราหรือทรัพย์สินอื่นในประเทศที่ไม่มีมาตรการทางกฎหมายในการกำกับดูแล หรือประเทศที่มีมาตรการทางกฎหมายที่ไม่เคร่งรัด ดังนั้น มาตรการทางกฎหมายจึงมีความสำคัญต่อการกำกับบริบทของเงินสกุลเข้ารหัส และควรร่วมกันยกระดับมาตรฐานกฎหมายและการบังคับใช้ให้มีความเป็นสากลที่เท่าเทียมกันทุกประเทศ หรือให้ครอบคลุมจำนวนประเทศให้มากที่สุด มิฉะนั้นก็จะประสบปัญหาเดียวกับระบบการจัดเก็บภาษี ที่ยังคงมีบางประเทศที่มีมาตรการปลอดจากภาษีอากร

จนกลายเป็นแหล่งในการหลบเลี่ยงภาษีระดับสากล และเป็นแหล่งในการฟอกเงินของอาชญากรโดยปริยาย

4.1.6 สรุปบริบทของเงินสกุลเข้ารหัสที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

ผลการศึกษา โดยการสังเคราะห์ข้อมูลการสัมภาษณ์เชิงลึกจากผู้ให้ข้อมูลสำคัญร่วมกับการทบทวนวรรณในงานวิจัยจากต่างประเทศ ที่เกี่ยวข้องในประเด็นกลไกการทำของระบบนิเวศเงินสกุลเข้ารหัส และปัจจัยสำคัญที่อาจมีอทธิพลต่ออาชญากรในการตัดสินใจใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน พบว่า ความเห็นเชิงทัศนะต่อปัจจัยที่อาจมีผลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสส่วนใหญ่มีความเห็นสอดคล้องกัน กล่าวคือ

(1) ปัจจัยกลไกการทำงานแบบกระจายศูนย์ ไร้การควบคุมจาหน่วยงานใด โดยระบบนิเวศเงินสกุลเข้ารหัสเปิดกว้างต่อผู้ใช้งานสามารถเข้าสู่ระบบ และโอนมูลค่าให้แก่กันได้อย่างไม่มีเงื่อนไข ผู้ใช้งานไม่จำเป็นต้องแสดงตัวตนก่อนใช้งาน จึงเป็นการเปิดโอกาสให้แก่อาชญากรสามารถทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยไม่อยู่ในกำกับของหน่วยงานใดที่จะรับรู้ตัวตนที่แท้จริงของผู้ใช้งาน ซึ่งสอดคล้องกับความเห็นจากงานวิจัยของ HouBen and Snyers (2018) ได้แสดงทัศนะว่า การไม่มีหน่วยงานตัวกลางในการกำกับ (No Central Intermediary) เป็นระบบการทำธุรกรรมโอนมูลค่าระหว่างผู้โอนและผู้รับโอนกันโดยตรง (Peer-to-Peer) โดยไม่มีกลไกของหน่วยงานตัวกลางใดกำกับดูแลระบบปฏิบัติการ แต่เป็นระบบบริการจัดการฐานข้อมูลแบบกระจายศูนย์ จึงสามารถดำเนินธุรกรรมได้ทันทีไม่ต้องรอการตรวจสอบหรืออนุญาตใด

(2) ปัจจัยการอำพรางตัวตน และความยากต่อการสืบค้นเส้นทางธุรกรรม จากทัศนะของ HouBen and Snyers (2018) ในประเด็นการปิดบังตัวตนผู้ใช้งาน เป็นคุณลักษณะเฉพาะที่สำคัญของเงินสกุลเข้ารหัส ซึ่งผู้ใช้งานสามารถใช้นามแฝงโดยไม่ต้องระบุข้อมูลส่วนบุคคล ซึ่งเป็นปัจจัยทางธรรมชาติของระบบงานที่ป้องกันการตรวจสอบและการเข้าถึงตัวตนของผู้ใช้งาน อีกทั้งการปกป้องข้อมูลส่วนบุคคล ด้วยกลไกการโอนมูลค่าระหว่างผู้โอนตรงไปยังผู้รับโอน ระบบปฏิบัติการบล็อกเชนจะสร้างรหัสเปิดสาธารณะส่งไปยังผู้รับโอน เพื่อใช้ร่วมกับรหัสเปิดส่วนบุคคลในการเปิดกระเป๋าเงินปลายทาง จึงเป็นการปกป้องข้อมูลส่วนบุคคลโดยธรรมชาติของระบบปฏิบัติการ และไม่มีกฎระเบียบจากหน่วยงานใดที่จะสามารถใช้อำนาจทางกฎหมายในการเข้าถึงรหัสข้อมูลลับสำหรับเปิดกระเป๋าเงินหรือบังคับใช้อำนาจอายัดเงินสกุลเข้ารหัสได้ แต่ความเห็นของผู้ให้ข้อมูลสำคัญได้แสดงทัศนะเพิ่มเติมว่า โดยบริบทปัจจุบันของหลายประเทศได้เริ่มออกมาตรการทางกฎหมายในการเข้าไปกำกับธุรกรรมเงินสกุลเข้ารหัส อย่างไรก็ตามพัฒนาการทางเทคโนโลยีซึ่งได้สร้างระบบปฏิบัติการ

TOR Browser เพื่อลวงรหัสที่ตั้งของผู้ใช้งานในขณะติดต่อเข้าสู่ระบบ รวมถึงผู้ให้บริการ Crypto Mixer หรือ Tumbler ในการตัดความเชื่อมโยงเส้นทางธุรกรรมระหว่างต้นทางและปลายทาง อันเป็นนวัตกรรมทางเทคโนโลยีที่เอื้อประโยชน์ต่ออาชญากรในการเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน

(3) ปัจจัยด้านความสะดวก รวดเร็ว และสามารถทำธุรกรรมข้ามประเทศ โดยความเห็นที่สอดคล้องทำนองเดียวกันว่า เป็นการทำธุรกรรมแบบไร้พรมแดนได้เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสเป็นการดำเนินการบนระบบออนไลน์ ซึ่งปัจจุบันมีโครงข่ายการติดต่อสื่อสารเชื่อมโยงถึงกันทั้งในประเทศและระหว่างประเทศ จึงสามารถทำธุรกรรมการโอนระหว่างกันข้ามขอบเขตประเทศได้อย่างรวดเร็วและเสรี (HouBen & Snyers, 2018) และทัศนะของผู้ให้ข้อมูลสำคัญได้ขยายความเห็นถึงขนาดของรายการโอนที่ไม่มีข้อจำกัดมูลค่า โดยการทำธุรกรรมสามารถโอนมูลค่าจำนวนสูงเท่าใดก็ได้ในคราวเดียว ส่งผลให้มีความสะดวกรวดเร็วกว่าการฟอกเงินโดยเงินสดที่อาจมีหลายขั้นตอนในการถ่ายเทผลประโยชน์ที่ได้จากการกระทำผิด

(4) ปัจจัยการรักษามูลค่าทรัพย์สินด้วยต้นทุนการดูแลต่ำ ทั้งนี้จากงานวิจัยแสดงให้เห็นถึงปัจจัยต้นทุนการทำธุรกรรมในกระบวนการฟอกเงินที่ต้องทำการยักย้าย ถ่ายโอนในขั้นตอนกระจายรายย่อยเพื่อกลบเกลื่อนร่องรอยหลีกเลี่ยงการตรวจสอบ ก่อนจะรวบรวมกลับมาเป็นเงินที่ชอบด้วยกฎหมายนั้น เมื่อเปรียบเทียบกับการทำธุรกรรรมเงินสกุลเข้ารหัสที่สามารถกระจายรายการในกลุ่มเครือข่ายได้ด้วยความรวดเร็ว ต้นทุนดำเนินการต่อรายการต่ำกว่ามาก ทำให้สามารถสร้างความซับซ้อน และก่อภาระการสืบค้นตรวจสอบให้ยากต่อการเข้าถึงรายการได้มีประสิทธิภาพมากกว่าและต้นทุนดำเนินการรวมต่ำกว่า (Breing et al., 2015; HouBen & Snyers, 2018) ซึ่งสอดคล้องกับทัศนะของผู้ให้ข้อมูลสำคัญ นอกจากนี้ผู้ให้ข้อมูลสำคัญยังมีความเห็นเพิ่มในประเด็นเงินสกุลเข้ารหัสมีแนวโน้มที่จะใช้เป็นแหล่งในการเก็บรักษามูลค่าในระบบนิเวศได้อย่างปลอดภัยมากกว่าการถือครองทรัพย์สินอื่น ซึ่งผู้วิจัยมีความเห็นสอดคล้องกับผู้ให้ข้อมูลสำคัญในประเด็นนี้ ทั้งในเชิงมูลค่าทางเศรษฐกิจของเงินสกุลเข้ารหัส และวิธีการจัดเก็บกระเป๋าเงินประเภท Cold Wallet ซึ่งเป็นอุปรณ์คอมพิวเตอร์ที่จัดเก็บข้อมูลและไม่เชื่อมต่อกับระบบอินเตอร์เน็ต เช่น USB Drive ในปัจจุบันมีขนาดเล็กสามารถพกพาติดตัว เก็บซ่อนไว้ในพื้นที่เล็กขนาดเท่านิ้วหัวแม่มือเท่านั้น จึงมีโอกาสสูงที่อาชญากรจะเก็บรักษามูลค่าทรัพย์ไว้ใน Cold Wallet โดยลอดพ้นจากการตรวจสอบสืบค้นจากเจ้าหน้าที่

(5) ปัจจัยด้านมาตรการทางกฎหมายและการบังคับใช้เชิงปฏิบัติ ปรากฏความเห็นไปในทิศทางเดียวกันว่า เงินสกุลเข้ารหัสถือเป็นนวัตกรรมเทคโนโลยีทางการเงินที่ส่งผลกระทบต่อระบบการเงินโลก ซึ่งแต่ละประเทศมีมาตรการภายในประเทศต่อเงินสกุลเข้ารหัสที่แตกต่างกัน ตั้งแต่ยอมรับสถานภาพทางกฎหมายจนไปถึงขั้นต้องห้ามเป็นสิ่งผิดกฎหมาย อีกทั้งยังขาดมาตรการสากล

และนโยบายระหว่างประเทศต่อบริบทของเงินสกุลเข้ารหัส จึงถือเป็นโอกาสของผู้ใช้งานที่จะอาศัยช่องว่างทางกฎหมายระหว่างประเทศ ในการถ่ายโอนเพื่อการแปรสภาพเป็นเงินตราในประเทศที่ยอมรับสถานภาพทางกฎหมาย และหลีกเลี่ยงประเทศที่มีกฎหมายบังคับที่เข็มแข็ง (HouBen & Snyers, 2018)

อย่างไรก็ผู้ให้ข้อมูลสำคัญ #413 และ #421 ให้ทัศนะความเห็นเชิงขัดแย้งตรงกันในประเด็น**ความสำคัญผิดในสาระสำคัญของอาชญากรต่อระบบนิเวศเงินสกุลเข้ารหัส** ซึ่งมีความเข้าใจว่าเงินสกุลเข้ารหัสมีศักยภาพทางเทคโนโลยีการปิดตัวตน และปิดบังเส้นทางธุรกรรมด้วยความปลอดภัยสูงต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ซึ่งอาจนับเป็นอีกหนึ่งปัจจัยที่มีอทธิพลต่ออาชญากร เนื่องจากอาชญากรส่วนหนึ่งยังขาดองค์ความรู้ที่ทันสมัยเพียงพอ เกี่ยวกับพัฒนาการทางเทคโนโลยีและมาตรการป้องกันปราบปรามการฟอกเงิน โดยปัจจุบันหลายองค์กรได้พัฒนาโปรแกรมคอมพิวเตอร์ที่เชื่อมต่อกับฐานข้อมูลบนระบบปฏิบัติการบล็อกเชน เพื่อการวิเคราะห์พฤติกรรมกลุ่มผู้ใช้งานและความสัมพันธ์ของเส้นทางธุรกรรม รวมถึงพัฒนาศักยภาพการในการขโมยข้อมูล (Hack) รหัสเปิดส่วนบุคคลจากอุปกรณ์ที่เชื่อมต่อกับรหัสที่ตั้ง หรือกระเป๋าเงินต้องสงสัยได้อย่างมีประสิทธิภาพเพิ่มขึ้น ตัวอย่างเช่น การสืบสวนในระบบนิเวศของบิตคอยน์ และการจับกุมอาชญากรได้จนสามารถดำเนินการปิด Dark Web รายใหญ่ อันได้แก่ Silk Road และ Alphabay ดังนั้นทัศนะความเห็นนี้อาจเป็นการโต้แย้งต่อปัจจัยที่กล่าวมาแล้วข้างต้น แต่ผู้วิจัยก็มีความเห็นว่าควรนับเป็นอีกหนึ่งปัจจัยที่มีอิทธิพลต่ออาชญากรในการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน เนื่องจากฐานองค์ความรู้เกี่ยวกับบริบทของเงินสกุลเข้ารหัสที่ถูกนำไปเผยแพร่ต่อประชาชนทั่วไป หรือสังคมโลกก็ยังอยู่ในกลุ่มคนวงจำกัด อีกทั้งบริบทของเงินสกุลเข้ารหัสมีพลวัตเปลี่ยนแปลงทางเทคโนโลยีอย่างต่อเนื่อง ดังนั้นกลุ่มอาชญากรเองก็น่าจะมีการกระจายตัวของประชากรในกลุ่มลักษณะใกล้เคียงกับสังคมทั่วไป จึงคาดว่าน่าจะมีอาชญากรบางรายที่มีการตัดสินใจจากการสำคัญผิดในสาระสำคัญดังกล่าวได้

4.2 รูปแบบของอาชญากรรมที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการประกอบอาชญากรรม และในการทำธุรกรรมฟอกเงิน

การศึกษารูปแบบของอาชญากรรมเกี่ยวข้องกับการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการประกอบอาชญากรรม ซึ่งมีลักษณะที่อาชญากรดำเนินการประกอบอาชญากรรมที่อาจไม่ได้เกี่ยวข้องกับระบบนิเวศเงินสกุลเข้ารหัสโดยตรง หรืออาชญากรรมที่อาจไม่ได้กระทำบนระบบไซเบอร์ แต่อาศัยเงินสกุลเข้ารหัสเป็นเครื่องมือในการหลอกลวง สร้างแรงจูงใจให้เหยื่อหลงเชื่อ ทั้งที่อาชญากรอาจได้รับผลประโยชน์จากการกระทำผิดในรูปของเงิน หรือทรัพย์สินอื่นซึ่งไม่ใช่เงินสกุลเข้ารหัสโดยตรง

แต่ในท้ายที่สุด อาชญากรเหล่านั้นก็อาจตัดสินใจนำผลประโยชน์ขนาดมูลค่าสูงไปทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ซึ่งหมายรวมถึง อาชญากรรมที่ดำเนินการบนระบบไซเบอร์อยู่แล้ว ทั้งที่ได้รับผลประโยชน์จากการกระทำผิดเป็นเงินหรือทรัพย์สินอื่น แต่แนวโน้มโดยส่วนใหญ่อาชญากรมักจะได้รับผลประโยชน์ในรูปเงินสกุลเข้ารหัส เนื่องจากเป็นการประกอบอาญชากรรมบนระบบไซเบอร์ ซึ่งอาชญากรก็มักจะใช้เครือข่ายของกลุ่มผู้กระทำผิดบนระบบไซเบอร์นำเงินสกุลเข้ารหัสดังกล่าว ไปทำการฟอกเงินได้ทันทีเช่นกัน

ผลการศึกษาโดยการสัมภาษณ์เชิงลึกด้วยคำถามปลายเปิด เพื่อรวบรวมข้อมูลประสบการณ์ทั้งทางตรงและทางอ้อม ข้อมูลความเห็นเชิงทัศนะอย่างอิสระจากผู้ให้ข้อมูลสำคัญ พบว่า ผู้ให้ข้อมูลสำคัญให้ความเห็นอย่างเป็นฉันทามติว่ารูปแบบอาชญากรรมที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องมือ และเพื่อนำผลประโยชน์จากการกระทำผิดไปทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสนั้น คือ (1) อาชญากรรมเศรษฐกิจเกือบทุกประเภท เนื่องจากอาชญากรรมทางเศรษฐกิจมักจะก่อให้เกิดความเสียหายแก่เหยื่อในวงกว้าง และมีขนาดผลประโยชน์จากการกระทำผิดมูลค่าสูงที่จำเป็นต้องจัดการกระจายผลประโยชน์ และทำการฟอกเงินเป็นเงินที่ชอบด้วยกฎหมายในระยะสั้นให้เร็วที่สุด ดังนั้น ด้วยคุณลักษณะของเงินสกุลเข้ารหัสส่งผลให้อาชญากรส่วนหนึ่งอาจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน และ (2) อาชญากรรมไซเบอร์เกือบทุกประเภทเช่นกัน ซึ่งเป็นลักษณะการประกอบอาชญากรรมที่กระทำขึ้นบนระบบไซเบอร์ หมายรวมถึง การกระทำผิดบนระบบเครือข่ายอินเตอร์เน็ต หรือใช้ระบบอินเตอร์เน็ตเป็นเครื่องมือในการกระทำผิด และการกระทำผิดบนระบบโครงข่ายการสื่อสารในลักษณะทำนองเดียวกัน เนื่องจากอาชญากรที่กระทำการบนระบบไซเบอร์มักมีความเชี่ยวชาญด้านเทคโนโลยี ซึ่งอาชญากรมักปิดบังตัวตนและมีศักยภาพป้องกันการตรวจสอบรหัสที่ตั้งในการสั่งการก่ออาชญากรรม ดังนั้น การใช้เงินสกุลเข้ารหัสเป็นสื่อกลางในการส่งมอบผลประโยชน์ จึงสอดคล้องกับบริบทของเงินสกุลเข้ารหัสที่ผู้ใช้งานหรืออาชญากรผู้รับโอนผลประโยชน์จากการกระทำผิดที่ไม่ต้องแสดงตัวตนใด และโดยระบบการประกอบอาชญากรรมบนระบบไซเบอร์ จึงสามารถดำเนินกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้ทันทีอย่างต่อเนื่อง

ทั้งนี้ผู้ให้ข้อมูลสำคัญส่วนใหญ่ได้ให้ความเห็นอย่างเป็นอิสระว่าลักษณะการประกอบอาชญากรรมที่มีโอกาสเกิดขึ้นในรูปแบบของอาชญากรรมตามขอบเขตการศึกษานี้ ได้แก่ (1) การหลอกลวงฉ้อโกงประชาชนในลักษณะแชร์ลูกโซ่ (Ponzi Scheme) และ (2) การค้ายาเสพติด ทั้งในลักษณะองค์กรอาชญากรรม และการค้าสิ่งผิดกฎหมายบนระบบออนไลน์ (Dark Web) และผู้ให้ข้อมูลสำคัญส่วนหนึ่งได้ให้ความเห็นว่าอาชญากรรมอันดับสาม คือ (3) การเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิวเตอร์ (Ransomware) เข้าทำลายระบบปฏิบัติการคอมพิวเตอร์หรือระบบจัดการฐานข้อมูล

ขององค์กร ซึ่งเข้าข่ายอาญากรรมไซเบอร์ประเภททำลายล้างระบบ (Cybervandalism) และอันดับสี่ คือ (4) การพนันรวมถึงการพนันบนระบบออนไลน์ ตามลำดับ นอกจากนี้ผู้ให้ข้อมูลสำคัญได้ให้ความเห็นเพิ่มเติมถึงลักษณะการประกอบอาชญากรรม ที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องในการประกอบอาชญากรรมและการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ได้แก่ การทุนระดมเพื่อสนับสนุนการก่อการร้าย, การค้าอาวุธรวมถึงการค้าอาวุธบนระบบออนไลน์, การฉ้อโกงจากการระดมเงินทุนด้วยการออกเงินสกุลเข้ารหัสสกุลใหม่ (ICO Scam), การหลีกเลี่ยงภาษี และการคอรัปชั่น เป็นต้น ทั้งนี้ ผู้วิจัยได้สังเคราะห์ประสบการณ์และความเห็นเชิงทัศนะของผู้ให้ข้อมูลสำคัญต่อรูปแบบการประกอบอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และใช้เป็นเครื่องมือในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ดังนี้

4.2.1 การหลอกลวงฉ้อโกงประชาชนในลักษณะแชร์ลูกโซ่ (Ponzi Scheme)

อาชญากรรมหลอลวงหรือฉ้อโกงประชาชนในลักษณะแชร์ลูกโซ่ เป็นประเด็นปัญหาทางสังคมที่ได้รับรู้กันอย่างต่อเนื่อง ทั้งนี้อาชญากรรม Ponzi Scheme หรือแชร์ลูกโซ่ มีรูปแบบในการหลอกลวง เพื่อชักจูงให้เหยื่อเข้ามาร่วมลงทุนโดยการนำเงินทุนจากเหยื่อรายใหม่ไปหมุนเวียนชำระเป็นผลประโยชน์ให้แก่เหยื่อรายเดิม โดยอาชญากรจะหาสิ่งจูงใจเป็นกิจการบังหน้าที่สร้างภาพลักษณ์ให้เกิดความน่าเชื่อถือด้วยการให้คำมั่น หรือโน้มน้าวให้เชื่อว่าจะได้รับผลตอบแทนจากการลงทุนในอัตราสูง และไม่มีความเสี่ยงหรือมีความเสี่ยงต่ำมาก ทั้งนี้กิจการบังหน้าอาจเป็นการประกอบธุรกิจหรือการลงทุนตามกฎหมายที่ให้ผลตอบแทนบางส่วน รูปแบบอาชญากรรมนี้จะดำรงอยู่ต่อไปได้ยาวนานเพียงไร ขึ้นอยู่กับความต่อเนื่องของจำนวนเงินลงทุนที่เข้าร่วมของเหยื่อรายใหม่ และแนวโน้มที่เริ่มก่อให้เห็นถึงความเสียหาย เมื่อจำนวนเงินลงทุนจากเหยื่อรายใหม่น้อยลง หรือเหยื่อรายเดิมขอถอนการลงทุนจำนวนมากขึ้น (Siegel, 2013) ในท้ายที่สุดกิจการบังหน้าก็จะขาดกระแสเงินหมุนเวียน และปิดตัวลงทิ้งไว้แต่ความเสียหายไว้ให้แก่เหยื่อจำนวนมาก

จากข้อมูลการสัมภาษณ์ผู้ให้ข้อมูลสำคัญส่วนใหญ่ให้ความเห็นเชิงทัศนะตรงกัน ว่าเงินสกุลเข้ารหัสเป็นนวัตกรรมเทคโนโลยี่ทางการเงิน และเป็นองค์ความรู้ใหม่ที่มีบุคคลที่รู้และเข้าใจกลไกการทำงาน คุณลักษณะเฉพาะ และการประยุกต์ใช้งานอย่างเหมาะสม ยังมีจำนวนอยู่ในวงจำกัด แต่ความรู้ที่เผยแพร่ต่อสาธารณะมีเฉพาะส่วนที่ประชาชนส่วนใหญ่ได้รับรู้ คือ การลงทุนที่มีแนวโน้มให้อัตราผลตอบแทนสูงอย่างต่อเนื่อง จึงเข้าองค์ประกอบสำคัญของสิ่งจูงใจของกิจการบังหน้า คือ “ความไม่รู้” และ “ความโลภ” นอกจากนี้อาชญากรรมแชร์ลูกโซ่นี้มักสร้างเงินทุนหมุนเวียนจำนวนมาก และอาชญากรได้ผลประโยชน์มหาศาลจากการหลอกลวงจำเป็นต้องจัดการยักย้ายถ่ายเทเงินเหล่านี้ด้วยความรวดเร็ว กอรปกับเป็นการหลอกลวงด้วยเงินสกุลเข้ารหัสจึงอาจได้รับผลประโยชน์ใน

รูปของเงินสกุลเข้ารหัสอยู่แล้ว รวมถึงอาจอยู่ในรูปของเงินหรือทรัพย์สินอื่นที่สามารถแปลงค่าเป็นเงินสกุลเข้ารหัส และทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสในระหว่างกิจการบังหน้ายังดำเนินอยู่ ดังความเห็นของผู้ให้ข้อมูลสำคัญบางส่วน ดังนี้

ความเห็นของผู้ให้ข้อมูลสำคัญ #111

“การที่คนรู้น้อย รู้กันในเฉพาะกลุ่ม อาชญากรจึงปรับสิ่งจูงใจในการหลอกลวงฉ้อโกงลักษณะแชร์ลูกโซ่ Ponzi Scheme มาเป็นบิตคอยน์ หรือเงินสกุลเข้ารหัสอื่น ในการให้ผลตอบแทนอัตราสูง แต่รูปแบบกระบวนการการก่ออาชญากรรมยังเป็นลักษณะเดิม ที่มีการจัดตั้งทีมงานขยายจำนวนผู้สนใจ แบบมีแม่ข่ายส่งต่อไปยังลูกข่ายต่อลูกโซ่เป็นปริมิด และนำเงินบางส่วนไปทำการลงทุนในบิตคอยน์เพื่อแสดงให้สมาชิกได้รับรู้ว่ามีกิจกรรมธุรกิจ แต่ในความเป็นจริงอาจเป็นส่วนหนึ่งของการฟอกเงิน หรืออาจแสดงตนเป็นธุรกิจขุดบิตคอยน์[19] แต่กลับเป็นการถ่ายโอนบิตคอยน์เพื่อให้ดูเสมือนเป็นผลตอบแทนจากการขุด เพื่อจูงใจให้เหยื่อเข้าร่วมมากขึ้น ยังไม่รวมถึงลักษณะการระดมทุนในโครงการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ (ICO) ซึ่งมีความเสี่ยงที่โครงการธุรกิจที่นำเสนออาจดำเนินการไม่ประสบความสำเร็จร่วมอยู่ด้วย โดยมีทั้งโครงการที่ประกอบกิจการจริง และโครงการที่สร้างขึ้นเพื่อหลอกลวง และยังมีรูปแบบการขโมยเงินสกุลเข้ารหัสในขณะรวบรวมเงินระดมทุนจากการเสนอขายอีก

การหลอกลวงฉ้อโกงลักษณะนี้มักมีการดำนเนิการเป็นองค์กรที่มีเครือข่ายระหว่างประเทศ คือ มีหัวหน้าที่ร่วมกัน แต่กระจายดำเนินการโอนข้ามประเทศแสดงเป็นการลงทุนข้ามประเทศ แต่ทั้งหมดเป็นการโอนเงินระหว่างกลุ่มกิจการเดียวกันในต่างประเทศ เพื่อแสดงศักยภาพของธุรกิจในการหลอกลวง”

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ความเห็นของผู้ให้ข้อมูลสำคัญ #113

“ปัจจุบันเป็นที่รับรู้และดำเนินการกันอยู่ในวงแคบ ดังนั้นรูปอาชญากรรมที่มีโอกาสใช้เงินสกุลเข้ารหัสได้ก็น่าจะเป็นอาชญากรรมที่ได้ทรัพย์จำนวนมาก และเพื่อการฟอกเงินโดยรวดเร็ว

[19] ข่าวอาชญากรรม (2019) การหลอกลวงในปี 2019 ด้วยการโฆษณาในเว็บไซต์ Cryptominingfarm ซึ่งเป็นบริษัทผู้ให้เช่าเครื่องมือในการขุดบิตคอยน์ โดยผู้สนใจสามารถทำการลงทุนได้ตั้งแต่ 2,000 บาทขึ้นไป เพื่อเข้าเชื่อมต่อระบบนิเวศและทำหน้าที่ยืนยันรายการธุรกรรมบิตคอยน์ โดยได้รับค่าตอบแทนเป็นบิตคอยน์ ทั้งนี้ผู้กระทำผิดได้นำเงินที่ได้รับจากผู้ลงทุนไปแลกเปลี่ยนเป็นบิตคอยน์และนำไปกระจายส่งมอบเป็นค่าตอบแทนให้แก่นักลงทุน เพื่อสร้างแรงจูงใจให้เหยื่อในการขยายการลงทุนและขยายฐานจำนวนนักลงทุน จนในที่สุดเว็บไซต์นี้ได้ปิดตัวลงโดยสร้างความเสียหายให้แก่นักลงทุนที่หลงเชื่อจากการหลอกลวงจำนวนรวมสูงถึงประมาณ 500 ล้านบาท https://news.thaipbs.or.th/content/277818

ได้แก่ การฉ้อโกงประชาชนแบบแชร์โซ่ ซึ่งติดอันดับต้น ของสำนักงานป้องกันและปราบปรามการฟอกเงินมาต่อเนื่อง เนื่องจากได้รับเงินจำนวนมากในเวลารวดเร็ว ซึ่งกลไกการรับเงินอยู่ในระบบบัญชีเงินฝากของธนาคารอยู่แล้ว ก็สามารถผลักเข้าไปหมุนเวียนในตลาดหุ้น หรือ ตลาดเงินสกุลเข้ารหัสได้โดยง่าย ถ้าระบบการตรวจสอบพิสูจน์ตัวตนผู้ใช้งานยังไม่ดีพอ หรือโอนต่อไปยังผู้ให้บริการอื่นนอกระบบ หรือผู้ให้บริการต่างประเทศ”

ความเห็นของผู้ให้ข้อมูลสำคัญ #232

“การหลอกลวงแชร์ลูกโซ่โดยใช้เงินสกุลเข้ารหัสเป็นสิ่งจูงใจเพื่อให้เหยื่อเข้าใจว่าการลงทุนให้ผลตอบแทนสูง ในขณะที่อาจใช้เงินตราปกติในการหมุนเวียนโดยไม่ผ่านเงินสกุลเข้ารหัสเลยก็เป็นได้เพื่อสะดวกในการจัดการเงิน หรืออาจมีการลงทุนเงินสกุลเข้ารหัสร่วมด้วยก็เป็นได้”

ความเห็นของผู้ให้ข้อมูลสหคัญ #321

“การหลอกลวงฉ้อโกงประชาชนแบบแชร์ลูกโซ่ ทำเป็นกิจการซื้อขายเงินเหรียญดิจิทัล หรือ โทเคนดิจิทัลบังหน้า เช่น คดีโอดี แคปปิตอล (OD Capital) และเอฟวีไอ (FVI)[20] ที่สร้างความเสียจำนวนมาก นอกจากนี้ยังมีกรณีการหลอกลวงประชาชนให้ทำการซื้อขายบิตคอยน์ผ่านตัวแทนซื้อขายสินทรัพย์ดิจิทัลต่างประเทศ ซึ่งตัวแทนนั้นก็ไม่ใช่คนทำการซื้อขายจริง หรืออาจเป็นการซื้อขายจากตัวแทนที่ไม่ได้รับอนุญาต (ตัวแทนเถื่อน)”

ความเห็นของผู้ให้ข้อมูลสำคัญ #331

“มีการสร้างเรื่องว่าไปลงทุนในบิตคอยน์ แล้วได้ผลตอบแทนคืนมาจำนวนมากเพื่อทำการชักชวนคนมาร่วมลงทุนซึ่งอันที่จริงไม่ได้มีการลงทุนจริงเพียงแต่เป็นการสร้างเรื่องราวเพื่อจูงใจให้คนแห่มาลงทุนเป็นการหลอลวงประชาชนแชร์ลูกโซ่ และทำการฟอกเงินโดยโอนเงินสกุลเข้ารหัสไป

[20] สนามข่าว 7 สี รายงานว่า กลุ่มผู้เสียหายมีด้วยกันประมาณ 50 คน บอกว่าเป็นตัวแทนของกลุ่มผู้เสียหายแชร์ลูกโซ่ โอดี แคปปิตอล (OD CAPITAL) และ เอฟวีไอ (FVI) ที่มีเกือบ 1,000 คน มูลค่าความเสียหายเกือบ 1,000 ล้านบาท ไปยื่นหนังสือถึงอธิบดีกรมสอบสวนคดีพิเศษ หรือ ดีเอสไอ เพื่อขอให้รับเรื่องนี้เป็นคดีพิเศษ บริษัทดังกล่าวสร้างความน่าเชื่อถือ ด้วยการพาผู้เสียหายไปดูกิจการที่ต่างประเทศ ซึ่งผู้เสียหายเห็นว่าบริษัทมีอยู่จริง สามารถจับต้องได้ จึงยอมลงทุนเพิ่ม แต่พอลงทุนไปได้ 5 เดือน ทางบริษัทกลับอ้างว่าต้องปิดปรับปรุงระบบ และเปลี่ยนการจ่ายเงินเป็นสกุลเงินดิจิทัล จึงเชื่อว่าเป็นการหลอกลวงให้ลงทุน ตัดสินใจจะไปแจ้งความ ก็ถูกคนที่ชักชวนขู่เตือนว่าแม่ทีมมีทนายความ จะแจ้งความกลับ ทำให้ไม่ได้เงินคืน จริง ๆ แล้ว คดีนี้เริ่มขึ้นเมื่อปี 2561 เคยมีผู้เสียหายไปแจ้งความเอาผิดกับบริษัทนี้มาแล้ว 400 ราย และ ปปง. ได้ยึดอายัดทรัพย์สินไปแล้วจำนวน 102 ล้านบาท ซึ่งวานนี้ศาลแพ่งเพิ่งมีคำพิพากษาให้ ปปง. นำทรัพย์ที่ยึดอายัดจากผู้ต้องหาไปเฉลี่ยชดใช้ให้กับผู้เสียหายที่ร้องทุกข์ไว้กับ ปปง. ส่วนผู้เสียหายที่ไปร้องกับดีเอสไอ เป็นผู้เสียหายอีกกลุ่มหนึ่งที่คดีความยังไม่คืบหน้า และได้รับความเดือดร้อนจากการลงทุน (สำนักข่าว 7 สี, 4 ธันวาคม 2019) https://news.ch7.com/detail/379267

ยังประเทศเพื่อนบ้าน แล้วแปลงค่าออกมาเป็นเงินท้องถิ่นจากนั้นก็นำไปเปลี่ยนเป็นทรัพย์สินอื่นต่อไป อย่างไรก็ตามยังมีข้อจำกัดที่อาจไม่สามารถหาแหล่งที่จะรับแปลงค่าเป็นเงินตราปกติได้มากเพียงพอ”

ความเห็นของผู้ให้ข้อมูลสำคัญ #341

“การหลอกลวงแบบแชร์ลูกโซ่ โดยใช้การอ้างผลตอบแทนสูงมาบังหน้าเพื่อชักชวนประชาชนให้มาร่วมลงทุน สิ่งจูงใจที่มาอ้างบังหน้าเป็นไปได้หลายกรณี เงินสกุลเข้ารหัสก็เป็นตัวเลือกหนึ่ง เมื่อระดมเงินได้มากจำนวนหนึ่งก็จะใช้วิธีการฟอกเงินด้วยการโอนเงินจากบัญชีธนาคารไปซื้อบิตคอยน์กับศูนย์ซื้อขายเงินสกุลเข้ารหัสที่ถูกต้องตามกฎหมาย แล้วทำการโอนบิตคอยน์ต่อออกไปนอกประเทศทำให้ไม่สามารถติดตามต่อไปได้”

ดังนั้น ด้วยพฤติกรรมของบุคคลที่จะตกเป็นเหยื่อจากการหลอกลวงแชร์ลูกโซ่ในลักษณะการลงทุนเงินสกุลเข้ารหัส จึงน่าจะมีสาเหตุมาจากการขาดความรู้เกี่ยวกับบริบทของเงินสกุลเข้ารหัส หรือมีความเข้าใจที่คลาดเคลื่อน รับรู้ข่าวสารเฉพาะด้านเดียว เนื่องจากแนวโน้มของเงินสกุลเข้ารหัสทุกสกุลปรับตัวสูงขึ้นอย่างต่อเนื่อง โดยเฉพาะเมื่อมีข่าวสารจากองค์กรธุรกิจรายใหญ่ยอมรับการซื้อขายสินค้าด้วยบิตคอยน์ ยิ่งเป็นการเสริมภาพความเชื่อมั่นได้อย่างดี แต่องค์ประกอบที่สำคัญอีกประการ คือความโลภของเหยื่อทำให้ถูกชักจูงจากผลตอบแทนระยะสั้นได้โดยง่าย และเมื่อจำนวนเงินรวบรวมได้จากการหลอกลวงมีจำนวนมาก อาชญากรจึงจำเป็นต้องทำการฟอกเงินโดยเลือกใช้เงินสกุลเข้ารหัสที่สามารถโยกย้ายถ่ายเทกระจายไปหลายบัญชีย่อยได้รวดเร็ว และยังสามารถทำรายการข้ามประเทศไปเก็บไว้ยังผู้ให้บริการนอกระบบได้ในระหว่างกิจการยังดำเนินการอยู่

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

4.2.2 การค้ายาเสพติด รวมถึงการค้าบนระบบออนไลน์

การค้ายาเสพติด เป็นอาชญากรรมที่มีสถิติคดีที่ถูกการดำเนินการจับกุมยึดอายัดทรัพย์สินจากการกระทำผิดมูลฐาน ตามกฎหมายป้องกันและปราบปรามการฟอกเงินสูงสุดอย่างต่อเนื่องทุกปี กล่าวคือ สำนักงานป้องกันและปราบปรามการฟอกเงิน (2019) ได้รายงานผลการปฏิบัติงานประจำปี 2562 สถิติเรื่องร้องเรียน ร้องทุกข์ และแจ้งแบะแสเกี่ยวกับการกระทำความผิดมูลฐานเกี่ยวกับการฟอกเงินและการก่อการร้าย ปรากฏว่า ความมูลผิดฐานมาตรา 3(1) ยาเสพติด มีสถิติสูงสุดจำนวน 1,149 เรื่องในปี 2561 และจำนวน 917 เรื่องในปี 2560 ในขณะที่อันดับสองความผิดมูลฐานมาตรา 3(3) การฉ้อโกงประชาชน มีจำนวน 485 เรื่อง และจำนวน 434 เรื่องในปี 2560 ซึ่งสอดคล้องกับความเห็นส่วนใหญ่ของผู้ให้ข้อมูลสำคัญที่ระบุว่า รูปแบบอาชญากรรมการค้ายาเสพติดมีโอกาสสูงในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เนื่องจากการกระทำผิดในการค้ายาเสพติดมักกระทำกันเป็นกระบวนการ หรือองค์กรข้ามชาติที่ร่วมกระทำความผิดเป็น

เครือข่ายและแบ่งหน้าที่กระทำการตั้งแต่ต้นสายการผลิต การกระจายสินค้าให้แก่สายจัดส่ง จนถึงปลายทางการจำหน่ายตรงแก่ผู้เสพ ซึ่งผลประโยชน์จากการค้ายาเสพติดในแต่ละปีมีมูลค่ามหาศาล อาชญากรเองก็มีพัฒนาการรูปแบบการฟอกเงินที่หลากหลาย และเปลี่ยนรูปแบบดำเนินการอย่างต่อเนื่อง โดยเงินสกุลเข้ารหัสก็เป็นเป้าหมายหนึ่งในการใช้เป็นเครื่องมือในการฟอกเงิน เนื่องจากความสะดวกในโอนย้ายถ่ายผลประโยชน์ในจำนวนมูลค่ามากระห่างกัน ทั้งภายในประเทศและข้ามประเทศได้ด้วยความรวดเร็ว อีกทั้งสามารถใช้เงินสกุลเข้ารหัสเป็นสื่อกลางในการชำระราคาค่าซื้อสินค้ากับผู้ค้ายาเสพติดบนระบบออนไลน์ใน Dark Web ได้ความคล่องตัว ดังความเห็นของผู้ให้ข้อมูลสำคัญบางส่วน ดังนี้

ความเห็นของผู้ให้ข้อมูลสำคัญ #111

“การฟอกเงินของกระบวนการค้ายาเสพติดก็ถือเป็นลักษณะปกติที่เกิดขึ้นทั่วไป แต่ก็ทีอาจทำการฟอกเงินผ่าน Dark Web ร่วมด้วย และปัจจุบันก็มีแนวโน้มผู้กระทำผิดชาวไทยเองที่มีความรู้ด้านนี้ ก็อาจเลือกใช้การฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เพื่อการอำพรางแหล่งเก็บซ่อนทรัพย์ เนื่องจากเชื่อว่าปัจจุบันเจ้าหน้าที่สืบสวนส่วนใหญ่ยังขาดองค์ความรู้เรื่องเงินสกุลเข้ารหัส ไม่รู้วิธีการที่จะติดตามตรวจสอบอย่างเท่าทันสถานการณ์ โดยเฉพาะอย่างยิ่งเจ้าหน้าที่ประจำท้องถิ่นต่างจังหวัดอาจไม่รู้จักด้วยซ้ำว่าเงินสกุลเข้ารหัสคืออะไร”

ความเห็นของผู้ให้ข้อมูลสำคัญ #113

“ในกรณียาเสพติดเท่าที่ปฏิบัติงานมาก็มีเกี่ยวข้องกับเงินสกุลเข้ารหัสบ้าง แต่มักเป็นการเปลี่ยนรูปแบบของทรัพย์ในลักษณะเดิมๆ มาเป็นเงินสกุลเข้ารหัส เช่น บิตคอยน์เพราะมองว่าบิตคอยน์เป็นทรัพย์ประเภทหนึ่ง เมื่อทำการซื้อบิตคอยน์จากศูนย์ซื้อขายรับอนุญาตเสร็จเรียบร้อย ก็มักจะโอนบิตคอยน์ออกไปยังกระเป๋าเงินอื่นนอกระบบหรือที่อยู่ต่างประเทศ ซึ่งก็เป็นการตัดตอนพยานหลักฐานในการสืบค้น แม้ว่าในระบบปฏิบัติการบล็อกเชนจะปรากฏหลักฐานเป็นเส้นทางธุรกรรมให้เห็นแต่ก็อยู่นอกเขตอำนาจในการติดตามแล้ว”

ความเห็นของผู้ให้ข้อมูลสำคัญ #332

“เนื่องจากปัจจุบันเงินสกุลเข้ารหัสมีทิศทางปรับตัวในเชิงมูลค่าสูงขึ้นต่อเนื่อง จึงเป็นสินทรัพย์ที่องค์กรอาชญากรรมข้ามชาติให้ความสนใจ โดยเฉพาะบิตคอยน์ที่ปัจจุบัน 1 เหรียญ (BTC) มีมูลค่าล้านกว่าบาทแล้ว และมีขนาดการตลาดเกือบ 60% ของมูลค่าตลาดรวมทั้งโลก จึงมีสภาพคล่องทางการเงินสูง และสามารถทำการโอนมูลค่าจำนวนมากได้อย่างสะดวก รวมถึงมีความซับซ้อนยากต่อการติดตามสืบค้น โดยเฉพาะอาชญากรรมที่มีผลประโยชน์สูง เช่น การค้ายาเสพติด”

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ความเห็นของผู้ให้ข้อมูลสำคัญ #412

“ผู้ค้ายาเสพติดข้ามประเทศหลายรายเริ่มให้ความสนใจ ในระบบนิเวศเงินสกุลเข้ารหัส โดยการซื้อขายข้ามประเทศในลักษณะเดิมต้องชำระเงินสด เมื่อทำการส่งมอบของลักษณะยื่นหมูยื่นแมว จึงมีภาระในกระบวนการดูแลการส่งมอบกันด้วยเงินสด โดยต้องว่าจ้างสำนักกฎหมายเป็นตัวแทนในการจัดการ Escrow Account เพื่อแจ้งการปล่อยเงินให้แก่ผู้ขาย เมื่อผู้ซื้อได้รับของเรียบร้อยแล้ว ซึ่งมีค่าใช้จ่ายค่อนข้างสูง แต่ในกลไกของเงินสกุลเข้ารหัสโดยระบบปฏิบัติการบล็อกเชนมี Smart Contract ที่สามารถเข้ามาดูแลจัดการเงินแทนระบบ Escrow Account โดยระบบนิเวศจะปล่อยเงินสกุลเข้ารหัสเข้ากระเป๋าเงินปลายทางโดยอัตโนมัติ เมื่อผู้ขายปฏิบัติตามเงื่อนไขที่กำหนดไว้ใน Smart Contract โดยที่ไม่ต้องมีเจ้าหน้าที่ใดกำกับดูแล จึงเป็นการประหยัดค่าใช้จ่ายอย่างมาก ตัวอย่างข่าวในประเทศเวเนลูเอล่า และเคนยา ผู้ค้ายาเสพติดส่งของผ่านทางไปรษณีย์ระหว่างประเทศ ไปยังผู้รับปลายทางอีกประเทศหนึ่ง[21] ผู้ซื้อก็ทำการส่งคำสั่งชำระเงินผ่านระบบเงินสกุลเข้ารหัสโดยกำหนดเงื่อนไขใน Smart Contract ว่าเมื่อระบบติดตามไปรษณีย์ Tracking System แสดงผลการส่งสินค้าถึงปลายทาง โดยเมื่อรหัส URL ของการเปิดเว็บไซต์ในขณะที่ทำการตรวจสอบผลการจัดส่งได้แสดงสถานะแสดงแจ้งสินค้าถึงปลายทาง ระบบเงินสกุลเข้ารหัสก็จะใช้รหัส URL นั้นเป็นรหัสเปิดกระเป๋าเงิน และเงินสกุลเข้ารหัสก็จะถูกโอนไปเข้ากระเป๋าเงินของผู้ขายทันทีโดยไม่ต้องมีการจ้างผู้ใดมาดำเนินการ เพราะผู้ซื้อและผู้ขายมีความเชื่อมั่นต่อเทคโนโลยีระบบปฏิบัติการบล็อกเชนที่ไม่มีความคลาดเคลื่อน และไม่สามารถเปลี่ยนแปลงข้อมูลเมื่อส่งคำสั่งออกไปเรียบร้อยแล้ว”

อาชญากรรมการค้ายาเสพติดนั้น มักมีการกระทำความผิดลักษณะอาชญากรรมองค์กรหรืออาชญากรรมองค์กรข้ามชาติที่มีแหล่งเงินทุนสนับสนุนการดำเนินงาน และมีเครือข่ายบุคคลากรในหลายระดับ รวมถึงบุคคลากรที่มีความเชี่ยวชาญด้านการเงินและเทคโนโลยีในการดูแลจัดการผลประโยชน์ ทั้งนี้เงินสกุลเข้ารหัสจึงไม่ถือเป็นสิ่งใหม่ของกระบวนการค้ายาเสพติดข้ามชาติ ที่ได้พัฒนารูปแบบการฟอกเงินมาใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงินตั้งแต่ปี 2012 โดยความเคลื่อนไหวของราคาบิตคอยน์ปรับตัวไต่ระดับราคาขึ้นไปถึง 1 บิตคอยน์มีมูลค่าสูงเกือบ 20,000 เหรียญสหรัฐในปี 2017 ก่อนที่มูลค่าของบิตคอยน์จะลดลงอย่างต่อเนื่องหลังจากกลุ่มอาชญากรรมค้าสิ่งผิดกฎหมายรวมถึงการค้ายาเสพติดทางออนไลน์ (Dark Net) รายใหญ่ถูกกวาดล้างจับกุม

[21] UNODC (2021) ได้รายงานกระบวนการขนส่งยาเสพติดของผู้ค้ายาเสพติดในเขตตะวันออกของทวีปแอฟาริกาด้วยวิธีการขนส่งทางบก ทางเรือ และทางอากาศ รวมถึงมีแนวโน้มการส่งของด้วยไปรษณีย์มากขึ้น เช่น ในประเทศเคนยา (Drug Trafficking Patterns to and from Eastern Africa) https://www.unodc.org/easternafrica/en/illicit-drugs/drug-trafficking-patterns.html

จนกระทั่งราคาบิตคอยน์ลดลงมาเคลื่อนไหวอยู่ในระดับ 5,000 - 7,000 เหรียญสหรัฐต่อ 1 ต่อบิตคอยน์ ตัวอย่างเช่น Silk Road กลุ่มค้าสิ่งผิดกฎหมายทางออนไลน์ที่ถูกจับกุมและสั่งปิดในปี 2013 และอีกรายหนึ่งคือ AlphaBay ถูกจับกุมและสั่งปิดในปี 2017 (Fanusie & Robinson, 2018)

4.2.3 การเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิวเตอร์เข้าทำลายระบบงาน

การส่งไวรัสคอมพิวเตอร์เข้าทำลายระบบปฏิบัติงาน และระบบจัดการฐานข้อมูลของระบบงานเป้าหมาย เป็นอาญชกรรมไซเบอร์รูปแบบหนึ่งในลักษณะการเข้าทำลายระบบงานไซเบอร์ (Cybervandalism) โดยใช้ระบบงานคอมพิวเตอร์เพื่อการตอบโต้และการมุ่งหมายสู่การทำลายล้างระบบปฏิบัติการ หรือระบบฐานข้อมูลของเป้าหมาย เช่น ไวรัสคอมพิวเตอร์ (Viruses) ที่มุ่งหมายขัดขวางหรือทำลายระบบปฏิบัติการคอมพิวเตอร์ หรือการส่งข้อมูลเข้าสู่ระบบเพื่อผลิตซ้ำข้อมูลนั้นให้ขยายตัวในระบบการทำงาน (Worms) การส่งชุดรหัสข้อมูลเข้าสู่ระบบเพื่อรอการกระจายตัวเมื่อมีผู้เปิดใช้งานเพื่อทำลายระบบงาน (Trojan House) การส่งชุดรหัสข้อมูลเข้าสู่ระบบเพื่อรอเวลาที่ตั้งค่าล่วงหน้าหรือรอเวลารหัสลับให้ปฏิบัติงานเพื่อทำลายระบบงาน (Logic Bomb) ทั้งนี้การกระทำการข้างต้น มีวัตถุประสงค์เพื่อเรียกร้องผลประโยชน์จากเหยื่อเป็นการตอบแทนในการบรรเทาความเสียหายของระบบงานเป้าหมายในลักษณะการเรียกค่าไถ่ (Ransom) หรือที่เรียกว่า Ransomware (Siegel, 2013) เมื่ออาชญากรกระทำการบนระบบไซเบอร์ จึงมักเรียกร้องผลประโยชน์เป็นเงินสกุลเข้ารหัสซึ่งสามารถปิดบังตัวตนได้จากระบบนิเวศเงินสกุลเข้ารหัส ที่สร้างความยากในการสืบหาตัวผู้กระทำความผิด และการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสสามารถดำเนินการได้ทันที

ในช่วงที่ผ่านมา ปรากฏกรณีการเรียกค่าไถ่จากการส่งไวรัสคอมพิวเตอร์เข้าสู่ระบบปฏิบัติการคอมพิวเตอร์ของโรงพยาบาลสระบุรี โดย The Reporter Asia Online (2020) ได้นำเสนอข่าว การโจมตีดังกล่าว เริ่มเกิดขึ้นเมื่อวันที่ 5 กันยายน 2020 ซึ่งหลังจากที่มีการตรวจพบเมื่อวันที่ 7 กันยายน 2020 ผู้อำนวยการศูนย์เทคโนโลยีสารสนเทศและการสื่อสาร สำนักงานปลัดกระทรวงสาธารณสุข ระบุว่า ได้ประสานงานไปยังศูนย์ประสานการรักษาความมั่นคงปลอดภัยระบบคอมพิวเตอร์ประเทศไทย (ไทยเซิร์ต : ThaiCERT) ทันที ซึ่งโรงพยาบาลสระบุรี ประเทศไทย โดนแรนซัมแวร์ที่ยังไม่ระบุกลุ่มเข้าโจมตีล็อกไฟล์เพื่อเรียกค่าไถ่เป็นเงิน 20,000 บิตคอยน์ (ราว 6.3 หมื่นล้านบาทในขณะนั้น) โดยข้อมูลส่วนใหญ่เป็นข้อมูลผู้ป่วย ทำให้ระบบงานทั้งโรงพยาบาลไม่สามารถเข้าใช้งานได้ ขณะที่การสำรองข้อมูลของโรงพยาบาลครั้งล่าสุด คือเมื่อ 5 ปีที่แล้ว ทำให้ข้อมูลผู้ป่วยช่วง 5 ปีล่าสุดไม่สามารถเข้าใช้งานได้ นอกจากนี้ ผู้ให้ข้อมูลสำคัญได้ให้ความเห็นเชิงทัศนะเพิ่มเติมดังนี้

ความเห็นของผู้ให้ข้อมูลสำคัญ #211

“วิวัฒนาการของการเรียกค่าไถ่จากเดิมที่เรียกร้องเป็นเงินสด หรือให้โอนเงินไปเข้าบัญชีเงินฝากที่เปิดอยู่ในประเทศปลอดภาษี เปลี่ยนมาเป็นกาเรียกค่าไถ่เป็นบิตคอยน์ที่โอนเข้ากระเป๋าเงินของคนร้ายโดยไม่สามารถทราบตัวตนของผู้กระทำผิด โดยมากมักเป็นอาชญากรรมทางไซเบอร์ เช่น การขโมยข้อมูลสำคัญ (Hack) การปล่อยไวรัสเข้าทำลายระบบปฏิบัติการ (Ransomware) หรือการเรียกค่าไถ่จากการข่มขู่ที่จะประจานคลิปวิดีโอ (Abuse) และกรณีตัวอย่างที่เพิ่งเกิดขึ้นกับโรงพยาบาลสระบุรี”

ความเห็นของผู้ให้ข้อมูลสำคัญ #232

“การเรียกค่าไถ่ Ransomware โดยอาชญากรส่งไวรัสหรือมัลแวร์เข้าสู่ระบบงานของเหยื่อ ซึ่งเหยื่อก็รู้แต่เพียงว่าระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ และถ้าจะกลับสู่ระบบงานปกติก็จะต้องจ่ายค่าไถ่ เพื่อแลกกับรหัสปลดล็อคระบบโดยให้โอนเงินสกุลเข้ารหัสไปยังรหัสที่ตั้ง หรือกระเป๋าเงินที่แจ้งไว้ ระบบก็จะส่งรหัสปลดล็อคให้โดยอัตโนมัติ ซึ่งเหยื่อจะไม่ทราบว่าถูกกระทำมาจากใครหรือสถานที่ใด ซึ่งระบบการเรียกค่าไถ่โดยเงินสกุลเข้ารหัส จึงสามารถให้ประโยชน์ทางตรงต่ออาชญากรในส่วนของการรักษาความลับส่วนบุคคลได้ดี”

ความเห็นของผู้ให้ข้อมูลสำคัญ #411

“อาชญากรรมที่สร้างความเสียหายอย่างมาก น่าจะเป็นอาชญากรรมไซเบอร์ การเรียกค่าไถ่ การโจมตีทางไซเบอร์ ดังมีข่าวมาต่อเนื่องว่า เกาหลีเหนือส่งทีมงานเข้าไป Hack ระบบการทำงานของรัฐบาลอื่น ระบบคอมพิวเตอร์ของสถาบันการเงิน[22] เพื่อให้ไม่สามารถใช้งานระบบได้เป็นการข่มขู่ เพื่อแลกเปลี่ยนกับค่าไถ่เป็นบิตคอยน์ หรือเงินสกุลเข้ารหัสอื่น ดังนั้น การโจรกรรมข้อมูลการโจมตีระบบงานภาครัฐที่น่าจะก่อความเสียหายจำนวนมากกว่า อาชญากรรมอื่นๆ ไม่ว่าการค้ายาเสพติด การค้ามนุษย์ การพนัน”

[22] The Standard Online(2019) รายงานว่า สหประชาชาติเผย กำลังตรวจสอบกรณีเกาหลีเหนือโจมตีทางไซเบอร์ระดมเงินทุนผิดกฎหมายใน 17 ประเทศ โดยการโจมตีทางไซเบอร์ส่วนใหญ่จะโจมตีผ่านระบบสื่อสารด้านการเงินระหว่างธนาคารผ่านระบบคอมพิวเตอร์ที่มีเครือข่ายเชื่อมโยงทั่วโลก ที่ให้บริการโดย Society for Worldwide Interbank Financial Telecommunication (SWIFT) รวมถึงการโจมตีสถาบันการเงินและอัตราแลกเปลี่ยนสกุลเงินดิจิทัล (Cryptocurrency) ซึ่ง Bithumb หนึ่งในผู้สนับสนุนการใช้สกุลเงินดิจิทัลรายใหญ่ของเกาหลีใต้ตรวจพบการโจมตีทางไซเบอร์ถึง 4 ครั้ง ในระยะเวลา 3 ปีที่ผ่านมา รวมมูลค่าความเสียหายราว 65 ล้านเหรียญสหรัฐ (ราว 2 พันล้านบาท) https://thestandard.co/un-probing-35-north-korean-cyberattacks-in-17-countries/

ความเห็นของผู้ให้ข้อมูลสำคัญ #413

“การเรียกค่าไถ่ Ransomware ที่มีการเข้าไปรบกวนระบบคอมพิวเตอร์ และให้จ่ายค่าไถ่เป็นบิตคอยน์ เรียบร้อยแล้วก็จะให้กุญแจรหัสไปแก้ไขระบบคอมพิวเตอร์ให้กลับสู่ปกติ หรือการข่มขู่จากการเข้าไปขโมยข้อมูลในลักษณะ Data Leaked ซึ่งได้จากการเข้าระบบฐานข้อมูลเพื่อไปขโมยข้อมูลสำคัญ และเรียกค่าไถ่หากไม่จ่ายก็จะเปิดเผยข้อมูลเหล่านั้นต่อสาธารณะ ซึ่งเป็นรูปแบบหนึ่งของอาชญากรรมไซเบอร์ด้วยการให้จ่ายเป็นเงินสกุลเข้ารหัส”

รูปแบบอาชญากรรมการเรียกค่าไถ่โดยเงินสกุลเข้ารหัสโดยเฉพาะการเรียกค่าไถ่จากอาชญากรรมไซเบอร์ ไม่ว่าจะเป็นการขโมยข้อมูลสำคัญ (Hack) การทำลายระบบปฏิบัติการของเป้าหมายด้วยมัลแวร์ หรือไวรัสคอมพิวเตอร์ (Ransomware) หรือแม้แต่การส่งชุดรหัสคำสั่งเข้าสู่ระบบงานของเป้าหมายเพื่อรอเวลาที่ตั้งค่าล่วงหน้าที่จะเริ่มทำลายระบบปฏิบัติการเป้าหมาย (Logic Bomb) ผู้วิจัยมีความเห็นว่ารูปแบบอาชญากรรมดังกล่าวมีความเป็นไปได้สูงที่จะเรียกผลประโยชน์ค่าไถ่เป็นเงินสกุลเข้ารหัส เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสช่วยสนับสนุนการโอนเงินเข้ากระเป๋าเงินที่ไม่ต้องระบุตัวตน เพราะอาชญากรสั่งการเข้าระบบจากแหล่งที่ไม่ระบุตัวตนเช่นกัน จึงเป็นการเสริมความเข็มแข็งแก่รูปแบบของการก่อกาชญากรรมที่สร้างความยากแก่การสืบค้นติดตามของเจ้าหน้าที่

4.2.4 การพนันรวมถึงการพนันบนระบบออนไลน์

โดยปกติแหล่งการพนัน ทั้งในรูปแบบมาตรฐานในลักษณะคาสิโนที่ได้รับการรับรองจากรัฐ หรือบ่อนการพนันที่เป็นแหล่งที่ไม่ชอบด้วยกฎหมาย ก็เป็นแหล่งที่เอื้ออำนวยต่อกระบวนการฟอกเงินของอาชญากร และที่ยากต่อการพิสูจน์เส้นทางการเงินที่ได้รับโชคจากการพนันเป็นเงินที่ชอบด้วยกฎหมายหรือไม่ ปัจจุบันพัฒนาการทางเทคโนโลยีเข้ามาเปลี่ยนรูปแบบของบ่อนการพนันปรับรูปแบบเข้าสู่ระบบคอมพิวเตอร์ด้วยระบบออนไลน์ ทำให้สามารถขยายฐานผู้เข้าร่วมกิจกรรมได้ง่ายและกว้างขึ้น รวมถึงไม่มีข้อจำกัดด้านเวลาและสถานที่ และโดยระบบปฏิบัติการอยู่บนระบบอินเตอร์เน็ตเช่นเดียวกับระบบนิเวศเงินสกุลเข้ารหัส การใช้เงินสกุลเข้ารหัสเป็นอีกหนึ่งทางเลือกให้ผู้ร่วมกิจกรรมใช้เงินสกุลเข้ารหัสเป็นสื่อกลางในการชำระได้ ซึ่งถือเป็นสกุลเงินกลางที่ไม่ต้องไปแปลงค่าจากเงินตราสกุลท้องถิ่นของแต่ละประเทศอีกทอดหนึ่ง และเป็นการเอื้อประโยชน์แก่เจ้าของกิจการบ่อนการพนันออนไลน์ ในการรวบรวมผลประโยชน์เป็นเงินสกุลเข้ารหัสสะดวกต่อการโยกย้ายถ่ายเท โดยผู้ให้ข้อมูลสำคัญได้ให้ความเห็นเพิ่มเติม ดังนี้

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ความเห็นของผู้ให้ข้อมูลสำคัญ #241

“อันที่จริงคนที่ชอบการพนัน มักเป็นคนที่มีมีจริตชอบเสี่ยงทางพฤติกรรมอยู่แล้ว ดังนั้น การยอมรับการถือครองเงินสกุลเข้ารหัสเป็นผลประโยชน์จากกิจกรรมบ่อนการพนัน ก็เป็นการเสี่ยงโชคของตัวอาชญากรเองเช่นกัน เนื่องจากการเคลื่อนไหวของเงินสกุลเข้ารหัสมีราคาผันผวนบนความเสี่ยงที่กำหนดไม่ได้ จึงเหมาะกับพฤติกรรมของอาชญากรประเภทนี้”

4.2.5 สรุปรูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและใช้เป็นเครื่องมือในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

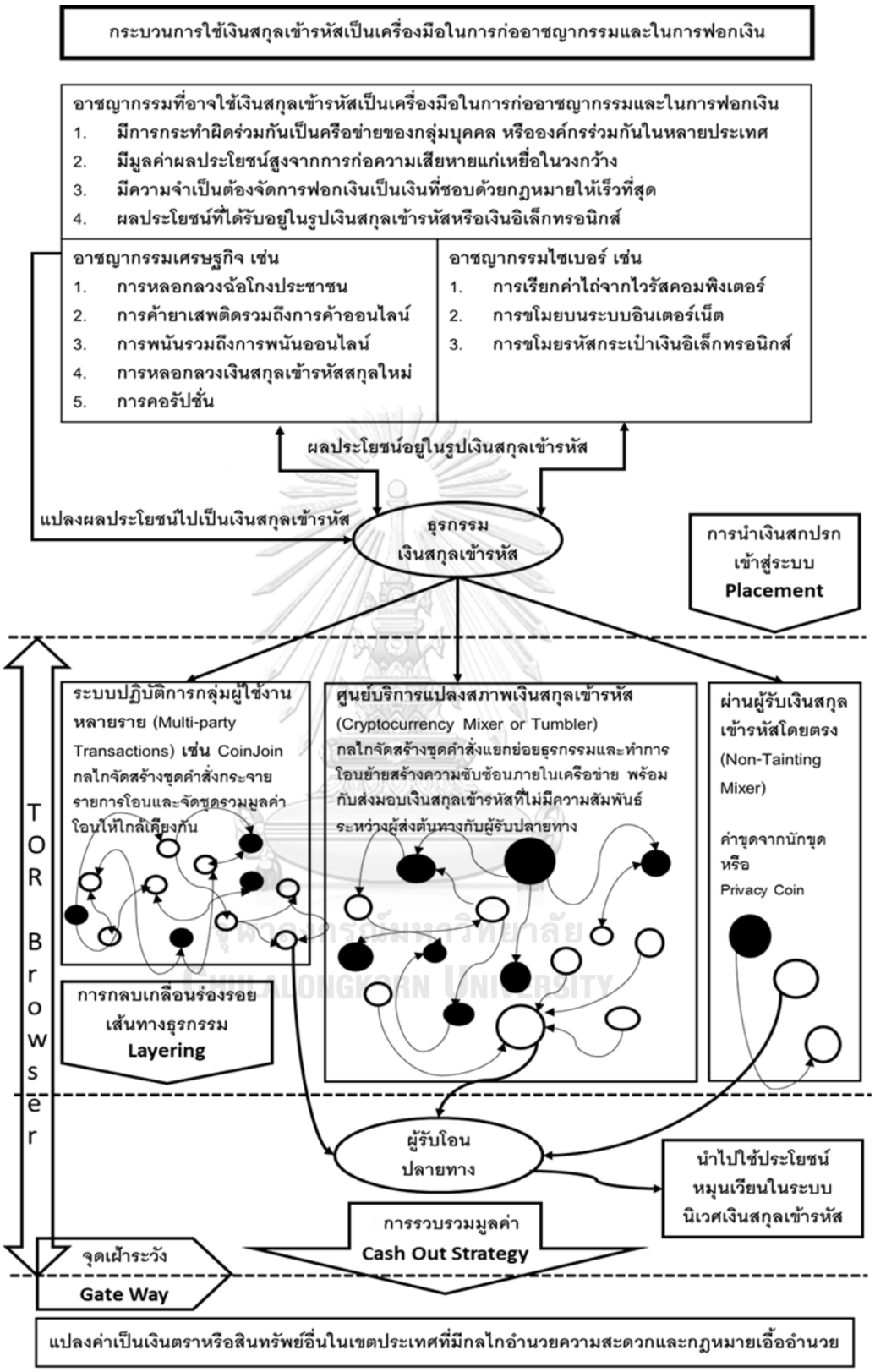
จากรูปแบบอาชญากรรมที่ผู้ให้ข้อมูลสำคัญ ให้ความเห็นเชิงทัศนะในการจัดอันดับความสำคัญ 4 รูปแบบที่กล่าวถึงข้างต้นนั้น ปรากฏว่า สำนักงานป้องกันและปราบปรามการฟอกเงิน (2019) ได้รายงานผลการปฏิบัติงานประจำปี 2562 สถิติเรื่องร้องเรียน ร้องทุกข์ และแจ้งแบะแสเกี่ยวกับการกระทำความผิดมูลฐานเกี่ยวกับการฟอกเงินและการก่อการร้าย ปรากฏว่า ความมูลผิดฐานมาตรา 3(1) ยาเสพติด มีสถิติสูงสุดอันดับหนึ่งจำนวน 1,149 เรื่องในปี 2561 และจำนวน 917 เรื่องในปี 2560 ในขณะที่อันดับสองความผิดมูลฐานมาตรา 3(3) การฉ้อโกงประชาชน มีจำนวน 485 เรื่อง และจำนวน 434 เรื่องในปี 2560 อันดับที่สามคือความผิดมูลฐานมาตรา 3(5) คามผิดต่อตำแหน่งหน้าที่ราชการ อันดับที่สี่คือความมูลฐานมาตรา 3(2) การค้ามนุษย์ ผู้หญิงและเด็ก อันดับที่ห้าคือความผิดมูลฐานมาตรา 3(13) การละเมิดทรัพย์สินทางปัญญา และอันดับที่หกคือความผิดมูลฐานมาตรา 3(9) การจัดให้มีการเล่นการพนันรวมถึงการพนันทางสื่ออิเล็กทรอนิกส์ มีจำนวน 40 เรื่องในปี 2561 และจำนวน 163 เรื่องในปี 2560 แต่ไม่ปรากฏว่ามีการบัญญัติอาชญากรรมทางไซเบอร์เป็นความผิดมูลฐานในกฎหมายป้องกันและปราบปรามการฟอกเงินโดยตรง ทั้งนี้ในการบังคับใช้กฎหมายอาจต้องบังคับใช้มูลฐานความผิดในลักษณะอื่น หรือวิเคราะห์จากพฤติกรรมการกระทำผิดเทียบเคียงเข้าข่ายมูลฐานความผิดอื่นแทน เช่น ความผิดมูลฐานมาตรา 3(24) การมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ซึ่งโดยพฤติการณ์ของอาชญากรมักจะไม่ดำเนินการภายในเขตประเทศไทย แต่มักจะส่งคำสั่งจากแหล่งต่างประเทศเข้าจู่โจมระบบปฏิบัติงานเป้าหมายในประเทศ หรือความผิดมูลฐานมาตรา 3(18) การกรรโชก รีดเอาทรัพย์ที่มีลักษณะเป็นปกติธุระ ซึ่งก็เป็นภาระในการพิสูจน์ของเจ้าหน้าที่ต่อการกระทำการเรียกค่าไถ่ของผู้กระทำผิดเป็นพฤติการณ์ประจำเยี่ยงปกติธุระหรือไม่ หรือความผิดมูลฐานมาตรา 3(6) การกรรโชก รีดเอาทรัพย์ที่มีลักษณะช่องโจร อย่างไรก็ตามผู้วิจัยมีความเห็นว่าขนาดของความเสียหายที่อาจเกิดขึ้นจากอาชญากรรมไซเบอร์ในอนาคตจะมีความรุนแรงและมูลค่าความเสียหายสูงขึ้น รวมถึงมักเป็นการกระทำที่มาจากต่างประเทศ หากไม่มีการบัญญัติ

ความผิดมูลฐานที่ชัดเจน ก็อาจเป็นอุปสรรคต่อการขอความร่วมมือในการติดตามผู้กระทำผิดในต่างประเทศภายใต้ความร่วมมือของหน่วยต่อต้านการฟอกเงินระดับสากล

ดังนั้นจึงอาจกล่าวโดยสรุปได้ว่า รูปแบบของอาชญากรรมที่อาจใช้เงินสกุลเข้ารหัสเป็นเครื่องในการก่ออาชญากรรม และดำเนินกระบวนการฟอกผลประโยชน์ที่ได้รับจากการกระทำผิดโดยธุรกรรมเงินสกุลเข้ารหัสให้เป็นเงินตราหรือทรัพย์สินอื่นที่ชอบด้วยกฎหมายนั้น ส่วนใหญ่มีแนวโน้มของอาชญากรรมในลักษณะที่มักกระทำความผิดร่วมกันเป็นกลุ่มบุคคล หรือองค์กรทั้งภายในประเทศและต่างประเทศ โดยอาศัยเครือข่ายในหลายประเทศเพื่อการโอนย้ายถ่ายเทผลประโยชน์ข้ามประเทศ ภายในเครือข่ายได้อย่างรวดเร็ว และอาชญากรรมดังกล่าวมักก่อให้เกิดความเสียหายทางเศรษฐกิจแก่เหยื่อจำนวนมากรายในวงกว้าง มีขนาดของผลประโยชน์ที่ได้รับจากการกระทำผิดจำนวนมูลค่าสูงในระยะเวลาสั้น โดยมีข้อจำกัดด้านเวลาจำเป็นต้องจัดการกระจายผลประโยชน์และทำการฟอกเงินเป็นเงินที่ชอบด้วยกฎหมายในระยะสั้นให้เร็วที่สุด ทั้งในกรณีที่ได้รับผลประโยชน์เป็นเงินสกุลเข้ารหัสโดยตรง และเป็นการแปลงผลประโยชน์เป็นเงินสกุลเข้ารหัสเพื่อดำเนินการฟอกเงินต่อไป ทั้งนี้โดยส่วนใหญ่มักจะเป็นอาชญากรรมทางเศรษฐกิจ และอาชญากรรมไซเบอร์ดังกรณีศึกษาที่ได้อธิบายไว้ข้างต้น เช่น การหลอกลวงประชาชนแบบแชร์ลูกโซ่ การค้ายาเสพติดรวมถึงการค้ายาเสพติดบนระบบออนไลน์ การเรียกค่าไถ่จากไวรัสคอมพิวเตอร์ และการพนันรวมถึงการพนันออนไลน์ เป็นต้น

ทั้งนี้ เมื่ออาชญากรได้รับประโยชน์จากการกระทำความผิดไม่ว่าเป็นรูปแบบของเงินตราหรือทรัพย์สินอื่นที่สามารถนำมาดำเนินการแปลงค่าเป็นเงินสกุลเข้ารหัส หรือได้รับเป็นเงินสกุลเข้ารหัสโดยตรงนั้น อาชญากรจะทำการส่งเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมายเข้าสู่ระบบนิเวศเพื่อทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส (Placement) จากนั้นจะเป็นขั้นตอนการกลบเกลื่อนร่องรอยเส้นทางธุรกรรมในระบบนิเวศ (Layering) เนื่องจากระบบจัดการฐานข้อมูลสาธารณะแบบกระจายศูนย์ในระบบปฏิบัติการบล็อกเชนเปิดกว้างต่อผู้ใช้งานทั่วไปสามารถนำโปรแกรมประยุกต์เข้าเชื่อมต่อระบบ เพื่อการสืบค้นข้อมูลเส้นทางการทำธุรกรรมระหว่างผู้ใช้งานทั้งหลายได้ ซึ่งขึ้นอยู่กับศักยภาพของโปรแกรมและประสิทธิภาพของเครื่องมืออุปกรณ์ในการตรวจสอบ ส่งผลให้การโอนย้ายถ่ายเทผลประโยชน์ของผู้กระทำผิดในระบบนิเวศเงินสกุลเข้ารหัสมีโอกาสที่ถูกติดตามสืบค้นเส้นทางธุรกรรมได้ ดังนั้นอาชญากรอาจเลือกแนวทางการกลบเกลื่อนร่องรอยเส้นทางธุรกรรมในระบบนิเวศ เพื่อให้กระบวนการโอนเงินสกุลเข้ารหัสที่ได้รับจากการกระทำความผิดสร้างความยากต่อการติดตามสืบค้น และได้รับมอบเงินสกุลเข้ารหัสที่ผู้รับปลายทางโดยไม่มีความสัมพันธ์เชื่อมโยงถึงผู้ส่งต้นทาง ดังวิธีการที่แสดงในแผนภาพกระบวนการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการก่ออาชญากรรมและในการฟอกเงิน

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY



แหล่งที่มา : จัดทำโดยผู้วิจัย

กล่าวคือ วิธีการใช้บริการปนเงินสกุลเข้ารหัสโดยศูนย์บริการแปรสภาพเงินสกุลเข้ารหัส เนื่องจากผู้ให้บริการมีกลไกในการกระจายธุรกรรมจากผู้ส่งต้นทางเป็นธุรกรรมย่อย พร้อมจัดชุดคำสั่งในการโอนย้ายปนเงินสกุลเข้ารหัสกับผู้ใช้งานรายอื่น เพื่อให้ผู้รับปลายทางได้รับเงินสกุลเข้ารหัสจากผู้ใช้งานรายอื่นที่ไม่มีความสัมพันธ์กับผู้ส่งต้นทาง ทั้งนี้การส่งมอบมักเป็นธุรกรรมย่อยของมูลค่าสุทธิหลังหักค่าธรรมเนียมที่เป็นอัตราแปรผัน และทำการทยอยส่งมอบเงินสกุลเข้ารหัสหลายช่วงเวลาจนครบมูลค่าที่จัดส่งเข้าสู่ระบบสุทธิหลังหักค่าธรรมเนียม ทำให้เกิดความซับซ้อนของธุรกรรมสร้างความยากต่อการตรวจสอบกระทบยอดมูลค่า และเส้นทางธุรกรรม หรืออาจใช้วิธีการเข้าร่วมทำธุรกรรมกับกลุ่มเครือข่ายผู้ใช้งานหลายรายในระบบปฏิบัติการ CoinJoin ที่มีกลไกการกระจายธุรกรรมของผู้ใช้งานหลายรายร่วมกัน และจัดชุดคำสั่งเพื่อทำการโอนธุรกรรมย่อยไข้วกันไปมาระหว่างผู้ใช้งานภายในกลุ่มเครือข่าย พร้อมทั้งทำการทยอยส่งมอบเงินสกุลเข้ารหัสไปยังผู้รับปลายทางที่กำหนด ด้วยมูลค่ารวมใกล้เคียงกับเงินสกุลเข้ารหัสที่ส่งเข้าสู่ระบบ ซึ่งผู้รับปลายทางอาจได้รับเงินสกุลเข้ารหัสรวมต่ำกว่าจำนวนที่ส่งเข้าสู่ระบบ และมีความเสี่ยงที่อาจได้รับการโอนธุรกรรมย่อยซึ่งเชื่อมโยงกับผู้ส่งต้นทางได้ แต่โอกาสการเกิดธุรกรรมเช่นนี้ค่อนข้างต่ำมาก หรืออาจเลือกวิธีการรับเงินสกุลเข้ารหัสจากนักขุด ซึ่งเป็นค่าขุดที่ได้รับเงินสกุลเข้ารหัสโดยตรงจากระบบ จึงไม่มีเส้นทางธุรกรรม และเป็นการรับเงินสกุลเข้ารหัสโดยไม่เชื่อมโยงกับบุคคลใด อย่างไรก็ตามจำนวนมูลค่าขุดมีอัตราลดลงอย่างต่อเนื่อง และมีการกระจายไปยังนักขุดจำนวนมากในระบบนิเวศ จึงมีข้อจำกัดด้านปริมาณและความสะดวกในการดำเนินการ หรืออาจใช้การฟอกเงินโดย Privacy Coin ซึ่งเป็นเงินสกุลเข้ารหัสประเภทหนึ่งที่มีกลไกควบคุมการปกปิดข้อมูล เส้นทางธุรกรรมระหว่างผู้โอนและผู้รับ รวมถึงการใช้เทคโนโลยีการปกปิดข้อมูลอีกหลายวิธี เช่น การเผาและสร้างใหม่ (Burn and Mint) เป็นการเผาทิ้งเงินสกุลเข้ารหัส หรือทำลายรหัสข้อมูลที่ต้นทาง แล้วไปทำการสร้างรหัสข้อมูลเป็นเงินสกุลเข้ารหัสเกิดขึ้นใหม่ที่ปลายทาง ในลักษณะคล้ายการให้ผลตอบแทนจากการขุด ส่งผลให้ไม่ปรากฏร่องรอยของธุรกรรมใด เนื่องจากเงินสกุลเข้ารหัสที่ได้รับจะมาจากระบบโดยตรงเช่นกัน

นอกจากนี้ อาชญากรอาจเสริมการดำเนินการกลบเกลื่อนร่องรอยเส้นทางธุรกรรมโดยการทำธุรกรรมบนระบบปฏิบัติการเฉพาะเพื่อการปกปิดตัวตนของผู้ใช้งาน เช่น TOR Browser ซึ่งระบบงานนี้จะมีกลไกการลวงรหัสที่ตั้งของผู้ใช้งาน และมีระบบการเคลื่อนย้ายรหัสที่ตั้งในระหว่างการใช้งานตลอดเวลา รวมถึงการเคลื่อนย้ายรหัสที่ตั้งข้ามประเทศ จึงเป็นอุปสรรคต่อการติดตามสืบค้น และหากอาชญากรใช้ผลประโยชน์ที่ได้จากการกระทำผิดหมุนเวียนภายในระบบนิเวศเงินสกุลเข้ารหัส หรือทำการเก็บรักษาเงินสกุลเข้ารหัสไว้ในกระเป๋าเงินแบบ Cold Wallet ซึ่งไม่ได้เชื่อมต่อกับระบบอินเตอร์เน็ตแล้ว ก็จะเป็นการยากต่อการติดตามสืบค้นอย่างมาก อย่างไรก็ตาม เมื่ออาชญากรมีการเคลื่อนย้ายเงินสกุลเข้ารหัสออกจากระบบนิเวศไปสู่ระบบสถาบันการเงิน หรือระบบจัดการทรัพย์สินอื่น (Cash Out Strategy) หรือที่เรียกว่า เปลี่ยนสภาพจากเงินบนโลกเสมือนมาสู่

เงินตราบนโลกกายภาพ ซึ่งเป็นจุดเฝ้าระวัง (Gateway) โดยหน่วยบังคับใช้กฎหมายต่อต้านการฟอกเงินก็จะสามารถตรวจสอบข้อมูลที่เกี่ยวข้องกับการทำธุรกรรม และเข้าถึงรายการธุรกรรมนั้นได้ ดังนั้นอาชญากรอาจเลือกทำการแปลงค่าเงินสกุลเข้ารหัสเป็นเงินตราหรือทรัพย์สินอื่น ในเขตประเทศที่มีเครื่องมือในการอำนวยความสะดวกต่อการดำเนินธุรกรรม รวมถึงในเขตประเทศที่มีการบังคับใช้กฎหมายไม่เข็มแข็ง หรือไม่มีกฎหมายใดที่ใช้บังคับเกี่ยวกับธุรกรรมเงินสกุลเข้ารหัส

4.3 เทคนิควิธีการติดตามสืบค้นหาผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัสที่ใช้เป็นเครื่องมือในการฟอกเงิน

การศึกษาเทคนิควิธีการติดตามสืบค้นหาตัวผู้ต้องสงสัยในระบบนิเวศเงินสกุลข้ารหัสนั้น ผู้วิจัยได้นำข้อมูลการสัมภาษณ์เชิงลึก เพื่อรวบรวมข้อมูลประการณ์ทั้งทางตรงและทางอ้อม ข้อมูลเชิงทัศนะจากผู้ให้ข้อมูลสำคัญมาสังเคราะห์ร่วมกับงานวิจัยจากการทบทวนวรรณกรรม และแหล่งข้อมูลภาคราชการและภาคเอกชนที่เกี่ยวข้อง พบว่า ผู้ให้ข้อมูลสำคัญมีความเห็นเชิงทัศนะอย่างเป็นฉันทามติในเทคนิควิธีการติดตามสืบค้นหาตัวผู้ต้องสงสัยเป็นไปในแนวทางเดียวกัน โดยเทคนิวิธีแรกได้รับฉันทามติร่วมของผู้ให้ข้อมูลสำคัญ คือ การสืบค้นผู้ต้องสงสัยผ่านทางผู้ให้บริการรับอนุญาต และเทคนิควิธีที่สองได้รับความเห็นด้วยเสียงส่วนใหญ่ คือ การใช้โปรแกรมการตรวจสอบ Digital Forensic Program ช่วยสืบค้นโดยการเชื่อมต่อกับระบบฐานข้อมูลแบบเปิดบนระบบปฏิบัติการบล็อกเชน และเทคนิควิธีที่สามได้รับความเห็นสนับสนุน คือ การวิเคราะห์พฤติกรรมและเชื่อมโยงความมีตัวตนของผู้ต้องสงสัยกับระบบงานอื่น สำหรับความเห็นเพิ่มเติมต่อเทคนิควิธีการสืบค้นหาตัวผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส คือ การสร้างความร่วมมือของหน่วยงานที่เกี่ยวข้องทั้งในประเทศและต่างประเทศ เพื่อสนับสนุนทางด้านเทคโนโลยีการตรวจสอบสืบค้น และด้านการแบ่งปันข้อมูลเพื่อการตรวจสอบบุคคล หรือรหัสที่ตั้งบนระบบนิเวศเงินสกุลเข้ารหัสที่อยู่ในข่ายบัญชีกลุ่มบุคคลที่เฝ้าติดตาม (Watch List) หรือบัญชีกลุ่มบุคคลที่กระทำความผิด (Black List) ทั้งนี้ ผู้วิจัยได้สังเคราะห์ข้อมูลจากผู้ให้ข้อมูลสำคัญต่อเทคนิควิธีการติดตามสืบค้นหาตัวผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส ดังนี้

4.3.1 การสืบค้นผู้ต้องสงสัยผ่านทางผู้ให้บริการรับอนุญาต

กลไกการทำงานของธุรกรรมบนระบบนิเวศเงินสกุลเข้ารหัส เป็นการติดต่อโอนมูลค่าด้วยรหัสข้อมูลกันโดยตรงระหว่างผู้ใช้งาน (Peer-to-Peer หรือ P2P) โดยไม่มีหน่วยงานกลางตัวแทน หรือผู้ดูแลระบบนิเวศเงินสกุลเข้ารหัสเป็นผู้กำกับจัดการควบคุมระบบการทำงาน ซึ่งระบบจะปฏิบัติงานต่อเนื่องไปตามข้อมูลกลไกการทำงานที่ระบุใน White Paper (Nakamoto, 2008) และ

ผู้ใช้งานไม่จำเป็นต้องลงทะเบียนอัตลักษณ์ตัวตนแท้จริงของผู้ใช้งานก่อนเข้าสู่ระบบ (Anonymity) (Girasa, 2018) อีกทั้งผู้ใช้งานทุกคนสามารถเข้าถึงฐานข้อมูลที่ถูกบันทึกในสมุดบัญชีอิเล็กทรอนิกส์ของระบบนิเวศเป็นรูปแบบกระจายศูนย์ (Distributed) ได้อย่างไม่มีข้อจำกัด สามารถติดตามความเคลื่อนไหวของรายการระหว่างผู้ใช้งานต่างๆได้ หรือที่เรียกว่า Distributed Ledger Technology – DLT (Burniske & Tara, 2017) ดังนั้นในทางหลักการเชิงทฤษฎีแล้วการสืบค้นเส้นทางการทำธุรกรรมเงินสกุลเข้ารหัสบนระบบนิเวศสามารถดำเนินการได้ แต่ในทางปฏิบัติแล้วปริมาณธุรกรรมเงินสกุลเข้ารหัสที่เกิดขึ้นในระบบนิเวศมีปริมาณมหาศาลรวมทั้งธุรกรรมภายในประเทศ และธุรกรรมข้ามประเทศ จึงเป็นอุปสรรคสำคัญในการสืบค้นและถ้าปราศจากซึ่งเครื่องมือทางเทคโนโลยีขั้นสูงแล้วระยะเวลาในการติดตามอาจล่าช้าไม่ทันการเคลื่อนย้าย หรือการกระจายเงินสกุลเข้ารหัสของอาชญากรได้ อีกทั้งเมื่อสามารถหลักฐานพิสูจน์ระบุรหัสที่ตั้งเป้าหมายหรือกระเป๋าเงินต้องสงสัยได้ชัดเจนแล้ว ก็ยังไม่สามารถจะดำเนินการยึดอายัดได้ เนื่องจากต้องใช้รหัสเปิดส่วนบุคคลจากเจ้าของในการเปิดกระเป๋าเงิน และยิ่งไปกว่านั้นการสืบหาพิสูจน์ตัวตนของเจ้าของกระเป๋าก็เป็นอีกปัญหาสำคัญ เนื่องจากระบบนิเวศไม่มีเงื่อนไขให้ผู้ใช้งานต้องแสดงตัวตนก่อนใช้งาน

ผู้ให้ข้อมูลสำคัญทุกท่านมีความเห็นเป็นฉันทามติตรงกัน ถึงเทคนิคสืบค้นหาตัวผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัสที่เหมาะสมกับบริบทของประเทศไทยในปัจจุบันนั้น ได้ให้ความสำคัญต่อกระบวนการรู้จักตัวตนของผู้ขอใช้บริการ (KYC – Know Your Customer) และพิสูจน์ความมีตัวตนก่อนอนุญาตให้เริ่มใช้งาน (KYC on Boarding) รวมถึงการปรับปรุงข้อมูลของผู้ใช้บริการให้เป็นปัจจุบันอย่างสม่ำเสมอ (KYC on Going) และวิเคราะห์ความสมเหตุผลต่อพฤติกรรมการทำธุรกรรมของผู้ใช้บริการ (CDD – Customer Due Diligent) โดยผู้ให้บริการรับอนุญาต ทั้งนี้ไม่จำกัดเฉพาะผู้ให้บริการรับอนุญาตที่เกี่ยวข้องกับเงินสกุลเข้ารหัส เช่น ศูนย์ซื้อขาย นายหน้า ผู้ค้า หรือผู้เสนอขายสินทรัพย์ดิจิทัล ตามกฎระเบียบของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (สำนักงาน กลต.) เท่านั้น แต่หมายรวมถึงผู้ให้บริการรับอนุญาตที่มีหน้าที่ในการตรวจพิสูจน์ความมีตัวตนของผู้ใช้งาน ตามกฎหมายป้องกันและปราบปรามการฟอกเงิน เช่น ธนาคาร บริษัทหลักทรัพย์ บริษัทบัตรเครดิต และผู้ให้บริการทางการเงินอื่น เนื่องจากผู้ให้ข้อมูลสำคัญทุกท่านเล็งเห็นถึงปัญหาเดียวกันคือ ระบบนิเวศเงินสกุลเข้ารหัสถูกพัฒนาขึ้นเพื่อการทำธุรกรรมโดยไม่ผ่านตัวกลาง และไม่มีเงื่อนไขให้ระบุตัวตนก่อนใช้งาน แม้ว่าระบบเงินสกุลเข้ารหัสจะดำเนินการบนระบบปฏิบัติการบล็อกเชน ซึ่งมีการบันทึกรายการธุกรรมลักษณะสมุดบัญชีอิเล็กทรอนิกส์รูปแบบกระจายศูนย์ที่สามารถตามเส้นทางธุรกรรมได้ก็ตาม แต่ต้นทุนในการติดตามเส้นทางธุรกรรมในระบบนิเวศเงินสกุลเข้ารหัสที่ต้องอาศัยเทคโนโลยีขั้นสูง และอาจต้องใช้ระยะเวลาในการสืบค้นติดตาม อีกทั้งเมื่อสามารถสืบค้นเป้าหมายผู้ต้องสงสัยได้แล้วก็ยังไม่สามารถระบุตัวตนของเจ้าของได้ ทั้งนี้โดยพฤติกรรมของอาชญากรเมื่อก่ออาชญากรรมแล้ว ย่อมประสงค์ที่ได้รับผลตอบแทนหรือผลประโยชน์ที่

ได้จากการกระทำผิด และในกรณีที่อาชญากรทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ย่อมต้องมีช่วงเวลาหนึ่งที่ต้องการแปลงค่าให้เป็นเงินตราปกติ หรือทรัพย์สินอื่น เพื่อประโยชน์ในการนำไปใช้ประโยชน์และเป็นแหล่งเงินทุนเพื่อการก่ออาชญากรรมต่อไป

วิธีการนี้คือการเฝ้าระวัง ณ จุดที่ผู้ต้องสังสัยในระบบนิเวศเงินสกุลเข้ารหัส *"ข้ามจากระบบการเงินบนโลกเสมือนมาสู่ระบบการเงินบนโลกกายภาพ"* ซึ่งผู้ให้ข้อมูลสำคัญทุกท่านมีความเชื่อมั่นต่อระบบฐานข้อมูล ในการจัดเก็บข้อมูลตัวตนของผู้ใช้บริการในธุรกิจที่เกี่ยวข้องกับเงินสกุลเข้ารหัส ระบบสถาบันการเงิน และผู้ให้บริการทางการเงินอื่น ที่มีหน้าที่ตรวจสอบตัวตนผู้ใช้งาน ซึ่งจะเป็นเครื่องมือสำคัญ ในการช่วยติดตามสืบค้นตัวผู้ต้องสงสัย หรือบุคคลในเครือข่ายที่สามารถสืบหาหลักฐานเชื่อมโยงถึงตัวผู้ต้องสัยสัยได้ เมื่อมีการทำธุรกรรมเข้าจุดผ่านดังกล่าว แม้ว่าจะเป็นธุรกรรมการโอนโดยตรง แต่หากผู้รับโอนใช้กระเป๋าเงินที่ได้ลงทะเบียนกับผู้ให้บริการรับอนุญาต ก็จะเป็นข้อมูลที่สามารถเชื่อมโยงได้ อย่างไรก็ตามโดยวิธีการนี้ต้องอาศัยโปรแกรมการตรวจสอบทางเทคโนโลยี่ ในการเชื่อมโยงรหัสที่ตั้งของผู้ต้องสังสัยกับผู้ใช้งานที่ลงทะเบียนไว้กับผู้ให้บริการรับอนุญาตเช่นกัน

ทั้งนี้ทัศนะของผู้ให้ข้อมูลสำคัญสอดคล้องกับ หลักปฏิบัติการป้องกันการฟอกเงินของสหภาพยุโรปภายใต้กรอบแนวคิดในการกำกับดูแลในระบบสถาบันการเงินเป็นสำคัญ ดังนั้นมาตรการจึงมุ่งเฝ้าระวังผู้ใช้บริการในระบบสถาบันการเงิน แม้ว่าระบบการเงินโลกจะได้มีการพัฒนาเงินสกุลเข้ารหัส ที่มีคุณลักษณะเฉพาะเอื้อต่อการใช้เป็นเครื่องมือในการทำธุรกรรมฟอกเงินก็ตาม แนวปฏิบัติของมาตรการ ก็ยังคงมุ่งจุดเฝ้าระวัง ณ ระบบสถาบันการเงินซึ่งจะเป็นจุดแลกเปลี่ยนในลักษณะ "ผู้เฝ้าประตู (Gate Keeper)" โดยมุ่งกำกับดูแลการหมุนเวียนเงินเฉพาะ เมื่อทำธุรกรรมแปลงเงินสกุลเข้ารหัสเป็นเงินตราทั่วไป หรือการแปลงเป็นสินทรัพย์ที่มีตัวตนเป็นสำคัญ (Frick, 2019) และ FATF (Financial Action Task Force on Money Laundering) ได้ปรับปรุงข้อแนะนำที่ 15 (Recommendation 15 – New Technologies) เพื่อการจัดการลดความเสี่ยงจากสินทรัพย์เสมือน (Virtual Assets) โดยแนะนำให้รัฐควรจะให้ความเชื่อมั่นได้ว่า ผู้ให้บริการที่เกี่ยวข้องกับสินทรัพย์เสมือน (Virtual Assets Service Providers - VASP) จะต้องอยู่ภายใต้กฎระเบียบ การกำกับ การอนุญาตเพื่อให้ระบบการติดตามและสร้างความมั่นใจ ด้วยมาตรการป้องกันและปราบปรามการฟอกเงินอย่างเหมาะสม โดยหมายรวมถึงระบบการตรวจสอบข้อมูลตัวตนผู้ใช้งาน และการรายงานธุรกรรมต้องสงสัย เป็นต้น (Federico Paesano, 2019; Frick, 2019)

อย่างไรก็ตาม ปัจจุบันความยอมรับเงินสกุลเข้ารหัสเป็นสื่อกลางในการซื้อขายแลกเปลี่ยนทรัพย์สิน เพื่อธุรกิจการค้ายังอยู่ในวงจำกัด อาชญากรจึงจำเป็นต้องหาวิธีการแปลงค่าเป็นเงินตราปกติเพื่อจัดการผลประโยชน์ เว้นแต่ในอนาคตหากพัฒนาการของบริบทเงินสกุลเข้ารหัสเป็นที่

ยอมรับในสังคมวงกว้าง และมีสภาพคล่องมากพอที่จะทำธุรกรรมโดยตรงระหว่างคู่ค้าเป็นปกติธุระ ไม่ต้องจัดการแปลงค่าผ่านผู้ให้บริการรับอนุญาตใดแล้ว ก็อาจเป็นปัจจัยสำคัญที่ต้องกลับมาพิจารณาทบทวนว่า วิธีการนี้ยังมีประสิทธิภาพเพียงพอหรือไม่อย่างไรต่อไป

4.3.2 การใช้โปรแกรมการตรวจสอบ Digital Forensic Program ช่วยสืบค้น

เทคนิควิธีการสืบค้นผู้ต้องสงสัยโดยการเฝ้าระวัง ณ จุดที่อาชญากรจะทำธุรกรรมแปลงค่าเงินสกุลเข้ารหัสผ่านทางผู้ให้บริการรับอนุญาตนั้น อาจเป็นเทคนิควิธีการที่แก้ไขปัญหาในการพิสูจน์ตัวตนผู้ใช้งานหรือผู้ต้องสงสัยได้โดยตรง แต่ก็มีข้อจำกัดในการดำเนินการจะสัมฤทธิ์ผลได้ก็ต่อเมื่ออาชญากรทำธุรรรมเชื่อมโยงมายังผู้ให้บริการรับอนุญาตเท่านั้น ดังนั้นธุรกรรมที่ยังดำเนินการอยู่ภายในระบบนิเวศเงินสกุลเข้ารหัส เช่น การกระจายไปยังผู้รับโอนรายอื่นในระบบนิเวศ การจัดเก็บรักษาไว้ในกระเป๋าเงินโดยไม่เคลื่อนไหว หรือการโอนผ่านช่องทางผู้ให้บริการนอกระบบการกำกับ ก็ยังเป็นสภาพปัญหาที่ไม่สามารถแก้ไขได้ ผู้ให้ข้อมูลสำคัญส่วนใหญ่ได้ให้ความเห็น ถึงเทคนิควิธีการที่ใช้เทคโนโลยี่เข้าช่วยในการสืบค้น กล่าวคือ การใช้โปรแกรมพิสูจน์พยานหลักฐานทางดิจิทัล Digital Forensic Program ที่มีระบบประมวลผลจากฐานข้อมูลแบบเปิดของสมุดบัญชีอิเล็กทรอนิกส์โดยการเชื่อมต่อกับระบบปฏิบัติการบล็อกเชนในลักษณะ API (Application Program Interface) เพื่อช่วยในการวิเคราะห์พฤติกรรมการทำธุรกรรมของกลุ่มต้องสงสัย เชื่อมโยงพยานหลักฐานของธุรกรรมไปยังรหัสที่ตั้งต้องสงสัย หรืออาจสามารถสืบค้นหลักฐานเชื่อมโยงไปถึงผู้ให้บริการรับอนุญาตที่กระทำการช่วยเหลืออาชญากรทางอ้อมในการฟอกเงินได้ แต่ข้อจำกัดสำคัญของเทคนิควิธีการนี้คือ ต้นทุนการดำเนินงานสูง ดังนั้นหากจะดำเนินการอาจต้องพิจารณากำหนดผู้รับผิดชอบเป็นศูนย์ปฏิบัติการติดตามธุรกรรมของเงินสกุลเข้ารหัส ทั้งนี้ผู้ให้ข้อมูลสำคัญได้ให้ข้อมูลอ้างอิงถึงโปรแกรมการตรวจพิสูจน์หลักฐานทางดิจิทัลที่มีการใช้งานอย่างแพร่หลายของหลายหน่วยงานในต่างประเทศ เช่น

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Chainalysis,[23] CipherTrace[24] และ Elliptic[25] เป็นต้น (ผู้ให้ข้อมูลสำคัญ #221, #331) แต่ด้วยระบบฐานมูลแบบเปิดก็ยังมีความเชื่อว่า นักพัฒนาระบบงานคอมพิวเตอร์ของไทยก็น่าจะมีศักยภาพในการพัฒนาโปรแกรมสำเร็จรูปที่เหมาะสมกับบริบทของประเทศ เนื่องจากประเทศไทยก็ไม่น่าจะใช่เป้าหมายสำคัญของกลุ่มอาชญากร ที่จะใช้เป็นฐานในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส นอกจากนี้ผู้ให้ข้อมูลสำคัญได้ให้ความเห็นเพิ่มเติมบางส่วน ดังนี้

ความเห็นของผู้ให้ข้อมูลสำคัญ #111

“อาจไม่จำเป็นต้องใช้โปรแกรมการวิเคราะห์ชั้นสูง แต่ใช้โปรแกรมประยุกต์ที่พัฒนาขึ้นเชื่อมต่อกับระบบปฏิบัติการบล็อกเชน ร่วมกับการสร้างผู้ใช้งานแฝงตัวเข้าไปล่อซื้อในระบบการค้าสิ่งผิดกฎหมาย เพื่อให้โปรแกรมติดตามเส้นทางธุรกรรมเฉพาะรหัสของเงินสกุลเข้ารหัสที่แฝงตัวในระบบนิเวศสามารถเข้าถึงตัวของอาชญากรได้”

ความเห็นของผู้ให้ข้อมูลสำคัญ #112

“ทางเลือกในการสืบค้นอีกวิธีหนึ่งคือ การไปสืบค้นจากผู้ผลิตโปรแกรมสำเร็จที่คาดว่าอาชญากรใช้ในกระบวนการฟอกเงิน ถ้าเป็นผู้ผลิตต่างประเทศก็ติดตามสืบสวนจากตัวแทน หรือผู้แทนจำหน่าย โดยวิธีการนี้ไม่ต้องเข้าไปสืบสวนในระบบปฏิบัติการบล็อกเชนโดยตรง”

---

[23] Chainalysis เป็นบริษัทที่ให้บริการเกี่ยวกับการวิเคราะห์ระบบปฏิบัติการบล็อกเชน ทั้งในลักษณะให้บริการโปรแกรมสำเร็จรูป ข้อมูล และงานวิจัย แก่ภาครัฐ สถาบันการเงิน ศูนย์ซื้อขายแลกเปลี่ยน รวมถึงบริษัทรักษาความปลอดภัยทางไซเบอร์ไม่น้อยกว่า 50 ประเทศ โดยได้รับความเชื่อมั่นในศักยภาพการตรวจสอบ ทั้งกรณีอาชญากรรมทางไซเบอร์และการรักษาความปลอดภัยให้แก่ผู้ใช้งานธุรกรรมเงินสกุลเข้ารหัส https://www.chainalysis.com/company/

[24] CipherTrace เป็นองค์กรที่ก่อตั้งเมื่อ 2015 ด้วยการสนับสนุนจาก U.S. Department of Homeland Security โดยมีเป้าหมายในการปฏิบัติหน้าที่บริหารความเสี่ยง จากการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสให้แก่สถานบันการเงินและผู้ให้บริการต่างๆ รวมถึงส่งเสริมพัฒนาการทางเศรษฐกิจดิจิทัลที่มีความปลอดภัยต่อผู้ใช้งาน ปัจจุบันมีผู้ใช้บริการทั้งภาครัฐ ภาคเอกชนและสถาบันการเงินกว่า 150 ราย และมีสำนักงานประจำภูมิภาคใน 7 เมืองสำคัญของโลก https://ciphertrace.com/about-us/

[25] Elliptic เป็นบริษัทที่ได้รับการสนับสนุนจากกองทุนภาคเอกชนตั้งแต่ 2013 โดยเป็นบริษัทแรกของโลกที่ได้นำเสนอเทคโนโลยีในการติดตามเส้นทางธุรกรรมในระบบนิเวศเงินสกุลเข้ารหัสเพื่อการต่อต้านการฟอกเงิน และได้รับการยอมรับใช้เป็นเครื่องมือในการสร้างความปลอดภัยจากอาชญากรรมการเงินบนระบบไซเบอร์จากผู้ใช้บริการมากกว่า 100 รายใน 29 ประเทศ https://www.elliptic.co/

ความเห็นของผู้ให้ข้อมูลสำคัญ #232

“แม้การใช้โปรแกรมเทคโนโลยีขั้นสูง เพื่อการพิสูจน์ติดตามเส้นทางธุรกรรมเงินสกุลเข้ารหัส ก็อาจไม่ได้ผลถ้าอาชญากรใช้ Privacy Coin เข้ามาร่วมในการรับโอนเงินสกุลเข้ารหัสและการฟอกเงิน เช่น Manero เป็นเงินสกุลเข้ารหัสระบบ Many-to-One ทำให้ยากต่อการติดตามร่องรอยจากการโอนหลายรายการย่อยไปยังเจ้าของกระเป๋าเงินสุดท้าย เพื่อปิดบังการเชื่อมโยงรายการ หรืออีกระบบใช้วิธี Burn and Mint เป็นการเผาทิ้งเหรียญหรือทำลายรหัสเหรียญที่ต้นทางและไปสร้างเหรียญใหม่ที่ปลายทางคล้ายกับได้ผลตอบแทนจากการขุด จึงไม่ปรากฏร่องรอยของธุรกรรมใด เนื่องจากเหรียญที่ได้รับจะมาจากระบบโดยตรง เช่น เงินสกุลเข้ารหัสที่พัฒนาขึ้นโดยนักคิดไทยในนาม Firo ซึ่งเดิมชื่อ ZCoin ด้วยระบบแนวคิด Zero-Knowledge Proof”

ความเห็นของผู้ให้ข้อมูลสำคัญ #412

“เมื่อใช้โปรแกรมการพิสูจน์เส้นทางธุรกรรมแล้ว ก็ควรเชื่อมต่อโปรแกรมกับระบบฐานข้อมูลระดับสากล World Check[26] ที่รวบรวมข้อมูลตัวตนของบุคคลต่างๆทั่วโลกเพื่อตรวจสอบสถานะรหัสที่ตั้ง หรือเจ้าของกระเป๋าเงินที่เป็นผู้โอนหรือผู้ที่รับโอนนั้นอยู่ในบัญชีเฝ้าติดตาม (Watch List) หรือบัญชีต้องสงสัย (Black List) หรือไม่ ซึ่งหน่วยงานผู้บังคับใช้กฎหมายสามารถมีมาตรการในการระงับธุรกรรมชั่วคราวเพื่อการตรวจสอบต่อไป นอกจากนี้ควรพิจารณาการให้ความร่วมมือกับ Digital Assets Associations[27] ซึ่งเป็นองค์ความร่วมมือระหว่างประเทศด้านเงินสกุลเข้ารหัสโดยตรง”

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[26] World Check หรือ Refinitiv World-Check Risk Intelligence เป็นองค์กรในการบริหารจัดเก็บระบบฐานข้อมูลของบุคคลและองค์กรทั่วโลก พร้อมให้บริการตรวจสอบสถานะของบุคคลหรือองค์กรในระบบออนไลน์ เพื่อสนับสนุนการต่อต้านการฟอกเงินมากว่า 2 ทศวรรษ โดยแหล่งข้อมูลสำคัญที่เชื่อมโยงฐานข้อมูลจากเว็บไซต์หน่วยงานภาครัฐ ภาคเอกชน ข่าวสาร สื่อสังคมออนไลน์ และข้อมูลบุคคลต้องห้ามตามกฎหมายของแต่ละประเทศ https://www.refinitiv.com/en

[27] International Digital Asset Exchange Association เป็นองค์กรระหว่างประเทศที่จัดตั้งขึ้นในการประชุม G20 ณ เมืองโอซากา ประเทศญี่ปุ่นในปี 2019 ในวาระ V20-Vertual Asset Service Provider Summit เพื่อเป็นองค์ที่เข้ามาช่วยส่งเสริมอุตสาหกรรมและกำกับดูแลเงินเสมือน เพื่อป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยการประสานความร่วมมือกับ FATF https://www.idaxa.org/

4.3.3 การวิเคราะห์พฤติกรรมและเชื่อมโยงความมีตัวตนกับระบบงานอื่น

เมื่อใช้เทคนิควิธีในการพิสูจน์เส้นทางธุรกรรม และวิเคราะห์พฤติกรรมของธุรกรรมต้องสงสัยแล้ว โดยโปรแกรมเทคโนโลยีขั้นสูง หรือการใช้โปรแกรมประยุกต์ที่พัฒนาขึ้น หรือการสืบสวนโดยวิธีการอื่น ประเด็นปัญหาต่อไปคือ การพิสูจน์ทราบตัวตนของเจ้าของกระเป๋าเงินต้องสงสัย ผู้ให้ข้อมูลสำคัญส่วนหนึ่งได้ให้ความเห็นว่า วิธีการพิสูจน์ตัวตนในระบบนิเวศเงินสกุลเข้ารหัส ควรจะมีโปรแกรมที่เข้าเชื่อมโยงกับระบบข้อมูลที่ผู้ใช้งานต้องแสดงตัวตนก่อนใช้งาน หรือมีข้อมูลส่วนบุคคลในระบบฐานข้อมูลนั้น นอกเหนือจากการแสดงต้วตนเพื่อใช้บริการทางการเงินซึ่งเป็นมาตราการพิสูจน์ตัวตนของผู้ใช้งาน (KYC) ตามกฎหมายป้องกันและปราบปรามการฟอกเงินอยู่แล้ว ทั้งนี้การเชื่อมโยงตัวตนของผู้ใช้งาน โดยเปรียบเทียบรหัสที่ตั้งของเครื่องมือสื่อสารที่ใช้งาน ฐานข้อมูลที่อยู่ในสื่อสารสังคมออนไลน์ เช่น Facebook, Twitter, Email เป็นต้น (ผู้ให้ข้อมูลสำคัญ #112, #332, #412) ตามหลักการที่ว่าอาชญากรรมย่อมต้องทิ้งร่องรอยเสมอ ดังนั้นจึงควรอาศัยการพิสูจน์ทราบหลักฐานแวดล้อมอื่นประกอบ (ผู้ให้ข้อมูลสำคัญ #311) เช่น การสังเกตุพฤติกรรมการโอนของผู้ใช้งาน มีลักษณะรูปแบบซ้ำรอยเดิมๆเป็นกิจวัตรหรือไม่ เนื่องจากอาจต้องการจำกัดให้มีผู้เกี่ยวข้องน้อยที่สุด สะดวกต่อการจัดการ โดยทำการโอนกันในกลุ่มผู้ใช้งานเพียงไม่กี่ราย ซึ่งแตกต่างจากธุรกรรมปกติที่มีความเป็นธรรมชาติมักจะไม่มีรูปแบบธุรกรรมการโอนลักษณะที่อาจตายตัว (ผู้ให้ข้อมูลสำคัญ #241) หรือมีธุรกรรมการโอนระหว่างกระเป๋าเงินของเจ้าของเดียวกันบ่อยครั้ง รวมถึงมีการโอนไปยังกระเป๋าเงินของเจ้าของรายหลายที่ใช้งานอยู่บนรหัสที่ตั้งเดียวกัน เป็นต้น (ผู้ให้ข้อมูลสำคัญ #412)

ทั้งนี้เทคนิคการวิเคราะห์พิสูจน์ตัวตนของผู้ต้องสงสัย โดยความเชื่อมโยงกับการระบุตัวตนในระบบงานอื่น จะมีผลสัมฤทธิ์ได้ ก็ต่อเมื่อจะต้องอยู่ในอำนาจรัฐที่จะออกกฎระเบียบบังคับได้ เช่น ผู้ให้บริการธุรกิจสื่อสาร หรืออาศัยความร่วมมือโดยเฉพาะองค์ระหว่างประเทศที่เป็นผู้ประกอบการสื่อสังคมออนไลน์ ที่จะต้องให้ความร่วมมือในการตรวจพิสูจน์ตัวตนผู้ต้องสงสัยจากหลักฐานรหัสทางคอมพิวเตอร์ที่เชื่อมโยงกันกับฐานข้อมูลของผู้ให้บริการ

4.3.4 สรุปเทคนิควิธีการติดตามสืบค้นหาตัวผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส

เทคนิควิธีที่ผู้ให้ข้อมูลสำคัญ ได้ให้ความเห็นมีความสอดคล้องกับแนวปฏิบัติองค์กรต่อต้านการฟอกเงินระดับสากล รวมถึงหน่วยงานผู้บังคับใช้กฎหมายในต่างประเทศ เช่น หลักการกำกับการแสดงตัวตน และการตรวจพิสูจน์ตัวตนของผู้ใช้งานก่อนที่จะอนุญาตให้เข้าใช้ระบบงานได้ (KYC on Boarding) ถือเป็นมาตราการกลั่นกรองบุคคลด่านแรกที่สำคัญ แต่หากขั้นตอนนี้ไม่ได้รับการ

ปฏิบัติที่รัดกุม ก็เหมือนกับเปิดช่องโอกาสสำคัญให้แก่อาชญากร ในขณะเดียวระบบการทบทวนความทันสมัยของข้อมูลส่วนบุคคลนั้น ควรมีการกำหนดวงรอบที่เหมาะสมก็จะเป็นอีกขั้นตอนที่ความสำคัญซึ่งเข้ามาช่วยบรรเทาปัญหาการบันทึกข้อมูลส่วนบุคคลที่ไม่ชัดเจนในขั้นตอนแรกได้ นอกจากนี้การวิเคราะห์พฤติกรรมของผู้ใช้งานในการทำธุรกรรมจนอาจเข้าข่ายต้องสงสัยเพื่อการเฝ้าระวัง แต่เทคนิควิธีเฝ้ารอ ณ จุดที่อาชญากรข้ามจากการเงินโลกเสมือนมาสู่การเงินโลกกายภาพ อาจมีประสิทธิภาพลดลงเมื่อเงินสกุลเข้ารหัสได้รับการยอมรับจากสังคมอย่างแพร่หลาย และยอมรับเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการเยี่ยงปกติธุระ โอกาสที่ธุรกรรมการเงินของอาชญากรจะข้ามเข้าสู่ระบบสถาบันการเงินก็อาจยากขึ้นหรือไม่เกิดขึ้นเลย เพราะธุรกรรมเงินสกุลเข้ารหัสสามารถทดแทนธุรกรรมการซื้อขายสินค้าหรือทรัพย์สินด้วยเงินตราปกติได้อย่างสมบูรณ์

เนื่องจากธุรกรรมเงินสกุลเข้ารหัสดำเนินการบนระบบออนไลน์ สามารถทำธุรกรรมทั้งภายในประเทศและข้ามประเทศได้อย่างรวดเร็ว จึงเป็นความจำเป็นของหน่วยงานบังคับใช้กฎหมายต้องมีพัฒนาการด้านเทคโนโลยี่ให้เท่าทัน รวมถึงการพัฒนาบุคคลที่เกี่ยวข้องให้ทันต่อพลวัตการเปลี่ยนแปลงคุณลักษณะเฉพาะของเงินสกุลเข้ารหัส กลไกการกลบเกลื่อร่องรอย โดยควรจะเลือกใช้ เทคโนโลยี่การตรวจพิสูจน์หาตัวตนของผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัสที่เหมาะสมกับบริบทของประเทศไทย หรืออาจส่งเสริมการพัฒนาโปรแกรมประยุกต์เพื่อช่วยงานด้านการตรวจติดตามที่เหมาะสมในระบบปฏิบัติการบล็อกเชนขึ้นใช้เองในหน่วยงาน และเทคนิควิธีการเชื่อมโยงข้อมูลด้านเทคโนโลยี่กับการพิสูจน์ตัวตนผู้ใช้งานในระบบงานอื่น ซึ่งสอดคล้องกับข้อเสนอในงานวิจัยต่างประเทศ โดยการตรวจพิสูจน์ตัวตนผู้ใช้งานด้วยการวิเคราะห์เปรียบเทียบกลุ่มรหัสที่ตั้งของผู้ใช้งาน (Cluster) กับรหัสที่ตั้งในฐานข้อมูลนอกระบบนิเวศเงินสกุลเข้ารหัส (Andrew & Douglas, 2018) หรือกล่าวอีกนัยหนึ่ง คือการนำรหัสที่ตั้งของผู้ใช้งานต้องสงสัยสืบค้นเปรียบเทียบกับธุรกรรมประจำวันบนระบบอินเตอร์เน็ต ไม่ว่าจะเป็นตรวจเปรียบเทียบกับการใช้ Email, Facebook, Twitter รวมถึงสื่อสังคมออนไลน์อื่นๆ เพื่อการสืบค้นและเข้าถึงตัวบุคคลของผู้ใช้งานต้องสังสัย (Hazar, 2019)

4.4 แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน และแนวทางปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะ และสามารถเพิ่มประสิทธิภาพการบังคับใช้เชิงปฏิบัติการ

การศึกษา แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส รวมถึงแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมนั้น ผู้วิจัยได้ใช้วิธีการวิจัยโดยเทคนิควิธีเดลฟายรูปแบบปรับปรุงด้วยวิธีการสัมภาษณ์เชิงลึก

จากผู้ให้ข้อมูลสำคัญชุดเดียวกันทั้ง 19 ราย แทนวิธีการสำรวจความเห็นอิสระโดยตรงในรอบที่ 1 (ภาคผนวก ค) ทั้งนี้การสำรวจความเห็น จากผู้ให้ข้อมูลสำคัญได้ดำเนินการพร้อมกันในขณะทำการสัมภาษณ์เชิงลึกด้วยคำถามปลายเปิดในประเด็นข้อเสนอแนะต่อการกำหนดนโยบาย หรือแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อบริบทของประเทศไทย และสากลในสถานการณ์ปัจจุบัน รวมถึงข้อเสนอแนะต่อแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม และสามารถเพิ่มประสิทธิภาพในการปฏิบัติงาน

โดยผู้วิจัยได้สังเคราะห์ความคิดเห็น และทัศนะเชิงเสนอแนะของผู้ให้ข้อมูลสำคัญประมวลความเห็นสรุป ได้เป็นข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลที่เหมาะสมได้จำนวน 13 แนวทาง และข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม และสามารถเพิ่มประสิทธิภาพในการปฏิบัติงานได้จำนวน 10 แนวทาง จากนั้นได้ประมวลผลสัดส่วนร้อยละความเห็นของผู้ให้ข้อมูลสำคัญในแต่ละแนวทาง เพื่อจัดทำเป็นแบบสำรวจความเห็นต่อแนวทางการป้องกันและแนวปฏิบัติสำหรับการสำรวจความเห็นในรอบที่ 2 (ภาคผนวก ง) ทั้งนี้การติดต่อผู้ให้ข้อมูลสำคัญนั้นดำเนินการด้วยการจัดส่ง และตอบกลับความเห็นทางจดหมายอิเล็กทรอนิกส์ (Email) โดยให้ผู้ให้ข้อมูลสำคัญระบุความเห็นอิสระเป็น 5 ระดับ คือ 1 ถึง 5 สำหรับแต่ละข้อเสนอ ซึ่งความเห็นระดับ 1 หมายถึง แนวทางที่นำเสนอเหมาะสมต่อการนำไปบังคับใช้ได้**น้อยที่สุด** หรือแนวปฏิบัติที่นำเสนอน่าจะมีโอกาสเพิ่มประสิทธิภาพใน การปฏิบัติงานได้ “**น้อยที่สุด**” และเพิ่มระดับความเห็นจนถึงระดับ 5 หมายถึง “**มากที่สุด**”

ทั้งนี้ ในการสำรวจความเห็นรอบที่ 2 ผู้ให้ข้อมูลสำคัญได้ตอบกลับแบบสำรวจความเห็นจำนวน 18 ราย โดยผู้วิจัยได้ประมวลผลแบบสำรวจความเห็นของผู้ให้ข้อมูลสำคัญ พร้อมวิเคราะห์ข้อมูลเชิงสถิติเบื้องต้นของแต่ละข้อเสนอ อันประกอบด้วยสัดส่วนร้อยละของผู้ให้ความเห็นแต่ละระดับ ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐานของระดับความเห็น เพื่อจัดทำเป็นแบบสำรวจฉบับทบทวนหรือยืนยันความเห็นในการดำเนินการสำรวจความเห็นในรอบที่ 3 (ภาคผนวก จ) โดยผู้ให้ข้อมูลสำคัญจะได้รับทราบ ผลสรุปจากการประมวลความเห็นในภาพรวมของผู้ให้ข้อมูลสำคัญ พร้อมกับความเห็นของตนเองที่แสดงไว้ในการสำรวจรอบที่ 2 ทั้งนี้การติดต่อผู้ให้ข้อมูลสำคัญยังคงดำเนินการด้วยวิธีการจัดส่งและตอบกลับความเห็นทางจดหมายอิเล็กทรอนิกส์ (Email) เช่นเดียวกัน โดยผู้ให้ข้อมูลสำคัญสามารถยืนยันความเห็นเดิมทุกประการ หรือทบทวนปรับแก้ความเห็นอย่างอิสระเป็น 5 ระดับ คือ 1 ถึง 5 สำหรับแต่ละข้อเสอน ซึ่งความเห็นระดับ 1 หมายถึง **”น้อยที่สุด”**, ระดับ 2 หมายถึง **“น้อย”**, ระดับ 3 หมายถึง **“ปานกลาง”**, ระดับ 4 หมายถึง **“มาก”** และ ระดับ 5 หมายถึง **“มากที่สุด”**

ทั้งนี้ ได้รับการตอบกลับแบบสำรวจความเห็นฉบับทบทวนหรือยืนยันความเห็นจากผู้ให้ข้อมูลสำคัญในรอบที่ 3 ได้จำนวน 18 ราย ซึ่งเกินกว่าเกณฑ์ขั้นต่ำที่จะต้องมีผู้ตอบกลับจำนวนตั้งแต่ 17 รายขึ้นไป ดังนั้นการสำรวจความเห็นตามวิธีการเดลฟายจึงสามารถดำเนินการต่อไปได้ โดยผู้วิจัยได้ทำการวิเคราะห์ผลการศึกษาโดยเทคนิควิธีเดลฟาย ประกอบด้วย **เกณฑ์การวิเคราะห์ระดับความคงที่ของความเห็น (Stability)** จากการสำรวจความเห็นในรอบที่ 3 ด้วยการตรวจสอบความเปลี่ยนแปลงของสัดส่วนร้อยละความเห็นของแต่ละข้อเสนอในรอบที่ 2 และเปรียบเทียบกับรอบที่ 3 ในกรณีที่มีความแตกต่างกันไม่เกินร้อยละ 15.00 และทำการทดสอบค่าสถิติ F-Test ของค่าความแปรปรวนของระดับความเห็นของแต่ละข้อเสนอในรอบที่ 2 เทียบกับรอบที่ 3 ณ ระดับนัยสำคัญเท่ากับ 0.05 (α=0.05) ถ้าไม่มีนัยสำคัญแสดงว่าค่าความแปรปรวนของทั้งสองรอบไม่มีความแตกต่างกัน จึงถือว่าการสำรวจความเห็นมีระดับความคงที่ ดังนั้นถ้าผลการศึกษาการสำรวจความเห็นในรอบที่ 2 และรอบที่ 3 มีผลทดสอบเข้าเกณฑ์ครบทั้งสองกรณี แสดงว่าความเห็นจากการสำรวจโดยภาพรวมของรอบที่ 2 และรอบที่ 3 ไม่มีความแตกต่างกันอย่างมีนัยสำคัญ จึงเป็นเกณฑ์ให้ยุติการสำรวจความเห็นเพื่อทำการวิเคราะห์ข้อมูลและรายงานผลการศึกษาต่อไป

และเกณฑ์การวิเคราะห์ความเป็นฉันทามติ (Consensus) ของผู้ให้ข้อมูลสำคัญต่อแต่ละข้อเสนอ โดยผู้วิจัยตรวจสอบค่าสัมประสิทธิ์การกระจาย (coefficient of variation) ที่คำนวณจากค่าเบี่ยงเบนมาตรฐานหารด้วยค่าเฉลี่ยของระดับความเห็นแต่ละข้อเสนอในรอบที่ 3 มีค่าการกระจายไม่เกิน 0.5 และค่าสัมบูรณ์ของ ผลต่างระหว่างค่ามัธยฐานกับค่าฐานนิยมของความเห็นแต่ละข้อเสนอในรอบที่ 3 ด้วยเกณฑ์ไม่เกิน 1.00 และค่าพิสัยระหว่างควอไทล์[28] ของความเห็นแต่ละข้อเสนอในรอบที่ 3 ด้วยเกณฑ์ไม่เกิน 1.50 โดยมีผลทดสอบเข้าเกณฑ์ครบทั้งสามกรณี แสดงว่าความเห็นต่อข้อเสนอนั้นได้รับฉันทามติจากผู้ให้ข้อมูลสำคัญ (วรสิทธิ์ เจริญพุฒ & ศิรินัง, 2015) ซึ่งอาจเป็นได้ทั้งฉันทามติเสียงข้างมากหรือข้างน้อย และในการวิจัยนี้ ได้กำหนดเกณฑ์ประมวลผลข้อเสนอที่เหมาะสมด้วย **ฉันทามติเสียงข้างมาก (Majority of Consensus)** โดยเกณฑ์ ค่าผลรวมสัดส่วนร้อยละของความเห็นระดับ 5 (“มากที่สุด”) และระดับ 4 (“มาก”) มีค่าตั้งแต่ร้อยละ 75.00 ขึ้นไป และค่าเฉลี่ยของระดับความเห็นตั้งแต่ 4.00 ขึ้นไป และค่ามัธยฐานของระดับความเห็นตั้งแต่ 4.00 ขึ้นไป ในกรณีข้อเสนอมีผลทดสอบเข้าเกณฑ์ครบทั้งสามกรณี แสดงว่าข้อเสนอเข้าข่ายได้รับฉันทามติเป็นเสียงข้างมากต่อข้อเสนอนั้น หรือกล่าวอีกนัยหนึ่งคือ เป็นข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลที่มีความเหมาะสมอย่างมาก หรือเป็นข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่มีความเหมาะสมอย่างมากเช่นกัน

[28] ค่าพิสัยระหว่างควอไทล์ (Interquartile range, IQR) เป็นการวัดการกระจายของข้อมูลด้วยผลต่างระหว่างควอไทล์ที่ 3 และควอไทล์ที่ 1

จากเกณฑ์การวิเคราะห์ผลการศึกษาโดยเทคนิควิธีเดลฟายที่กล่าวข้างต้น ผู้วิจัยได้ประมวลข้อมูลและสังเคราะห์ความเห็นจากผู้ให้ข้อมูลสำคัญ เป็นกรอบข้อเสนอต่อแนวทางการป้องกันและแนวปฏิบัติเพื่อการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เพื่อสำรวจความเห็นจากผู้ให้ข้อมูลสำคัญชุดเดียวกันอย่างต่อเนื่อง ตามขั้นตอนเทคนิควิธีเดลฟายจนได้ระดับความคงที่จากการสำรวจความเห็นในรอบที่ 3 จึงได้ยุติการสำรวจความเห็นรอบต่อไป และได้วิเคราะห์ผลการศึกษาโดยเกณฑ์ฉันทามติเสียงข้างมากของแต่ละข้อเสนอแนวทางการป้องกัน และแนวปฏิบัติเพื่อการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ทั้งนี้ได้เสนอผลการศึกษาเป็นขั้นตอนตามลำดับเทคนิควิธีการ ดังนี้

4.4.1 ข้อเสนอต่อแนวการทางป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

ผู้วิจัยได้รวบรวมข้อมูลทัศนะเชิงเสนอแนะ ด้วยความเห็นอิสระจากผู้ให้ข้อมูลสำคัญชุดเดียวกันในขณะทำการสัมภาษณ์เชิงลึก จากผู้ให้ข้อมูลสำคัญจำนวนทั้งสิ้น 19 ราย ในประเด็นการกำหนดนโยบาย หรือแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลที่เหมาะสมต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน และได้ประมวลข้อมูลพร้อมทั้งสังเคราะห์ความเห็น และจัดกลุ่มแนวคิด ได้เป็นข้อเสนอต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลที่เหมาะสมได้จำนวน 13 แนวทาง โดยเสนอตามลำดับความเห็นเสียงส่วนใหญ่ของผู้ให้ข้อมูลสำคัญจากมากไปน้อย ดังนี้

แนวทางที่ 1 กระบวนการตรวจพิสูจน์ตัวตนของผู้ใช้งาน (KYC – Know Your Customer) โดยเสนอให้หน่วยบังคับใช้กฎหมายควรกำหนดหลักเกณฑ์มาตรฐานสำหรับการบันทึกข้อมูลเพื่อการตรวจพิสูจน์ตัวตน (KYC) ของผู้ใช้งาน ซึ่งหมายรวมถึง บุคคลที่ประสงค์จะทำธุรกรรมเงินสกุลเข้ารหัส หรือใช้บริการกับผู้ให้บริการเกี่ยวกับเงินสกุลเข้ารหัสนั้น โดยควรคำนึงถึงข้อมูลที่จำเป็นเพื่อการรู้จักตัวตนผู้ใช้งานก่อนการอนุญาตให้เข้าใช้ระบบงาน รวมถึงสามารถพิสูจน์ความเป็นตัวตนของผู้ใช้งานได้อย่างเพียงพอ พร้อมทั้งกำหนดให้มีกระบวนการตรวจสอบและทบทวนข้อมูลส่วนบุคคลของผู้ใช้งานให้ทันสมัยอย่างสม่ำเสมอ เพื่อเป็นฐานข้อมูลสำคัญในการตรวจสอบตัวตนของเจ้าของกระเป๋าเงินหรือผู้ใช้งานเมื่อต้องการสืบค้นธุรกรรมที่อาจเข้าข่ายต้องสงสัย

แนวทางที่ 2 การเผยแพร่องค์ความรู้เกี่ยวกับเงินสกุลเข้ารหัสให้แก่สาธารณชน โดยเสนอให้หน่วยงานกำกับ หรือหน่วยงานอื่นที่เกี่ยวข้องกับการประชาสัมพันธ์สาธารณะจัดให้ทำการรวบรวมสาระองค์ความรู้ และควรจัดให้มีการเผยแพร่ส่งเสริมความรู้ให้แก่สาธารณะ ประชาชนทั่วไปได้ทราบถึงคุณลักษณะเฉพาะ กลไกการทำงานของเงินสกุลเข้ารหัส และความเสี่ยงที่อาจเกิดขึ้นจากการทำธุรกรรมเงินสกุลเข้ารหัส รวมถึงระบบปฏิบัติการบล็อกเชนซึ่งเป็นเทคโนโลยีสนับสนุนระบบ

นิเวศเงินสกุลเข้ารหัสที่สามารถทำธุรกรรมโดยตรงและข้ามประเทศ โดยไม่มีตัวกลางในการกำกับดูแล แต่เป็นระบบฐานข้อมูลแบบเปิด และมีระบบสมุดบัญชีอิเลคทรอนิกส์สาธารณะแบบกระจายศูนย์ ส่งผลให้มีโอกาสในการถูกตรวจสอบ และเข้าถึงเส้นทางการทำธุรกรรมในระบบนิเวศเงินสกุลเข้ารหัสได้ เพื่อให้ประชาชนได้ทราบระบบการทำงานของธุรกรรมเงินสกุลเข้ารหัส และเข้าใจถึงความเสี่ยงที่อาจเกิดอาชญากรรมไซเบอร์ รวมถึงอาจถูกใช้เป็นเครื่องมือในการฟอกเงิน ในขณะเดียวกันอาจช่วยสร้างความเข้าใจที่ถูกต้องแก่อาชญากร ที่ต้องหลีกเสี่ยงการถูกตรวจสอบเส้นทางกธุรกรรมเงินสกุลเข้ารหัสเมื่อใช้เป็นเครื่องมือในการฟอกเงิน

แนวทางที่ 3 การสร้างกรอบความร่วมมือระหว่างประเทศ เพื่อการต่อต้านการฟอกเงิน เนื่องจากธุรกรรมเงินสกุลเข้ารหัสเป็นประเด็นใหม่ของสังคมโลก ดังนั้นความร่วมมือระหว่างประเทศที่มีอยู่ในปัจจุบันอาจไม่ครอบคลุม หรือไม่เพียงพอต่อประสิทธิภาพการปฏิบัติงาน ดังนั้นจึงควรสร้างกรอบความร่วมมือกับองค์กรระหว่างประเทศ และหน่วยงานของแต่ละประเทศที่รับผิดชอบงานด้านการต่อต้านการฟอกเงิน เพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสเป็นการเฉพาะ โดยการประสานความร่วมมือในการแลกเปลี่ยนข้อมูลสำคัญที่เกี่ยวข้อง เทคโนโลยีการสืบค้นผู้ต้องสงสัย รวมถึงองค์ความรู้ประสบการณ์จากกรณีศึกษาการกระทำความผิดที่เกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัส และกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เพื่อเสริมสร้างทักษะของผู้ปฏิบัติงานในการประสานงานระหว่างประเทศ เมื่อเกิดกรณีขึ้นจะสามารถดำเนินการได้เท่าทันกับการเคลื่อนไหวของอาชญากร

แนวทางที่ 4 การส่งเสริมศักยภาพการแข่งขันให้แก่ผู้ให้บริการรับอนุญาต ทั้งนี้ผู้ให้บริการรับอนุญาต หมายรวมถึง Exchanger, Broker, Portal, Wallet Provider ที่ได้รับอนุญาตให้ประกอบกิจการตามกฎหมาย เพื่อให้ผู้ให้บริการรับอนุญาตสามารถอำนวยความสะดวกในการทำธุรกรรมเงินสกุลเข้ารหัสให้แก่ผู้ใช้งาน และสร้างแรงจูงใจแก่ผู้ใช้งานให้เลือกใช้บริการกับผู้ให้บริการรับอนุญาต มากกว่าการใช้บริการกับผู้ให้บริการนอกระบบ หรือผู้ให้บริการต่างประเทศ ซึ่งเป็นมาตรการที่ช่วยลดฐานจำนวนผู้ใช้งานนอกระบบการกำกับของหน่วยงานบังคับใช้กฎหมาย

แนวทางที่ 5 การออกกฎระเบียบในการกำกับการทำธุรกรรมเงินสกุลเข้ารหัส หรือผู้ให้บริการรับอนุญาตอย่างเหมาะสม ทั้งนี้เทคโนโลยีระบบปฏิบัติการบล็อกเชน รวมถึงธุรกรรมเงินสกุลเข้ารหัส มีแนวโน้มที่อาจสร้างการขับเคลื่อนระบบเศรษฐกิจยุคดิจิทัลของบริบทการเงินโลก โดยเฉพาะอย่างยิ่งนโยบายส่งเสริมระบบการเงินแบบไร้เงินสด และใช้ระบบเทคโนโลยีการเงินของรัฐบาลหลายประเทศ รวมถึงประเทศไทย ดังนั้นในกระบวนการออกกฎระเบียบเพื่อการกำกับการทำธุรกรรมเงินสกุลเข้ารหัส หรือผู้ให้บริการรับอนุญาตที่เกี่ยวข้องกับเงินสกุลเข้ารหัสควรคำนึงถึงการสร้างความสมดุลระหว่างประโยชน์สาธารณะที่จะได้รับจากความคล่องตัวทางธุรกิจ และลดต้นทุนการทำธุรกรรม กับการสร้างภาระและข้อจำกัดในการดำเนินธุรกิจ เพื่อการป้องกันอาชญากรรม

มิฉะนั้นอาจส่งผลทางกลับกลายเป็นเสมือนส่งเสริมให้ผู้ใช้งานในประเทศ ไปใช้บริการกับผู้ให้บริการนอกระบบ หรือผู้ให้บริการต่างประเทศที่มีความคล่องตัว เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสเป็นธุรกรรมโลกาภิวัตร ไม่จำกัดเฉพาะขอบเขตประเทศใด

แนวทางที่ 6 การอ้างอิงแนวทางการกำกับหรือข้อแนะนำการปฏิบัติตามหลักมาตรฐานสากล เนื่องจากธุรกรรมบนระบบนิเวศเงินสกุลเข้ารหัสสามารถดำเนินการข้ามเขตประเทศได้อย่างรวดเร็ว ดังนั้นแนวทางในการออกกฎระเบียบการกำกับธุรกรรมและผู้ให้บริการเงินสกุลเข้ารหัสควรอ้างอิงกับแนวทางหรือข้อแนะนำตามหลักมาตรฐานการปฏิบัติสากล เช่น FATF Recommendations เพื่อให้สร้างบรรทัดฐานร่วมกัน ทั้งในกรณีที่มีความจำเป็นต้องประสานขอความร่วมมือในการตรวจสอบสืบค้นผู้ต้องสงสัยกับฐานข้อมูลระหว่างประเทศ รวมถึงความร่วมมือในการสร้างระบบการป้องกันการฟอกเงินโดยธุรรมเงินสกุลเข้ารหัส

แนวทางที่ 7 การสร้างเครือข่ายความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมาย เนื่องจากการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส มีขอบข่ายที่เกี่ยวข้องกับหลายหน่วยงานทั้งด้านการปฏิบัติงานว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และด้านการกำกับดูแลการกิจกรรมด้านเทคโนโลยีการเงินเพื่อเศรษฐกิจและสังคม เช่น สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ธนาคารแห่งประเทศไทย สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานอัยการ กรมสรรพากร กรมบังคับคดี สำนักงานคณะกรรมการกิจการกระจายเสียง กิจการโทรทัศน์ และโทรคมนาคมแห่งชาติ เป็นต้น ดังนั้นจึงควรสร้างระบบเครือข่ายความร่วมมือ ในการประสานความช่วยเหลือระหว่างหน่วยงานในการเข้าถึงข้อมูลส่วนบุคคลของผู้ต้องสงสัย รวมถึงเส้นทางการทำธุรกรรมเงินสกุลเข้ารหัสต้องสงสัย เพื่อเสริมสร้างประสิทธิภาพในการป้องปราม และตรวจสอบสืบค้นได้ทันต่อการโยกย้ายธุรกรรมเงินสกุลเข้ารหัสในระบบไซเบอร์

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

แนวทางที่ 8 การบูรณาการหน่วยงานหลักที่รับผิดชอบร่วมทำงานแบบองค์รวม ดังที่กล่าวข้างต้น อาจมีหน่วยงานที่เกี่ยวข้องกับการป้องกันและปราบปรามการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน ดังนั้นหน่วยงานหลักที่รับผิดชอบจึงควรร่วมกันบรูณาการการทำงานแบบองค์รวมเพื่อร่วมกันกำหนดแผนปฏิบัติงานตามลำดับขั้นตอนปฏิบัติการ ลดการปฏิบัติงานที่อาจทับซ้อนของขอบเขตหน้าที่รับผิดชอบ และอาจเพิ่มประสิทธิภาพการปฏิบัติงานโดยมีการจัดตั้งคณะทำงานเฉพาะกิจ หรือแต่งตั้งผู้เชี่ยวชาญเป็นที่ปรึกษาให้การสนับสนุนเชิงเทคนิคและแนวทางในการปฏิบัติงาน

แนวทางที่ 9 การสร้างความร่วมมือขององค์กรภาคเอกชนที่เกี่ยวข้องกับธุรกิจเงินสกุลเข้ารหัส เนื่องจากองค์กรภาคเอกชนผู้ให้บริการเกี่ยวข้องกับเงินสกุลเข้ารหัส ปฏิบัติหน้าที่ในฐานะตัวกลางระหว่างผู้ใช้งานกับหน่วยงานรัฐที่ทำหน้าที่กำกับดูแลธุรกรรมเงินสกุลเข้ารหัส จึงควร

ส่งเสริมให้ผู้ให้บริการ หรือองค์กรภาคเอกชนที่เกี่ยวข้องสร้างกรอบความร่วมมือในการสนับสนุนการดำเนินงานกำกับดูแลกันเองภายในอุตสาหกรรมเงินสกุลเข้ารหัส และเป็นองค์กรที่ร่วมประสานงานกับหน่วยงานรัฐ ในทำนองเดียวกับสมาคมธนาคารไทย สมาคมบริษัทหลักทรัพย์ หรือสมาคมผู้ประกอบธุรกิจการเงินอื่น ซึ่งเป็นช่องทางในการส่งเสริมพัฒนาการและความเข็มแข็งของอุตสาหกรรมเงินสกุลเข้ารหัส และเพิ่มประสิทธิภาพการประสานความร่วมมือกับหน่วยงานรัฐ

แนวทางที่ 10 มาตรการกำหนดให้ผู้ใช้งานทำธุรกรรมกับผู้ให้บริการรับอนุญาตเนื่องด้วยผู้ใช้งานในระบบนิเวศเงินสกุลเข้ารหัสสามารถทำธุรกรรมได้ โดยไม่มีข้อจำกัดด้านเทคโนโลยีที่กำหนดขอบเขตการทำธุรกรรม เช่น ผู้ใช้งานสามารถสร้างกระเป๋าเงินของตนได้ไม่จำกัดจำนวนทำธุรกรรมระหว่างกันโดยไม่ต้องตรวจสอบผู้โอนหรือผู้รับโอน ด้วยความเชื่อมมั่นต่อการพิสูจน์ยืนยันรายการในระบบปฏิบัติการบล็อกเชน ดังนั้นเพื่อให้การกำกับดูแลธุรกรรมเงินสกุลเข้ารหัสได้อย่างมีประสิทธิภาพ จึงควรออกมาตรการกำหนดให้ผู้ใช้งานที่จะต้องการทำธุรกรรมจะต้องดำเนินการเฉพาะกับผู้ให้บริการที่ได้รับอนุญาต และหากเป็นการทำธุรกรรมข้ามประเทศก็ให้ดำเนินการเฉพาะกับผู้ให้บริการที่ได้รับอนุญาตของประเทศนั้นๆ เพื่อเป็นการกรองผู้ใช้งานสุจริตออกจากผู้ใช้งานที่อาจมีประสงค์ในการกระทำธุรกรรมที่ไม่สุจริต

แนวทางที่ 11 การออกกฎระเบียบปฏิบัติในกระบวนการสืบสวนเกี่ยวข้องกับบริบทธุรกรรมเงินสกุลเข้ารหัสอย่างชัดเจน เนื่องด้วยธุรกรรมเงินสกุลเข้ารหัสเป็นลักษณะการกระทำกิจกรรมหรือธุรกรรมที่อาจไม่เข้าข่ายกฎระเบียบปฏิบัติที่มีอยู่ในปัจจุบัน อันอาจเป็นอุปสรรคต่อกระบวนการสืบสวน เช่น ลักษณะพยานหลักฐานดิจิทัลที่ระบุในระบบนิเวศเงินสกุลเข้ารหัส การสืบสวนเพื่อเข้าถึงกระเป๋าเงินของอาชญากร ที่อาจต้องเข้าไปกระทำบางประการต่อหลักฐานกระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัยไปยังกระเป๋าเงินของหน่วยงานใด ที่จะทำหน้าที่เป็นผู้เก็บรักษาโดยมีกฎหมายรองรับ หรือปรับแก้ไขกฎหมายที่เกี่ยวข้องให้สามารถดำเนินการได้ เป็นต้น

แนวทางที่ 12 การสร้างระบบจัดการฐานข้อมูลกลางของการแสดงตัวตนผู้ใช้งาน (KYC Bureau หรือ KYC Data Center) เนื่องจากระบบบริหารจัดการฐานข้อมูลแสดงตัวตนของผู้ใช้งาน หรือการพิสูจน์ความมีตัวตนของผู้ใช้งานยังเป็นระบบที่ถูกจัดเก็บไว้เฉพาะผู้ให้บริการรับอนุญาตแต่ละราย เมื่อผู้ให้บริการรับอนุญาตรายใดทำการปรับปรุงฐานข้อมูล ก็จะมีความทันสมัยเฉพาะฐานข้อมูลของตน ดังนั้นจึงขาดความทันสมัยของข้อมูลตัวตนของผู้ใช้งานกับผู้ให้บริการรับอนุญาตรายอื่น หรือกับผู้ให้บริการธุรกรรมการเงินประเภทอื่น ข้อเสนอควรให้สร้างระบบจัดการฐานข้อมูลกลางของการแสดงตัวตนผู้ใช้งานในลักษณะ KYC Bureau ในทำนองเดียวกับเครดิตบูโรของสถาบันการเงิน ซึ่งทำหน้าที่รวบรวมข้อมูลส่วนบุคคลของการใช้บริการด้านสินเชื่อจากผู้ให้บริการทางการเงินทุกประเภท เช่น ธนาคาร บริษัทเงินทุน บริษัทหลักทรัพย์ บรัษัทบัตรเครดิต บริษัทการเงิน

นอกระบบธนาคาร บริษัทบริการการเงินอิเล็กทรอนิกส์ รวมถึงธุรกิจเงินสกุลเข้ารหัส เพื่อให้สามารถเชื่อมโยงข้อมูลทั้งในส่วนธุรกรรมเงินสกุลเข้ารหัส และธุรกรรมทางการเงินทั่วไป

แนวทางที่ 13 มาตรการต้องห้ามผู้ให้บริการรับอนุญาตทำธุรกรรมใดๆที่เกี่ยวข้องกับเงินสกุลเข้ารหัสซึ่งมีความเสี่ยงทางเทคโนโลยี่สูงต่อการใช้เป็นเครื่องมือในการฟอกเงิน เช่น Privacy Coin สกุลเงินต่างๆ ซึ่งมีคุณสมบัติทางเทคโนโลยี่ในความสามารถปกปิดร่องรอยของผู้ทำธุรกรรม เส้นทางธุรกรรม และมูลค่าในกระเป๋าเงิน (Wallet) จึงเป็นการลดภาระต่อการบริการความเสี่ยงในการกำกับธุรกรรมเงินสกุลเข้ารหัสในประเทศไทย อีกทั้งเป็นการลดโอกาสที่อาชญากรจะใช้ Privacy Coin เป็นเครื่องมือในการกระทำผิดหรือในการฟอกเงิน อย่างไรก็ตามสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ได้นำเสนอแนวทางนี้ต่อสาธารณะ และอยู่ระหว่างประเมินผลการรับฟังความคิดเห็นสาธารณะ[29]

4.4.2 ข้อเสนอต่อแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

นอกจากนี้ ผู้วิจัยได้รวบรวมข้อมูลทัศนะเชิงเสนอแนะด้วยความเห็นอิสระจากผู้ให้ข้อมูลสำคัญชุดเดียวกัน ในประเด็นแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม และได้ประมวลข้อมูลพร้อมทั้งสังเคราะห์ความเห็น และจัดกลุ่มแนวคิดได้เป็นข้อเสนอต่อแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม และสามารถเพิ่มประสิทธิภาพในการปฏิบัติงานได้จำนวน 10 แนวปฏิบัติ โดยเสนอตามลำดับความเห็นเสียงส่วนใหญ่ของผู้ให้ข้อมูลสำคัญจากมากไปน้อย ดังนี้

แนวปฏิบัติที่ 1 การพัฒนาองค์ความรู้เกี่ยวกับระบบนิเวศ และการทำธุรกรรมเงินสกุลเข้ารหัสให้แก่เจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบ เนื่องด้วยคุณลักษณะเฉพาะสำคัญของธุรกรรมเงินสกุลเข้ารหัสสามารถใช้งานทำธุรกรรมได้อย่างไม่จำกัดสถานที่และเวลา ในขณะที่กลุ่มบุคคลที่มีองค์ความรู้และความเข้าใจเกี่ยวกับเงินสกุลเข้ารหัสยังอยู่ในวงจำกัด ดังนั้นจึงควรเร่งพัฒนาองค์ความรู้ และเผยแพร่ขยายความรู้สร้างความเข้าใจเกี่ยวกับคุณลักษณะเฉพาะ กลไกการทำงานของธุรกรรมเงินสกุลเข้ารหัสให้แก่เจ้าหน้าที่ผู้มีหน้าที่รับผิดชอบ และเจ้าหน้าที่อื่นที่อาจมีส่วนเกี่ยวข้องทางอ้อม รวมถึงการแลกเปลี่ยนประสบการณ์ทั้งทางตรงและทางอ้อมเป็นกรณีศึกษาให้แก่

[29] เอกสารรับฟังความคิดเห็น เลขที่ อกต. 4/2564 เรื่อง แนวทางการกำกับดูแลเพื่อป้องกันการใช้สินทรัพย์ดิจิทัลเป็นเครื่องมือ กระทำความผิดและแนวทางการกำกับดูแลผู้ให้บริการกระเป๋าสินทรัพย์ดิจิทัลที่รับฝากสินทรัพย์ดิจิทัล (custodial wallet provider) เผยแพร่เมื่อวันที่27 มกราคม 2564
https://www.sec.or.th/Documents/PHS/Main/690/hearing042564.pdf

เจ้าหน้าที่ในกลุ่มหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง เพื่อเป็นการเพิ่มศักยภาพของเจ้าหน้าที่ซึ่งไม่จำกัดเฉพาะเจ้าหน้าที่ปฏิบัติการในส่วนกลาง ยังหมายรวมถึงเจ้าหน้าที่ส่วนภูมิภาคประจำพื้นที่

แนวปฏิบัติที่ 2 การสร้างกลไกความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง ในปัจจุบันบริบทของเงินสกุลเข้ารหัสมีพัฒนาการและพลวัตตลอดเวลา ดังนั้นในการบังคับใช้กฎหมาย จึงมีลักษณะของการปรับใช้อำนาจตามกฎหมายของแต่ละหน่วยงานในการปฏิบัติหน้าที่ตามขอบเขตหน้าที่รับผิดชอบ จึงควรร่วมกันสร้างกลไกระบบประสานความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง เพื่อร่วมกันจัดการลดความทับซ้อนของการปฏิบัติหน้าที่ และแบ่งปันข้อมูลความเชื่อมโยงธุรกรรมต้องสงสัยระหว่างกันให้สามารถติดตามสืบค้นผู้ต้องสงสัย และผู้กระทำความผิดได้อย่างมีประสิทธิภาพ

แนวปฏิบัติที่ 3 การพัฒนาคู่มือแนวปฏิบัติงานที่เกี่ยวข้อง กับกระบวนการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องควรร่วมกันสังเคราะห์ ประมวลขั้นตอนการปฏิบัติงานที่เหมาะสมกับบริบทของกฎหมายปัจจุบัน ในลักษณะการจัดทำความตกลงร่วมเป็นคู่มือมาตรฐานความร่วมมือในการปฏิบัติงานที่เกี่ยวข้องกับกระบวนการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ตั้งแต่ขั้นตอนการกำกับดูแลต้นทางเพื่อการป้องกัน จนถึงขั้นตอนการบังคับคดีปลายทางของกระบวนการยุติธรรม เพื่อเป็นแนวปฏิบัติที่พนักงานเจ้าหน้าที่สามารถดำเนินการได้อย่างคล่องตัวตามแนวทางที่เหมาะสม ซึ่งเป็นการเสริมสร้างความเข้มแข็งในความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมาย

แนวปฏิบัติที่ 4 การสร้างกลไกความร่วมมือระหว่างประเทศ กับหน่วยงานบังคับใช้กฎหมายต่างประเทศ รวมถึงองค์กรระหว่างประเทศที่เกี่ยวข้อง ในปัจจุบันมาตรการทางกฎหมายของแต่ละประเทศที่มีต่อการกำกับดูแลเงินสกุลเข้ารหัสยังมีความแตกต่างกัน ส่งผลต่อมาตรการทางกฎหมายที่บังคับใช้ต่อผู้ให้บริการที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และการทำธุรกรรมเงินสกุลเข้ารหัสมีความแตกต่างกัน รวมถึงหน่วยงานที่มีหน้าที่กำกับดูแลของแต่ละประเทศ ก็จะถูกกำหนดขึ้นตามบริบทของประเทศนั้น ดังนั้นจึงควรสร้างเครือข่ายความร่วมมือกับองค์กรระหว่างประเทศด้านการต่อต้านการฟอกเงิน หรือด้านการสืบสวนคดีทางการเงินระหว่างประเทศ รวมถึงการสร้างกลไกความร่วมมือระหว่างประเทศที่เกี่ยวข้อง กับการป้องกันและปราบปรามเพื่อช่วยเหลือสนับสนุนการปฏิบัติการข้ามประเทศ

แนวปฏิบัติที่ 5 การสร้างกลไกความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องในลักษณะศูนย์ปฏิบัติการเฉพาะกิจ เพื่อการสร้างความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องในสนับสนุนการปฏิบัติงานให้บรรลุเป้าหมายได้อย่างมีประสิทธิภาพ แต่ด้วยข้อจำกัดหรืออุปสรรคในกระบวนการสร้างความร่วมมือ จึงมีข้อเสนอให้สร้างระบบความร่วมมือการทำงานในลักษณะคณะทำงานเฉพาะกิจ หรือศูนย์ปฏิบัติการประสานงานที่บูรณาการหน้าที่

ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง เพื่อสร้างการบริการจัดการอย่างเป็นระบบให้การทำงานเคลื่อนตัวไปในทิศทางเดียวกัน โดยไม่จำเป็นต้องจัดตั้งเป็นองค์ถาวร

แนวปฏิบัติที่ 6 การออกกฎระเบียบเกี่ยวกับกระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย เนื่องด้วยมาตรการทางกฎหมายที่สำคัญต่อการยับยั้งกระบวนการฟอกเงิน คือการยึดอายัดทรัพย์สินของผู้กระทำผิดในกระบวนการฟอกเงิน ในปัจจุบันยังไม่มีมาตรการเกี่ยวกับการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย จึงมีข้อเสนอให้พิจารณาออกกฎระเบียบเกี่ยวกับกระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัยที่ชัดเจนต่อการปฏิบัติงาน โดยมอบหมายหน้าที่แก่หน่วยงานใดหน่วยงานหนึ่งรับผิดชอบดูแลกระเป๋าเงินอิเล็กทรอนิกส์กลางของภาครัฐ (State Wallet) เพื่อการรวบรวม เก็บรักษา และจัดการเงินสกุลเข้ารหัสของกลางในคดี

แนวปฏิบัติที่ 7 การรับฟังความคิดเห็นจากหน่วยงานปฏิบัติการก่อนการบังคับใช้มาตราการต่างๆ ทั้งนี้การออกประกาศมาตรการที่เกี่ยวข้องกับการกำกับเงินสกุลเข้ารหัส ซึ่งเป็นสินทรัพย์ดิจิทัลที่มีลักษณะเกี่ยวเนื่องทั้งด้านเทคโนโลยี เศรษฐกิจ และสังคม ดังนั้นจึงควรจัดให้มีกระบวนการรับฟังความคิดเห็นจากหน่วยงานปฏิบัติการที่เกี่ยวข้อง เพื่อร่วมให้ความเห็นต่อการปรับปรุงแนววิธีการดำเนินงานให้เหมาะสมต่อการปฏิบัติงาน รวมทั้งได้สร้างความเข้าใจแก่หน่วยปฏิบัติการก่อนการออกประกาศมาตรการที่เกี่ยวข้องกับการกำกับเงินสกุลเข้ารหัสนั้น

แนวปฏิบัติที่ 8 การปรับปรุงแนวปฏิบัติ เพื่อการแสวงหาลักษณะพยานหลักฐานทางเทคโนโลยี่ เนื่องกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสบนระบบปฏิบัติการบล็อกเชน จึงสามารถสืบค้นหาร่องรอยเส้นทางธุรกรรมต้องสงสัยของผู้กระทำผิด โดยใช้เครื่องมือทางเทคโนโลยี่โปรแกรมประยุกต์เข้าร่วมวิเคราะห์ข้อมูลจากฐานข้อมูลสาธารณะได้ และด้วยความมั่นคงของระบบการพิสูจน์ยืนยันรายการ จึงควรปรับปรุงแนวปฏิบัติเพื่อการแสวงหาพยานหลักฐานทางเทคโนโลยี่และเส้นทางร่องรอยธุรกรรมบนระบบปฏิบัติการบล็อกเชนที่ยอมรับโดยกฎหมาย เพื่อใช้เป็นพยานหลักฐานในวิธีการพิจารณาคดีได้โดยชอบ

แนวปฏิบัติที่ 9 การใช้เครื่องมือในทางเทคโนโลยี่ ในการตรวจสอบสืบค้นเส้นทางธุรกรรมต้องสงสัย ทั้งนี้เครื่องมือทางเทคโนโลยี่ในการตรวจสอบสืบค้นในลักษณะดังกล่าวอาจเป็นการจัดหาเครื่องมือโดยหน่วยงานเอง หรือพัฒนาขึ้นเองภายในหน่วยงาน หรืออาจเป็นการว่าจ้างบริษัทภายนอกใช้เครื่องมือตรวจสอบทางเทคนิคร่วมกันทำการวิเคราะห์ธุรกรรม เพื่อสืบค้นเส้นทางธุรกรรมต้องสงสัย โดยการเชื่อมต่อกับฐานข้อมูลสาธารณะในระบบปฏิบัติการบล็อกเชนของเงินสกุลเข้ารหัสเป้าหมาย

แนวปฏิบัติที่ 10 การบังคับใช้มาตรการทางกฎหมายอย่างจริงจัง แม้ว่าธุรกรรมเงินสกุลเข้ารหัสจะเป็นนวัตกรรมใหม่ทางเทคโนโลยี่การเงิน แต่มาตรการทางกฎหมายที่บังคับใช้อยู่ในปัจจุบันก็สามารถนำมาตีความปรับใช้เชิงปฏิบัติการได้ เพื่อให้สามารถนำกฎหมายมาบังคับใช้ได้

อย่างรวดเร็ว มีความชัดเจนแน่นอน และใช้บทลงโทษระดับรุนแรง เพื่อให้สังคมได้รับรู้และตระหนักถึงผลร้ายของการกระทำผิด

4.4.3 การสำรวจความเห็นอิสระและการวิเคราะห์โดยเทคนิควิธีเดลฟาย

เมื่อผู้วิจัยได้สังเคราะห์ข้อมูลความเห็นเชิงเสนอแนะจากผู้ให้ข้อมูลสำคัญ ในขั้นตอนการสัมภาษณ์เชิงลึกต่อประเด็นแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส และแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสแล้วนั้น ผู้วิจัยได้ประมวลผลข้อมูลเพื่อจัดทำเป็นแบบสำรวจความเห็นต่อแนวทางและแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ซึ่งได้แสดงไว้ในภาคผนวก ฉ สำหรับการสำรวจความเห็นรอบที่ 2 จากผู้ให้ข้อมูลสำคัญชุดเดียวกันจำนวน 19 ราย โดยได้รับการตอบกลับแบบสำรวจความเห็นจำนวน 18 ราย และผู้วิจัยได้ประมวลผลข้อมูลความเห็นที่ได้รับการตอบกลับพร้อมวิเคราะห์ข้อมูลเชิงสถิติเบื้องต้นของแต่ละข้อเสนอ เพื่อจัดทำเป็นแบบสำรวจฉบับทบทวนหรือยืนยันความเห็น สำหรับการสำรวจความเห็นจากผู้ให้ข้อมูลสำคัญชุดเดียวกันเป็นรอบที่ 3 จำนวน 18 รายและได้รับการตอบกลับแบบสำรวจความเห็นทั้ง 18 ราย

ทั้งนี้ ผู้วิจัยได้ทำการวิเคราะห์ผลการศึกษาโดยวิธีการเดลฟาย ซึ่งได้แสดงไว้ในภาคผนวก ฉ โดยเริ่มต้นจาก **การวิเคราะห์ระดับความคงที่ของความเห็น (Stability)** จากการสำรวจความเห็นในรอบที่ 3 ด้วยการตรวจสอบความเปลี่ยนแปลงของสัดส่วนร้อยละความเห็นของแต่ละข้อเสนอในรอบที่ 2 เมื่อเปรียบเทียบกับรอบที่ 3 ตามรายงานการตรวจสอบระดับความคงที่ (ตารางที่ 2) ผลปรากฏว่า สัดส่วนร้อยละความเห็นของแต่ละข้อเสนอในรอบที่ 2 และเปรียบเทียบกับรอบที่ 3 **ไม่มีความแตกต่างกันเกินกว่าร้อยละ 15.00 ในทุกกรณี** และการทดสอบค่าสถิติ F-Test ของค่าความแปรปรวนของระดับความเห็นของแต่ละข้อเสนอในรอบที่ 2 เทียบกับรอบที่ 3 ณ ระดับนัยสำคัญเท่ากับ 0.05 (α=0.05) โดยมี ค่าสถิติทดสอบ F-test ที่ระดับ 2.3216 (df17,17) ซึ่งผลการทดสอบปรากฏว่า ค่าความแปรปรวนของความเห็นจากการสำรวจในรอบที่ 2 และรอบที่ 3 ของ **ข้อเสนอสำหรับแนวทางและแนวปฏิบัติส่วนใหญ่ แสดงค่าสถิติไม่มีความแตกต่างกันอย่างมีนัยสำคัญ ณ ระดับ 0.05 ถือว่าความเห็นมีระดับความคงที่ ยกเว้นแนวทางที่ 7 มีค่า F-test จากการสำรวจเท่ากับ 2.8362 และแนวปฏิบัติที่ 8 มีค่า F-test เท่ากับ 2.867 ซึ่งมากกว่าค่าสถิติทดสอบ F-test ที่ 2.3216 (df17,17)** ดังนั้นแสดงว่าแนวทางป้องกันที่ 7 และแนวปฏิบัติที่ 8 มีค่าความแปรปรวนของความเห็นจากการสำรวจของทั้งสองรอบ มีความแตกต่างกันอย่างมีนัยสำคัญ หรือแสดงว่าความเห็นจากการสำรวจในรอบที่ 2 และรอบที่ 3 ของข้อเสนอทั้ง 2 ข้อเสนอมีระดับความเห็นที่ยังไม่คงที่ **อย่างไรก็ตามผู้วิจัยได้ยุติการสำรวจความเห็นในรอบต่อไป** เนื่องจากผลการทดสอบแสดงว่า มีข้อเสนอของแนวทางป้องกันจำนวน 12 แนวทางจาก 13 ข้อเสนอ

และแนวปฏิบัติเพื่อการป้องกันจำนวน 9 แนวปฏิบัติจาก 10 ข้อเสนอ มีระดับความคงที่ของความเห็นยกเว้นแนวทางป้องกันที่ 7 และแนวปฏิบัติที่ 8 เท่านั้น ซึ่งคิดเป็นสัดส่วนเพียงร้อยละ 8.70 ของจำนวนข้อเสนอทั้งหมด 23 ข้อเสนอ โดยในขณะที่ทุกข้อเสนอ ไม่มีความแตกต่างกันของความเห็นทั้งสองรอบเกินกว่าร้อยละ 15.0

และผู้วิจัยได้ทำ **การวิเคราะห์ความเป็นฉันทามติ (Consensus)** ของผู้ให้ข้อมูลสำคัญต่อแต่ละข้อเสนอ โดยการตรวจสอบค่าสัมประสิทธิ์การกระจาย (coefficient of variation) ที่คำนวณจากค่าเบี่ยงเบนมาตรฐานหารด้วยค่าเฉลี่ยของระดับความเห็นในรอบที่ 3 **ผลปรากฏว่า ไม่มีข้อเสนอใดที่มีค่าสัมประสิทธิ์การกระจายเกิน 0.5 และการตรวจสอบค่าสัมบูรณ์ของผลต่างระหว่างค่ามัธยฐานและค่าฐานนิยมของความเห็นในรอบที่ 3** ตามรายงานการตรวจสอบความเป็นฉันทามติ (ตารางที่ 3) **ผลปรากฏว่า ไม่มีข้อเสนอใดมีค่าเกิน 1.00 และการตรวจสอบค่าพิสัยระหว่างควอไทล์ของความเห็นในรอบที่ 3 ผลปรากฏว่า ข้อเสนอส่วนใหญ่มีค่าพิสัยระหว่างควอไทล์ไม่เกิน 1.50 ยกเว้นบางข้อเสนอ** กล่าวคือแนวทางป้องกันที่ 4 มีค่าเท่ากับ 1.75, แนวทางป้องกันที่ 10 มีค่าเท่ากับ 2.00, แนวทางป้องกันที่ 12 มีค่าเท่ากับ 1.50 และแนวทางป้องกันที่ 13 มีค่าเท่ากับ 1.75 นอกจากนี้ ยังปรากฏว่า มีแนวปฏิบัติที่ 4 มีค่าเท่ากับ 2.00 และแนวปฏิบัติที่ 10 มีค่าเท่ากับ 2.00 **ดังนั้นจึงสรุปผลได้ว่า ข้อเสนอแนวทางป้องกัน และแนวปฏิบัติเพื่อการป้องกันส่วนใหญ่ได้รับความเห็นอย่างเป็นฉันทามติจากผู้ให้ข้อมูลสำคัญ ยกเว้นแนวทางการป้องกันที่ 4, 10, 12, 13 และแนวปฏิบัติเพื่อการป้องกันที่ 4, 10**

จากนั้น ได้วิเคราะห์ระดับความเห็นเฉพาะข้อเสนอที่ผ่านเกณฑ์ได้รับฉันทามติจากผู้ให้ข้อมูลสำคัญข้างต้น กล่าวคือ ยกเว้นข้อเสนอแนวทางการป้องกันที่ 4,10, 12, 13 และแนวปฏิบัติเพื่อการป้องกันที่ 4, 10 เพื่อสรุปความเห็นต่อแต่ละข้อเสนอด้วย **การวิเคราะห์เกณฑ์ฉันทามติเสียงข้างมาก (Majority of Consensus)** โดยการตรวจสอบค่าเฉลี่ยของระดับความเห็นตั้งแต่ 4.00 ขึ้นไป และค่ามัธยฐานของระดับความเห็นตั้งแต่ 4.00 ขึ้นไป ตามรายงานการวิเคราะห์ความเห็นต่อข้อเสนอเกณฑ์ฉันทามตีเสียงข้างมาก (ตารางที่ 4) ผลปรากฏว่า **ทุกข้อเสนอแนวทางป้องกันมีค่าเฉลี่ยและค่ามัธยฐานตั้งแต่ 4.00 ขึ้นไป และแนวปฏิบัติเพื่อการป้องกันส่วนใหญ่มีค่าเฉลี่ยและค่ามัธยฐานตั้งแต่ 4.00 ขึ้นไป ยกเว้นบางข้อเสนอ** กล่าวคือแนวปฏิบัติที่ 5 มีค่าเฉลี่ย และค่ามัธยฐานเท่ากันที่ 3.50 สำหรับการตรวจสอบค่าผลรวมสัดส่วนร้อยละของความเห็นระดับ 5 (“มากที่สุด”) และระดับ 4 (“มาก”) ด้วยเกณฑ์ตั้งแต่ร้อยละ 75.00 ขึ้นไป **ผลปรากฏว่า ทุกข้อเสนอแนวทางป้องกันมีค่าผลรวมสัดส่วนระดับมากและมากที่สุดตั้งแต่ร้อยละ 75.00 ขั้นไป และแนวปฏิบัติเพื่อการป้องกันส่วนใหญ่ มีค่าผลรวมสัดส่วนระดับมากและมากที่สุดตั้งแต่ร้อยละ 75.00 ขั้นไป ยกเว้นบางข้อเสนอ** กล่าวคือ แนวปฏิบัติที่ 3 มีค่าผลรวมร้อยละ 72.22 และแนวปฏิบัติที่ 5 มีค่าผลรวมร้อยละ 50.0 ดังนั้น ข้อเสนอแนวทางป้องกันที่ได้รับฉันทามติเสียงข้างมาก และถือเป็น

ข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลที่ มีความเหมาะสมอย่างมากจำนวน 9 แนวทาง ประกอบด้วย แนวทางป้องกันที่ 1, 2, 3, 5, 6, 7, 8, 9 และ 11 สำหรับแนวปฏิบัติได้รับฉันทามติเสียงข้างมาก และถือเป็นข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่มีความเหมาะสมอย่างมากจำนวน 6 แนวปฏิบัติ ประกอบด้วย แนวปฏิบัติที่ 1, 2, 6, 7, 8, และ 9 **ส่วนแนวปฏิบัติที่ 3 และ 5 ได้รับฉันทามติเสียงข้างน้อย จึงถือว่า เป็นการให้ความเห็นพ้องเชิงปฏิเสธต่อแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินว่าไม่เหมาะสมต่อการนำมาบังคับใช้**

4.4.4 สรุปผลการศึกษาข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม รวมถึงข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินที่เหมาะสมและเพิ่มประสิทธิภาพในการบังคับใช้เชิงปฏิบัติการ

จากผลการศึกษาความเห็นเชิงเสนอแนะจากผู้ให้ข้อมูลสำคัญ โดยเทคนิควิธีเดลฟายปรากฏว่า มีข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่ได้รับฉันทามติเสียงข้างมากจำนวน 9 แนวทาง ซึ่งแสดงให้เห็นว่า **เป็นมาตรการป้องกันและปราบปรามที่ผู้ให้ข้อมูลสำคัญมีความเห็นว่าเหมาะสมต่อการนำไปบังคับใช้** โดยเสนอตามลำดับความเห็นเสียงส่วนใหญ่ของผู้ให้ข้อมูลสำคัญจากมากไปน้อย ดังนี้

(1) แนวทางที่ 1 กระบวนการตรวจพิสูจน์ตัวตนของผู้ใช้งาน (KYC – Know Your Customer) นั้น ควรกำหนดหลักเกณฑ์มาตรฐานสำหรับการบันทึกข้อมูลเพื่อการตรวจพิสูจน์ตัวตนผู้ใช้งานอย่างเพียงพอก่อนอนุญาตให้เข้าใช้ระบบงาน รวมถึงกำหนดมาตรการตรวจสอบและทบทวนข้อมูลส่วนบุคคลของผู้ใช้งานให้ทันสมัยอย่างสม่ำเสมอ เพื่อเป็นฐานข้อมูลสำคัญในการตรวจสอบตัวตนของเจ้าของกระเป๋าเงินหรือผู้ใช้งาน เมื่อต้องการสืบค้นธุรกรรมที่อาจเข้าข่ายต้องสงสัย

(2) แนวทางที่ 2 การเผยแพร่องค์ความรู้เกี่ยวกับเงินสกุลเข้ารหัสให้แก่สาธารณชน โดยควรจัดรวบรวมสาระองค์ความรู้เกี่ยวกับคุณลักษณะเฉพาะ กลไกการทำงานของเงินสกุลเข้ารหัส และความเสี่ยงที่อาจเกิดขึ้นจากการทำธุรกรรมเงินสกุลเข้ารหัส เพื่อเผยแพร่ส่งเสริมความรู้ให้แก่สาธารณะ ประชาชนทั่วไปได้เข้าใจถึงประโยชน์ของระบบนิเวศเงินสกุลเข้ารหัส และการป้องกันตนเองจากความเสี่ยงที่อาจตกเป็นเหยื่อของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส

(3) แนวทางที่ 6 การออกกฎระเบียบในการกำกับธุรกรรม และผู้ให้บริการเงินสกุลเข้ารหัสควรอ้างอิงกับแนวทางหรือข้อแนะนำตามหลักมาตรฐานการปฏิบัติงานสากล เช่น FATF Recommendations เพื่อเป็นบรรทัดฐานการปฏิบัติงานร่วมกันในกรณีที่มีความจำเป็นต้องประสาน

ขอความร่วมมือในการตรวจสอบสืบค้นผู้ต้องสงสัยกับฐานข้อมูลระหว่างประเทศ รวมถึงความร่วมมือในการสร้างระบบการป้องกันการฟอกเงินโดยธุรรมเงินสกุลเข้ารหัส

(4) แนวทางที่ 7 การสร้างเครือข่ายความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง ทั้งด้านการปฏิบัติงานว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และด้านการกำกับดูแลการกิจกรรมด้านเทคโนโลยี่การเงินเพื่อเศรษฐกิจและสังคม เช่น สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ธนาคารแห่งประเทศไทย สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานอัยการ กรมสรรพากร กรมบังคับคดี สำนักงานคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และโทรคมนาคมแห่งชาติ เป็นต้น เพื่อเสริมสร้างประสิทธิภาพในการป้องปราม และตรวจสอบสืบค้นได้ทันต่อการโยกย้ายธุรกรรมเงินสกุลเข้ารหัสในระบบไซเบอร์

(5) แนวทางที่ 3 การสร้างกรอบความร่วมมือระหว่างประเทศ เพื่อการต่อต้านการฟอกเงิน โดยการประสานความร่วมมือในการแลกเปลี่ยนข้อมูลสำคัญ ด้านระบบนิเวศเงินสกุลเข้ารหัส พัฒนาการเทคโนโลยี่การสืบค้นผู้ต้องสงสัย รวมถึงองค์ความรู้ประสบการณ์กรณีศึกษาการกระทำความผิดที่เกี่ยวข้องกับการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เพื่อเสริมสร้างทักษะของผู้ปฏิบัติงานในการประสานงานระหว่างประเทศได้เท่าทันกับการเคลื่อนไหวของอาชญากร

(6) แนวทางที่ 11 การออกกฎระเบียบปฏิบัติในกระบวนการสืบสวนเกี่ยวข้องกับบริบทธุรกรรมเงินสกุลเข้ารหัสอย่างชัดเจน เช่น ลักษณะพยานหลักฐานดิจิทัลที่ระบุในระบบนิเวศเงินสกุลเข้ารหัส การสืบสวนที่อาจต้องเข้าถึงหลักฐานซึ่งเป็นกระเป๋าเงินของอาชญากร การยึดอายัดเงินสกุลเข้ารหัสต้องสงสัยโดยมีกฎหมายรองรับ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

(7) แนวทางที่ 5 การออกกฎระเบียบเพื่อการกำกับการทำธุรกรรมเงินสกุลเข้ารหัสหรือผู้ให้บริการรับอนุญาตที่เกี่ยวข้องกับเงินสกุลเข้ารหัส ควรคำนึงถึงการสร้างความสมดุลระหว่างประโยชน์สาธารณะที่จะได้รับจากความคล่องตัวทางธุรกิจ และลดต้นทุนการทำธุรกรรมกับการสร้างภาระและข้อจำกัดในการดำเนินธุรกิจเพื่อการป้องกันอาชญากรรม ทั้งนี้เพื่อไม่ให้ผู้ใช้งานในประเทศหลีกเลี่ยงไปใช้บริการกับผู้ให้บริการนอกระบบ หรือผู้ให้บริการต่างประเทศที่มีความคล่องตัวมากกว่า

(8) แนวทางที่ 8 การบูรณาการหน่วยงานหลักที่รับผิดชอบร่วมทำงานแบบองค์รวมเพื่อร่วมกันกำหนดแผนปฏิบัติงานตามลำดับขั้นตอนลดการปฏิบัติงาน ที่อาจทับซ้อนของขอบเขตหน้าที่รับผิดชอบ ทั้งนี้อาจเพิ่มประสิทธิภาพการปฏิบัติงาน โดยมีการจัดตั้งคณะทำงานเฉพาะกิจ หรือแต่งตั้งผู้เชี่ยวชาญเป็นที่ปรึกษาให้การสนับสนุนเชิงเทคนิคและแนวทางในการปฏิบัติงาน

(9) แนวทางที่ 9 การสร้างความร่วมมือขององค์กรผู้ให้บริการภาคเอกชนที่เกี่ยวข้องกับธุรกิจเงินสกุลเข้ารหัสเพื่อส่งเสริมพัฒนาการ และการสร้างความแข็งแกร่งในกำกับดูแลผู้ประกอบการกันเองภายในอุตสาหกรรมเงินสกุลเข้ารหัส และเพิ่มประสิทธิภาพการประสานความร่วมมือกับหน่วยงานรัฐ ในทำนองเดียวกับสมาคมธนาคารไทย สมาคมบริษัทหลักทรัพย์ หรือสมาคมผู้ประกอบธุรกิจการเงินอื่น

และผู้ให้ข้อมูลสำคัญได้แสดงความเห็นอย่าง**ไม่เป็นฉันทามติ** ต่อข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ซึ่งแสดงให้เห็นว่า**แนวทางป้องกันที่จะกล่าวถึงต่อไปนี้ เป็นข้อเสนอที่ยังไม่ได้รับความเห็นพ้องร่วมกันจากผู้ให้ข้อมูลสำคัญอย่างเพียงพอโดยความเห็นเสียงส่วนใหญ่ ต่อการรับรองให้เป็นแนวทางที่เหมาะสมใน การนำไปบังคับใช้** มี 4 แนวทาง ตามลำดับจากมากไปน้อย ดังนี้

(1) แนวทางที่ 4 การส่งเสริมศักยภาพการแข่งขันให้แก่ผู้ให้บริการรับอนุญาตเพื่อให้สามารถอำนวยความสะดวกในการทำธุรกรรมเงินสกุลเข้ารหัสให้แก่ผู้ใช้งาน และสร้างแรงจูงใจแก่ผู้ใช้งานให้เลือกใช้บริการกับผู้ให้บริการรับอนุญาต มากกว่าการใช้บริการกับผู้ให้บริการนอกระบบหรือผู้ให้บริการต่างประเทศ

(2) แนวทางที่ 12 การสร้างระบบจัดการฐานข้อมูลกลางของการแสดงตัวตนผู้ใช้งานในลักษณะ KYC Bureau ในทำนองเดียวกับเครดิตบูโรของระบบสถาบันการเงิน ซึ่งทำหน้าที่รวบรวมข้อมูลส่วนบุคคลการใช้บริการด้านสินเชื่อจากผู้ให้บริการทางการเงินทุกประเภท และปรับปรุงข้อมูลร่วมกันให้ทันสมัยตลอดเวลา เพื่อให้สามารถเชื่อมโยงข้อมูลตัวตนผู้ใช้งานทั้งในส่วนธุรกรรมเงินสกุลเข้ารหัสและธุรกรรมทางการเงินทั่วไป

(3) แนวทางที่ 13 มาตรการห้ามผู้ให้บริการรับอนุญาตทำธุรกรรมใดๆที่เกี่ยวข้องกับเงินสกุลเข้ารหัสที่มีความเสี่ยงทางเทคโนโลยีต่อการใช้เป็นเครื่องมือในการฟอกเงินสูง ซึ่งสามารถปกปิดร่องรอยของผู้ทำธุรกรรม เส้นทางธุรกรรม และมูลค่าในกระเป๋าเงิน (Wallet) ได้

(4) แนวทางที่ 10 มาตรการกำหนดให้ผู้ใช้งานต้องทำธุรกรรมเฉพาะกับผู้ให้บริการรับอนุญาตในประเทศ และหากประสงค์จะทำธุรกรรมข้ามประเทศก็กำหนดให้ดำเนินการเฉพาะกับผู้ให้บริการที่ได้รับอนุญาตของประเทศนั้นๆ

อย่างไรก็ตาม **ผู้วิจัยมีความเห็นว่าควรนำข้อเสนอแนวทางป้องกันบางข้อเสนอที่ไม่ได้รับความเห็นอย่างฉันทามติเสียงข้างมากจากผู้ให้ข้อมูลสำคัญ มาพิจารณาทบทวนให้เป็นข้อเสนอแนวทางการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม** จำนวน 2 แนวทาง ได้แก่

(1) แนวทางที่ 4 การส่งเสริมศักยภาพการแข่งขันให้แก่ผู้ให้บริการรับอนุญาต เพื่อให้สามารถอำนวยความสะดวกในการทำธุรกรรมเงินสกุลเข้ารหัสให้แก่ผู้ใช้งาน และสร้างแรงจูงใจแก่ผู้ใช้งานให้เลือกใช้บริการกับผู้ให้บริการรับอนุญาต มากกว่าการใช้บริการกับผู้ให้บริการนอกระบบหรือผู้ให้บริการต่างประเทศ ซึ่งเป็นยุทธวิธีสำคัญในการแยกกลุ่มผู้ใช้งานสุจริตออกจากกลุ่มอาชญากร เพราะถ้าการให้บริการของผู้ให้บริการรับอนุญาตสร้างภาระข้อจำกัดมาก จนผู้ใช้งานสุจริตไปทำธุรกรรมนอกระบบมากขึ้น ก็จะกลับเป็นการสร้างภาระให้แก่หน่วยงานบังคับใช้กฎหมายในท้ายที่สุด

(2) แนวทางที่ 12 การสร้างระบบจัดการฐานข้อมูลกลางของการแสดงตัวตนผู้ใช้งานในลักษณะ KYC Bureau ในทำนองเดียวกับเครดิตบูโรของสถาบันการเงิน โดยรวบรวมข้อมูลส่วนบุคคลของผู้ใช้งานจากผู้ให้บริการทางการเงินทุกประเภท เพื่อให้สามารถเชื่อมโยงข้อมูลตัวตนผู้ใช้งานทั้งในส่วนธุรกรรมทางการเงินทั่วไปและธุรกรรมเงินสกุลเข้ารหัส ซึ่งจะทำให้หน่วยงานบังคับใช้กฎหมายสามารตรวจสอบสืบค้นผู้ต้องสัยได้ด้วยความรวดเร็ว และสามารถเชื่อมโยงเข้าถึงบุคคลและกลุ่มบุคคลต้องสงสัยได้โดยสะดวก แม้ว่าอาจมีข้อกังวลในประเด็นกฎหมายการปกป้องสิทธิข้อมูลส่วนบุคคล แต่ด้วยการดำเนินการย่อมต้องปฏิบัติตามขั้นตอนของกฎหมาย และผู้มีสิทธิเข้าถึงข้อมูลดังกล่าวก็เป็นเฉพาะหน่วยงานบังคับใช้กฎหมายเท่านั้น

สำหรับผลการศึกษาความเห็นเชิงเสนอแนะจากผู้ให้ข้อมูลสำคัญ ต่อแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสนั้น ปรากฏว่า ข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ที่ได้รับความเห็นอย่างเป็นฉันทามติเสียงข้างมากจำนวน 6 แนวปฏิบัติ ซึ่งแสดงให้เห็นว่าเป็น **แนวปฏิบัติเพื่อการป้องกันที่ผู้ให้ข้อมูลสำคัญเห็นว่าเหมาะสมต่อการนำไปบังคับใช้** ซึ่งได้อธิบายตามลำดับความเห็นโดยเสียงส่วนใหญ่ของผู้ให้ข้อมูลสำคัญจากมากไปน้อย ดังนี้

(1) แนวปฏิบัติที่ 1 ซึ่งเป็นแนวปฏิบัติที่ได้รับฉันทามติอย่างเป็นเอกฉันท์จากผู้ให้ข้อมูลสำคัญทุกท่าน ในการพัฒนาองค์ความรู้เกี่ยวกับระบบนิเวศ และการทำธุรกรรมเงินสกุลเข้ารหัส รวมถึงการแลกเปลี่ยนประสบการณ์ทั้งทางตรงและทางอ้อมเป็นกรณีศึกษาให้แก่ ผู้มีหน้าที่รับผิดชอบตามกฎหมายและเจ้าหน้าที่อาจมีส่วนเกี่ยวข้อง เพื่อเพิ่มศักยภาพให้แก่หน่วยงานบังคับใช้กฎหมายโดยไม่จำกัดเฉพาะบุคคลากรในส่วนกลาง ยังให้หมายรวมถึงเจ้าหน้าที่ส่วนภูมิภาคประจำพื้นที่

(2) แนวปฏิบัติที่ 2 การสร้างกลไกความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง เพื่อร่วมกันจัดการลดความทับซ้อนของการปฏิบัติหน้าที่ และแบ่งปันข้อมูลความเชื่อมโยงธุรกรรมต้องสงสัยระหว่างกันให้สามารถติดตามสืบค้นผู้ต้องสงสัย และผู้กระทำผิดได้อย่างมีระสิทธิภาพ

(3) แนวปฏิบัติที่ 7 การรับฟังความคิดเห็นจากหน่วยงานปฏิบัติการที่เกี่ยวข้องก่อนการออกประกาศมาตรการที่เกี่ยวข้อง กับการกำกับเงินสกุลเข้ารหัสซึ่งมีลักษณะเกี่ยวเนื่อง ทั้งด้านเทคโนโลยี เศรษฐกิจและสังคม เพื่อได้สร้างความเข้าใจต่อแจตนารมย์ของมาตรการ และร่วมแสดงความเห็นต่อวิธีการดำเนินงานที่เหมาะสมต่อการปฏิบัติงาน

(4) แนวปฏิบัติที่ 8 การปรับปรุงแนวปฏิบัติเพื่อการแสวงหาหลักฐานทางเทคโนโลยีจากการสืบค้นหาร่องรอยเส้นทางธุรกรรมต้องสงสัย โดยใช้โปรแกรมประยุกต์เข้าร่วมวิเคราะห์ข้อมูลจากฐานข้อมูลแบบกระจายศูนย์ในระบบนิเวศเงินสกุลเข้ารหัส เพื่อให้ได้มาซึ่งการพิสูจน์พยานหลักฐานในวิธีการพิจารณาคดีได้โดยชอบ

(5) แนวปฏิบัติที่ 9 การใช้เครื่องมือในทางเทคโนโลยีในการตรวจสอบสืบค้นเส้นทางธุรกรรมต้องสงสัย ซึ่งอาจเป็นการจัดหาเครื่องมือโดยหน่วยงานเอง หรือพัฒนาขึ้น และอาจเป็นการว่าจ้างบริษัทตรวจสอบทางเทคนิคภายนอกร่วมทำการวิเคราะห์ธุรกรรม เพื่อสืบค้นเส้นทางธุรกรรมต้องสงสัย

(6) แนวปฏิบัติที่ 6 การออกกฎระเบียบเกี่ยวกับ กระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย เพื่อยับยั้งกระบวนการฟอกเงินโดยธุรกรรมเข้าสกุลเข้ารหัส โดยมอบหมายหน้าที่แก่หน่วยงานหนึ่งรับผิดชอบดูแลกระเป๋าเงินอิเล็กทรอนิกส์กลางของรัฐ (State Wallet) เพื่อการรวบรวม เก็บรักษา และจัดการเงินสกุลเข้ารหัสของกลางในคดี

ในขณะเดียวกัน ผู้ให้ข้อมูลสำคัญได้ให้ความเห็นอย่างเป็นฉันทามติแต่ไม่ถึงระดับความเห็นเป็นเสียงข้างมากต่อข้อเสนอแนวปฏิบัติเพื่อการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสจำนวน 2 แนวปฏิบัติ ซึ่งแสดงให้เห็นว่าเป็น **แนวปฏิบัติเพื่อการป้องกันที่ผู้ให้ข้อมูลสำคัญมีความเห็นพ้องเชิงปฏิเสธ ว่าเป็นข้อเสนอแนวปฏิบัติที่ไม่เหมาะสมต่อการนำไปบังคับใช้ในทางปฏิบัติ** มี 2 แนวปฏิบัติ ดังนี้

(1) แนวปฏิบัติที่ 3 การพัฒนาคู่มือแนวปฏิบัติงานที่เกี่ยวข้องกับกระบวนการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องควรร่วมทำความตกลงเป็นคู่มือมาตรฐานในการปฏิบัติงาน ตั้งแต่ขั้นตอนการกำกับดูแลต้นทางเพื่อการป้องกันจนถึงขั้นตอนการบังคับคดีปลายทางของกระบวนการยุติธรรม

(2) แนวปฏิบัติที่ 5 การสร้างกลไกความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องในลักษณะศูนย์ปฏิบัติการเฉพาะกิจ เพื่อสร้างการบริการจัดการอย่างเป็นระบบทำให้การทำงานเคลื่อนตัวไปในทิศทางเดียวกันโดยไม่จำเป็นต้องจัดตั้งเป็นองค์ถาวร

นอกจากนี้ผู้ให้ข้อมูลสำคัญได้แสดงความเห็นอย่างไม่เป็นฉันทมติต่อบางข้อเสนอ ซึ่งแสดงว่า **แนวปฏิบัติเพื่อป้องกันดังกล่าวยังไม่ได้รับความเห็นร่วมกันจากผู้ให้ข้อมูลสำคัญอย่างเพียงพอโดยเสียงข้างมากต่อการรับรองให้เป็นแนวปฏิบัติที่เหมาะสม** มี 2 แนวปฏิบัติ ดังนี้

(1) แนวปฏิบัติที่ 4 การสร้างกลไกความร่วมมือระหว่างประเทศกับหน่วยงานบังคับใช้กฎหมายต่างประเทศ รวมถึงองค์กรระหว่างประเทศที่เกี่ยวข้องกับการต่อต้านการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสในด้านการสืบสวนคดีทางการเงินระหว่างประเทศ รวมถึงการสนับสนุนการปฏิบัติการข้ามประเทศ

(2) แนวปฏิบัติที่ 10 การบังคับใช้มาตรการทางกฎหมายอย่างจริงจัง รวดเร็ว มีความชัดเจนแน่นอน และใช้บทลงโทษระดับรุนแรง เพื่อให้สังคมได้รับรู้และตระหนักถึงผลร้ายของการกระทำผิด

ทั้งนี้ จากผลการศึกษาข้อเสนอแนวทางการป้องกันและแนวปฏิบัติเพื่อการป้องกันโดยความเห็นเชิงเสนอแนะของผู้ให้ข้อมูลสำคัญข้างต้นนั้น **ปรากฏว่ามีความเห็นอย่างฉันทามติเสียงข้างมากต่อข้อเสนอแนวทางการป้องกันบางกรณี ที่อาจขัดแย้งหรือไม่สอดคล้องกับความเห็นต่อแนวปฏิบัติเพื่อการป้องกัน** ได้แก่

(1) แนวทางที่ 3 ได้รับความเห็นอย่างฉันทามติเสียงข้างมาก ในการสร้างกรอบความร่วมมือระหว่างประเทศ เพื่อการต่อต้านการฟอกเงินโดยการประสานความร่วมมือในการแลกเปลี่ยนข้อมูลสำคัญด้านระบบนิเวศเงินสกุลเข้ารหัส พัฒนาการเทคโนโลยีการสืบค้นผู้ต้องสงสัย รวมถึงองค์ความรู้ประสบการณ์ ในขณะที่แนวปฏิบัติที่ 4 ไม่ได้รับความเห็นจากผู้ให้ข้อมูลสำคัญอย่างเพียงพอต่อการรับรองเป็นแนวปฏิบัติที่เหมาะสม ในการสร้างกลไกความร่วมมือระหว่างประเทศกับหน่วยงานบังคับใช้กฎหมายต่างประเทศ รวมถึงองค์กรระหว่างประเทศที่เกี่ยวข้องกับการต่อต้านการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสในด้านการสืบสวนคดีทางการเงินระหว่างประเทศ และการสนับสนุนการปฏิบัติการข้ามประเทศ ทั้งนี้จึงอาจสรุปความเห็นได้ว่า มีความจำเป็นในการสร้างกรอบความร่วมมือระหว่างประเทศ แต่อาจไม่เหมาะสมหากจะให้สร้างความร่วมมือจนถึงขั้นสนับสนุนการสืบสวนคดีและการปฏิบัติการข้ามประเทศซึ่งอาจกระทบต่ออำนาจอธิปไตยของประเทศ

(2) แนวทางที่ 7 และแนวทางที่ 8 ได้รับความเห็นอย่างฉันทามติเสียงข้างมาก ในการสร้างเครือข่ายความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง ทั้งด้านการปฏิบัติงานว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และด้านการกำกับดูแลการกิจกรรมด้านเทคโนโลยีการเงินเพื่อเศรษฐกิจและสังคม เพื่อเสริมสร้างประสิทธิภาพในการป้องปรามและตรวจสอบสืบค้นได้ทันต่อการโยกย้ายธุรกรรมเงินสกุลเข้ารหัสในระบบไซเบอร์ และในการบูรณาการหน่วยงานหลักที่

รับผิดชอบร่วมทำงานแบบองค์รวม เพื่อร่วมกันกำหนดแผนปฏิบัติงานตามลำดับขั้นตอน ลดการปฏิบัติงานที่อาจทับซ้อนของขอบเขตหน้าที่รับผิดชอบ ซึ่งมีความเห็นไม่สอดคล้องกับความเห็นต่อแนวปฏิบัติที่ 5 ซึ่งไม่ได้รับความเห็นจากผู้ให้ข้อมูลสำคัญอย่างเพียงพอต่อการรับรองเป็นแนวปฏิบัติที่เหมาะสม ในการสร้างกลไกความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องในลักษณะศูนย์ปฏิบัติการเฉพาะกิจ ทั้งนี้จึงอาจสรุปความเห็นได้ว่า การสร้างเครือข่ายความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องมีความจำเป็น และเป็นประโยชน์ต่อการเพิ่มประสิทธิภาพปฏิบัติงาน แต่ไม่มีความเหมาะสมที่จะจัดตั้งกระบวนการทำงานเป็นรูปแบบศูนย์ปฏิบัติการเฉพาะกิจ

4.5 การอภิปรายผลการศึกษา

ผลการศึกษาเรื่อง “แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส” ที่ได้นำเสนอข้างต้น ผู้วิจัยได้อภิปรายประเด็นที่น่าสนใจจากการศึกษา ดังนี้

4.5.1 กระบวนทัศน์ต่อมุมมองเงินสกุลเข้ารหัสกับความเป็นเงินตรา และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัสที่เหมาะสมต่อบริบทของประเทศไทย

กระบวนทัศน์ต่อความสงบเรียบร้อยในสังคมและความมั่งคงทางเศรษฐกิจแห่งรัฐนั้น เงินตรา (Currency) หมายถึง วัตถุ หรือสิ่งของซึ่งมนุษย์กำหนดขึ้น และเป็นที่ยอมรับกันโดยทั่วไปเพื่อวัตถุประสงค์ใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการระหว่างกัน (A Medium of Exchange) ภายใต้ฉันทามติของคนในขอบเขตแห่งสังคมนั้น เช่น เปลือหอย เครื่องปันดินเผา โลหะ ทองคำ รวมถึงธนบัตรกระดาษ เป็นต้น อีกทั้งเงินตรายังมีวัตถุประสงค์ใช้เป็นหน่วยวัดมูลค่าสินค้าและบริการ (A Unit of Account) และเพื่อการดำรงรักษาสะสมความมั่งคั่งทางเศรษฐกิจ (A Store of Value) โดยรัฐบาลของแต่ประเทศเป็นผู้มีอำนาจที่ชอบด้วยกฎหมายในการรับประกันการคงมูลค่าของเงินตราเพื่อเป็นสื่อกลางในการชำระหนี้ และการบริหารนโยบายปริมาณเงินตราที่ใช้หมุนเวียนในระบบการเงินเพื่อรักษาเสถียรภาพทางเศรษฐกิจของประเทศ ปัจจุบันสังคมโลกในบริบทโลกาภิวัตส่งผลให้เกือบทุกประเทศมีการติดต่อปฏิสัมพันธ์ทั้งทางการค้าและวัฒนธรรม ซึ่งมีการแลกเปลี่ยนผลผลิตและบริการระหว่างประเทศกันเป็นปกติธุระ เงินตราจึงถูกขยายขอบเขตการยอมรับเพื่อเป็นการชำระหนี้ค่าสินค้าและบริการแก่บุคคลนอกราชอาณาจักร ในลักษณะเงินตราต่างประเทศที่ชอบด้วยกฎหมายภายใต้ระบบกฎหมายระหว่างประเทศ ในการรับรองอำนาจอันชอบธรรมของแต่ละอาณาเขตประเทศ รวมถึงการรับรองในระดับสากลขององค์กรการเงินระหว่างประเทศ (IMF) ซึ่งทำ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

หน้าที่ให้การรับรอง ความเป็นเงินตราของประเทศหนึ่งไปใช้ในการชำระหนี้นอกเขตประเทศโดยชอบด้วยกฎหมาย

ทั้งนี้ เงินสกุลเข้ารหัสซึ่งมีคุณลักษณเฉพาะ เป็นรหัสข้อมูลอิเล็กทรอนิกส์ในลักษณะสินทรัพย์ไร้รูปร่าง ที่สามารถทำการโอนมูลค่าระหว่างผู้ใช้งานกันโดยตรงข้ามเขตประเทศแบบไร้พรมแดนในระบบนิเวศบนระบบปฏิบัติการบล็อกเชนโดยไม่หน่วยงานตัวกลางใดกำกับ แต่ระบบนิเวศเงินสกุลเข้ารหัสมีกระบวนการสร้างความน่าเชื่อถือ และการยอมรับของผู้ใช้งานด้วยระบบพิสูจน์ยืนยันรายการแบบกระจายศูนย์ ดังนั้นเมื่อวิเคราะห์ความเป็นเงินตราของเงินสกุลเข้ารหัสในกระบวนทัศน์ต่อความมั่นคงแห่รัฐเยี่ยงปัจจุบัน ย่อมเป็นความยากที่รัฐบาลไทยจะให้การรับรองความเป็นเงินตราที่ชอบด้วยกฎหมายแก่เงินสกุลเข้ารหัส เนื่องจากคุณลักษณะที่เป็นสินทรัพย์ไร้รูปร่าง ไม่มีหน่วยงานกลางใดหรือโดยอำนาจของรัฐใด ในการกำกับดูแลการหมุนเวียนธุรกรรมเงินสกุลเข้ารหัสได้ อีกทั้ง ความผันผวนเชิงมูลค่าของเงินสกุลเข้ารหัสที่เปลี่ยนแปลงไปตามปริมาณความต้องการถือครองหรือการแลกเปลี่ยนภายในระบบนิเวศในแต่ละช่วงเวลา ในขณะที่ปริมาณเงินสกุลเข้ารหัสมีจำนวนจำกัดชัดเจนตามที่ระบุใน White Paper จึงส่งผลต่อเสถียรภาพด้านราคาของเงินสกุลเข้ารหัสในการใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการ รวมถึงการใช้เป็นหน่วยวัดมูลค่าของสินค้าและบริการที่ขาดความเสถียร และขาดความมั่นคงในการรักษาสะสมความมั่งคั่งทางเศรษฐกิจสำหรับอนาคต อีกทั้งเป็นการขัดต่อพระราชบัญญัติเงินตรา ปี 1958 (พ.ศ.2501) มาตรา 9 *“ห้ามมิให้ผู้ใด ทำ จำหน่าย ใช้ หรือนำออกใช้ซึ่งวัตถุหรือเครื่องหมายใด ๆ แทนเงินตราเว้นแต่จะได้รับอนุญาตจากรัฐมนตรี”*

อย่างไรก็ตาม หากทำการวิเคราะห์เงินสกุลเข้ารหัสในกระบวนทัศน์ของกลุ่มบุคคลที่ปฏิเสธการผูกขาดการให้บริการทางการเงินโดยระบบสถาบันการเงินที่ถูกควบคุมจากอำนาจรัฐ ตามแนวคิดวัตถุนิยมวิภาษวิธีแนวมาร์กซิส ดังปรากฏการณ์ที่แสดงให้เห็นถึงเหตุผลโดยชอบในการปฏิเสธระบบผูกขาดทางการเงิน จากปัญหาวิกฤติเศรษฐกิจครั้งสำคัญที่เกิดขึ้นกับอุตสาหกรรมการเงินของสหรัฐอเมริกาในปี 2008 สถาบันการเงินรายใหญ่ของสหรัฐและเป็นรายใหญ่ของโลกหลายแห่งประสบปัญหาด้านการประกอบกิจการที่เข้าข่ายอาจล้มละลาย จากสาเหตุในการปล่อยสินเชื่อที่อยู่อาศัย (Subprime) อย่างไร้ความรับผิดชอบ รวมถึงการสร้างนวัตกรรมทางการเงินบนสินเชื่อดังกล่าวเพื่อหมุนเวียนสร้างกำไรต่อและจัดสรรผลประโยชน์แก่กลุ่มของตน จนกลายเป็นชนวนเหตุสำคัญที่สร้างความเสียหายแก่ระบบเศรษฐกิจที่ส่งทอดเป็นลูกโซ่อย่างทวีคูณ จนสถานะของสถาบันการเงินขนาดใหญ่หลายแห่งขาดทุนจนถึงขั้นล้มละลาย แต่รัฐบาลกลางสหรัฐกลับออกนโยบายการเงินด้วยมาตรการหลายรูปแบบ รวมถึงการใช้เงินทุนของรัฐเข้าพยุงสถานะของสถาบันการเงินและระบบเศรษฐกิจ (Burniske & Tara, 2017) ในขณะที่ประชาชนทั่วไปของสหรัฐเองยังขาดโอกาสในการ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

เข้าถึงแหล่งเงินและบริการทางการเงินของสถาบันการเงิน อันเป็นการจัดสรรทรัพยากรอย่างไม่เป็นธรรมและสร้างความเหลื่อมล้ำในสังคม ดังเช่นวิกฤติเศรษฐกิจครั้งสำคัญของประเทศไทยในปี 1997 (ปี พ.ศ.2540) ระบบสถาบันการเงินของประเทศไทย รวมถึงกลุ่มธุรกิจและอุตสาหกรรมไทยหลายแห่งได้รับผลกระทบจากเศรษฐกิจถดถอย และนโยบายการเงินของรัฐบาลไทยในการปรับเปลี่ยนระบบกำกับเงินตราต่างประเทศเป็นแบบลอยตัวที่มีการจัดการ ส่งผลให้ค่าเงินบาทอ่อนค่าอย่างเฉียบพลัน จนหนี้สินที่เป็นเงินตราต่างประเทศของทุกภาคส่วนมีภาระเพิ่มสูงขึ้นเกินกว่าเท่าตัว หลายกิจการได้รับผลกระทบจากวิฤกติเศรษฐกิจจนถึงขั้นปิดกิจการหรือเกิดการล้มละลายในที่สุด ในขณะที่ระบบสถาบันการเงินก็ได้รับผลกระทบในลักษณะเดียวกัน แต่รัฐบาลได้ออกหลายมาตรการเพื่อเข้าพยุงสถาบันการเงินโดยบางมาตรการได้สร้างภาระให้แก่ประชาชนผู้ฝากเงินจำนวนมาก

โดยกระบวนทัศน์ของบุคคลกลุ่มนี้ รวมถึงกลุ่มนักพัฒนาระบบงานคอมพิวเตอร์ ที่ได้พยายามพัฒนานวัตกรรมทางการเงินแบบกระจายศูนย์ และไร้การกำกับควบคุมโดยหน่วยงานใดอย่างต่อเนื่อง เพื่อเป็นระบบการเงินอิเล็กทรอนิกส์ที่สามารถโอนระหว่างกันได้โดยตรงและสร้างความน่าเชื่อถือโดยมีความโปร่งใสสามารถตรวจสอบได้ จนกระทั่งประสบความสำเร็จเป็น *“บิตคอยน์”* เงินสกุลเข้ารหัสสกุลแรกที่มีความสมบูรณ์ทางเทคโนโลยี่ ซึ่งมีประสิทธิภาพเป็นที่ยอมรับของกลุ่มผู้ใช้งาน เมื่อทำการวิเคราะห์พฤติการณ์ของกลุ่มบุคคลในกระบวนทัศน์นี้ต่อเงินสกุลเข้ารหัส โดยอาศัยแนวคิดกระบวนทัศน์การเคลื่อนย้าย (Mobility Paradigm) ในการพิจารณาจากอิทธิพลต่อกระบวนการเคลื่อนย้ายทางสังคม ด้วยการพัฒนาเทคโนโลยี่การติดต่อสื่อสารระหว่างบุคคลในสังคมและระหว่างสังคม ทำให้เกิดการเดินทางและติดต่อสื่อสารเชื่อมโยงระหว่างประเทศต่อประเทศแบบไร้พรมแดน (Globalization) เกิดปรากฏการณ์ในการลดช่องว่างของข้อจำกัดด้านเวลาและสถานที่ ยิ่งไปกว่านั้นเทคโนโลยี่การสื่อสารได้สร้างจุดเปลี่ยนสำคัญ ทำให้ผู้คนทั่วไปสามารถติดต่อถ่ายทอดพฤติกรรมทางสังคมระหว่างกันได้แบบไร้ข้อจำกัดบนระบบเครือข่ายอินเตอร์เน็ต และทำให้เกิดปฏิสัมพันธ์เชื่อมโยงผู้คนทั่วโลกเข้าใกล้กันเสมือนอยู่ในพื้นที่เดียวกันและเวลาเดียวกัน ส่งผลให้เกิดการเปลี่ยนแปลงทางสังคมในมติใหม่เป็น *”พลเมืองโลก”* (Cosmopolitan) (Mini Sheller & Urry, 2006) และโดยเหตุข้างต้น ปัจจัยชี้นำเศรษฐกิจและสังคมของโลกจึงได้ปรับเปลี่ยนจากอิทธิพลชี้นำด้านพลังงาน มาเป็นปัจจัยการเคลื่อนย้ายเงินทุนระหว่างประเทศ ระบบการเงินที่สร้างการหมุนเวียนและกระจายการลงทุนไปทั่วโลกได้อย่างรวดเร็วผ่านระบบปฏิบัติการออนไลน์ สร้างธุรกรรมการค้าได้หลายล้านเหรียญสหรัฐภายในเพียงวินาทีเดียว จึงเป็นปัจจัยที่ทรงอิทธิพลต่อกระบวนการทางสังคมได้อย่างกว้างและไกล (Mimi Sheller, 2017)

ดังนั้น เงินสกุลเข้ารหัสจึงเกิดการยอมรับในความเป็นเงินตราของกลุ่มบุคคลในกระบวนทัศน์นี้ ที่ประกอบไปด้วยประชากรซึ่งมีทัศนคติและอุดมการณ์ร่วมกันในการปฏิเสธอำนาจ

การกำกับควบคุมจากตัวกลาง แต่เชื่อมั่นต่อความโปร่งใสของระบบนิเวศเงินสกุลเข้ารหัสที่ไม่สามารถลบล้างแก้ไขธุรกรรมได้ อีกทั้งสามารถตรวจพิสูจน์ยืนยันได้จากผู้ใช้งานทั่วไปบนระบบฐานข้อมูลสาธารณะแบบกระจายศูนย์ จึงบังเกิดเป็นพลเมืองโลกเงินสกุลเข้ารหัส ที่ไม่อยู่ภายใต้ขอบเขตประเทศของอำนาจรัฐใดในลักษณะดั่งเดิม แต่เป็นประชากรที่เชื่อมโยงธุรกรรมเงินสกุลเข้ารหัสบนระบบเครือข่ายอินเตอร์เน็ตแบบไร้พรมแดนประเทศ โดยยอมรับเงินสกุลเข้ารหัสเป็นสื่อกลางในการโอนมูลค่าระหว่างกัน ติดต่อทำธุรกรรมระหว่างกันโดยเชื่อมโยงกับเงื่อนไขตรรกะเฉพาะ Smart Contract ของเงินสกุลเข้ารหัส ทั้งนี้รวมถึงอาชญากรซึ่งอาจเป็นส่วนหนึ่งของพลเมืองโลกเงินสกุลเข้ารหัส แต่เป็นกลุ่มบุคคลที่กระทำความผิด หรือหลีกเลี่ยงกฎหมาย และแสวงหาการหลุดพ้นจากการกำกับควบคุมทางการเงินของอำนาจรัฐ โดยอีกปรากฏการณ์หนึ่งที่แสดงความเป็นพลมืองโลกบนสื่อสังคมออนไลน์ โดยเจ้าของเฟซบุ๊กได้นำเสนอเงินสกุลเข้ารหัสใหม่ที่ชื่อว่า *“ลิบรา (Libra)”* บนระบบปฏิบัติการของเฟซบุ๊ก (Facebook) ซึ่งเป็นเครือข่ายสังคมออนไลน์ขนาดใหญ่ที่มีผู้ใช้งานมากกว่า 1 ใน 4 ของประชากรทั่วโลก (หรือมีจำนวนมากกว่า 2,000 ล้านบัญชีผู้ใช้งาน) และถือเป็นประชากรของพลเมืองโลกขนาดใหญ่ที่สุด เพื่อใช้เป็นเงินตรารูปแบบดิจิทัลในการชำระค่าสินค้าและบริการหมุนเวียนในเครือข่ายของผู้ใช้งานเฟซบุ๊ก ซึ่งอาจสามารถช่วยลดความเหลื่อมล้ำให้แก่ประชากรโลกที่ไม่สามารถเข้าถึงบัญชีสถาบันการเงินจำนวนประมาณ 1,700 ล้านคนทั่วโลก เนื่องจากสามารถเข้าถึงระบบสื่อสารอินเตอร์เน็ตและการใช้งานเฟซบุ๊ก โดยมีระบบการกำกับดูแลธุรกรรมข้ามเขตประเทศจากกลุ่มองค์กรสมาชิกของเฟซบุ๊กที่มาจากหลากหลายประเทศ (เกาะกระแส, 2019) แต่ในท้ายที่สุด รัฐบาลสหรัฐอเมริกาในช่วงเวลานั้นโดยประธานาธิบดีโดนัลทรัมป์ก็ได้ใช้อำนาจแห่งรัฐมีคำสั่งถึงเจ้าของเฟซบุ๊กซึ่งประกอบกิจการในสหรัฐให้ระงับการดำเนินงานโครงการดังกล่าว

กล่าวโดยสรุป ความเป็นเงินตราของเงินสกุลเข้ารหัส จึงขึ้นอยู่กับกระบวนทัศน์ที่มีต่อระบบนิเวศเงินสกุลเข้ารหัส หากพิจารณาบนกระบวนทัศน์ความมั่นคงแห่งรัฐที่รัฐควรมีอำนาจในการกำกับควบคุมการกระทำของประชาชนในอาณาเขตของรัฐนั้น หรือที่เรียกว่าแนวคิดการรวมศูนย์อำนาจการควบคุม (Centralization Aspect) เงินสกุลเข้ารหัสย่อมขาดคุณลักษณะสำคัญของความเป็นเงินตรา เนื่องจากระบบปฏิบัติดำเนินการภายใต้เงื่อนไขที่กำหนดขึ้นอย่างอัตโนมัติไร้การควบคุมจากหน่วยงานใด แต่หากพิจารณาบนกระบวนทัศน์ของประสิทธิผลทางเศรษฐกิจที่เหมาะสม เงินสกุลเข้ารหัสก็อาจถูกยอมรับเป็นเงินตราที่ชอบด้วยกฎหมาย ซึ่งช่วยสร้างประสิทธิภาพการหมุนเวียนทางการเงินในระบบเศรษฐกิจ ด้วยความรวดเร็วไร้พรมแดนและต้นทุนการดำเนินการต่ำ แต่อยู่ภายใต้ระบบการจัดการแบบกระจายศูนย์ (Decentralization Aspect) ดังเช่น เมื่อเดือนมิถุนายน 2021 *“เอลซัลวาดอร์”* ประเทศขนาดเล็กในทวีปอเมริกากลางได้ยอมรับบิตคอยน์เป็นเงินตราตามกฎหมาย เนื่องด้วยขนาดเศรษฐกิจของประเทศเกินกว่าร้อยละ 20 ของผลิตภัณฑ์มวลรวม (GDP) มีแหล่งรายได้เกิดจากเงินส่งกลับประเทศของแรงงานในต่างประเทศ อีกทั้งประชากรมากกว่าร้อยละ 70 ของ

ประชากรทั้งประเทศไม่มีบัญชีธนาคารเป็นของตนเอง โดยประชาชนต้องรับภาระค่าธรรมเนียมและค่าดำเนินการโอนเงินข้ามประเทศไม่น้อยกว่าร้อยละ 10 ของมูลค่ารับโอนเงินและต้องเดินทางระยะไกลเพื่อไปรับเงินสดกับธนาคาร (พงศภัค รจนา, 2021) ดังนั้นการยอมรับบิตคอยน์เป็นเงินตราตามกฎหมายของเอลซัลวาดิร์ จึงช่วยเพิ่มประสิทธิภาพทางการเงินในระบบเศรษฐกิจ และประชาชนสามารถใช้จ่ายหมุนเวียนชำระค่าสินค้าและบริการได้โดยตรง เนื่องจากบิตคอยน์เป็นเงินสกุลเข้ารหัสที่สามารถโอนเงินในระบบอินเตอร์เน็ตข้ามประเทศ หรือการโอนระหว่างกันให้เข้าถึงผู้รับได้ทันทีโดยไม่ต้องใช้บัญชีธนาคารด้วยค่าใช้จ่ายต่ำ

อย่างไรก็ตาม ปัจจุบันแต่ละประเทศมีการนิยามสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส หรือการออกมาตรการทางกฎหมายที่บังคับแก่เงินสกุลเข้ารหัสอย่างไม่เป็นสากล ทั้งนี้ ขึ้นอยู่กับพื้นฐานของระบบกฎหมายด้านเศรษฐกิจในประเทศนั้น ที่จะให้ความหมายหรือนิยามของเงินสกุลเข้ารหัสว่าควรเข้าข่ายสถานภาพการบังคับใช้กฎหมายในลักษณะใด กล่าวคือควรมีสถานภาพทางกฎหมายของเงินสกุลเข้ารหัสเสมือนเป็น *“เงินตรา (Currency)”* หรือ *“สินทรัพย์ (Property)”* หรือ *“สินค้า (Commodity)”* หรือ *“หลักทรัพย์ (Security)”* (Cvetkova, 2018) รวมถึงการให้ความสำคัญต่อการกำกับระบบนิเวศเงินสกุลเข้ารหัสในรูปแบบการกระจายศูนย์ (Decentralized Digital Currency) หรือในรูปแบบระบบนิเวศที่มีเครือข่ายการปฏิบัติงานแบบรวมศูนย์กลาง (Centralized Digital Currency) (Yang, 2016) ซึ่งจะถือเป็นบรรทัดฐานสำคัญในการปรับใช้มาตรการทางกฎหมายเพื่อการกำกับดูแลในลำดับต่อไป

สำหรับประเทศไทย ได้มีการตราพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัลขึ้นในปี 2018 (พ.ศ. 2561) ซึ่งเป็นกฎหมายที่เกี่ยวกับเงินสกุลเข้ารหัส โดยมีเจตนารมย์เพื่อกำกับดูแลการะดมทุนผ่านสินทรัพย์ดิจิทัล การประกอบธุรกิจและการดำเนินกิจการเกี่ยวกับสินทรัพย์ดิจิทัล ส่งเสริมการนำเทคโนโลยีมาพัฒนาเศรษฐกิจและสังคมอย่างยั่งยืน คุ้มครองผู้ลงทุนและป้องกันการนำสินทรัพย์ดิจิทัลไปใช้สนับสนุนธุรกรรมที่ผิดกฎหมาย โดยอยู่ภายใต้การกำกับของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ซึ่งมีหลักปฏิบัติทางกฎหมายทำนองเดียวกับการกำกับดูแลผู้ประกอบธุรกิจเกี่ยวกับหลักทรัพย์ ดังนั้นจึงสามารถอนุมานได้ว่าประเทศไทยได้กำหนดสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส มีลักษณะทำนองเดียวกับ *“หลักทรัพย์”* ซึ่งเป็นสินทรัพย์เพื่อการลงทุนประเภทหนึ่ง ทั้งนี้ผู้วิจัยมีความเห็นว่าการกำหนดมาตรการทางกฎหมายต่อเงินสกุลเข้ารหัส เสมือนเป็น *“หลักทรัพย์”* มีความเหมาะสมกับบริบทของประเทศไทย ซึ่งสอดคล้องกับความเห็นของศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย (2018) ในการศึกษาการบังคับคดีกับสินทรัพย์ดิจิทัล ซึ่งได้เทียบเคียงวิธีปฏิบัติต่อสินทรัพย์ดิจิทัลรวมถึงเงินสกุลเข้ารหัสในทำนองเดียวกับวิธีบังคับคดีต่อหลักทรัพย์ อีกประการหนึ่งเงินสกุลเข้ารหัสขาดคุณสมบัติ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ความเป็นเงินตราในหลายประการดังกล่าวข้างต้น และการกำกับดูแลในลักษณะหลักทรัพย์ซึ่งเป็นสินทรัพย์เพื่อการลงทุนที่มีความเสี่ยงสูง ด้วยวิธีการจำกัดความเสี่ยงให้อยู่ในขอบเขตเฉพาะการทำธุรกรรมเงินสกุลเข้ารหัสภายใต้กลุ่มบุคคลในวงจำกัด และการประกอบธุรกิจของผู้ให้บริการที่เกี่ยวข้องเท่านั้นเป็นแนวทางที่เหมาะสมกับบริบทในปัจจุบัน เพราะถ้ากำหนดให้เงินสกุลเข้ารหัสเป็น *“เงินตรา”* ย่อมส่งผลให้เกิดการหมุนเวียนธุรกรรมแก่บุคคลทั่วไปในวงกว้าง ในขณะที่ประเทศไทยยังขาดความพร้อมในหลายประการ เช่น ประชาชนทั่วไปและเจ้าหน้าที่ยังขาดความรู้ความเข้าใจที่ถูกต้องต่อบริบทของเงินสกุลเข้ารหัส การให้บริการเทคโนโลยี่การสื่อสารยังขาดความเสถียร และการพัฒนาระบบนิเวศโครงสร้างพื้นฐานในการอำนวยบริการธุรกรรม ยังอยู่ระหว่างในการทดสอบระบบโครงสร้างพื้นฐานของธนาคารแห่งประเทศไทยภายใต้โครงการอินทนนท์ และการเตรียมขยายการให้บริการธุรกรรมในวงกว้าง (Scalability) ในระยะต่อไปอย่างมั่งคงทั้งระบบจัดการธุรกรรมและการรักษาความปลอดภัยทางไซเบอร์

4.5.2 ปัจจัยสำคัญในกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสที่อาจมีอิทธิพลต่ออาชญากรในการตัดสินใจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องในการทำธุรกรรมฟอกเงิน

การฟอกเงิน เป็นกระบวนการจัดการซ่อนเร้นผลประโยชน์ที่อาชญากรได้รับจากการกระทำผิด เพื่อกลบเกลื่อนร่องรอย ปิดบังที่ซ่อนแหล่งเงินจากการกระทำผิด ป้องการการติดตามจับกุม (Unite Nations Office on Drugs and Crime, 2020) หรืออาจเรียกได้ว่า เป็นกระบวนการที่อาชญากรใช้เพื่อการสร้างความชอบด้วยกฎหมายให้แก่เงินจากการกระทำผิด ซึ่งส่วนใหญ่จะเกี่ยวข้องกับอาชญากรรมองค์กรที่สามารถสร้างผลประโยชน์มหาศาล (European Commission, 2020) เพื่อนำเงินและทรัพย์สินนั้นไปใช้กระทำผิดต่อไปอีก ทำให้ยากแก่ปราบปรามอาชญากรรม ดังนั้นเพื่อเป็นการตัดวงจรการประกอบอาชญากรรม จึงจำเป็นต้องตรากฎหมายบัญญัติให้เป็นความผิดทางอาญา ในการจัดการกับอาชญากรและเงินหรือทรัพย์สินที่ได้จากการกระทำผิด ให้สามารถดำเนินมาตรการป้องกันและปราบปรามการฟอกเงินได้อย่างมีประสิทธิภาพ (สำนักงานป้องกันและปราบปรามการฟอกเงิน, 2017) โดยความร่วมมือระหว่างประเทศและกับองค์กรสากล ซึ่งอาชญากรได้มีพัฒนาในการจัดการซ่อนเร้นผลประโยชน์ ด้วยวิธีการกลบเกลื่อนร่องรอยเส้นทางการเงิน เพื่อไม่ให้สามารถตรวจพิสูจน์แหล่งที่มาของแหล่งผลประโยชน์รวมถึงการตรวจสอบย้อนกลับไปถึงตัวอาชญากรได้ เช่น การนำเงินจากการกระทำผิดไปซื้อ เพชรพลอย ทองคำ รถยนต์หรู งานศิลปะ หรือวัตถุโบราณ โดยไม่ระบุแหล่งที่มาของเงินในการซื้อทรัพย์สินดังกล่าว รวมถึงการถ่ายโอนทรัพย์ที่ถือครองไปหลายลำดับชั้น การให้กู้ยืมเงินแก่บุคคลรายย่อย การทยอยโอนเงิน

ระหว่างประเทศ จนในที่สุดไม่สามารถตรวจสอบย้อนกลับไปยังแหล่งที่มาของเส้นทางการเงินตั้งต้นได้ (Baath & Zellhorn, 2016)

อาชญากรมักจะมีพัฒนาการแสวงหาช่องโอกาสจากเครื่องมือรูปแบบใหม่เสมอ เพื่อหลีกหนีกฎระเบียบและข้อจำกัดของหน่วยงานบังคับใช้กฎหมาย ในการจัดการกับผลประโยชน์จากการฟอกเงิน และเงินสกุลเข้ารหัสก็เป็นนวัตกรรมทางเทคโนโลยีการเงินที่ลักษณะหลายประการที่เอื้อประโยชน์ต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ไม่ว่าจะเป็นระบบปฏิบัติการบล็อกเชนที่เป็นระบบงานแบบกระจายศูนย์ ไม่มีหน่วยงานกลางใดกำกับ ระบบการอำพรางตัวตนของผู้ใช้งาน ระบบสนับสนุนการหลีกเลี่ยงการสืบค้นเส้นทางธุรกรรม รวมถึงความสะดวกในการทำธุรกรรมที่ไม่มีข้อจำกัดต่อขนาดมูลค่ารายการ และสามารถทำธุกรรมข้ามประเทศได้ด้วยความรวดเร็ว โดยปัจจัยที่กล่าวถึงข้างต้น ล้วนแต่เป็นโอกาสอย่างมีนัยสำคัญต่อาชญากรในการเลือกเงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน โดยเมื่อวิเคราะห์พฤติการณ์ข้างต้นของอาชญกรด้วยทฤษฎีปกตินิสัย พบว่า ผู้กระทำผิด หรือ อาชญากรมีแรงจูงใจที่โน้มเอียงให้ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน เนื่องจากเมื่อประเมินผลประโยชน์ที่จะได้รับจากการฟอกเงินสำเร็จ เปรียบเทียบกับผลร้ายที่อาจได้รับโทษ หรือการสูญเสียเงินและทรัพย์สินอื่นจากการกระทำผิด ซึ่งประกอบการวิเคราะห์ตามแนวคิดทฤษฎีการเลือกกระทำอย่างมีเหตุผลแล้ว เงินสกุลเข้ารหัสมีแนวโน้มที่จะสามารถหลีกเลี่ยงหลุดพ้นจากการติดตามในระบบนิเวศเงินสกุลเข้ารัหสได้ โดยพื้นฐานหลักทางเทคโนโลยี่ และเทคโนโลยี่สนับสนุนจากผู้ให้บริการในการกลบเกลื่อนร่องรอยเส้นทางธุรกรรมเสริมอีก นอกจากนี้ มาตรการทางกฎหมายในการกำกับและป้องกันปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสของหลายประเทศในปัจจุบันยังมีความแตกต่างกัน ตั้งแต่ประเทศที่มีกฎระเบียบในการกำกับอย่างเคร่งครัด ประเทศที่มีมาตรการไม่เคร่งครัด จนถึงขั้นประเทศที่ไม่มีมาตราใดกำกับ จึงเป็นการขาดประสิทธิภาพการพิทักษ์ปกป้องและป้องกันเหตุ เนื่องด้วยความเป็นโลกภิวัติของเงินสกุลเข้ารหัส ความอ่อนแอในการกำกับธุรกรรมเงินสกุลเข้ารหัส ณ พื้นที่ใด หรือประเทศใดเพียงแหล่งเดียวก็ถือเป็นการขาดประสิทธิภาพการกำกับของบริบทโดยรวม เนื่องจากเป็นช่องโอกาสที่อาชญากรอาจเลือกใช้พื้นที่นั้นเป็นแหล่งในการฟอกเงินได้โดยง่าย และประการสุดท้ายเหยื่อ หรือในความหมายที่นี้คือรัฐและผลประโยชน์แห่งรัฐ หากรัฐไม่สามารถดำเนินนโยบายหรือกำหนดมาตรการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสอย่างมีประสิทธิภาพเพียงพอ ก็อาจส่งผลทางร้ายต่อรัฐและประโยชน์สาธารณะแห่งรัฐ จากการขาดศักยภาพในการทำลายแหล่งผลประโยชน์ของอาชญากร และการตัดวงจรการประกอบอาชญกรรมลงได้

ดังนั้น ผู้วิจัยจึงมีความเห็นว่า การศึกษาทำความเข้าใจถึงปัจจัยที่มีอิทธิพลต่ออาชญากรในการตัดสินใจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน เพื่อให้ทราบและเข้าใจถึงช่องโอกาส ข้อจำกัด และพฤติกรรมของอาชญากรในบริบทของเงินสกุลเข้ารหัส ซึ่งจะเป็น

ประโยชน์ต่อหน่วยงานบังคับใช้กฎหมาย ได้พัฒนาแนวปฏิบัติเพื่อการป้องกันและปราบปรามให้ทันต่อการเคลื่อนไหวของอาชญากรในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ดังคติโปราณที่ว่า *"รู้เขา รู้เรา รบร้อยครั้ง ชนะร้อยครั้ง"* ทั้งนี้ผู้วิจัยได้ทำการสังเคราะห์การดำเนินการเชิงเปรียบเทียบระหว่างกระบวนการฟอกเงินและกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยสรุปได้ดังนี้

การดำเนินการ	**กระบวนการฟอกเงิน**	**กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส**
1. การนำผลประโยชน์จากการกระทำผิดเข้าสู่กระบวนการฟอกเงิน	- อาชญากรมีทางเลือกได้หลายแนวทาง เช่น การคงการถือครองเป็นเงินตรา หลักทรัพย์ หรือทรัพย์สินอื่น รวมถึงการแปลงค่าทรัพย์สินดังกล่าวเป็นเงินตราเพื่อดำเนินการอื่นต่อไป	- อาชญากรได้รับผลประโยชน์จากการกระทำผิดเป็นเงินสกุลเข้ารหัสหรือเป็นเงินตราทั่วไปโดยดำเนินการแปลงค่าเป็นเงินสกุลเข้ารหัสเพื่อดำเนินการต่อไป
2. กลไกการกลบเกลื่อนร่องรอยเส้นทางธุรกรรมการเงิน เพื่อหลีกเลี่ยงและตัดความสัมพันธ์เชื่อมโยงระหว่างผู้ส่งต้นทางกับผู้รับปลายทาง	- การถ่ายโอนกระจายการถือครองเงินตรา หรือทรัพย์สินให้แก่ผู้ถือแทนจำนวนหลายราย รวมถึงการทยอยโอนเงินไปต่างประเทศ เพื่อหลบเลี่ยงเกณฑ์การตรวจสอบกับธุรกรรมรายการขนาดย่อย - การซื้อทรัพย์สินที่มีค่าสูง และมีความอ่อนไหวต่อการประเมินมูลค่า เช่น เพชรพลอย รถยนต์หรู งานศิลปะ วัตถุโบราณ พระเครื่อง เพื่อการสร้างธุรกรรมครอบคลุมมูลค่าเป้าหมายของการฟอกเงิน - การลงทุนในกิจการบังหน้าในลักษณะประกอบธุรกิจการค้าและบริการระหว่างประเทศ เพื่อสร้างธุรกรรมโอนเงินชำระค่าสินค้าส่งออกและนำเข้า ค่าบริการ	- การทำธุรกรรมเงินสกุลเข้ารหัสบนระบบปฏิบัติการ TOR Browser เพื่อปกปิดรหัสที่ตั้งขณะทำธุรกรรม - การใช้บริการกับ Mixer ผู้ให้บริการแปรสภาพเงินสกุลเข้ารหัสในการปนเงินสกุลเข้ารหัสกับผู้ใช้บริการรายอื่น โดยผู้ใช้งานจะได้รับเงินสกุลเข้ารหัสปลายทางที่ไม่มีเส้นทางธุรกรรมเชื่อมโยงกับผู้โอนต้นทาง - การใช้บริการกับ CoinJoin ระบบปฏิบัติการแบ่งปันธุรกรรมโดยการจัดสรรธุรกรรมของผู้ใช้บริการหลายราย เพื่อจัดสรรธุรกรรมย่อยและรวบรวมมูลค่าโอนเงินสกุลเข้ารหัสไปยังผู้รับปลายทางให้ได้รับมูลค่าใกล้เคียงต้นทาง แต่

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

	ท่องเที่ยว หรือการให้กู้ยืมและชำระหนี้ระหว่างประเทศ - การพนันโดยการลวงด้วยการชนะพนัน หรือการซื้อรางวัลสลากกินแบ่งรัฐบาล เพื่อสร้างหลักฐานแหล่งที่มาของเงิน - และอื่นๆ	อาจมีโอกาสได้รับเงินสกปรกของผู้ใช้บริการรายอื่น หรือได้รับโอนเงินสกลุเข้าหรัสของตนเองเองบางส่วน - การรับเงินสกลุเข้ารหัสโดยตรงจากระบบซึ่งจะไม่มีเส้นทางธุรกรรม โดยการเข้าซื้อค่าขุดที่นัดขุดได้รับเงินสกุลเข้ารหัสโดยตรงจากระบบ หรือการซื้อ Privacy Coin ที่มีระบบการโอนมูลค่าโดยไม่สร้างเส้นทางธุรกรรม ด้วยการทำลายรหัสข้อมูลแสดงมูลค่าของผู้โอนต้นทางและสร้างรหัสข้อมูลแสดงมูลค่าใหม่จากระบบที่กระเป๋าเงินของผู้รับโอนปลายทาง
การดำเนินการ	**กระบวนการฟอกเงิน**	**กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส**
3. กลไกการถ่ายโอนผลประโยชน์ข้ามประเทศ	- การขนย้ายทรัพย์สินทางกายภาพข้ามพรมแดนประเทศ เป็นภาระการขนย้ายและความเสี่ยงต่อการถูกตรวจสอบจับกุม ไม่ว่าจะเป็นเงินสด ทรัพย์สินอื่น เช่น เพชรพลอย รถยนต์หรู - การทำธุรกรรมโอนเงินไปต่างประเทศผ่านผู้ให้บริการโอนเงินระหว่างประเทศ เช่น Paypal, Western Union แต่อาจมีข้อจำกัดด้านจำนวนมูลค่าโอน และประเทศในเครือข่ายการให้บริการ - การทำธุรกรรมชำระค่าสินค้าและบริการ รวมถึงชำระหนี้ผ่านระบบธนาคาร จากกิจการบังหน้าที่ประกอบกิจการนำเข้าส่งออก กิจการท่องเที่ยว กิจการให้สินเชื่อ	- ธุรกรรมบนระบบนิเวศเงินสกุลเข้ารหัสไม่มีเงื่อนไขในการระบุตัวตนของผู้ใช้งานและสามารถทำธุรกรรมถ่ายโอนมูลค่าข้ามประเทศได้สะดวกรวดเร็วบนระบบอินเตอร์เน็ต โดยไม่มีข้อจำกัดด้านเวลา สถานที่ รวมถึงจำนวนมูลค่าในการโอน

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

4. ต้นทุนการดำเนินการ	- เนื่องจากการดำเนินการมีความซับซ้อน เกี่ยวข้องกับผู้แทนดำเนินการจำนวนมากในหลายขั้นตอน จึงมีค่าใช้จ่ายในการดำเนินการสูง - ค่าใช้จ่ายในการเก็บรักษา ซ่อนเร้นผลประโยชน์ เช่น การจ้างผู้ดูแลรักษาบัญชีเงิน ตู้เซฟสำหรับเงินสด เพชรพลอย พระเครื่อง และอาคารโรงรถ อีกทั้งทรัพย์บางประเภทต้องมีการดูแลบำรุงรักษาประจำ - ความเสี่ยงจากการถูกยักยอกผลประโยชน์กันเองโดยผู้แทนดำเนินการในระหว่างการฟอกเงิน ซึ่งเป็นต้นทุนดำเนินการที่สำคัญอีกประการหนึ่ง	- การทำธุรกรรมกระจายการถือครองหรือการถ่ายโอนธุรกรรมไปในหลายขั้นตอนสร้างความซับซ้อนได้รวดเร็ว และต้นทุนดำเนินการต่ำภายในวงจำกัดของผู้แทนดำเนินการที่เกี่ยวข้อง - ค่าใช้จ่ายในการดูแลเก็บรักษาค่อนข้างต่ำ โดยเฉพาะการจัดเก็บเงินสกุลเข้ารหัสในกระเป๋าเงิน Cold Wallet ที่ไม่เชื่อต่อกับระบบอินเตอร์เน็ต ซึ่งมีความเสี่ยงต่อการถูกตรวจสอบสืบค้นต่ำ - อาจมีความเสี่ยงจากการถูกโจรกรรมทางไซเบอร์ ทั้งนี้หากเกิดเหตุขึ้นจะมีความเสียหายค่อนข้างสูง
การดำเนินการ	**กระบวนการฟอกเงิน**	**กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส**
5. มาตรการทางกฎหมาย	- มีมาตรการทางกฎหมายในการต่อต้านการฟอกเงินในระดับสากลที่พัฒนาการอย่างต่อเนื่อง โดยมีความร่วมมือระดับประเทศ ในการกำกับธุรกรรมทางการเงินกับสถาบันการเงิน	- อยู่ระหว่างการพัฒนามาตรการทางกฎหมายในการกำกับธุรกรรมเงินสกุลเข้ารหัสในระดับสากลให้มีความชัดเจน โดยหลายประเทศมีมาตรการกำกับดูแลที่ต่างกัน ตั้งแต่ประเทศที่มีมาตรการต้องห้ามทำธุรกรรม จนถึงยอมรับการทำธุรกรรมเงินสกุลเข้ารหัส
6. กลไกการรวบรวมเป็นเงินที่ชอบด้วยกฎหมาย	- การรวบรวมเงินที่กระจายการถือครอง โอนย้ายกลับมายังอาชญากรในลักษณะป็เงินที่ชอบด้วยกฎหมาย สามารถระบุแหล่งที่มาของเงินได้ - การขายทรัพย์สินมีค่าที่ได้จากการแปรสภาพ แต่อาจขาดสภาพคล่องในการซื้อขาย เนื่องจากเป็น	- อาชญากรสามารถใช้ประโยชน์จากเงินสกุลเข้ารหัสหมุนเวียนในระบบนิเวศเงินสกุลเข้ารหัสต่อได้ - การแปลงค่าเงินสกุลเข้ารหัสเป็นเงินที่ชอบด้วยกฎหมาย ในเขตประเทศที่ยอมรับการทำธุรกรรม

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

	ทรัพย์สินที่มีความต้องการของผู้สนใจในวงจำกัด - การรวบรวมผลประโยชน์กลับคืนในรูปของผลตอบแทนจากการลงทุนในกิจการบังหน้า	

แหล่งที่มา : จัดทำโดยผู้วิจัย

4.5.2 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และใช้เป็นเครื่องมือในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

จากผลการศึกษา พบว่า รูปแบบอาชญากรรมที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการประกอบอาชญากรรม และเพื่อนำผลประโยชน์จากการกระทำผิดไปทำการฟอกเงินโดยธุกรรมเงินสกุลเข้ารหัสนั้น คือ อาชญากรรมเศรษฐกิจเกือบทุกประเภท ที่มักจะก่อให้เกิดความเสียหายแก่เหยื่อในวงกว้าง โดยมีขนาดผลประโยชน์จากการกระทำผิดมูลค่าสูง และจำเป็นต้องจัดการฟอกเงินเป็นเงินที่ชอบด้วยกฎหมายให้เร็วที่สุด ดังนั้นอาชญากรส่วนหนึ่งอาจใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน ส่วนอาชญากรรมอีกลักษณะหนึ่งคืออาชญากรรมไซเบอร์ ซึ่งมักจะการกระทำผิดบนระบบเครือข่ายอินเตอร์เน็ต หรือระบบโครงข่ายการสื่อสารอื่นในทำนองเดียวกัน รวมถึงอาจใช้ระบบอินเตอร์เน็ตและระบบโครงข่ายการสื่อสารอื่นเป็นเครื่องมือในการกระทำผิด โดยอาชญากรอาศัยความเชี่ยวชาญด้านเทคโนโลยีในการปิดบังตัวตน และป้องกันการตรวจสอบรหัสที่ตั้งในระบบสั่งการก่ออาชญากรรม ดังนั้น เงินสกุลเข้ารหัสจึงอาจถูกใช้เป็นสื่อกลางในการส่งมอบผลประโยชน์ เนื่องจากไม่ต้องแสดงตัวตนผู้ใช้งานในระบบปฏิบัติการบล็อกเชน อีกทั้งสามารถดำเนินกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้ทันทีอย่างต่อเนื่อง โดยผู้ให้ข้อมูลสำคัญได้ให้ความเห็นต่อรูปแบบอาชญากรรมตามลำดับ ดังนี้คือ การหลอกลวงฉ้อโกงประชาชนในลักษณะแชร์ลูกโซ่ (Ponzi Scheme) การค้ายาเสพติดรวมถึงการค้ายาเสพติดบนระบบออนไลน์ (Dark Web) การเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิวเตอร์ (Ransomware) และการพนันรวมถึงการพนันบนระบบออนไลน์ เป็นต้น

ดังนั้น เมื่อทำการวิเคราะห์รูปแบบอาชญากรรมข้างต้น โดยอาศัยแนวคิดทางอาชญาวิทยา ได้แก่ แนวคิดอาชญากรรมคอปกขาวของ เอ็ดวิน เฮช ซัตเธอร์แลนด์ (Edwin H. Sutherland) ซึ่งหมายรวมถึงอาชญากรรมธุรกิจ อาชญากรรมการเงิน หรืออาชญากรรมเศรษฐกิจในปัจจุบัน ซึ่งได้กล่าวถึง ผู้กระทำผิดมักเป็นบุคคลที่มีฐานะทางเศรษฐกิจมั่งคั่ง หรือมีความสัมพันธ์เชิงอำนาจกับผู้มีอิทธิพลโดยตำแหน่งหน้าที่การงานในการสนับสนุนกระทำผิด ซึ่งมักส่งผลกระทบร้ายแรงต่อระบบเศรษฐกิจ ประกอบกับแนวคิดอาชญากรรมไซเบอร์ ซึ่งผู้กระทำผิดมักมีวัตถุประสงค์

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

โดยคาดหวังได้รับผลประโยชน์จากเป้าหมายที่เป็นทั้งปัจเจกบุคคล หรือผลประโยชน์องค์กรเอกชน รวมถึงประโยชน์สาธารณะของภาครัฐที่อาจส่งผลกระทบในวงกว้าง (Siegel, 2013) โดยเหยื่อซึ่งอาจเป็นทั้งผู้ใช้ระบบงาน อุปกรณ์เครื่องคอมพิวเตอร์ หรือระบบปฏิบัติการ และผู้กระทำผิดซึ่งมีศักยภาพด้านเทคโนโลยีที่สามารถเข้าไปประกอบอาชญากรรมในระบบงานเป้าหมาย และองค์ประกอบสุดท้าย คือระบบการสื่อสารและเครื่องมือในการเชื่อมต่อระบบงานของผู้กระทำผิด เข้าสู่ระบบงานเป้าหมาย หรือกล่าวอีกนัยหนึ่งคือ การกระทำผิดกฎหมายโดยใช้อุปกรณ์คอมพิวเตอร์ เครื่องมือสื่อสาร ระบบข้อมูลสารสนเทศ รวมถึงระบบอินเตอร์เน็ตเป็นเครื่องมือในการก่ออาชญากรรมโดยบุคคล กลุ่มบุคคล หรือองค์กรอาชญากรรม (McQuade, 2006) และประกอบกับแนวคิดองค์กรอาชญากรรมข้ามชาติ ในลักษณะอาชญากรรรมที่เกิดขึ้นโดยบุคคล หรือองค์กรจากหลายประเทศร่วมมือกันกระทำผิด หรือการจัดเตรียมวางแผนก่อเหตุ ณ ประเทศหนึ่งแต่ไปปฏิบัติการก่อเหตุ ณ อีกประเทศหนึ่ง หรือ กระทำความผิดในรัฐหนึ่งแต่มีความร่วมมือจากบุคคลหรือองค์กรหลายประเทศ หรือกระทำความผิดในประเทศหนึ่ง แต่ส่งผลกระทบสร้างความเสียหายเป็นวงกว้างในหลายประเทศ ปรากฏว่า

การหลอกลวงฉ้อโกงประชาชนในลักษณะแชร์ลูกโซ่ (Ponzi Scheme) มีรูปแบบในการประกอบกาชญากรรมโดยการชักจูง หรือชวนเชื่อให้เหยื่อเข้ามาร่วมลงทุนในลักษณะการขยายฐานจำนวนเหยื่อมากราย ด้วยการนำเงินทุนจากเหยื่อรายใหม่ไปหมุนเวียนชำระเป็นผลประโยชน์ให้แก่เหยื่อรายเดิม โดยอาศัยสิ่งจูงใจซึ่งเป็นกิจการบังหน้าที่สร้างภาพลักษณ์ให้เกิดความน่าเชื่อถือด้วยการให้คำมั่น หรือโน้มน้าวให้เชื่อว่าจะได้รับผลตอบแทนจากการลงทุนในอัตราสูงและไม่มีความเสี่ยงหรือมีความเสี่ยงต่ำมาก ทั้งนี้ เงินสกุลเข้ารหัสเป็นนวัตกรรมเทคโนโลยีทางการเงิน และเป็นองค์ความรู้ใหม่ที่มีบุคคลรู้และเข้าใจอยู่ในวงจำกัด อาชญากรจึงอาจเลือกใช้เป็นเครื่องมือที่จะสร้างสิ่งจูงใจในการลงทุน โดยเฉพาะอย่างยิ่งปัจจุบันความเคลื่อนไหวของราคาเงินสกุลเข้ารหัสมีโน้นสูงขึ้นแบบก้าวกระโดดอย่างต่อเนื่อง จึงเป็นชุดข้อมูลสาธารณะที่อาชญากรสามารถนำไปบิดเบือน และโฆษณาชวนเชื่อชักจูงเหยื่อได้อย่างสมเหตุผลแก่สถานการณ์ จาก *“ความไม่รู้”* และ *“ความโลภ”* ของเหยื่อ ซึ่งผลประโยชน์จากอาชญากรรมประเภทนี้ มักสร้างเงินทุนหมุนเวียนจำนวนมหาศาลที่อาชญากรจำเป็นต้องจัดการยักย้ายถ่ายเทอย่างรวดเร็ว ด้วยการแปลงค่าเงินหรือทรัพย์สินอื่นเป็นเงินสกุลเข้ารหัส หรืออาจได้รับผลประโยชน์ในรูปของเงินสกุลเข้ารหัสอยู่แล้ว ก็สามารถทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้ต่อเนื่อง ก่อนที่จะขาดกระแสเงินหมุนเวียน และปิดตัวลงทิ้งไว้แต่ความเสียหายให้แก่เหยื่อในที่สุด รูปแบบอาชญากรรมนี้ จึงเข้าลักษณะอาชญกรรมทางเศรษฐกิจที่สร้างความเสียหายแก่ผู้ได้รับผลกระทบในวงกว้าง และมีขนาดความเสียหายจำนวนสูง ซึ่งในบางกรณีก็อาจมีความเกี่ยวข้องกับผู้มีชื่อเสียงทางสังคม ซึ่งมีอิทธิพลต่อการสร้างความน่าเชื่อถือหรือเป็นแรงจูงใจ และการก่ออาชญากรรม มักเกิดจากความร่วมมือของบุคคลหรือกลุ่มบุคคลหลายฝ่ายที่แบ่งหน้าที่กระทำการ เข้าลักษณะองค์กรอาชญากรรม หรือในบางลักษณะก็อาจเข้าข่ายเป็นองค์กร

อาชญากรรมข้ามชาติ เมื่อได้รับผลประโยชน์เป็นเงินสกุลเข้ารหัส หรือการทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสด้วยการยักย้ายถ่ายเทเงินสกุลเข้ารหัสเข้าสู่ระบบนิเวศโดยตรง ที่ไร้ขอบเขตจำกัดของพรมแดน และด้วยความร่วมมือกับผู้ให้บริการแปรสภาพเงินสกุลเข้ารหัส เพื่อกลบเกลื่อนร่องรอยเส้นทางธุกรรม หรือการแปลงค่าเป็นเงินที่ชอบด้วยกฎหมายในประเทศที่มีกฎหมายรองรับ

การค้ายาเสพติดรวมถึงการค้ายาเสพติดบนระบบออนไลน์ (Dark Web) มักมีรูปแบบการกระทำผิดเป็นกระบวนการที่ร่วมกระทำการเป็นเครือข่าย แบ่งหน้าที่กระทำการตั้งแต่ต้นทางดูแลการปลูกพืชเสพติดและการผลิตเป็นผลิตภัณฑ์ การขนส่งและกระจายสินค้าผ่านแดนถึงผู้ค้าจนกระทั่งถึงปลายทางการจำหน่ายตรงแก่ผู้เสพ โดยผลประโยชน์จากกระบวนการค้ายาเสพติดมีวงเงินหมุนเวียนมูลค่ามหาศาล รวมถึงการค้ายาเสพติดบนระบบออนไลน์ใน Dark Web ซึ่งเป็นเว็บไซต์การค้าสิ่งผิดกฎหมาย ที่สามารถใช้เงินสกุลเข้ารหัสเป็นสื่อกลางในการชำระราคาค่าซื้อสินค้า ในส่วนของอาชญากรก็มีพัฒนาการปรับเปลี่ยนรูปแบบการฟอกเงินอย่างต่อเนื่อง โดยเงินสกุลเข้ารหัสก็เป็นเครื่องมือในการฟอกเงิน ที่อำนวยความสะดวกในโอนย้ายถ่ายผลประโยชน์ได้จำนวนมูลค่ามากทั้งภายในประเทศและข้ามประเทศได้ด้วยความรวดเร็ว รูปแบบของกระบวนการค้ายาเสพติด จึงมีการกระทำความผิดในลักษณะอาชญากรรมองค์กร หรืออาชญากรรมองค์กรข้ามชาติที่การวางแผนการดำเนินงานอย่างเป็นระบบ โดยมีแหล่งผลิตพืชเสพติดหรือสารตั้งต้นในประเทศหนึ่ง และลำเลียงจัดส่งไปยังฐานโรงงานผลิตเพื่อผลิตเป็นยาเสพติดพร้อมจำหน่ายในอีกประเทศหนึ่ง จากนั้นก็จะเป็นหน้าที่ของการขนส่งและกระจายยาเสพติดไปยังแหล่งตลาดผู้เสพ ที่มีการจัดเตรียมแผนการขนย้ายผ่านหลายประเทศจนถึงประเทศปลายทาง รวมถึงมีลักษณะเป็นอาชญากรรมเศรษฐกิจโดยผู้กระทำผิดมักมีการสะสมผลประโยชน์จากกระบวนค้าขายเสพติด และใช้เป็นแหล่งเงินทุนในการขยายโอกาสการกระทำผิดโดยใช้ฐานะทางเศรษฐกิจ และความร่วมมือกับอำนาจอิทธิพลช่วยเหลือการสั่งการให้ผู้อื่นกระทำ ร่วมกระทำ หรือกระทำความผิดด้วยตนเอง ด้วยความเชื่อมั่นว่าสามารถปิดกั้นการตรวจสอบจับกุมของเจ้าหน้าที่ หรือทำให้การตรวจสอบสืบค้นร่องรอยการกระทำผิดมีความยากขึ้น

การเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิวเตอร์ (Ransomware) อาชญากรรมลักษณะนี้ผู้กระทำความผิด มักจะส่งชุดคำสั่งจากระบบงานที่ตั้งอยู่ในต่างประเทศเข้าสู่ระบบงานเป้าหมายโดยมุ่งหวังที่เข้าทำลายระบบปฏิบัติการ หรือระบบจัดการฐานข้อมูล โดยการตั้งเงื่อนไขการทำงานผ่านการเปิดจดหมายอิเล็กทรอนิกส์ การเปิดเว็บไซต์ หรือการตั้งค่าเวลาล่วงหน้า เพื่อเป็นการข่มขู่ระบบงานเป้าหมาย ด้วยปฏิบัติการก่อกวนระบบงานให้เกิดความขัดข้อง ประมวลผลข้อมูลผิดพลาดหรือฐานข้อมูลสูญเสีย และเรียกร้องผลประโยชน์เป็นค่าไถ่ เพื่อแลกกับการถอนชุดคำสั่งที่เข้าก่อกวนระบบงานให้กลับสู่สภาพเดิม หรือให้เกิดความเสียหายน้อยที่สุด โดยมีความเป็นไปได้สูงที่ผู้กระทำผิดจะเรียกผลประโยชน์ค่าไถ่เป็นเงินสกุลเข้ารหัส เนื่องจากปัจจัยพื้นฐานของระบบนิเวศเงินสกุลเข้ารหัส

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ช่วยสนับสนุนการโอนค่าไถ่โดยตรงไปยังกระเป๋าเงินที่ไม่ต้องระบุตัวตน เพราะอาชญากรก็มักสั่งการชุดคำสั่งเข้าสู่ระบบงานเป้าหมายจากแหล่งที่ไม่สามารถพิสูจน์ตัวตนได้เช่นกัน เพื่อสร้างความซับซ้อนยากแก่การสืบค้นติดตามของเจ้าหน้าที่ รูปแบบของอาชญากรรม จึงเข้าข่ายทั้งอาชญากรรมไซเบอร์ อาชญากรรมเศรษฐกิจ และองค์กรอาชญากรรมข้ามชาติ เนื่องจากเป็นการกระทำความผิดผ่านระบบอินเตอรเน็ตที่ก่อให้เกิดความเสียหายแก่ระบบปฏิบัติการคอมพิวเตอร์ของเป้าหมายโดยตรง ซึ่งอาจเป็นการกระทำโดยบุคคล หรือการร่วมมือวางแผนและปฏิบัติการเป็นกลุ่มบุคคล หรือองค์กรสมคบกันกระทำความผิดจากต่างประเทศ เพื่อดำเนินการก่อเหตุอาชญากรรมในประเทศเป้าหมาย โดยผู้กระทำผิดมักเรียกร้องผลประโยชน์เป็นค่าไถ่จำนวนมูลค่าสูง เนื่องจากได้ประเมินค่าไถ่เปรียบเทียบผลกระทบของต้นทุนการเรียกคืนระบบฐานข้อมูล หรือค่าเสียโอกาสจากระยะเวลาในการเรียกคืนระบบงานของเป้าหมาย

การพนันรวมถึงการพนันบนระบบออนไลน์ เป็นอาชญากรรมลักษณะความผิด Mala Prohibita บัญญัติให้การจัดให้มีการพนันเสี่ยงโชคเป็นการกระทำที่ไม่ชอบด้วยกฎหมาย ทั้งในลักษณะจัดการสถานที่เป็นบ่อนการพนัน รวมถึงการจัดให้มีระบบปฏิบัติการเพื่อการพนันออนไลน์ ทั้งนี้การพนันเป็นอีกแหล่งสำคัญที่เอื้ออำนวยต่อกระบวนการฟอกเงิน เนื่องจากความยากต่อการพิสูจน์เส้นทางการเงินของผู้เล่นพนันได้รับผลตอบแทนจากการชนะพนัน หรือสูญเสียจากการเสี่ยงโชคพนัน เป็นการหลีกเลี่ยงความเชื่อมโยงของแหล่งเงินที่ไม่ชอบด้วยกฎหมาย และปัจจุบันการพนันได้พัฒนาสู่ระบบคอมพิวเตอร์ออนไลน์ ทำให้สามารถขยายฐานผู้เข้าร่วมกิจกรรมได้ง่ายและกว้างขึ้น รวมถึงไม่มีข้อจำกัดด้านเวลาและสถานที่ในการเข้าร่วมกิจกรรม นอกจากนี้การใช้เงินสกุลเข้ารหัสเป็นสื่อกลางในการชำระหนี้พนันออนไลน์ ส่งผลให้ผู้กระทำผิดไม่ต้องแปลงค่าเป็นเงินตราสกุลท้องถิ่นของแต่ละประเทศ และเอื้อประโยชน์ต่อการโยกย้ายถ่ายเทผลประโยชน์ในรูปแบบเงินสกุลเข้ารหัสบนระบบออนไลน์ได้ทุกขณะ

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ทั้งนี้ เมื่อศึกษาอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงินเปรียบเทียบกับบริบทสากล จาก Chainalysis (2021) ซึ่งได้นำเสนอรายงานอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส (The 2021 Crypto Crime Report) ปรากฏว่าอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสมีปริมาณลดลง กล่าวคือในปี 2019 มีธุรกรรมผิดกฎหมายในระบบนิเวศเงินสกุลเข้ารหัสประมาณ 21.4 พันล้านเหรียญสหรัฐ คิดเป็นร้อย 2.10 ของมูลค่าตลาดเงินสกุลเข้ารหัส ในขณะที่ปี 2020 มีธุรกรรมผิดกฎหมายประมาณ 10.0 พันล้านเหรียญสหรัฐ คิดเป็นร้อย 0.34 ของมูลค่าตลาดเงินสกุลเข้ารหัส ซึ่งประกอบด้วยอาชญากรรมหลักได้แก่ การหลอกลวงฉ้อโกงประชาชนในลักษณะแชร์ลูกโซ่ (Ponzi Scheme) มีเหยื่อที่ได้รับความเสียหายหลายล้านรายเป็นมูลค่าประมาณ 2.0 พันหลายเหรียญ เช่น Mirror Trading International (MIT) เป็นเว็บไซต์หลอกลวงขนาดใหญ่ที่มีถิ่นที่ตั้งในประเทศแอฟาริกาใต้ โดยมีเหยื่อที่ร่วมลงทุนจำนวนหลายแสนราย

ซึ่งมีมูลค่าความเสียหายประมาณ 589 ล้านเหรียญสหรัฐ กระจายอยู่ในกระเป๋าเงินมากกว่า 471,000 รหัสที่ตั้ง เป็นต้น การค้าสิ่งผิดกฎหมายบนระบบออนไลน์ (Dark Web) รวมถึงยาเสพติด ในปี 2020 มีมูลค่าประมาณ 1.7 พันล้านเหรียญสหรัฐ ซึ่งสูงขึ้นจากปี 2019 ที่มีมูลค่าประมาณ 1.3 พันล้านเหรียญสหรัฐ โดยเว็บไซต์การค้าสิ่งผิดกฎหมาย Hydra ซึ่งมีถิ่นที่ตั้งในประเทศรัสเซียเป็นเว็บไซต์รายใหญ่ที่มีปริมาณธุรกรรมรวมสูงถึงร้อยละ 75.0 ของปริมาณการค้ารวม และการเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิวเตอร์ (Ransomware) ในปี 2020 มีมูลค่าความเสียหาย 350 ล้านเหรียญสหรัฐ ซึ่งมีอัตราเติบโตถึง 311% เมื่อเทียบกับปี 2019 เนื่องจากภาวะการแพร่ระบาดของเชื้อโควิด-19 ทำให้มีการปรับวิธีการทำงานที่บ้านเพิ่มมากขึ้น (Work From Home) จนเกิดเป็นจุดเปราะบางในระบบการรักษาความปลอดภัยทางไซเบอร์ของระบบงานในหลายองค์กร ทั้งนี้อาชญากรจะแบ่งหน้าที่การทำงานเป็นขั้นตอน เริ่มจากทีมงานส่งรหัสข้อมูลเข้าระบบอินเตอรเน็ตเพื่อการทดสอบจุดอ่อนของระบบงานเป้าหมาย จากนั้นทีมงานจะประเมินหาโปรแกรมไวรัสที่เหมาะสมเพื่อเตรียมส่งมัลแวร์เข้าสู่ระบบงานเป้าหมาย และขั้นตอนสุดท้ายคือการประสานงานกับทีมขโมยข้อมูลระบบคอมพิวเตอร์ (Hacker) เพื่อเจาะระบบปฏิบัติการและส่งมัลแวร์เข้าสู่ระบบงานเป้าหมาย ทั้งนี้โดยส่วนใหญ่จะปฏิบัติการกับระบบงานของหน่วยราชการท้องถิ่น ธุรกิจขนาดเล็ก รวมถึงกิจการโรงพยาบาล (Chainalysis, 2021) ซึ่งรูปแบบอาญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสในบริบทสากลข้างต้น มีลักษณะการประกอบอาชญากรรมในทำนองเดียวกับที่เคยปรากฏในประเทศไทย

สำหรับการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสในบริบทสากล โดยส่วนใหญ่จะทำธุรกรรมเคลื่อนย้ายเงินสกุลเข้ารหัสมูลค่าสูงผ่านผู้ให้บริการผิดกฎหมาย เช่น ผู้ให้บริการแลกเปลี่ยนนอกระบบ โปรแกรมการพนันออนไลน์ ผู้ให้บริการกลบเกลื่อนร่องรอย (Mixer) และผู้ให้บริการที่จัดตั้งในประเทศที่มีความเสี่ยงต่อการฟอกเงิน ทั้งนี้จากรายงานวิเคราะห์เส้นทางธุรกรรมผิดกฎหมายในระบบนิเวศเงินสกุลเข้ารหัส ปรากฏว่า ประเทศรัสเซียมีการทำธุรกรรมการฟอกเงินมากที่สุด โดยส่วนใหญ่เป็นการค้าสิ่งผิดกฎหมายบนระบบออนไลน์ โดยเฉพาะอย่างยิ่งจาก Dark Web ชื่อ Hydra ซึ่งเป็นเว็บไซต์ค้าสิ่งผิดกฎหมายที่ใหญ่ที่สุดในปัจจุบัน ส่วนในประเทศจีนมีการฟอกเงินจากธุรกรรมการขโมยเงินสกุลเข้าหรัสบนระบบโปรแกรมออนไลน์และการเรียกค่าไถ่โดยความร่วมมือกับ Lazarus Group ซึ่งอาจเป็นหน่วยงานที่อาจเกี่ยวข้องกับรัฐบาลเกาหลีเหนือ สำหรับประเทศสหรัฐอเมริกานั้นปรากฏมีความเกี่ยวข้องกับธุรกรรมการหลอกลวง และการขโมยเงินสกุลเข้ารหัสบนระบบโปรแกรมออนไลน์ สำหรับประเทศที่มีปริมาณธุรกรรมการเคลื่อนย้ายเงินสกุลเข้ารหัสจากผู้ให้บริการนอกระบบที่สำคัญคือ ประเทศแอฟาริกาใต้ อังกฤษ ยูเครน เกาหลีใต้ เวียดนาม เตรกี และฝรั่งเศส เป็นต้น (Chainalysis, 2021)

ปัจจุบันพฤติกรรมการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ได้ปรับเปลี่ยนรูปแบบจากการใช้บริการกับผู้ให้บริการหลากหลายราย หรือใช้รหัสที่ตั้งกระเป๋าเงินจำนวนมากมาเป็น

การเลือกใช้บริการเฉพาะกลุ่ม โดยในปี 2020 มีการทำธุรกรรมฟอกเงินผ่านผู้ให้บริการผิดกฎหมาย 1,867 รายแรก รวมมูลค่าประมาณ 1.70 พันล้านเหรียญสหรัฐ หรือคิดเป็นร้อยละ 75.0 ในขณะที่มีการทำธุรกรรมผ่านผู้ให้บริการผิดกฎหมาย 24 รายแรก สูงถึง 566 ล้านเหรียญสหรัฐ และจากรายงานได้ชี้ให้เห็นว่า ผู้ให้บริการผิดกฎหมายรายใหญ่มักมีธุรกรรมที่เกี่ยวข้องกัน หรือมีลักษณะความสัมพันธ์เป็นกลุ่มผู้ให้บริการขนาดใหญ่ จึงนับว่าประเด็นข้อสังเกตุที่ควรเสนอให้หน่วยบังคับใช้กฎหมายให้ความสำคัญในการสืบค้นติดตามแบะแสจากผู้ให้บริการผิดกฎหมายรายใหญ่ข้างต้นเป็นสำคัญ และควรมีมาตรการเฝ้าระวังอย่างเคร่งครัด ในการตรวจสอบการแปลงค่าเป็นเงินตราปกติจากรหัสที่ตั้งจากกระเป๋าเงินที่มีส่วนเกี่ยวข้องกับกลุ่มผู้ให้บริการดังกล่าว (Chainalysis, 2021)

4.5.3 แนวทางแนวทางการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน และแนวทางปฏิบัติเพื่อการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะ และสามารถเพิ่มประสิทธิภาพการบังคับใช้เชิงปฏิบัติการ

Financial Action Task Force (FATF) ได้ให้ความสำคัญต่อเงินสกุลเข้ารหัสซึ่งเป็นนวัตกรรมทางการเงินที่ส่งผลกระทบต่อระบบการเงินโลก โดยมีกลไกการดำเนินการที่สามารถปิดบังตัวตนผู้ใช้งาน ข้ามเขตประเทศแบบไร้พรมแดนด้วยความรวดเร็ว จึงเป็นมูลเหตุจูงใจที่สำคัญต่อผู้กระทำผิด หรืออาชญากรทางเศรษฐกิจให้ความสนใจในการนำไปใช้เป็นเครื่องมือในการทำธุรกรรมฟอกเงินที่ไม่ชอบด้วยกฎหมาย (FATF, 2019) ทั้งนี้เนื่องจากการนำเงินสกปรกเข้าสู่กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส (Placement Stage) มีความสะดวกแก่อาชญากรที่ไม่ต้องระบุตัวตนผู้ใช้งาน และการโยกย้ายถ่ายเทเงินสกุลเข้ารหัสด้วยความรวดเร็วแบบไร้พรมแดนสามารถสร้างความซับซ้อนของธุรกรรม (Layering) เพื่อเพิ่มภาระการติดตามสืบค้น และกลบเกลื่อนร่องรอยเส้นทางธุรกรรมความเชื่อมโยงระหว่างต้นทางกับปลายทาง และผู้รับปลายทางสามารถดำเนินการแปลงสภาพเงินสกุลเข้ารหัสไปเป็นเงินตราทั่วไป หรือทรัพย์สินอื่นที่ชอบด้วยกฎหมาย (Cash Out Strategy) ได้โดยง่าย

ดังนั้น เมื่อประมวลความเห็นเชิงเสนอแนะต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสด้วยเทคนิควิธีเดลฟาย ร่วมกับการสังเคราะห์ความเห็นประกอบกับหลักการของทฤษฎีการเลือกกระทำอย่างมีเหตุผล ทฤษฎีปกตินิสัย และทฤษฎีป้องกันอาชญากรรม เพื่อให้ได้ข้อเสนอแนวทางที่จะบรรลุเป้าหมายการป้องปราม ในการลดโอกาสการก่อเหตุกระทำผิด และย่อมส่งผลในทิศทางให้การก่ออาชญากรรมเกิดขึ้นน้อยลงเช่นเดียวกัน (Lilly et al., 2015) และการลดทอนประโยชน์ที่พึงได้รับจากการกระทำผิด หรือการก่อภาระเพิ่มต้นทุนการสูญเสียจากการก่อเหตุ (Siegel, 2013) โดยมี หลักการสำคัญของการป้องปรามอาชญากรรม คือ การเพิ่มภาระ

ความยากลำบากแก่ผู้กระทำผิดในการก่อเหตุ (Increase the Effort Needed to Committing Crime) การเพิ่มความเสี่ยงต่อการถูกตรวจพบการกระทำผิดหรือถูกจับกุม (Increase the Risks of Committing Crime) การลดผลตอบแทนหรือประโยชน์ที่ได้รับจากการก่อเหตุ (Reduce the Rewards of Committing Crime) การลดแรงกระตุ้นและสร้างสำนึกผิดเพื่อหลีกเลี่ยงจากเหตุกระทำผิด (Reduce Provocation/ Induce Guilt or Shame for Committing Crime) และการลดเหตุและข้ออ้างที่ผู้กระทำผิดจะใช้แก้ตัวเมื่อก่อเหตุ (Reduce excuses for committing crime) ทั้งนี้ การป้องปรามจะบรรลุตามวัตถุประสงค์ได้ ยังขึ้นอยู่กับความร่วมมือของ ผู้มีหน้าที่รับผิดชอบ 3 กลุ่ม ซึ่งปฏิบัติหน้าที่กำกับดูแลปัจจัยสำคัญที่เป็นสาเหตุให้เกิดการก่ออาชญากรรมขึ้นได้ คือ ผู้พิทักษ์ (Guardians) รับผิดชอบหน้าที่ในการตรวจตราดูแลให้ความปลอดภัยป้องกันการตกเป็นเหยื่อ ผู้ดูแล (Handler) รับผิดชอบหน้าที่ดูแลบุคคลที่มีโอกาสจะเป็นผู้กระทำผิด และผู้จัดการ (Manager) รับผิดชอบหน้าที่ดูแลเฝ้าระวังพื้นที่เสี่ยงที่มีโอกาสต่อการเกิดเหตุ (Lilly et al., 2015; Siegel, 2013) โดยสามารถสังเคราะห์แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสตามหลักการของทฤษฎีป้องกันอาชญากรรมได้ดังนี้

การเพิ่มภาระความยากลำบากแก่ผู้กระทำผิดในการก่อเหตุ โดยผู้จัดการ ซึ่งเป็นหน่วยงานบังคับใช้กฎหมายควรกำหนดหลักเกณฑ์มาตรฐานสำหรับการบันทึกข้อมูล เพื่อการตรวจพิสูจน์ตัวตนของผู้ใช้งาน (KYC) โดยให้ระบุข้อมูลที่จำเป็น เพื่อการรู้จักตัวตนอย่างเพียงพอก่อนอนุญาตให้เข้าใช้ระบบงาน และให้มีกระบวนการตรวจสอบทบทวนข้อมูลส่วนบุคคลของผู้ใช้งานให้ทันสมัยอย่างสม่ำเสมอ เพื่อใช้เป็นฐานข้อมูลสำคัญในการตรวจสอบตัวตนของเจ้าของกระเป๋าเงินหรือผู้ใช้งาน เมื่อต้องการสืบค้นธุรกรรมที่อาจเข้าข่ายต้องสงสัย ซึ่งเป็นแนวทางที่พยายามสร้างภาระเพิ่มแก่ผู้ใช้งานด้วยระบบการกำกับจากหน่วยงานของรัฐ เข้าไปจัดการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัส โดยที่เป็นแนวทางขัดแย้งกับปรัชญาพื้นฐานทางเทคโนโลยีของระบบปฏิบัติการบล็อกเชนของเงินสกุลเข้ารหัส แต่หน่วยงานสากลและหน่วยงานต่อต้านการฟอกเงินของหลายประเทศก็ให้ความสำคัญกับแนวทางป้องกันนี้เช่นกัน อย่างไรก็ตาม การออกกฎระเบียบในการกำกับดูแลการทำธุรกรรมเงินสกุลเข้ารหัส หรือผู้ให้บริการรับอนุญาตควรคำนึงถึงความสมดุลระหว่างการสร้างภาระและข้อจำกัดในการดำเนินธุรกิจ เพื่อการป้องกันอาชญากรรม กับประโยชน์สาธารณะที่จะได้รับจากความคล่องตัวทางธุรกิจและลดต้นทุนการทำธุรกรรม และควรมีกระบวนการรับฟังความคิดเห็นจากหน่วยงานปฏิบัติการที่เกี่ยวข้อง เพื่อให้ได้แนววิธีการที่เหมาะสมต่อการปฏิบัติงานก่อนการออกประกาศมาตรการนั้น มิฉะนั้นอาจส่งผลกระทบทางกลับเสมือนส่งเสริมให้ผู้ใช้งานในประเทศไปใช้บริการกับผู้ให้บริการนอกระบบ หรือผู้ให้บริการต่างประเทศที่มีความคล่องตัวกว่า อีกทั้งการออกกฎระเบียบในลักษณะดังกล่าว ควรอ้างอิงกับแนวทางหรือข้อแนะนำตามหลักมาตรฐานการ

ปฏิบัติงานสากล เช่น FATF Recommendations ในการสร้างบรรทัดฐานการปฏิบัติงานร่วม เพื่อการตรวจสอบสืบค้นผู้ต้องสงสัย กับฐานข้อมูลระหว่างประเทศ

การเพิ่มความเสี่ยงต่อการถูกตรวจพบการกระทำผิดหรือถูกจับกุม นับเป็นแนวทางการป้องกันสำคัญซึ่งได้รับความเห็นเชิงเสนอแนะหลายแนวทาง โดยผู้พิทักษ์ ซึ่งเป็นหน่วยงานปฏิบัติการควรสร้างเครือข่ายความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมาย ทั้งด้านการปฏิบัติงานว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และด้านการกำกับดูแลการกิจกรรมด้านเทคโนโลยีการเงินเพื่อเศรษฐกิจและสังคม เพื่อช่วยเหลือสนับสุนนตรวจสอบสืบค้นเข้าถึงข้อมูลส่วนบุคคลของผู้ต้องสงสัย และเส้นทางการทำธุรกรรมเงินสกุลเข้ารหัสให้ทันต่อการโยกย้ายธุรกรรมเงินสกุลเข้ารหัสในระบบนิเวศ เช่น สำนักงานป้องกันและปราบปรามการฟอกเงิน สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ธนาคารแห่งประเทศไทย สำนักงานตำรวจแห่งชาติ กรมสอบสวนคดีพิเศษ สำนักงานอัยการ กรมสรรพากร กรมบังคับคดี สำนักงานคณะกรรมการกิจการกระจายเสียงกิจการโทรทัศน์และโทรคมนาคมแห่งชาติ เป็นต้น รวมถึงบูรณาการหน้าที่รับผิดชอบของหน่วยงานแบบองค์รวม ด้วยแผนปฏิบัติงานร่วมตามลำดับขั้นตอนที่ช่วยลดการปฏิบัติงานที่อาจมีขอบเขตงานทับซ้อนกัน อีกทั้งควรสร้างกรอบความร่วมมือกับองค์กรระหว่างประเทศและหน่วยงานของแต่ละประเทศที่รับผิดชอบงานด้านการต่อต้านการฟอกเงิน เพื่อประสานความร่วมมือในการแลกเปลี่ยนข้อมูลสำคัญที่เกี่ยวข้อง เทคโนโลยีการสืบค้นผู้ต้องสงสัย รวมถึงองค์ความรู้ประสบการณ์กรณีศึกษาการกระทำความผิดที่เกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัส และกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ซึ่งจะช่วยเสริมสร้างทักษะของผู้ปฏิบัติงานได้เท่าทันกับการเคลื่อนไหวของอาชญากร โดยเฉพาะอย่างยิ่งด้านเครื่องมือทางเทคโนโลยีในการตรวจสอบสืบค้นวิเคราะห์เส้นทางธุรกรรมต้องสงสัย โดยการเชื่อมต่อกับฐานข้อมูลสาธารณะในระบบปฏิบัติการ บล็อกเชนของเงินสกุลเข้ารหัสเป้าหมายนั้น ซึ่งเป็นแนวทางในการเพิ่มศักยภาพของผู้พิทักษ์ ในขณะเดียวกันก็เป็นการเพิ่มความเสี่ยงต่ออาชญากรที่อาจการถูกตรวจพบการกระทำผิดมากขึ้นได้

การลดผลตอบแทนหรือประโยชน์ที่ได้รับจากการก่อเหตุ โดยผู้จัดการ ซึ่งเป็นหน่วยงานบังคับใช้กฎหมาย ควรออกกฎระเบียบเกี่ยวกับกระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัยที่ชัดเจนต่อการปฏิบัติงาน โดยมอบหมายหน้าที่แก่หน่วยงานหนึ่งรับผิดชอบดูแลกระเป๋าเงินอิเล็กทรอนิกส์กลางของรัฐ (State Wallet) เพื่อการรวบรวมจัดเก็บและจัดการเงินสกุลเข้ารหัสของผู้ต้องสงสัยหรือของกลางแห่งคดี ซึ่งเป็นการการยับยั้งกระบวนการฟอกผลประโยชน์จากการกระทำผิด นอกจากนี้ควรออกกฎระเบียบปฏิบัติในกระบวนการสืบสวนเกี่ยวข้องกับบริบทธุรกรรมเงินสกุลเข้ารหัสอย่างชัดเจน[30] เช่น การแสวงหาพยานหลักฐานดิจิทัลในระบบนิเวศ

[30] ทั้งนี้ในปี 2018 กรมบังคับคดี กระทรวงยุติธรรม ได้มอบหมายให้ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย ทำการศึกษาเรื่องการบังคับคดีกับสินทรัพย์ดิจิทัล ตามรายงานฉบับสมบูรณ์

เงินสกุลเข้ารหัส โดยเครื่องมือทางเทคโนโลยีโปรแกรมประยุกต์เข้าร่วมวิเคราะห์ข้อมูลจากฐานข้อมูลสาธารณะ การสืบสวนเพื่อเข้าถึงกระเป๋าเงินของอาชญากรที่อาจต้องเข้าไปกระทำบางประการต่อหลักฐาน ซึ่งจะช่วยเพิ่มประสิทธิภาพในกระบวนการยึดอายัดเงินสกุลเข้ารหัสจากกระเป๋าเงินต้องสงสัย เป็นการลดทอนและประโยชน์สำคัญที่ผู้กระทำผิดคาดหวังจะได้รับ

การลดแรงกระตุ้นและสร้างสำนึกผิดเพื่อหลีกเลี่ยงจากเหตุกระทำผิด โดยผู้พิทักษ์ซึ่งเป็นหน่วยงานปฏิบัติการ ควรเผยแพร่องค์ความรู้เกี่ยวกับเงินสกุลเข้ารหัสเป็นการทั่วไปไม่จำกัดเฉพาะเจ้าหน้าที่ผู้รับผิดชอบงานโดยตรงทั้งบุคคลากรในส่วนกลางและเจ้าหน้าที่ประจำพื้นที่ แต่ให้หมายรวมถึง สาธารณะ และ ประชาชนทั่วไปได้ทราบถึงกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัส และความเสี่ยงที่อาจเกิดขึ้นจากการทำธุรกรรมเงินสกุลเข้ารหัส หรืออาจถูกนำไปใช้เป็นเครื่องมือในการฟอกเงิน รวมถึงช่วยสร้างความเข้าใจที่ถูกต้องแก่อาชญากรที่ต้องหลีกเลี่ยง การถูกตรวจสอบเส้นทางธุรกรรมเงินสกุลเข้ารหัส เมื่อใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงินเนื่องจากระบบปฏิบัติการบล็อกเชน ซึ่งเป็นเทคโนโลยี่สนับสนุนระบบนิเวศเงินสกุลเข้ารหัสเป็นระบบฐานข้อมูลแบบกระจายศูนย์ส่งผลให้มีโอกาสในการถูกตรวจสอบ และเข้าถึงเส้นทาง การทำธุรกรรมในระบบนิเวศเงินสกุลเข้ารหัสได้ เพื่อลดแรงกระตุ้นในการนำเงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน

และเป็นการลดเหตุและข้ออ้างที่ผู้กระทำผิดจะใช้แก้ตัวเมื่อก่อเหตุ โดยผู้ดูแล ซึ่งเป็นหน่วยงานสนับสนุน ควรสร้างความร่วมมือขององค์กรภาคเอกชนที่เกี่ยวข้องกับธุรกิจเงินสกุลเข้ารหัส ซึ่งปฏิบัติหน้าที่ในฐานะตัวกลางระหว่างผู้ใช้งานกับหน่วยงานรัฐที่ทำหน้าที่กำกับดูแลธุรกรรมเงินสกุลเข้ารหัส เพื่อเพิ่มประสิทธิภาพการประสานความร่วมมือกับหน่วยงานรัฐ และสนับสนุนส่งเสริมพัฒนาการแนวทางการกำกับดูแลกันเอง และสร้างความเข็มแข็งต่ออุตสาหกรรมเงินสกุลเข้ารหัสในทำนองเดียวกับสมาคมธนาคารไทย สมาคมบริษัทหลักทรัพย์ หรือสมาคม ผู้ประกอบธุรกิจการเงินอื่น เป็นต้น เพื่อช่วยเสริมความเข้าใจต่อบริบทของเงินสกุลเข้ารหัส และลดเหตุข้ออ้างจากการสำคัญผิดในการก่อเหตุของอาชญากร

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

โครงการศึกษาเรื่องการบังคับคดีกับสินทรัพย์ดิจิทัล (ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2018)

บทที่ 5
สรุปผลการศึกษาและข้อเสนอแนะ

การศึกษาวิจัยเรื่อง “แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส” มีวัตถุประสงค์เพื่อศึกษาคุณลักษณะเฉพาะ กลไกการทำงาน และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส ซึ่งเป็นปัจจัยที่มีอิทธิพลต่ออาชญากรในการตัดสินใจใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน รวมถึงรูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และใช้กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส สำหรับผลประโยชน์ที่ได้จากการกระทำผิด และแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากลในปัจจุบัน

ในการศึกษาวิจัยนี้ ผู้วิจัยใช้ระเบียบวิธีการวิจัยเชิงคุณภาพ (Qualitative Research) ซึ่งประกอบด้วยเทคนิคการวิจัยในขั้นตอนการดำเนินการวิจัย คือ (1) การวิจัยเชิงเอกสาร Documentary Research) เพื่อทำความเข้าใจบริบทของประเด็นที่ทำการศึกษา และการสร้างกรอบแนวคิดการวิจัย (2) การสัมภาษณ์เชิงลึก (In-depth Interviews) เพื่อรวบรวมข้อมูลและวิเคราะห์ผลการศึกษาตามวัตถุประสงค์การวิจัย (3) เทคนิควิธีเดลฟาย (Delphi Technique) เพื่อสำรวจความเห็นอิสระเชิงเสนอแนะ ต่อประเด็นศึกษาแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมสำหรับบริบทในประเทศไทยและสากล โดยวิธีการเลือกผู้ให้ข้อมูลสำคัญแบบเฉพาะเจาะจง (Purposive Sampling) จำนวน 19 ราย จาก 4 กลุ่มผู้เชี่ยวชาญ ซึ่งเป็นบุคคลากรประจำหน่วยงาน ซึ่งมีหน้าที่รับผิดชอบเกี่ยวข้องกับการปฏิบัติงานตามมาตรการสากลว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย รวมถึงการกำกับดูแลการดำเนินกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม ประกอบด้วย กลุ่มที่ 1 กลุ่มหน่วยงานหลักของภาครัฐมีหน้าที่รับผิดชอบโดยตรงต่อการป้องกันและปราบปรามการฟอกเงิน ซึ่งรวมถึงหน่วยงานรัฐที่มีหน้าที่รับผิดชอบกิจกรรมด้านเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม กลุ่มที่ 2 หน่วยงานองค์สถาบันการเงินทั้งภาครัฐและภาคเอกชน กลุ่มที่ 3 หน่วยงานในกระบวนการยุติธรรม และกลุ่มที่ 4 หน่วยงานผู้ประกอบวิชาชีพที่ไม่ใช่สถาบันการเงิน ซึ่งหมายรวมถึงผู้ประกอบการที่เกี่ยวข้องกับกิจกรรมเทคโนโลยีดิจิทัลเพื่อเศรษฐกิจและสังคม

ทั้งนี้ ผู้วิจัยได้นำข้อมูลจากการสมัภาษณ์เชิงลึกมาวิเคราะห์เนื้อหาในส่วนที่เกี่ยวกับกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัส และปัจจัยที่อาจมีอิทธิพลต่ออาชญากรในการเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และมีโอกาสทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส รวมถึงเทคนิควิธีการในกระบวนการติดตามสืบสวนหาผู้ต้องสังสัย ในระบบนิเวศเงินสกุลเข้ารหัสที่ใช้เงินสกุลเข้ารหัสเป็น

เครื่องมือในการฟอกเงิน นอกจากนี้ ผู้วิจัยได้วิเคราะห์ข้อมูลโดยอาศัยข้อมูลเชิงคุณภาพจากการสัมภาษณ์เชิงลึกร่วมกับเทคนิควิธีเดลฟาย เพื่อวิเคราะห์เนื้อหาและประมวลผลสังเคราะห์ข้อเสนอแนะ ในส่วนที่เกี่ยวกับแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากลในปัจจุบัน และแนวทางปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะ และสามารถเพิ่มประสิทธิภาพการดำเนินงาน อันนำมาสู่การสร้างข้อสรุปตลอดจนการตีความข้อค้นพบที่ได้จากการศึกษาวิจัยนี้ ดังนี้

5.1 สรุปผลการศึกษา

5.1.1 คุณลักษณะเฉพาะ กลไกการทำงาน และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส รวมถึงบริบทของเงินสกุลเข้ารหัสที่เป็นปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

5.1.2 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และใช้กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส สำหรับผลประโยชน์ที่ได้จากการกระทำผิด

5.1.3 แนวทางการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากล

5.2 ข้อเสนอแนะ

5.2.1 ข้อเสนอแนะเชิงนโยบาย

5.2.2 ข้อเสนอแนะเชิงปฏิบัติการ

5.2.3 ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

5.1 สรุปผลการศึกษา

ผู้วิจัยได้ดำเนินวิจัยตามระเบียบวิธีที่กล่าวถึงข้างต้น โดยได้สรุปผลการศึกษาตามวัตถุประสงค์การวิจัย ดังนี้

5.1.1 คุณลักษณะเฉพาะ กลไกการทำงาน และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส รวมถึงบริบทของเงินสกุลเข้ารหัสที่เป็นปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

จากการศึกษาวิจัยเอกสารร่วมกับการสัมภาษณ์เชิงลึก ทำให้ทราบถึงคุณลักษณะเฉพาะ กลไกการทำงาน และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัสที่อาจมีอิทธิพลต่อ

การตัดสินใจของอาชญากร เป็นปัจจัยให้ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมการฟอกเงินโดยเงินสกุลเข้ารหัส โดยสรุปดังนี้

5.1.1.1 *“เงินสกุลเข้ารหัส”* มีคุณลักษณะเป็นหน่วยชุดรหัสข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบเครือข่ายอิเล็กทรอนิกส์ เพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนมูลค่า หรือสิทธิอื่นใดระหว่างบุคคลต่อบุคคลโดยตรง โดยซาโตชิ นากาโมโต ได้พัฒนาและนำเสนอ *“บิตคอยน์”* เป็นเงินสกุลเข้ารหัสสกุลแรกของโลกตั้งแต่ปี 2008 และในเวลาต่อมานักพัฒนาระบบงานได้นำเสนอเงินสกุลเข้ารหัสใหม่สู่ระบบเครือข่ายอย่างต่อเนื่อง จนถึงเดือนมีนาคม 2021 มีเงินสกุลเข้ารหัสหมุนเวียนอยู่ในระบบตลาดเงินอิเล็กทรอนิกส์ไม่น้อยกว่า 8,900 สกุลเงิน ด้วยขนาดตลาดมูลค่ารวมประมาณ 1.8 ล้านล้านเหรียญสหรัฐ ทั้งนี้เงินสกุลเข้ารหัสแต่ละสกุลอาจมีคุณลักษณะเฉพาะ และกลไกการทำงานแตกต่างกันเป็นการเฉพาะ แต่มักจะมีคุณลักษณะเฉพาะ และกลไกการทำงานทั่วไปทำนองเดียวกัน กล่าวคือ

เงินสกุลเข้ารหัสดำเนินการบนระบบปฏิบัติบล็อกเชน เพื่อการติดต่อโอนรหัสข้อมูลแสดงมูลค่า หรือสิทธิบางประการระหว่างผู้ใช้งาน (Peer-to-Peer หรือ P2P) โดยไม่มีหน่วยงานใดเป็นผู้กำกับดูแลระบบนิเวศเงินสกุลเข้ารหัส ซึ่งระบบจะปฏิบัติงานต่อเนื่องไปตามเงื่อนไขที่ระบุใน White Paper โดยผู้ใช้งานสามารถเข้าสู่ระบบได้อย่างไม่มีเงื่อนไข และไม่จำเป็นต้องลงทะเบียนอัตลักษณ์ตัวตนแท้จริงของผู้ใช้งานก่อนเข้าสู่ระบบ ทั้งนี้ธุรกรรมการโอนมูลค่าเงินสกุลเข้ารหัสระหว่างผู้โอนและผู้รับโอนจะถูกบันทึกเป็นรหัสข้อมูล (Cryptographic) ของรายการลักษณะคล้ายสมุดบัญชีเรียงลำดับตามชุดข้อมูล (Block) ซึ่งแต่ละชุดข้อมูลจะมีรหัสความสัมพันธ์กับชุดข้อมูลในลำดับถัดไปอย่างต่อเนื่องคล้ายห่วงโซ่ (Chain) พร้อมทั้งทำการส่งรหัสเปิดสาธารณะ (Public Key) ซึ่งกำกับชุดข้อมูลที่ถูกบันทึกไว้ในระบบไปยังปลายทาง โดยผู้รับโอนจะนำรหัสเปิดส่วนบุคคล (Private Key) เสมือนเป็นลายมือดิจิทัลของเจ้าของบัญชี ร่วมกับรหัสเปิดสาธารณะเพื่อเปิดรายการข้อมูลที่ถูกจัดส่งมา ทั้งนี้รายการธุรกรรมดังกล่าวจะถูกบันทึกในสมุดบัญชีอิเล็กทรอนิกส์เป็นฐานข้อมูลแบบกระจายศูนย์ (Distributed) ซึ่งผู้ใช้งานทุกคนสามารถเข้าถึงฐานข้อมูลที่นี้ได้อย่างไม่มีข้อจำกัด และสามารถติดตามความเคลื่อนไหวของรายการระหว่างผู้ใช้งานต่างๆได้ หรือที่เรียกว่า Distributed Ledger Technology – DLT

อีกทั้งระบบการตรวจพิสูจน์ยืนยันรายการ (Proof of Work – PoW) ถือเป็นหัวใจสำคัญของกลไกในการสร้างความน่าเชื่อถือ ต่อระบบการโอนมูลค่าเงินสกุลเข้ารหัสระหว่างผู้โอนและผู้รับโอนที่อาจไม่มีประวัติความสัมพันธ์ต่อกัน และเป็นการโอนมูลค่าข้ามเขตประเทศ ซึ่งไม่มีหน่วยงานของรัฐใดให้การรับรอง โดยระบบงานได้สร้างกลไกให้ผู้ใช้งานทั่วไปเข้าร่วมเป็นผู้ตรวจพิสูจน์ด้วยการแก้โจทย์รหัสทางคณิตศาสตร์ประจำชุดข้อมูล เพื่อการยืนยันด้วยฉันทามติของผู้ร่วมดำเนินการ ที่เรียกว่า นักขุด (Miner) ซึ่งจะได้รับค่าตอบแทนเป็นเงินสกุลเข้ารหัสที่ถูกกำหนดไว้

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ล่วงหน้า ดังนั้น เมื่อชุดข้อมูลที่ได้รับการพิสูจน์ยืนยันแล้ว จะไม่สามารถแก้ไขเปลี่ยนแปลงข้อมูลได้ (Immutable) เนื่องจาก รหัสข้อมูลที่ได้รับการพิสูจน์ในส่วนท้ายของชุดข้อมูล จะมีความสัมพันธ์ทางคณิตศาสตร์กับรหัสส่วนต้นของชุดข้อมูลถัดไปอย่างต่อเนื่อง นอกจากนี้กลไกการทำงานของเงินสกุลเข้ารหัสดำเนินการบนระบบปฏิบัติการบล็อกเชน (Blockchain) ซึ่งเป็นระบบงานแบบเปิด (Open Source) โดยผู้พัฒนาระบบงานทั่วไปสามารถเข้าถึงฐานข้อมูลแบบกระจายศูนย์ และสามารถพัฒนาโปรแกรมประยุกต์ภายใต้เงื่อนไขเฉพาะเข้าเชื่อมต่อกับระบบปฏิบัติการบล็อกเชนได้ จึงเป็นประเด็นสำคัญ ที่สามารถสร้างโปรแกรมเข้าตรวจสอบเส้นทางการทำธุรกรรมระหว่างผู้ใช้งานในระบบนิเวศเงินสกุลเข้ารหัส แม้ว่าธุรกรรมนั้นจะดำเนินการข้ามประเทศแบบไร้พรมแดน แต่อยู่ในบนระบบเทคโนโลยี่เดียวกัน คือระบบอินเตอร์เน็ตและระบบปฏิบัติการบล็อกเชน

5.1.1.2 กลไกการทำงานของเงินสกุลเข้ารหัสมีผู้ดำเนินการที่เกี่ยวข้อง ซึ่งอาจเป็นทั้งองค์กร หน่วยงาน กลุ่มบุคคลหรือบุคคล รวมถึงเครื่องมือคอมพิวเตอร์และอุปกรณ์สื่อสาร ที่จะทำให้ระบบปฏิบัติการเงินสกุลเข้ารหัสสามารถดำเนินการให้บรรลุวัตถุประสงค์ของผู้ใช้งาน อันประกอบด้วย ผู้ดำเนินการสำคัญ ได้แก่ ผู้พัฒนาเงินสกุลเข้ารหัส (Inventor) หรือผู้ออกเงินสกุลเข้ารหัส (Issuer หรือ Promotor) ซึ่งอาจเป็นบุคคล กลุ่มบุคคล หรือองค์กรที่สร้างโครงสร้างระบบกลไกการทำงานเฉพาะของเงินสกุลเข้ารหัสนั้นบนระบบปฏิบัติการบล็อกเชน ดังเช่น ซาโตชิได้นำเสนอเงินสกุลเข้ารหัสสกุลแรกของโลกที่เรียกว่า *“บิตคอยน์”* เป็นต้น รวมถึงผู้โอนซึ่งเป็นบุคคลที่ประสงค์จะนำเงินสกุลเข้ารหัสเข้าสู่ระบบนิเวศ เพื่อส่งไปยังรหัสที่ตั้งปลายทางที่กำหนด และผู้รับโอนซึ่งเป็นบุคคลที่จะได้รับเงินสกุลเข้ารหัสตามคำสั่งของผู้โอน โดยไม่มีระบบการพิสูจน์ตัวตนที่แท้จริงของผู้ใช้งาน และระบบงานไม่อยู่ภายใต้การกำกับของหน่วยงานใด แต่มีนักขุด (Miner) เป็นบุคคลที่เข้าสู่ระบบ เพื่อร่วมปฏิบัติหน้าที่ในการพิสูจน์ยืนยันรายการด้วยการพิสูจน์รหัสคณิตศาสตร์ของแต่ละชุดข้อมูล โดยได้รับเงินสกุลเข้ารหัสดังกล่าวเป็นค่าตอบแทน

นอกจากผู้ดำเนินการหลัก ที่ทำให้เกิดธุรกรรมการโอนมูลค่าเงินสกุลเข้ารหัสในระบบนิเวศแล้ว ยังมีองค์ประกอบส่วนอื่นที่ควรทราบ เพื่อเข้าใจถึงกลไกการทำงานของเงินสกุลเข้ารหัส ซึ่งอาชญากรอาจนำไปใช้เป็นเครื่องมือในการฟอกเงิน รวมถึงเทคนิควิธีที่อาจช่วยเจ้าหน้าที่ในการติดตามเส้นทางธุรกรรมในระบบนิเวศเงินสกุลเข้ารหัส ได้แก่ กระเป๋าเงินอิเล็กทรอนิกส์ (Wallet) เป็นอุปกรณ์รักษาความปลอดภัยสำหรับบรรจุเงินสกุลเข้ารหัสที่เชื่อมต่อกับระบบนิเวศเพื่อการถือครอง การโอน และการรับโอนเงินสกุลเข้ารหัส โดยกระเป๋าเงินจะสามารถใช้งานได้ต้องประกอบ ด้วยรหัสเปิดสาธารณะ และรหัสเปิดส่วนบุคคลที่เป็นข้อมูลรหัสลับเฉพาะสำหรับแสดงความเป็นเจ้าของกระเป๋าเงิน ซึ่งมีระบบการทำงานหลายประเภทขึ้นอยู่กับอุปกรณ์สื่อสารที่เชื่อมต่อกับระบบนิเวศ กล่าวคือ Cold Wallet เป็นกระเป๋าเงินที่อยู่ในอุปกรณ์คอมพิวเตอร์ ซึ่งไม่มีการเชื่อมต่อกับระบบอินเตอร์เน็ต หรือ Hot Wallet เป็นกระเป๋าเงินที่อยู่ในคอมพิวเตอร์ส่วนตัว หรือ

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

โทรศัพท์เคลื่อนที่ซึ่งเชื่อมต่อกับระบบอินเตอร์เน็ตตลอดเวลา และอนุญาตให้เข้าถึงกระเป๋าเงินได้ ในกรณีที่ ผู้ใช้บริการไม่มีกระเป๋าเงินของตนเองเป็นการเฉพาะ ก็อาจจัดเก็บเงินสกุลเข้ารหัสไว้กับผู้ให้บริการกระเป๋าเงินอิเล็กทรอนิกส์ Wallet Provider ซึ่งเป็นผู้ให้บริการดูแลรักษาเงินสกุลเข้ารหัสแก่ผู้ใช้บริการทั่วไป รวมถึงดำเนินการโอน และการรับโอนมูลค่าตามคำสั่งของผู้ใช้บริการ

ทั้งนี้ ผู้ดำเนินการอีกส่วนหนึ่งที่มีส่วนช่วยในการอำนวยความสะดวก เพื่อการโอนมูลค่า ได้แก่ ผู้ให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัส (Cryptocurrency Exchanger) เป็นการให้บริการแลกเปลี่ยนระหว่างเงินสกุลเข้ารหัสกับเงินสกุลเข้ารหัสอื่น หรือเป็นเงินตราปกติ และผู้ให้บริการค้าเงินสกุลเข้ารหัส (Exchange Market) เป็นการดำเนินธุรกิจลักษณะตัวกลางในการค้าแลกเปลี่ยนเงินสกุลเข้ารหัสซึ่งการดำเนินงานคล้ายกับตลาดหลักทรัพย์ ซึ่งรวมถึงการแปลงมูลค่าระหว่างเงินตราปกติกับเงินสกุลเข้ารหัส นอกจากนี้ยังมีผู้ให้บริการค้าเงินสกุลเข้ารหัสในรูปแบบอัตโนมัติ (Trading Platform) ซึ่งดำเนินธุรกิจลักษณะตัวกลางเช่นกัน แต่เป็นรูปแบบการค้าออนไลน์ที่ดำเนินการโดยอัตโนมัติ และไม่มีหน่วยงานใดรับผิดชอบในการจัดการ (Decentralized Exchanger) แต่ระบบงานจะดำเนินการจับคู่คำสั่งโอนมูลระหว่างผู้ใช้บริการ ด้วยโปรแกรมการทำงานอัตโนมัติ รวมถึงผู้ให้บริการระบบชำระเงิน (Payment System) เป็นการให้บริการระบบการชำระเงินค่าสินค้าหรือบริการทั้งในรูปแบบเงินสกุลเข้ารหัส หรือการแปลงค่าเป็นเงินตราปกติ ซึ่งมีลักษณะคล้ายระบบการชำระเงินผ่านระบบออนไลน์ของธนาคารในปัจจุบัน และเครื่องให้บริการเบิกถอนเงินสกุลเข้ารหัส (Cryptocurrency Automatic Teller Machine หรือ Bitcoin ATM) เป็นเครื่องให้บริการอัตโนมัติ ซึ่งผู้ใช้บริการสามารถทำคำสั่งโอน รับโอน แลกเปลี่ยนเงินสกุลเข้ารหัสโดยตรง หรือทำการโอนแลกเปลี่ยนกับเงินตราปกติ ซึ่งผู้ดำเนินการที่กล่าวถึงทั้งหมดข้างต้น ในกลไกการทำงานของเงินสกุลเข้ารหัส อาจมีโอกาสเข้าไปมีส่วนเกี่ยวข้อง หรือร่วมดำเนินการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

5.1.1.3 ปัจจุบัน มาตรการทางกฎหมายในการให้นิยามความหมาย ของเงินสกุลเข้ารหัสควรเข้าข่ายลักษณะใด ยังมีความแตกต่างกันในหลายประเทศ ขึ้นอยู่กับพื้นฐานของระบบกฎหมายด้านเศรษฐกิจในประเทศนั้น ว่าสมควรกำหนดสถานภาพของเงินสกุลเข้ารหัส เพื่อให้มีสภาพบังคับทางกฎหมายเป็นไปในลักษณะใด กล่าวคือ ควรกำหนดให้เสมือนเป็นเงินตรา (Currency) สินทรัพย์ (Property) สินค้า (Commodity) หรือหลักทรัพย์ (Security) ซึ่งถือเป็นประเด็นสำคัญต่อกรอบแนวคิด ในการกำหนดนโยบาย และมาตรการทางกฎหมาย เพื่อการกำดับดูแลธุกรรมเงินสกุลเข้ารหัส และผู้ประกอบกิจการที่เกี่ยวข้อง รวมถึงการจัดเก็บภาษีอากร อย่างไรก็ตาม มีบางประเทศที่กำหนดมาตรการทางกฎหมาย ต้องห้ามการทำธุรกรรมเงินสกุลเข้ารหัสเป็นสิ่งที่ผิดกฎหมายภายในเขตอำนาจประเทศของตน กล่าวคือ

กลุ่มประเทศที่มีมาตรการทางกฎหมายรองรับสถานภาพเงินสกุลเข้ารหัส และยินยอมให้สามารถทำธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสได้อย่างชอบด้วยกฎหมาย ได้แก่ ประเทศญี่ปุ่น ซึ่งเป็นประเทศแรกที่ยอมรับสถานภาพทางกฎหมายของบิตคอยน์ ตั้งแต่เดือนเมษา 2017 จนกลายเป็นตลาดธุรกรรมเงินสกุลเข้ารหัสที่มีขนาดใหญ่ระดับโลกในปัจจุบัน ประเทศออสเตรีย ที่ให้การยอมรับบิตคอยน์ในปี 2017 เช่นเดียวกัน ประเทศมอร์ต้า ที่เป็นศูนย์กลางแลกเปลี่ยนเงินสกุลเข้ารหัสที่สำคัญของโลก และประเทศเยอรมัน บลาซิล เป็นต้น

กลุ่มประเทศที่มีมาตรการต้องห้าม และไม่ยอมรับสภานภาพเงินสกุลเข้ารหัส ถือเป็นสิ่งที่ไม่ชอบด้วยกฎหมาย ต้องห้ามสถาบันการเงินดำเนินธุรกรรมใดๆที่เกี่ยวข้อง รวมถึงการเสนอขายเงินสกุลเข้ารหัสสุกลใหม่ภายในขอบเขตประเทศของตน ได้แก่ ประเทศแอลจิเรีย โบลีเวีย โมรอคโค เนปาล ปากีสถาน และเวียดนาม รวมถึงประเทศที่มีเศรษฐกิจขนาดใหญ่ เช่น ประเทศจีน เกาหลีใต้ และรัสเซีย ส่วนประเทศการ์ตา และบาเรน ไม่ต้องห้ามเฉพาะธุรกรรมเงินสกุลเข้ารหัสที่ดำเนินการในต่างประเทศเท่านั้น

กลุ่มประเทศสุดท้าย ที่มีมาตรการทางกฎหมายยอมรับสถานภาพเงินสกุลเข้ารหัสในบางลักษณะ และอนุญาตให้ดำเนินธุรกรรมที่เกี่ยวข้องบางลักษณะที่อยู่ภายใต้กรอบมาตรการกำกับดูแลที่เคร่งครัด รวมถึงการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ ที่มีลักษณะเข้าข่ายหลักทรัพย์หรือตราสารหนี้ เช่น ประเทศนิวซีแลนด์ เนเธอร์แลนด์ โดยในบางประเทศไม่ต้องห้ามประชาชนในการถือครองเงินสกุลเข้ารหัสเพื่อการลงทุน แต่อาจมีข้อกำหนดในการกำกับการทำธุรกรรมของสถาบันการเงินที่เกี่ยวข้องกับเงินสกุลเข้ารหัส เช่น ประเทศบังคลาเทศ อิหร่าน ลิตเธอร์เนีย กัมพูชา และไทย เป็นต้น

ทั้งนี้ คณะทำงานขององค์สหประชาชาติ Financial Action Task Force on Money Laundering (FATF) ได้ให้ความสนใจต่อระบบนิเวศของระบบปฏิบัติการแบบกระจายศูนย์ (Distributed Ledger Technology – DLT) และบริบทของเงินสกุลเข้ารหัสที่ส่งผลต่อระบบการเงินโลกเพิ่มมากขึ้นตามลำดับ จึงได้พัฒนาแนวคิดเพื่อการปรับปรุงข้อแนะนำในการกำกับดูแลเงินสกุลเข้ารหัส โดยได้เสนอให้เพิ่มเติมนิยาม *“สินทรัพย์เสมือน (Virtual Assets) หมายถึงมูลค่าของหน่วยข้อมูลดิจิทัลที่สามารถใช้เพื่อการค้า การโอนมูลค่า การชำระเงิน และการลงทุนบนระบบเครือข่ายดิจิทัล”* พร้อมทั้งปรับปรุงข้อแนะนำที่ 15 (Recommendation 15 – New Technologies) เพื่อการจัดการลดความเสี่ยงจากสินทรัพย์เสมือน (Virtual Assets) และแนะนำให้รัฐควรให้ความเชื่อมั่นได้ว่า ผู้ให้บริการที่เกี่ยวข้องกับสินทรัพย์เสมือน (Virtual Assets Service Providers - VASP) จะต้องอยู่ภายใต้กฎระเบียบ การกำกับ การอนุญาตเพื่อให้ระบบการติดตามและสร้างความมั่นใจด้วยมาตรการป้องกันและปราบปรามการฟอกเงินอย่างเหมาะสม โดยหมายรวมถึงระบบการตรวจสอบข้อมูลตัวตนผู้ใช้งาน และการรายงานธุรกรรมต้องสงสัย เป็นต้น

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

นอกจากนี้ รัฐบาลจีนได้เริ่มตระหนักถึงผลกระทบจากนโยบายการกีดกัน และต้องห้ามธุรกรรมเงินสกุลเข้ารหัส โดยได้ให้คำนิยามเงินสกุลเข้ารหัส เป็น *"Virtual Currency"* เทียบเสมือนสินค้าที่เป็นทรัพย์สินไร้รูปร่างซึ่งจะได้รับความคุ้มครองภายใต้กฎหมาย และได้ปรับนโยบายโดยมอบหมายให้ธนาคารกลางแห่งชาติจีนพัฒนาเงินสกุลเข้ารหัสของชาติ หรือเรียกว่า *"Sovereign Cryptocurrency"* บนระบบนิเวศแบบเปิดทำนองเดียวกับระบบปฏิบัติการบล็อกเชน เพื่อให้บริการโอนมูลค่าแก่ผู้ใช้งานระหว่างกันโดยตรงเช่นเดียวกับเงินสกุลเข้ารหัสทั่วไป แต่จะมีการกำกับโดยธนาคารกลางจีน จึงถือเป็นเงินสกุลเข้ารหัสลักษณะแบบรวมศูนย์ (Centralized Cryptocurrency) หรือที่เรียกว่า *"Central Bank Digital Currency – CBDC"* เพื่ออำนวยความสะดวก สามารถเข้าถึงได้ง่าย มีความปลอดภัยสูง ต้นทุนธุรกรรมต่ำ และให้บริการประชาชนครอบคลุมวงกว้างรองรับนโยบายสังคมไร้เงินสดแทนระบบการเงินหยวนจีน ทั้งนี้ รัฐบาลจีนกำลังมีแผนพัฒนามาตรการทางกฎหมายที่จะรับรองธุรกรรมเงินสกุลเข้ารหัส ภายใต้หลักการเป็นมุ่งสร้างความสมดุลระหว่างการเสริมสร้างนวัตกรรมกับการป้องกันการเก็งกำไรโดยไม่เป็นธรรม เมื่อรัฐบาลได้ออกเงินสกุลเข้ารหัสของรัฐบาลจีนเอง ในขณะเดียวกันหลายประเทศได้ให้ความสนใจในการเริ่มพัฒนาเงินสกุลเข้ารหัสที่กำกับโดยหน่วยงานของรัฐเพื่อส่งเสริมระบบเศรษฐกิจดิจิทัลและระบบการเงินแบบไร้เงินสด รวมถึงประเทศไทย ซึ่งธนาคารแห่งประเทศไทยได้ริเริ่มพัฒนาโครงการอินทนนท์[31] โดยใช้ระบบจัดการฐานข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology – DLT) บนระบบปฏิบัติการบล็อกเชน ด้วยการแปลงเงินที่รับฝากจากสถาบันการเงินที่เข้าร่วมโครงการให้อยู่ในรูปสกุลเงินดิจิทัลที่ออกโดยธนาคารกลาง (Central Bank Digital Currency: CBDC) เพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนและโอนชำระเงินระหว่างกันได้ และพัฒนาไปสู่การทำธุรกรรมชำระเงินระหว่างประเทศโดยตรง ซึ่งจะช่วยเพิ่มประสิทธิภาพให้มีความรวดเร็ว มีต้นทุนธุรกรรมที่ถูกลง แต่ยังคงมีความปลอดภัยสูง

สำหรับประเทศไทย ได้มีการตราพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัลขึ้นในปี 2018 (พ.ศ. 2561) ซึ่งเป็นกฎหมายที่เกี่ยวกับเงินสกุลเข้ารหัส เพื่อกำกับดูแลการะดมทุนผ่าน

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

[31] โครงการอินทนนท์เป็นหนึ่งในโครงการที่ธนาคารแห่งประเทศไทย (ธปท.) ริเริ่มขึ้น โดยร่วมกับสถาบันการเงิน 8 แห่ง และบริษัท R3 (ผู้พัฒนา DLT ใน Corda Platform) ในการทดสอบความเป็นไปได้ในการประยุกต์ใช้ DLT กับระบบการชำระเงินของประเทศ ในลักษณะ Proof of Concept โดยมีวัตถุประสงค์เพื่อส่งเสริมให้ ธปท. และสถาบันการเงินมีความเข้าใจและเท่าทันเทคโนโลยี ผ่านการลงมือพัฒนาและจำลองระบบต้นแบบ โดยผู้เข้าร่วมโครงการทั้งสถาบันการเงินและ ธปท. ได้ร่วมกันออกแบบโครงสร้างพื้นฐานทางการเงิน โดยใช้กระบวนการคิดเชิงออกแบบรวมทั้งยังให้นักพัฒนาระบบจากสถาบันการเงินที่เข้าร่วมโครงการร่วมกันพัฒนาระบบการชำระเงินต้นแบบเพื่อเป็นรากฐานสำหรับการพัฒนาระบบการเงินของไทยในอนาคต
https://www.bot.or.th/Thai/BOTMagazine/Pages/256203TheKnowledge_ProjectInthanon.aspx

สินทรัพย์ดิจิทัล การประกอบธุรกิจและการดำเนินกิจการเกี่ยวกับสินทรัพย์ดิจิทัล ส่งเสริมการนำเทคโนโลยี่มาพัฒนาเศรษฐกิจและสังคมอย่างยั่งยืน คุ้มครองผู้ลงทุนมิให้ถูกฉ้อโกงหรือถูกหลอกลวงจากผู้ไม่สุจริต การป้องกันการนำสินทรัพย์ดิจิทัลไปใช้สนับสนุนธุรกรรมที่ผิดกฎหมาย รวมถึงดูแลการซื้อขายในศูนย์ซื้อขายสินทรัพย์ดิจิทัลให้มีความเป็นธรรม โปร่งใส และตรวจสอบได้ โดยอยู่ใต้การกำกับของสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ซึ่งตามเจตนารมณ์ของกฎหมายฉบับนี้ มีหลักการสำคัญในการกำกับดูแลผู้ประกอบธุกรกิจที่เกี่ยวข้องกับเงินสกุลเข้ารหัส ในทำนองเดียวกับการกำกับดูแลผู้ประกอบธุรกิจเกี่ยวกับหลักทรัพย์ ดังนั้น กล่าวโดยสรุปดูเสมือนว่าประเทศไทยได้กำหนดสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส มีลักษณะทำนองเดียวกับ *“หลักทรัพย์”* ซึ่งเป็นสินทรัพย์เพื่อการลงทุนประเภทหนึ่ง

ผู้วิจัยจึงมีความเห็นว่า ประเทศไทยได้กำหนดมาตรการทางกฎหมายต่อเงินสกุลเข้ารหัส เสมือนเป็น *“หลักทรัพย์”* มีความเหมาะสม เนื่องจากเงินสกุลเข้ารหัสขาดคุณสมบัติความเป็นเงินตราหลายประการ กล่าวคือ การเป็นสื่อกลางการแลกเปลี่ยนสินค้าและบริการ (A Medium of Exchange) ซึ่งมีการยอมรับความเป็นสื่อกลางในการอำนวยความสะดวก เพื่อการแลกเปลี่ยนสินค้าและบริการยังอยู่ในวงจำกัด แม้ว่าจะมีแนวโน้มของกลุ่มผู้ใช้บริการขยายตัวเพิ่มขึ้น แต่ส่วนใหญ่ยังจำกัดเฉพาะธุรกิจการค้าทางระบบออนไลน์ บริการเกมส์ออนไลน์ การบริการแลกเปลี่ยนเงินสกุลเข้ารหัส โดยเฉพาะอย่างยิ่งธุรกรรมที่เกิดขึ้นเกินกว่าร้อยละ 80 เป็นการทำธุรกรรมเพื่อการเก็งกำไร สำหรับการเป็นหน่วยวัดมูลค่าสินค้าและบริการ (A Unit of Account) เนื่องจากเงินสกุลเข้ารหัสไม่มีมูลค่าในตนเอง หรือมีมูลค่าของสินทรัพย์มีค่าใดหนุนหลัง หากแต่มูลค่าจะเป็นเท่าใดขึ้นอยู่กับปริมาณความต้องการและการยอมรับตามกลไกทางตลาดโดยตรง อีกทั้งมูลค่าของเงินสกุลเข้ารหัสมีความผันผวนเปลี่ยนแปลงค่าอย่างรวดเร็วอย่างไม่มีข้อจำกัดด้านเวลา ส่งผลให้ขาดเสถียรภาพในการรักษามาตรฐานของการเป็นหน่วยวัดมูลค่า และประการสุดท้ายการดำรงรักษาและสะสมความมั่งคั่งทางเศรษฐกิจ (A Store of Value) นั้น ด้วยราคาของเงินสกุลเข้ารหัสมีความผันผันเปลี่ยนแปลงอย่างมีนัยสำคัญ ทั้งทิศทางที่สูงค่าขึ้นหรือลดค่าลง จึงเป็นความเสี่ยงต่อการถือครองการถือครอง เพื่อสะสมความมั่งคั่งทางเศรษฐกิจ แต่จะมีลักษณะเป็นการเก็งกำไรมากกว่า

ในขณะเดียวกัน ธนาคารแห่งประเทศไทย ได้เริ่มพัฒนาโครงการอินทนนท์เป็นเงินสกุลดิจิทัลที่อยู่ภายใต้การกำกับของหน่วยงานรัฐ และมีสินทรัพย์เงินบาทหนุนหลัง ภายใต้เทคโนโลยี่บนระบบปฏิบัติการบล็อกเชนเช่นเดียวกับระบบนิเวศเงินสกุลเข้ารหัส เพื่อการแลกเปลี่ยนโอนชำระเงินระหว่างกันโดยตรง ทั้งในประเทศและระหว่างประเทศ และเมื่อสามารถขยายการให้บริการสู่วงกว้างในระดับรายย่อย เพื่อระบบเศรษฐกิจไร้เงินสดได้สำเร็จ ก็อาจเป็นอีกมาตรการสำคัญในการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เนื่องจากจะเกิดการเชื่อมต่อทางเทคโนโลยี่ระหว่างระบบการเงินดิจิทัลแบบรวมศูนย์ที่กำกับโดยรัฐ กับการหมุนเวียน

เงินสกุลเข้ารหัสแบบไร้ตัวกลาง บนระบบการจัดการฐานข้อมูลแบบกระจายศูนย์ทำให้สามารถติดตามเส้นทางธุรกรรมในระบบนิเวศเงินสกุลเข้ารหัสที่เชื่อมต่อ ถึงระบบรวมศูนย์ที่สามารถติดตามตัวตนผู้ทำธุรกรรมได้

5.1.1.4 บริบทของเงินสกุลเข้ารหัสที่เป็นปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

ดังที่ได้กล่าวถึง คุณลักษณะเฉพาะ และกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสข้างต้น จะเห็นได้ว่าปัจจัยที่มีอิทธิพลอาชญากรต่อในการเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน ส่วนหนึ่งเป็นปัจจัยจากพัฒนาการทางเทคโนโลยี่ของระบบปฏิบัติการบล็อกเชน และอีกส่วนหนึ่งเป็นปัจจัยจากมาตรการทางกฎหมายในการกำกับดูแลเงินสกุลเข้ารหัส ซึ่งสามารถกล่าวโดยสรุปได้ ดังนี้

ปัจจัยจากกลไกการทำงานแบบกระจายศูนย์ ไร้การควบคุมจากหน่วยงานใดบนระบบนิเวศเงินสกุลเข้ารหัส และเปิดกว้างต่อผู้ใช้งานสามารถเข้าสู่ระบบโอนมูลค่าให้แก่กันได้อย่างไม่มีเงื่อนไขรอการตรวจสอบหรืออนุญาตใด ผู้ใช้งานไม่จำเป็นต้องแสดงตัวตนก่อนใช้งาน อย่างไรก็ตามด้วยระบบจัดการฐานข้อมูลแบบกระจายศูนย์ จึงอาจมีความเสี่ยงต่อการสืบค้นเส้นทางการทำธุรกรรม แต่ในทางปฏิบัติยังมี ความซับซ้อนในการดำเนินการ และต้องใช้เทคโนโลยี่ขั้นสูงหรือโปรแกรมเฉพาะสนับสนุนการสืบค้น

แม้ว่าปัจจัยจากการอำพรางตัวตนผู้ใช้งาน และความยากต่อการสืบค้นเส้นทางธุรกรรมแล้ว กลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสยังสามารถปกป้องการเข้าถึงกระเป๋าเงินในกรณีที่เกิดการสืบค้นถึงเส้นทางธุรกรรมต้องสงสัย โดยการเปิดกระเป๋าเงินต้องสงสัยนั้นจะกระทำได้ก็ต่อเมื่อมีทั้งรหัสเปิดสาธารณะและรหัสเปิดส่วนบุคคลของเจ้าของพร้อมกันเท่านั้น จึงเป็นการช่วยปกป้องเงินสกุลเข้ารหัสของเจ้าของโดยธรรมชาติของระบบปฏิบัติการ และไม่มีกฎระเบียบจากหน่วยงานใด ที่จะสามารถใช้อำนาจทางกฎหมายในการเข้าถึงรหัสข้อมูลส่วนบุคคลสำหรับเปิดกระเป๋าเงินหรือบังคับใช้อำนาจอายัดเงินสกุลเข้ารหัสได้ นอกจากนี้ ยังมีเทคโนโลยี่ที่เข้าช่วยสนับสนุนกลไกการทำงานของเงินสกุลเข้ารหัส เพื่อเพิ่มความยากต่อการสืบค้นเส้นทางธุรกรรมขึ้นอีก โดยใช้งานร่วมบนระบบปฏิบัติการ TOR Browser เพื่อลวงรหัสที่ตั้งของผู้ใช้งานในขณะติดต่อเข้าสู่ระบบ รวมถึงการใช้บริการกับผู้ให้บริการ Crypto Mixer หรือ Tumbler ในการตัดความเชื่อมโยงเส้นทางธุรกรรมระหว่างต้นทางและปลายทาง

ปัจจัยอีกประการหนึ่ง คือ ความสะดวกรวดเร็วและสามารถทำธุรกรรมข้ามประเทศแบบไร้พรมแดนได้อย่างเสรี โดยไม่มีข้อจำกัดขนาดมูลค่าของรายการ เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสเป็นการดำเนินการบนระบบอินเตอร์เน็ต ซึ่งปัจจุบันมีโครงข่ายการสื่อสารเชื่อมโยงถึงกันทั้งในประเทศและระหว่างประเทศ ดังนั้น จึงสามารถทำธุรกรรมจำนวนมูลค่าสูงได้ในคราวเดียว

และสามารถกระจายถ่ายเทเป็นธุรกรรมย่อยได้สะดวก รวมถึงสามารถสร้างความซับซ้อนของเส้นทางธุรกรรมหลายชั้นได้อย่างรวดเร็ว และสามารถรวบรวมมูลค่าผ่านหลายประเทศไปยังปลายทางในประเทศที่สามารถแปลงค่าเป็นเงินตราปกติ หรือทรัพย์สินอื่นได้สะดวก

เมื่อเปรียบเทียบกับการฟอกเงินด้วยเครื่องมืออื่น ในกระบวนการยักย้ายถ่ายโอนในขั้นตอนกระจายรายย่อย เพื่อกลบเกลื่อนร่องรอยหลีกเลี่ยงการตรวจสอบ ก่อนจะรวบรวมกลับมาเป็นเงินที่ชอบด้วยกฎหมายนั้น ต้นทุนการจัดการเงินสด หรือแปลงเป็นทรัพย์สินอื่น เช่น รถยนต์หรูงานศิลป์ ที่ดิน หรือเครื่องลายคราม จะมีต้นทุนดำเนินการค่อนข้างสูง ในขณะที่ต้นทุนการทำธุรกรรมของเงินสกุลเข้ารหัสต่อรายการต่ำกว่ามาก จึงสามารถสร้างความซับซ้อนและก่อภาระการสืบค้นตรวจสอบให้ยากต่อการเข้าถึงรายการได้อย่างมีประสิทธิภาพมากกว่า ด้วยต้นทุนดำเนินการต่ำกว่า นอกจากนี้ วิธีการจัดเก็บกระเป๋าเงินประเภท Cold Wallet ซึ่งเป็นอุปรณ์คอมพิวเตอร์ที่จัดเก็บข้อมูลและไม่เชื่อมต่อกับระบบอินเตอร์เน็ต เช่น USB Drive ในปัจจุบันมีขนาดเล็กสามารถพกพาติดตัว เก็บซ่อนไว้ในพื้นที่เล็กขนาดเท่านิ้วหัวแม่มือเท่านั้น จึงมีโอกาสสูงที่จะเก็บรักษามูลค่าทรัพย์ไว้ได้โดยลอดพ้นจากการตรวจสอบสืบค้นจากเจ้าหน้าที่ จึงถือเป็นปัจจัยการรักษามูลค่าทรัพย์สินด้วยความปลอดภัย และต้นทุนการดูแลต่ำ

นอกจากปัจจัยที่เกี่ยวข้องกับกลไกการทำงานของเงินสกุลเข้ารหัสแล้ว ยังมีปัจจัยด้านมาตรการทางกฎหมาย และการบังคับใช้เชิงปฏิบัติที่มีอิทธิพลต่อการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน เนื่องจากเงินสกุลเข้ารหัสถือเป็นนวัตกรรมเทคโนโลยี่ทางการเงินที่ส่งผลกระทบต่อระบบการเงินโลก ซึ่งแต่ละประเทศมีมาตรการภายในประเทศต่อเงินสกุลเข้ารหัสที่แตกต่างกัน ตั้งแต่ยอมรับสถานภาพทางกฎหมายจนไปถึงขั้นต้องห้ามเป็นสิ่งผิดกฎหมาย อีกทั้ง ยังขาดมาตรการสากลและนโยบายระหว่างประเทศต่อบริบทของเงินสกุลเข้ารหัส จึงถือเป็นโอกาสแก่อาชญากรที่จะอาศัยช่องว่างทางกฎหมายระหว่างประเทศ ในการถ่ายโอนเพื่อการแปรสภาพเป็นเงินตราในประเทศที่ยอมรับสถานภาพทางกฎหมาย และหลีกเลี่ยงประเทศที่มีกฎหมายบังคับใช้เคร่งครัด

ทั้งนี้ การศึกษาถึงปัจจัยที่มีอิทธิพลต่อการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน เพื่อได้ทราบถึงมูลเหตุจูงใจของอาชญากรที่อาจใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการก่ออาชญากรรมและทำการฟอกเงินโดยธุรกรรเงินสกุลเข้ารหัส และเข้าใจถึงบริบทของหน่วยบังคับใช้กฎหมายในการพิพักษ์ป้องกันและปราบปรามอาชญากรรม รวมถึงผลกระทบที่อาจเกิดขึ้นต่อระบบเศรษฐกิจและสังคม ซึ่งจะนำไปสู่การศึกษาแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อบริบทประเทศไทยและสากลในปัจจุบัน รวมถึงแนวปฏิบัติเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้อย่างมีประสิทธิภาพในลำดับต่อไป

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

5.1.2 รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และใช้กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส สำหรับผลประโยชน์ที่ได้จากการกระทำผิด

รูปแบบของอาชญากรรม ที่อาจใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการก่ออาชญากรรม หรือใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกผลประโยชน์ที่ได้รับจากการกระทำผิดให้เป็นเงินตราหรือทรัพย์สินอื่นที่ชอบด้วยกฎหมาย เพื่อใช้เป็นแหล่งเงินทุนในการก่ออาชญากรรมต่อไปนั้น จากการศึกษาสามารถสรุปโครงสร้างของรูปแบบของอาชญากรรมในลักษณะดังกล่าวได้ว่าส่วนใหญ่มักเป็นอาชญากรรมที่ร่วมกันกระทำการกันเป็นกลุ่มบุคคล และมักก่อให้เกิดความเสียหายทางเศรษฐกิจแก่เหยื่อจำนวนมากรายในวงกว้าง มีขนาดของผลประโยชน์ที่ได้รับจากการกระทำผิดจำนวนมูลค่าสูงในระยะเวลาสั้น โดยมีข้อจำกัดด้านเวลาจำเป็นต้องจัดการกระจายผลประโยชน์และทำการฟอกเงินเป็นเงินที่ชอบด้วยกฎหมายในระยะสั้นให้เร็วที่สุด ซึ่งอาจเป็นอาชญากรรมที่ไม่ได้รับผลประโยชน์เป็นเงินสกุลเข้ารหัสโดยตรง แต่อาจใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน นอกจากนี้ ยังหมายรวมถึงอาชญากรรมที่กระทำความผิดบนระบบอินเตอร์เน็ตหรือระบบออนไลน์ ซึ่งส่วนใหญ่สามารถเรียกรับผลประโยชน์เป็นเงินสกุลเข้ารหัสบนระบบงานดียวกันได้ทันที จึงสามารถดำเนินการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้อย่างต่อเนื่อง โดยอาชญากรกลุ่มนี้อาจแบ่งหน้าที่ความรับผิดชอบกระทำการร่วมกันเป็นกลุ่มบุคคล หรือองค์กรอาชญากรรม ทั้งการกระทำโดยความร่วมกันภายในประเทศและกลุ่มบุคคลที่ปฏิบัติงานในต่างประเทศ โดยส่วนหนึ่งของบุคคลากรในขบวนการมักมีความรู้ ความเชี่ยวชาญทางเทคโนโลยี่ทางคอมพิวเตอร์ ระบบการสื่อสาร รวมถึงนวัตกรรมทางการเงิน ซึ่งรวมถึงระบบนิเวศเงินสกุลเข้ารหัส

ดังนั้น อาชญากรจึงได้พัฒนาแสวงหาช่องโอกาส จากการใช้เครื่องมือในการฟอกเงินรูปแบบใหม่ ที่จะช่วยให้สามารถหลีกเลี่ยงการตรวจติดตามร่องรอยของการยักย้ายถ่ายเทผลประโยชน์ที่ได้จากการกระทำผิดเสมอ แม้ว่าเงินสดจะเป็นเครื่องมือสามัญ แต่ก็เป็นเครื่องมือที่มีประสิทธิผลต่อกระบวนการฟอกเงินซึ่งสามารถยักย้าย ถ่ายเท กระจายแยกย่อยด้วยการส่งมอบโดยตรงต่อกัน อีกทั้งสามารถนำไปใช้จ่ายก่อให้เกิดประโยชน์ได้โดยตรง ไม่ต้องผ่านขั้นตอนการแปลงค่าใดอีก แต่ก็มีข้อจำกัดในการรวบรวมเงินสด หรือส่งมอบเงินสดจำนวนมูลค่าสูง รวมถึงการส่งมอบข้ามเขตแดนประเทศ เนื่องจากกฎระเบียบการป้องกันและปราบปรามการฟอกเงิน มีการกำกับสถาบันการเงินให้ดำเนินการตรวจสอบพิสูจน์ตัวตนเจ้าของบัญชีเงินฝาก และการติดตามเฝ้าระวังธุรกรรมการเงินที่มีความเคลื่อนไหวอย่างน่าสงสัย รวมถึงการจำกัดวงเงินการเบิกถอนเงินสด และรายงานธุรกรรมการเบิกถอนเงินสดที่เกินกว่าวงเงิน เมื่อวิเคราะห์เปรียบเทียบลักษณะของเงินสดกับเงินสกุลเข้ารหัสจะพบว่าคุณลักษณะที่เหมือนกัน คือ ผู้ถือครองเงินสดในกระเป๋าของตนก็ไม่จำเป็นต้องแสดงตัวตนและจำนวนการถือครองเงินสดในมือให้บุคคลใดทราบ ในขณะที่ผู้ใช้งานระบบนิเวศเงินสกุลเข้ารหัสก็จำเป็นไม่ต้องแสดงอัตลักษณ์ตัวตนก่อนเข้าใช้งาน และบุคคลภายนอกไม่

สามารถเข้าถึงข้อมูลจำนวนมูลค่าเงินสกุลเข้ารหัสในกระเป๋าเงินเช่นกัน โดยความแตกต่างสำคัญคือ ระบบนิเวศเงินสกุลเข้ารหัสไม่มีข้อจำกัดในการโอนส่งมอบเงินสกุลเข้ารหัส สามารถโอนให้บุคคลใดทั้งในประเทศและข้ามประเทศได้อย่างรวดเร็ว โดยไม่มีหน่วยงานใดทำหน้าที่กำกับดูแล แม้ว่าระบบปฏิบัติการบล็อกเชนจะเป็นระบบฐานข้อมูลแบบกระจายศูนย์ บุคคลทั่วไปสามารถเข้าถึง และตรวจสอบเส้นทางการทำธุรกรรมระหว่างผู้โอนและผู้รับโอนได้ ภายใต้การใช้โปรแกรมทางเทคโนโลยีขั้นสูงก็ตาม แต่เมื่อตรวจพบกระเป๋าเงินต้องสงสัยก็ไม่สามารถเข้ายึด อายัดเงินสกุลเข้ารหัสในกระเป๋าเงินของเจ้าของได้ เว้นแต่จะสามารถค้นพบรหัสเปิดส่วนบุคคลของเจ้าของกระเป๋าเงินได้ อย่างไรก็ตามในปัจจุบันเงินสกุลเข้ารหัสยังมีข้อด้อยกว่าเงินสด เนื่องจากความเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการโดยเงินสกุลเข้ารหัสยังอยู่ในวงจำกัด ดังนั้นจึงมีความจำเป็นต้องแปลงค่าเป็นเงินตราทั่วไป เพื่อนำไปใช้ประโยชน์ทางเศรษฐกิจได้

ในกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสนั้น อาชญากรจะดำเนินการส่งเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมายเข้าสู่ระบบนิเวศเงินสกุลเข้ารหัส เพื่อทำการฟอกเงิน (Placement) จากนั้นก็จะหาวิธีการกลบเกลื่อนร่องรอยเส้นทางธุรกรรมในระบบนิเวศ (Layering) เพื่อสร้างความยากต่อการติดตามสืบค้น และสามารถส่งมอบเงินสกุลเข้ารหัสแก่ผู้รับปลายทาง โดยไม่มีความสัมพันธ์เชื่อมโยงถึงผู้ส่งต้นทาง เนื่องจากระบบปฏิบัติการบล็อกเชนเปิดกว้างต่อผู้ใช้งานทั่วไป สามารถนำโปรแกรมประยุกต์เข้าเชื่อมต่อระบบ ในการสืบค้นข้อมูลเส้นทางการทำธุรกรรมระหว่างผู้ใช้งานทั้งหลายได้ โดยอาจใช้ศูนย์บริการแปรสภาพเงินสกุลเข้ารหัสเป็นผู้ดำเนินการกระจายธุรกรรมจากผู้ส่งต้นทาง เป็นธุรกรรมย่อยโอนย้ายไปปนกับเงินสกุลเข้ารหัสของผู้ใช้บริการรายอื่น พร้อมทั้งทยอยส่งมอบเงินสกุลเข้ารหัสของผู้ใช้บริการรายอื่น เป็นหลายช่วงเวลาให้แก่ผู้รับปลายทางจนครบมูลค่า เพื่อสร้างความซับซ้อนของธุรกรรมให้ยากต่อการตรวจสอบเส้นทางธุรกรรม หรืออาจใช้วิธีการเข้าร่วมทำธุรกรรมกับกลุ่มเครือข่ายผู้ใช้งานหลายรายในระบบปฏิบัติการ CoinJoin ที่มีกลไกการกระจายธุรกรรมของผู้ใช้งานหลายรายร่วมกัน และจัดชุดคำสั่งเพื่อทำการโอนธุรกรรมย่อยไข้วกันไปมาระหว่างผู้ใช้งานภายในกลุ่มเครือข่าย พร้อมทั้งทำการทยอยส่งมอบเงินสกุลเข้ารหัสไปยังผู้รับปลายทางที่กำหนดด้วยมูลค่ารวมใกล้เคียงกับเงินสกุลเข้ารหัสที่ส่งเข้าสู่ระบบ หรืออาจใช้วิธีการรับเงินสกุลเข้ารหัสจากนักขุด ซึ่งเป็นค่าขุดที่ได้รับเงินสกุลเข้ารหัสโดยตรงจากระบบที่สร้างขึ้น โดยไม่มีเส้นทางธุรกรรม รวมถึงการทำธุรกรรมโดย Privacy Coin ซึ่งเป็นเงินสกุลเข้ารหัสประเภทหนึ่งที่มีกลไกการควบคุมปกปิดข้อมูล เส้นทางธุรกรรมระหว่างผู้โอนและผู้รับ รวมถึงการใช้เทคโนโลยีการปกปิดข้อมูลอีกหลายวิธี อีกทั้งถ้าอาชญากรดำเนินการบนระบบปฏิบัติการ TOR Browser ก็จะยิ่งเพิ่มความยากต่อการสืบค้นตัวตนผู้ใช้งานที่ออกคำสั่งโอน เนื่องจากระบบงานมีกลไกการลวงรหัสที่ตั้งของผู้ใช้งาน และการเคลื่อนย้ายรหัสที่ตั้งในระหว่างการใช้งานตลอดเวลา และถ้าอาชญากรใช้ผลประโยชน์ที่ได้จากการกระทำผิดหมุนเวียนภายในระบบนิเวศเงินสกุลเข้ารหัส หรือทำการเก็บรักษา

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

เงินสกุลเข้ารหัสไว้ในกระเป๋าเงินแบบ Cold Wallet ซึ่งไม่ได้เชื่อมต่อกับระบบอินเตอร์เน็ตแล้ว ก็จะเป็นการยากต่อการติดตามสืบค้นมากยิ่งขึ้น ดังนั้น เมื่ออาชญากรทำการเคลื่อนย้ายเงินสกุลเข้ารหัสออกจากระบบนิเวศเงินสกุลเข้ารหัสในโลกเสมือนไปสู่ระบบสถาบันการเงินบนโลกกายภาพ (Cash Out Strategy) ซึ่งเป็นจุดเฝ้าระวัง (Gateway) ที่หน่วยบังคับใช้กฎหมายต่อต้านการฟอกเงินสามารถตรวจสอบข้อมูลเกี่ยวกับธุรกรรมและเข้าถึงรายการธุรกรรมนั้นได้ ในขณะเดียวกันอาชญากรอาจเลือกทำการแปลงค่าเงินสกุลเข้ารหัสเป็นเงินตรา หรือทรัพย์สินอื่นในเขตประเทศที่มีเครื่องมืออำนวยความสะดวกในการดำเนินธุรกรรม รวมถึงในเขตประเทศที่การบังคับใช้กฎหมายไม่เข้มงวด หรือไม่มีกฎหมายใดที่ใช้บังคับเกี่ยวกับธุรกรรมเงินสกุลเข้ารหัส

ทั้งนี้ จากการศึกษารูปแบบอาชญกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และทำการฟอกเงินโดยธุกรรมเงินสกุลเข้ารหัสนั้น ไม่ว่าจะเป็นอาชญากรรมจากการหลอกลวงฉ้อโกงประชาชนในลักษณะแชร์ลูกโซ่ (Ponzi Scheme) การค้ายาเสพติดรวมถึงการค้ายาเสพติดบนระบบออนไลน์ (Dark Web) การเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิวเตอร์ (Ransomware) และการพนันรวมถึงการพนันบนระบบออนไลน์ มักมีโครงสร้างรูปแบบอาชญากรรมที่คล้ายกัน กล่าวคือผู้กระทำความผิดมักร่วมกระทำการกันเป็นกลุ่มบุคคลโดยแบ่งหน้าที่การงาน ก่อให้เกิดความเสียหายทางเศรษฐกิจแก่เหยื่อจำนวนมากรายในวงกว้าง และอาชญากรได้รับประโยชน์จากการกระทำผิดจำนวนมูลค่าสูงในระยะเวลาสั้น ดังนั้น เงินสกุลเข้ารหัสจึงอาจถูกใช้เป็นเครื่องมือในการฟอกเงินด้วยมูลเหตุแห่งประโยชน์จากการอำพรางตัวตนผู้ใช้งาน ทำธุรกรรมได้ด้วยความรวดเร็ว ไร้ข้อจำกัดด้านเวลาและสถานที่ รวมถึงสามารถทำธุรกรรมข้ามประเทศ โดยไม่มีหน่วยงานใดกำกับควบคุม อีกทั้งสามารถดูแลรักษาเงินสกุลเข้ารหัสในระบบนิเวศได้อย่างปลอดภัยด้วยต้นทุนต่ำ และช่องโอกาสทางกฎหมายบนความแตกต่างของมาตราการในหลายประเทศ จึงเป็นปัจจัยที่มีอิทธิพลต่อการใช้เงินสกุลเข้ารหัสเป็นสื่อกลางในการกระทำผิด และเป็นเครื่องมือในการฟอกเงิน

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

อย่างไรก็ตามอาชญากรรมทางเศรษฐกิจและอาชญากรรมไซเบอร์ที่นอกเหนือจากที่ได้นำมากล่าวในที่นี้แล้ว ยังมีลักษณะการก่ออาชญากรรมอีกหลายประเภทที่อาจมีโครงสร้างรูปแบบทำนองเดียวกัน เช่น การคอรัปชั่น หรือที่เรียกว่า การฉ้อราษฎรบังหลวง เป็นการฉ้อโกงผลประโยชน์ขององค์กรทั้งภาครัฐและเอกชนในจำนวนมูลค่าสูง แต่อาจไม่ได้สร้างความเสียหายแก่เหยื่อจำนวนมากราย แต่องค์กรอาจได้รับความเสียหายในวงกว้างได้ การสร้างความไม่เป็นธรรมในการซื้อขายหลักทรัพย์ โดยปัจจุบันมีระบบการซื้อขายออนไลน์ทำให้สะดวกต่อการเชื่อมโยงเข้ากับระบบการซื้อขายเงินสกุลเข้ารหัส ซึ่งอาจก่อให้เกิดความเสียแก่เหยื่อหลายรายและขาดความเชื่อมั่นต่อระบบการซื้อขายหลักทรัพย์ การติดสินบนทั้งระบบราชการและภาคเอกชน รวมถึงการหลีกเลี่ยงภาษีที่อาจใช้เงินสกุลเข้ารหัสเป็นสื่อกลางในการส่งมอบผลประโยชน์ โดยเฉพาะอย่างยิ่งด้วยการทำธุรกรรมผ่านผู้ให้บริการนอกระบบ หรือผู้ให้บริการต่างประเทศ การหลอกลวงผ่านระบบพาณิชย์อิเล็กทรอนิกส์

จากการรับชำระค่าสินค้าล่วงหน้าโดยไม่ส่งมอบสินค้า หรือขอรับบริจาคการกุศลอันเป็นเท็จ ซึ่งอาจก่อให้เกิดความเสียหายแก่เหยื่อหลายรายในวงกว้าง และขนาดผลประโยชน์อาจมีจำนวนมูลค่าไม่สูงเท่าอาชญากรรมหลัก แต่ก็สามารถเชื่อมโยงการฟอกเงินบนระบบอินเตอร์เน็ตด้วยธุรกรรมเงินสกุลเข้ารหัสได้ทันที และการฉ้อโกงกรณีการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ (ICO) โดยการระดมเงินทุนบนโครงการที่ขาดความเป็นไปได้เชิงพาณชย์ หรือไม่มีโครงที่แท้จริงจากเหยื่อจำนวนมากราย เพื่อให้เข้ามาลงทุนซื้อเงินสกุลเข้ารหัสใหม่ด้วยเงินตราทั่วไปหรือเงินสกุลเข้ารหัสอื่น ซึ่งเงินที่ระดมทุนได้มักมีจำนวนมูลค่าสูง และอยู่ในรูปแบบของเงินสกุลเข้ารหัสที่สามารถทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสได้ทันที

นอกจากนี้ นวัตกรรมเงินสกุลเข้ารหัสมีพลวัตการพัฒนาเปลี่ยนแปลงอย่างต่อเนื่อง ปัจจุบันมีนักพัฒนาระบบงานเงินสกุลเข้ารหัส ได้สร้างระบบบริหารจัดการเงินแบบไร้ตัวกลาง (Decentralized Finance – DeFi Platform) ซึ่งใช้ระบบปฏิบัติการบล็อกเชนร่วมกับโปรแกรมตรรกะอย่างมีเงื่อนไข (Smart Contract) ของอีเทอเรียม เงินสกุลเข้ารหัสอันดับสอง เพื่อให้บริการทางการระดมเงินทุน การให้สินเชื่อ และการเรียกเก็บผลประโยชน์อย่างอัตโนมัติ ภายใต้เงื่อนไขการปฏิบัติที่กำหนดโดยระบบงานที่ไม่มีการควบคุมดูแลจากหน่วยงานใด จึงกลายเป็นเป้าหมายสำคัญของอาชญากรในการประยุกต์ระบบงานเป็นการหลอกลวงแบบแชร์ลูกโซ่ได้โดยง่าย รวมถึงการฉ้อโกงเงินกู้ยืมโดยตรง เนื่องจากผู้ใช้งานทุกคนทั้งผู้ฝากเงิน หรือผู้ให้กู้ และผู้กู้ซึ่งไม่มีความสัมพันธ์รู้จักตัวตนซึ่งกันและกัน โดยระบบนิเวศเงินสกุลเข้ารหัสสามารถอำนวยความสะดวกในการให้บริการ ทั้งนี้อาชญากรรมรูปแบบนี้เริ่มสร้างความเสียหายช่วงปลายปี 2020 จาก KuCoin Exchanger[32] ด้วยความเสียหายมูลค่าประมาณ 275 ล้านเหรียญสหรัฐ (Chainalysis, 2021)

และพัฒนาการระบบค้าสิ่งผิดกฎหมายบนระบบออนไลน์ (Dark Net) ได้สร้างนวัตกรรมระบบการค้าแบบไร้การควบคุม (Decentralized Model) โดยนำเสนอระบบโปรแกรม Televend ซึ่งดำเนินการบนระบบ Telegram Based Platform โดยผู้ซื้อผู้ขายสามารถติดต่อการค้าสิ่งผิดกฎหมายรวมถึงยาเสพติดผ่านระบบการโต้ตอบอัตโนมัติ (Chatbot) และข้อความสื่อสารทั้งหมดจะถูกแปลงเป็นรหัสในระหว่างสื่อสารและจะแปลงกลับเป็นข้อความ เมื่อถึงผู้รับปลายทางที่มีรหัสเปิดที่ถูกต้อง และเมื่อผู้ซื้อส่งคำสั่งซื้อเรียบร้อยแล้ว ระบบจะส่งรหัสที่ตั้งกระเป๋าเงินให้ผู้ซื้อโอนชำระด้วยเงินสกุลเข้ารหัสไปยัง Custodian Wallet จากนั้นผู้ขายจะส่งยาเสพติดให้ผู้ซื้อทางไปรษณีย์ เมื่อผู้ซื้อได้รับพัสดุแล้วระบบก็จะแปลงรหัสการรับพัสดุเป็นเงื่อนไขให้ Custodian Wallet ปลดรหัสเพื่อโอนจ่ายเงินสกุลเข้ารหัสให้ผู้ขาย ซึ่งปัจจุบันมีผู้ใช้งานในระบบ Televend แล้วประมาณ 150,000 ราย (Chainalysis, 2021)

[32] ผู้ให้บริการแลกเปลี่ยนเงินสกุลเข้ารหัสรายใหญ่อันดับ 1 ใน 4 ของผู้ให้บริการทั่วโลก

ดังนั้น รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน มีแนวโน้มที่พัฒนารูปแบบการกระทำผิดโดยใช้ระบบงานอัตโนมัติเพิ่มมากขึ้น ด้วยระบบปฏิบัติการบล็อกเชนและระบบงานที่ไร้การควบคุม ทำให้การสืบค้นและการเข้าถึงตัวผู้กระทำผิดเกิดความยากมากขึ้น เพราะนอกจากจะเป็นการเข้าถึงกระเป๋าเงินที่เป็นแหล่งรับผลประโยชน์จากการกระทำผิดแล้ว ยังมีความยากในการเข้าถึงผู้กระทำผิดจากระบบการค้าอัตโนมัติด้วย Chatbot ที่ไม่มีตัวตน และเมื่อเงินสกุลเข้ารหัสได้รับการยอมรับเป็นสื่อกลางในการชำระราคาสินค้าและบริการทั่วไปในวงที่กว้างมากขึ้น ก็จะยิ่งเพิ่มความยากต่อการสืบค้นติดตามมากขึ้น เนื่องจากเป็นการโอนเงินสกุลเข้ารหัสกันโดยตรงในระบบนิเวศแบบไร้รูปร่างและไม่มีการข้ามเข้าสู่ระบบการเงินทางกายภาพ หรือระบบสถาบันการเงิน

5.1.3 แนวทางการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากล

Chainalysis (2021) ได้รายงานอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสใน The 2021 Crypto Crime Report ว่าในปี 2020 มีธุรกรรมผิดกฎหมายในระบบนิเวศเงินสกุลเข้ารหัสประมาณ 10.0 พันล้านเหรียญสหรัฐ คิดเป็นร้อย 0.34 ของมูลค่าตลาดเงินสกุลเข้ารหัส ซึ่งลดลงเมื่อเปรียบเทียบกับปี 2019 ที่มีธุรกรรมผิดกฎหมายประมาณ 21.4 พันล้านเหรียญสหรัฐ คิดเป็นร้อย 2.10 ของมูลค่าตลาดเงินสกุลเข้ารหัส เนื่องจากวิฤติการแพร่ระบาดของเชื้อโควิด-19 ที่ส่งผลกระทบต่อภาวะการถดถอยทางเศรษฐกิจของทุกประเทศทั่วโลก แต่เงินสกุลเข้ารหัสกลับสวนทิศทางด้วยมูลค่าขนาดตลาดที่เพิ่มขึ้นนำ โดยบิตคอยน์ซึ่งได้รับการตอบรับจากกองทุนระดับโลกและสถาบันการเงินขนาดใหญ่จนทำให้ราคาบิตคอยน์ปรับเพิ่มขึ้นอย่างรวดเร็ว จากสิ้นเดือนมิถุนายน 2020 ที่ระดับประมาณ 9,150 เหรียญสหรัฐต่อ BTC ด้วยมูลค่าขนาดตลาดเท่ากับ 168 พันล้านเหรียญสหรัฐ ขยับขึ้นมาเป็นระดับประมาณ 27,980 เหรียญสหรัฐต่อ BTC ณ สิ้นปี 2020 ด้วยมูลค่าขนาดตลาด 540 พันล้านเหรียญสหรัฐ และก้าวกระโดดอย่างรวดเร็วขึ้นมาเป็นระดับประมาณ 59,000 เหรียญสหรัฐต่อ BTC ณ สิ้นเดือนมีนาคม 2021 ด้วยมูลค่าขนาดตลาด 1.078 ล้านล้านเหรียญสหรัฐ หรือประมาณ 33 ล้านล้านบาท[33] อย่างไรก็ตามอาชญากรยังทำธุรกรรมเงินสกุลเข้ารหัส และทำการฟอกเงินโดยเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมาย แม้ว่าจะเข้าใจเป็นอย่างดีว่าระบบนิเวศเงินสกุลเข้ารหัสสามารถสืบค้นติดตามร่องรอยเส้นทางธุรกรรมได้ แต่ได้มีการปรับเปลี่ยนพฤติกรรมการทำธุกรรมจากการฟอกเงินผ่านผู้ให้บริการที่หลากหลายมาเป็นกลุ่มจำกัดมากขึ้น โดยผู้ให้บริการเฉพาะกลุ่มจำนวน 1,867 รายแรกให้บริการฟอกเงินถึงร้อย 75.00 ของปริมาณรวม และมีผู้ให้บิการเฉพาะกลุ่ม 270 ราย

[33] ข้อมูลจากเว็บไซต์ Coinmarketcap.com; https://coinmarketcap.com/currencies/bitcoin/

แรกให้บริการฟอกเงินถึงร้อย 55.00 ของปริมาณรวม โดยที่ผู้ให้บริการเฉพาะกลุ่ม 24 รายแรกให้บริการถึง 500 ล้านเหรียญสหรัฐ หรือมากกว่า 16,000 ล้านบาท (Chainalysis, 2021)

แม้ว่ารายงานอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัส และการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสทั่วโลก ได้แสดงถึงแนวโน้มปริมาณธุรกรรมผิดกฎหมายที่ลดลงก็ตาม ผู้วิจัยมีความเห็นว่าการศึกษาแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ก็ยังมีความจำเป็น เพื่อการเตรียมความพร้อมต่อพัฒนาการรูปแบบการทำธุรกรรมการโอนระหว่างกันโดยตรงที่อาจเพิ่มมากขึ้น เมื่อระบบเศรษฐกิจการเงินยอมรับเงินสกุลเข้ารหัสเป็นสื่อกลางในการชำระค่าสินค้าและบริการได้อย่างกว้างขวางขึ้น โดยสรุปการศึกษาแนวทางการป้องกันและปราบปรามที่เหมาะสมต่อบริบทประเทศไทยและสากลในปัจจุบันได้ดังนี้

(1) มาตรการสำคัญ ซึ่งเป็นที่ยอมรับสำหรับการป้องกันและปราบปราม การฟอกเงินทั้งในระดับประเทศและสากล คือ การตรวจสอบพิสูจน์ตัวตนของผู้ขอใช้บริการก่อนการเริ่มใช้ระบบงาน (KYC) และการตรวจประเมินธุรกรรมต้องสงสัย (CDD) โดยผู้ให้บริการรับอนุญาตจากหน่วยงานบังคับใช้กฎหมาย ทั้งนี้ประสิทธิภาพของฐานข้อมูลเพื่อการติดตามสืบค้นเข้าถึงตัวตนของผู้ต้องสงสัยขึ้นอยู่กับขอบเขตของข้อมูลที่จำเป็นและเพียงพอต่อการพิสูจน์ตัวตน และการประเมินความเป็นไปได้ของธุรกรรมต้องสงสัย รวมถึงการปรับปรุงฐานข้อมูลของผู้ใช้บริการให้มีความทันสมัยอยู่เสมอ ซึ่งเป็นแนวการดำเนินงานในการกำกับธุรกรรมทางการเงินในระบบสถาบันการเงินในปัจจุบัน โดยมาตรการนี้ เป็นยุทธวิธีที่สร้างระบบการกำกับดูแลจากหน่วยงานรัฐ ซึ่งเสมือนเป็นตัวกลางของระบบงานเข้าไปเชื่อมต่อกับระบบนิเวศเงินสกุลเข้ารหัส ซึ่งปฏิบัติงานบนปรัชญาเชิงเทคโลโนโลยี่ที่ไร้การควบคุม อย่างไรก็ตามด้วยระบบนิเวศเงินสกุลเข้ารหัสมีโครงข่ายเชื่อมโยงแบบโลกาภิวัตรบนระบบอินเตอร์เน็ต ผู้ใช้งานทั่วโลกสามารถเข้าถึงและเชื่อมโยงธุรกรรมข้าพรมแดนต่อกันได้ ดังนั้นการขยายฐานข้อมูลตัวตนผู้ใช้งานได้มากขึ้นเท่าไร ก็จะยิ่งเพิ่มประสิทธิภาพการพิสูจน์ตัวตนของผู้ต้องสงสัยได้มากขึ้นเท่านั้น มาตรการนี้ จึงควรขยายฐานข้อมูลโดยการสร้างระบบจัดการฐานข้อมูลกลางในลักษณะศูนย์ข้อมูลส่วนบุคคลกลาง สำหรับผู้ใช้บริการธุรกรรมการเงินทุกประเภทรวมถึงธุรกรรมเงินสกุลเข้ารหัส (KYC Bureau หรือ KYC Data Center) โดยผู้เข้าถึงข้อมูลส่วนบุคคลนี้จำกัดเฉพาะเจ้าหน้าที่ของหน่วยงานซึ่งมีกฎหมายเฉพาะรองรับการปฏิบัติงาน นอกจากนี้ ยังเป็นการเตรียมความพร้อมรองรับความร่วมมือระหว่างประเทศ ในการแลกเปลี่ยนข้อมูลการตรวจสอบผู้ต้องสงสัยระหว่างกันต่อไปในอนาคต

(2) มาตรการเพิ่มศักยภาพของหน่วยงานบังคับใช้กฎหมาย โดยใช้เครื่องมือ ทางเทคโนโลยี่ขั้นสูง ในการเชื่อมต่อเข้ากับระบบฐานข้อมูลแบบกระจายศูนย์ของระบบปฏิบัติการบล็อก

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

เชนซึ่งสนับสนุนระบบนิเวศเงินสกุลเข้ารหัส ทั้งนี้อาจใช้รูปแบบการทำงานด้วยการพัฒนาโปรแกรมขึ้นเองภายในหน่วยงาน การจัดซื้อจัดหาโปรแกรมสำเร็จรูปการสืบค้นระดับมาตรฐานสากล หรือการว่าจ้างหน่วยงานเฉพาะกิจ เพื่อการสืบค้นเส้นทางธุรกรรมต้องสงสัยรวมถึงรหัสที่ตั้ง กระเป๋าเงินต้องสงสัยเป็นรายกรณีตามความจำเป็น ซึ่งเป็นเครื่องทางเทคโนโลยีที่สำคัญ เพื่อทำการวิเคราะห์เชื่อมโยงพฤติกรรมของผู้ต้องสงสัย ในระบบนิเวศเงินสกุลเข้ารหัสกับฐานข้อมูลตัวตนของผู้ใช้งานในระบบงานอื่นบนระบบอินเตอร์เน็ตที่มีความสัมพันธ์กันกับรหัสที่ตั้ง เครื่องมืออุปรณ์สื่อสาร ซึ่งมีเวลาและสถานที่ที่อาจมีความเชื่อมโยง เช่น สื่อสังคมออนไลน์ Facebook, Twitter, Email, IP Address หรือ Website ที่ใช้งานเป็นประจำของบุคคลนั้น เป็นต้น ทั้งนี้ขึ้นอยู่กับเงื่อนไขการพิจารณาถึงลักษณะพฤติกรรมของผู้กระทำผิด ขนาดความเสียหาย ความจำเป็นด้านทรัพยากรบุคคลและงบประมาณ

(3) มาตรการเฝ้าระวังการทำธุกรรมแปรสภาพระหว่างเงินสกุลเข้ารหัส เป็นเงินตราทั่วไป หรือเป็นสินทรัพย์อื่นที่มีระบบทะเบียนกำกับสำหรับการติดตามสืบค้น ซึ่งเป็นมาตรการเชิงตั้งรับ แต่ก็เป็นมาตรการที่มีประสิทธิภาพที่หลายประเทศในกลุ่มสหภาพยุโรปใช้แนวทางนี้เป็นมาตรการขั้นพื้นฐาน ภายใต้สภาพแวดล้อมปัจจุบันอาชญากรย่อมมีความประสงค์ที่จะยักย้ายถ่ายเทและแปรสภาพเงินที่ไม่ชอบด้วยกฎหมายให้เป็นเงินตราทั่วไปที่ชอบด้วยกฎหมาย เพื่อเป็นผลตอบแทนจากการก่ออาชญากรรม และใช้เป็นแหล่งเงินทุนสนับสนุนการก่ออาชญากรรมต่อไป โดยข้อจำกัดสภาพคล่องของเงินสกลุเข้ารหัส ที่ยังไม่ได้รับการยอมรับให้เป็นสื่อกลางในการชำระค่าสินค้าและบริการได้เยี่ยงปกติธุระ ดังนั้นธุรกรรมเงินสกุลเข้ารหัสที่หมุนเวียนอยู่ในระบบนิเวศ จึงย่อมมีโอกาสที่ธุรกรรมส่วนหนึ่งเชื่อมโยงเข้าสู่ระบบสถาบันการเงินทั่วไป ซึ่งเป็นระบบการกำกับที่รัดกุม ส่งผลให้สามารถเริ่มติดตามสืบค้น ถึงบุคคลที่มีส่วนเกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัสต้องสงสัยที่สัมพันธ์กัน แม้ว่ามาตรการนี้จะประหยัดทรัพยากรในการติดตามสืบค้นผู้ต้องสงสัยในระบบนิเวศ เงินสกุลเข้ารหัส แต่ก็ยังมีประเด็นที่พึงพิจารณาคือ อาชญากรอาจใช้ช่องว่างของมาตรการทางกฎหมายที่แตกต่างกันของแต่ละประเทศเป็นแนวทางในการเลือกสถานที่ ซึ่งเอื้ออำนวยต่อการแปรสภาพเป็นเงินที่ชอบด้วยกฎหมายได้เช่นกัน

(4) มาตรการสร้างความร่วมมือกับองค์กรนานาชาติ และหน่วยงานบังคับใช้กฎหมายของต่างประเทศที่เกี่ยวข้องกับต่อต้านการฟอกเงิน ซึ่งรวมถึงหน่วยงานเอกชนที่มีส่วนสนับสนุนการต่อต้านการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ทั้งในด้านองค์ความรู้เกี่ยวกับบริบทเงินสกุลเข้ารหัส พัฒนาการทางเทคโนโลยีการทำธุรกรรมและการสืบสวน ประสบการณ์ทางคดีในกรณีศึกษาเชิงปฏิบัติการ และการแลกเปลี่ยนข้อมูลเพื่อการสืบค้นติดตามตัวผู้ต้องสงสัยข้ามประเทศ แม้ว่าปัจจุบันจะมีแนวปฏิบัติมาตรฐานในการขอความร่วมมือทางคดีอาญาระหว่างประเทศอยู่แล้ว แต่

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

การสร้างกรอบความร่วมมือเฉพาะบริบทที่เกี่ยวข้องกับการฟอกเงินโดยธุกรรมเงินสกุลเข้ารหัส จะเสริมประสิทธิภาพในการประสานงานได้เท่าทันต่อการเปลี่ยนแปลงทางเทคโนโลยี และการปรับเปลี่ยนรูปแบบพฤติกรรมของอาชญากร ทั้งนี้ขึ้นอยู่กับข้อจำกัดทางกฎหมายระหว่างประเทศและของแต่ละประเทศที่เป็นคู่เจรจา

(5) มาตรการประมวลองค์ความรู้ และเผยแพร่ข้อมูลเกี่ยวกับกลไกการทำงานของระบบนิเวศเงินสกลุเข้ารหัสให้แก่สาธารณะ และประชาชนทั่วไปได้ทราบถึงประโยชน์ของธุรกรรมเงินสกุลเข้ารหัส และกระบวนการติดต่อใช้บริการกับผู้ให้บริการรับอนุญาตที่ถูกต้องตามกรอบของกฎหมาย รวมถึงความเสี่ยงที่อาจเกิดขึ้นทั้งด้านความไม่แน่นอนเชิงมูลค่า และโอกาสที่อาจตกเป็นหยื่อแก่อาชญากรที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการกระทำผิดและการฟอกเงิน นอกจากนี้การพัฒนาศักยภาพและทักษะของเจ้าหน้าที่ผู้รับผิดชอบทั้งในส่วนกลางและส่วนภูมิภาคประจำพื้นที่ก็มีความสำคัญยิ่ง เนื่องจากธุรกรรมเงินสกุลเข้ารหัสสามารถดำเนินการได้ทุกที่ในประเทศเท่าที่การให้บริการระบบอินเตอร์เน็ตครอบคลุมถึง โดยมาตรการนี้เป็นการเสริมภูมิคุ้มกันให้แก่บุคคลที่อาจตกเป็นเหยื่อ และเสริมสร้างศักยภาพของเจ้าหน้าที่ซึ่งเป็นผู้พิทักษ์ป้องกันเหตุแห่งอาชญากรรม

5.2 ข้อเสนอแนะ

ผู้วิจัยได้ประมวลความเห็นต่อแนวทางการป้องกัน และปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส เพื่อแสดงทัศนะเป็นข้อเสนอแนะ ดังนี้

5.2.1 ข้อเสนอแนะเชิงนโยบาย

5.2.1.1 ควรพิจารณาการจัดตั้งศูนย์ข้อมูลส่วนบุคคลกลางสำหรับผู้ใช้บริการธุรกรรมการเงินทุกประเภทรวมถึงธุรกรรมเงินสกุลเข้ารหัส (KYC Bureau หรือ KYC Data Center) ขึ้นเป็นหน่วยงานในรูปแบบองค์การมหาชน ซึ่งมีสภาพเป็นนิติบุคคลเฉพาะที่ไม่ใช่หน่วยงานรัฐหรือรัฐวิสากิจ เพื่อบูรณาการระบบจัดการฐานข้อมูลกลาง (Big Data) สำหรับข้อมูลส่วนบุคคลของผู้ใช้บริการที่เกี่ยวข้องกับเศรษฐกิจการเงินดิจิทัลได้อย่างมีประสิทธิภาพ เตรียมรองรับการนวัตกรรมระบบเศรษฐกิจการเงินโลกที่กำลังจะปรับเปลี่ยนรูปแบบเศรษฐกิจบนโลกเสมือนจริง คือเศรษฐกิจบนระบบดิจิทัลเข้าเชื่อมต่อกับระบบเศรษฐกิจบนโลกกายภาพ โดยระบบการเงินโลกมีแนวโน้มที่จะยกระดับพัฒนาการเป็นระบบการเงินไร้เงินสด หรือที่เรียกว่าระบบการเงินดิจิทัลเต็มรูปแบบ ดังนั้นระบบเศรษฐกิจ ระบบการเงิน และระบบเทคโนโลยีการสื่อสารจะถูกพัฒนาเชื่อมต่อกันทำให้บริการทางการเงินมีความรวดเร็ว ไร้พรมแดนประเทศ และระบบฐานข้อมูลธุรกรรมแบบกระจายศูนย์บนระบบปฏิบัติการบล็อกเชนของเงินสกุลเข้ารหัสก็จะเข้าเชื่อมต่อ กับระบบข้อมูลธุรกรรมของสถาบัน

การเงิน และผู้ให้บริการโทรคมนาคมที่กำกับโดยหน่วยงานรัฐ เป็นโครงข่ายที่สามารถถูกตรวจสอบสืบค้นถึงกันได้

ทั้งนี้ องค์การมหาชนนี้มีวัตถุประสงค์สำคัญในการทำหน้าที่รับผิดชอบดูแล และบริหารจัดการระบบฐานข้อมูลกลาง ของข้อมูลส่วนบุคคลผู้ใช้บริการทางการเงินกับผู้ให้บริการทุกประเภทที่อยู่ภายใต้กฎหมายป้องกันและปราบปรามการฟอกเงิน กฎหมายว่าด้วยการประกอบกิจการสินทรัพย์ดิจิทัล กฎหมายว่าด้วยระบบสถาบันการเงิน และกฎหมายว่าด้วยการสื่อสารโทรคมนาคม เป็นต้น ซึ่งหมายรวมถึงสถาบันการเงิน ผู้ให้บริการอื่นที่ไม่ใช่สถาบันการเงิน ผู้ให้บริการโทรคมมนาคม และผู้ให้บริการที่เกี่ยวข้องกับเงินสกุลเข้ารหัส เพื่อเป็นศูนย์กลางรวบรวมข้อมูลการแสดงตัวตนผู้ใช้งานก่อนใช้บริการ ข้อมูลของผู้ใช้งานที่ทำการปรับปรุงให้ทันสมัยจากผู้ใช้บริการทางการเงินทุกประเทศ และฐานข้อมูลที่เกี่ยวข้องกับการใช้บริการโทรคมนาคม เช่น รหัสที่ตั้ง (IP Address) ของเครื่องมือ อุปรณ์คอมพิวเตอร์และสื่อสารของผู้ใช้งาน เพื่อวิเคราะห์ประมวลผลความสัมพันธ์การใช้บริการของผู้ใช้งานทั้งการเงินและการสื่อสาร ในการจัดระบบรักษาความปลอดภัยทางการเงินดิจิทัล เช่น การประมวลข้อมูลธุรกรรมต้องสงสัย ธุรกรรมที่เกิดจากการกระทำผิด เป็นระบบฐานข้อมูลสถานะบุคคลในบัญชีรายชื่อเฝ้าติดตาม (Watch List) บัญชีรายชื่อต้องสงสัย (Black List) โดยเป็นศูนย์กลางแลกเปลี่ยนข้อมูลให้บริการตรวจสอบสถานะบุคคลที่ขอใช้งานกับผู้ให้บริการด้วยระบบออนไลน์ที่ จะทราบผลการตรวจทราบทันทีว่าผู้ขอใช้งานนั้นอยู่ในบัญชีรายชื่อเฝ้าติดตาม หรือบัญชีรายชื่อต้องสงสัยหรือไม่ ทำให้สามารถระงับการทำธุรกรรมชั่วคราวได้ทันทีเพื่อการตรวจสอบ และสนับสนุนการปฏิบัติหน้าที่ตามกฎหมายในพิสูจน์ตัวตนของอาชญากรที่มีการกระทำความผิดบนระบบการเงินดิจิทัล รวมถึงการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

นอกจากนี้ ยังสามารถมอบหมายให้องค์การมหาชนนี้เป็นหน่วยงานตัวแทนของประเทศไทยในการเข้าเป็นสมาชิกของ World Check World Check หรือ Refinitiv World-Check Risk Intelligence ซึ่งเป็นองค์กรในการบริหารจัดการและดูแลระบบฐานข้อมูลของบุคคล และองค์กรทั่วโลก พร้อมทั้งให้บริการตรวจสอบสถานะของบุคคลหรือองค์กรในระบบออนไลน์ เพื่อสนับสนุนการต่อต้านการฟอก โดยแหล่งข้อมูลสำคัญที่เชื่อมโยงฐานข้อมูลจากเว็บไซต์หน่วยงานภาครัฐ ภาคเอกชน ข่าวสาร สื่อสังคมออนไลน์ และข้อมูลบุคคลต้องห้ามตามกฎหมายในประเทศต่างๆ เพื่อสร้างกรอบความร่วมมือระหว่างประเทศ ในการตรวจสอบแหล่งที่มาของธุรกรรมที่เชื่อมโยงกับผู้ใช้บริการในประเทศ ทั้งนี้เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสให้บริการแก่ผู้ใช้งานโดยไม่ต้องระบุตัวตน และสามารถทำธุรกรรมข้ามประเทศแบบไร้ข้อจำกัดด้านเวลาและสถานที่ ดังนั้นมาตรการการป้องกันอาชญากรรมและการต่อต้านการฟอกเงิน จึงให้ความสำคัญต่อระบบจัดการฐานข้อมูลตัวตนผู้ใช้งานในทั้งระบบออนไลน์ และระบบกายภาพเป็นอันดับแรก

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

5.2.1.2 การส่งเสริมการพัฒนาโปรแกรมประยุกต์ที่เข้าเชื่อมกับฐานข้อมูลแบบกระจายศูนย์บนระบบปฏิบัติการบล็อกเชน (Application Programing Interface – API) โดยมีวัตถุประสงค์ใช้เป็นเครื่องมือในการวิเคราะห์พฤติกรรมการทำธุรกรรมเงินสกุลเข้ารหัส ความเชื่อมโยงของการทำธุรกรรมระหว่างรหัสที่ตั้งของกระเป๋าเงิน เพื่อการวิเคราะห์และสังเคราะห์พฤติกรรมกลุ่มผู้ใช้งานและเส้นทางธุรกรรมนำไปสู่การบริหารจัดการธุรกรรมต้องสงสัย และช่วยการติดตามสืบค้นผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส ในหลักการทำงานทำนองเดียวกับ Chainalysis, ChipherTrace หรือ Elliptic ทั้งนี้เพื่อสร้างความตระหนักรู้ให้แก่บุคคลากรที่มีหน้าที่เกี่ยวข้องกับธุรกรรมการเงินดิจิทัล การป้องกันอาชญากรรมและการต่อต้านการฟอกเงิน รวมถึงช่วยส่งเสริมศักยภาพของนักพัฒนาโปรแกรมซอฟแวร์และระบบสารสนเทศการสื่อสารของไทย อีกทั้งเป็นการประหยัดงบประมาณในการใช้บริการโปรแกรมจากต่างประเทศ รวมถึงสามารถยกระดับการป้องกันและปราบปรามอาชญากรรมการเงินดิจิทัล ได้ตามพลวัตการเปลี่ยนแปลงทางเทคโนโลยี่และพฤติกรรมของอาชญากร พร้อมทั้งเสริมสร้างคุณค่าของทรัพยากรบุคคลไทย โดยการจัดการแข่งขันระดับชาติในการพัฒนาโปแกรมซอฟแวร์ในลักษณะข้างต้น ภายใต้ความร่วมมือของหน่วยงานของรัฐที่เกี่ยวข้องกับการส่งเสริมนวัตกรรมทางเทคโนโลยี่การเงิน เช่น สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ สำนักงานส่งเสริมอุตสาหกรรมซอฟต์แวร์แห่งชาติ สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ธนาคารแห่งประเทศไทย สำนักงานป้องกันและปราบปรามการฟอกเงิน หรือกระทรวงเศรษฐกิจเพื่อเศรษฐกิจและสังคม เป็นต้น

5.2.1.3 การส่งเสริมแผนงานโครงการอินทนนท์ของธนาคารแห่งประเทศไทยในการพัฒนาโครงสร้างพื้นฐานของระบบการเงินไทย สู่การเป็นระบบการเงินดิจิทัลในรูปแบบเงินสกุลดิจิทัลที่ออกโดยธนาคารกลาง หรือ Central Bank Digital Currency (CBDC) ซึ่งมีคุณสมบัติในการเป็นสื่อกลางเพื่อชำระค่าสินค้าและบริการ สามารถรักษามูลค่า และเป็นหน่วยวัดทางบัญชีได้ ซึ่งแตกต่างจากเงินสกุลเข้ารหัสที่ออกโดยนักพัฒนาระบบเอกชนที่ไร้การกำกับ และมูลค่าของเงินสกุลเข้ารหัสมักผันผวนไปตามวัตถุประสงค์เพื่อการลงทุนมากกว่า โดยมีรูปแบบทั้งสำหรับการทำธุรกรรมระหว่างสถาบันการเงิน (wholesale CBDC) และสำหรับธุรกรรมรายย่อยของภาคธุรกิจและประชาชน (retail CBDC) เพื่อขยายเครือข่ายการให้บริการในวงกว้างและปรับเปลี่ยนโครงสร้างพื้นฐานระบบเศรษฐกิจการเงินไทยสู่ระบบเศรษฐกิจสังคมไร้เงินสด เนื่องจากระบบเงินสกุลดิจิทัล CBDC ดำเนินการบนระบบปฏิบัติการบล็อกเชนซึ่งมีระบบจัดการฐานข้อมูลแบบกระจายศูนย์ มีความโปร่งใสในการติดตามเส้นทางการทำธุรกรรมบนระบบนิเวศได้ เมื่อระบบการเงินดิจิทัลขยายวงกว้างจนกระทั่งภาคธุรกิจและประชาชนทำธุรกรรมเยี่ยงปกติธุระโดยไร้เงินสด ก็จะเป็นการจำกัดขอบเขตการใช้ผลประโยชน์ของอาชญากรที่ได้จากการกระทำผิดหรือการฟอกเงิน ทั้งนี้เมื่อระบบนิเวศเงินสกุลเข้ารหัสเชื่อมต่อกับระบบการเงินดิจิทัลของหน่วยงานรัฐ ก็จะเป็นการขยายจุดเฝ้าระวัง เพื่อการ

ตรวจสอบธุรกรรมต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส ได้อย่างกว้างขวางขึ้นทันทีที่ข้ามมาสู่ระบบเศรษฐกิจกายภาพในรูปแบบเงินสกุลดิจิทัลของรัฐ เนื่องจากภาคธุรกิจและประชาชนทั่วไปในระบบเงินสกุลดิจิทัลของรัฐจะถูกกำกับด้วยระบบฐานข้อมูลรู้จักตัวตนผู้ใช้งาน สำหรับทุกกระเป๋าเงินอิเล็กทรอนิกส์ในระบบเงินสกุลดิจิทัลของรัฐ จึงสามารถใช้เป็นเครื่องมือการตรวจสอบสืบค้นเส้นทางธุรกรรมต้องสงสัยจากระบบนิเวศเงินสกุลเข้ารหัส เชื่อมโยงสู่กลุ่มบุคคลในเครือข่ายที่ช่วยสนับสุนนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสในระบบเงินสกุลดิจิทัลของรัฐได้อย่างมีประสิทธิภาพมากขึ้น

5.2.1.4 การสร้างกรอบความร่วมมือระหว่างประเทศ แม้ว่าปัจจุบันคณะทำงานขององค์สหประชาชาติ Financial Action Task Force on Money Laundering (FATF) ได้พัฒนาปรับปรุงข้อแนะนำที่เกี่ยวข้องกับการจัดการความเสี่ยงจากธุรกรรมเงินสกุลเข้ารหัสอย่างต่อเนื่อง โดยนำเสนอแนวคิดแก่ประเทศสมาชิกในการกำกับดูแลเพื่อให้ความเชื่อมั่นได้ว่า ผู้ให้บริการที่เกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัส (Virtual Assets Service Providers – VASP) อยู่ภายใต้กฎระเบียบ การกำกับ การอนุญาต เพื่อให้ระบบการตรวจสอบข้อมูลตัวตนผู้ใช้งาน และการติดตามธุรกรรมต้องสงสัยได้อย่างมีประสิทธิภาพ สามารถสร้างความมั่นใจต่อมาตรการป้องกันและปราบปรามการฟอกเงินได้อย่างเหมาะสม

แต่การปฏิบัติตามแนวทางสากล อาจสร้างโอกาสทางเศรษฐกิจแก่ประเทศที่มีความพร้อมทั้งระบบการเงินและเทคโนโลยี่ แต่อาจสร้างภาระแก่ประเทศที่มีพัฒนาการด้อยกว่า กลุ่มประเทศที่มีพัฒนาด้อยกว่าทั้งด้านระบบการเงินและเทคโนโลยี่ จึงควรรวมตัวกันสร้างกรอบความร่วมมือเป็นกลุ่มประเทศ เพื่อสร้างกำลังต่อรองในระดับสากลและสร้างแนวปฏิบัติที่เหมาะสมแก่กลุ่มประเทศของตนโดยไม่เป็นการก่อภาระในทางปฏิบัติจนเกินควร (กมล สุปรียาสุนทรา, ข้อมูลสัมภาษณ์, มิถุนายน 2021) ดังนั้นกลุ่มประเทศอาเซียนซึ่งเป็นกลุ่มเศรษฐกิจที่มีความสำคัญต่อเศรษฐกิจโลก แต่มีระดับการพัฒนาทางเทคโนโลยี่ภายในกลุ่มประเทศมีความแตกต่างกัน รวมถึงการกำนดมาตรการทางกฎหมายในการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัสยังมีความแตกต่างเช่นกัน จึงควรร่วมกันสร้างกรอบความร่วมระหว่างประเทศในกลุ่มประเทศอาเซียนโดยการจัดตั้งคณะทำงาน (Task Force) เพื่อศึกษาและให้ข้อแนะนำต่อการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัสภายในกลุ่มประเทศอาเซียน และการกำกับดูแลธุรกรรมนอกกลุ่มประเทศ โดยสร้างเป็นเครือข่ายความร่วมมือทางระบบการเงินและเทคโนโลยี่ในเชิงสร้างสรรค์อย่างเหมาะสม ในการประยุกต์ประโยชน์ทางเศรษฐกิจระหว่างประเทศที่จะได้รับจากระบบนิเวศเงินสกุลเข้ารหัส โดยมีระบบการเฝ้าระวังต่อมาตรการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่สอดคล้องกับศักยภาพการดำเนินงาน และรองรับแนวคิดขององค์กรสากลได้อย่างเหมาะสม

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

5.2.2 ข้อเสนอแนะเชิงปฏิบัติการ

5.2.2.1 การเผยแพร่ความรู้ที่ถูกต้องเกี่ยวกับเงินสกุลเข้ารหัส และระบบนิเวศเงินสกุลเข้ารหัสให้แก่สาธารณะ เพื่อสร้างความเข้าใจ การตระหนักรู้ ถึงกลไกการทำงานระบบปฏิบัติการบล็อกเชน ความเสี่ยงที่อาจได้รับจากการทำธุรกรรมเงินสกุลเข้ารหัส ทั้งประเด็นความเสี่ยงด้านมูลค่าที่มีความผันผวนในลักษณะการลงทุนที่มีความเสี่ยงสูง และโอกาสการตกเป็นเหยื่อแก่กลุ่มอาชญากรในการหลอกลวง หรือการใช้เป็นเครื่องมือในการฟอกเงิน เนื่องจากบริบทของเงินสกุลเข้ารหัสยังเป็นสาระความรู้ใหม่สำหรับสังคมไทยและสากล ที่มีพลวัตทางเทคโนโลยีอย่างต่อเนื่อง และมาตรการทางกฎหมายของแต่ละประเทศต่อบริบทของเงินสกุลเข้ารหัสยังมีช่องว่างที่แตกต่างกัน ซึ่งอยู่ระหว่างการพัฒนามาตรการกำกับดูแลที่เป็นสากล ดังนั้นสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ ซึ่งเป็นหน่วยงานบังคับใช้กฎหมายที่เกี่ยวกับผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล และธนาคารแห่งประเทศไทย ซึ่งเป็นหน่วยงานดูแลโครงการอินทนนท์สู่การพัฒนาโครงสร้างพื้นฐานของระบบการเงินไทยเป็นรูปแบบระบบการเงินสกุลดิจิทัล รวมถึงสำนักงานตำรวจแห่งชาติ และสำนักงานป้องกันและปราบปรามการฟอกเงิน ซึ่งเป็นหน่วยงานป้องกันและปราบปรามอาชญากรรม และต่อต้านการฟอกเงิน ควรพัฒนาองค์ความรู้เกี่ยวกับระบบนิเวศเงินสกุลเข้ารหัสกรณีศึกษาของอาชญากรรมที่เกี่ยวข้อง และเตรียมความพร้อมในการเปลี่ยนผ่านสู่ระบบการเงินสกุลดิจิทัล เพื่อสร้างฐานความรู้ให้แก่สาธารณะ และประชาชนในวงกว้างขึ้นอันเป็นประโยชน์ต่อการสร้างภูมิคุ้มกันต่อสังคม ซึ่งอาจเป็นรูปแบบของสื่อสารมวลสาธารณะ หรือสื่อสังคมออนไลน์อื่นเป็นต้น

5.2.2.2 การออกกฎระเบียบที่เกี่ยวข้องกับระบบการเฝ้าระวังธุรกรรมทางการเงินเพื่อการบังคับใช้ให้เป็นตามกฎหมาย (Surveillance) นั้น ควรคำนึงถึงดุลยภาพของมาตรการเฝ้าระวังเพื่อความสมดุลใน 3 มิติ กล่าวคือ สภาพคล่องในการทำธุรกรรม (Liquidity) ความเป็นระเบียบเรียบร้อย (Ordinary) และความเป็นธรรม (Fairness) โดยมาตรการที่มุ่งรักษาความเป็นระเบียบเรียบร้อยมากเกินไป ก็อาจส่งผลต่อการลดถอยปริมาณธุรกรรมหรือขาดสภาพคล่องในการทำธุรกรรมและอาจสร้างภาระการดำเนินงานอย่างไม่เป็นธรรมต่อระบบได้ แต่หากมาตรการมุ่งสร้างความคล่องตัวในการทำธุรกรรมเป็นสำคัญก็จะเกิดสภาพคล่องมากจนอาจขาดความเป็นระเบียบเรียบร้อยในการกำกับดูแลได้เช่นกัน อย่างไรก็ตามทุกมาตรการยังคงต้องคำนึงถึงหลักความโปร่งใส (Transparency) ที่เปิดโอกาสให้ทุกคนสามารถเข้าถึงข้อมูลข่าวสารที่เกี่ยวข้องกับมาตรการได้อย่างเปิดเผย เพื่อสร้างความเข้าใจ ความตระหนักรู้ต่อกฎเกณฑ์ และมีกลไกการตรวจสอบความถูกต้องของการบังคับใช้กฎหมาย เพื่อสร้างความเชื่อมั่นต่อระบบการเฝ้าระวังทางการเงิน (กมล สุปรียาสุนทรา, ข้อมูลสัมภาษณ์, มิถุนายน 2021)

ดังนั้นจากผลการศึกษาได้มีข้อเสนอแนะต่อการออกมาตรการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัสที่ควรจะมีระบบการเฝ้าระวังที่เหมาะสม โดยไม่ปิดกันประโยชน์ทางเศรษฐกิจที่ควรได้รับจากนวัตกรรมเทคโนโลยี่ทางการเงิน อีกทั้งระบบนิเวศเงินสกุลเข้ารหัสเป็นระบบเปิดที่ให้บริการไม่จำกัดเฉพาะภายในประเทศ แต่ยังมีความเชื่อมโยงทางเทคโนโลยี่บนระบบอินเตอร์เน็ตโดยผู้ใช้งานในประเทศสามารถเลือกใช้บริการกับผู้ให้บริการต่างประเทศในระบบนิเวศได้ด้วยความสะดวกแบบไร้พรมแดน จึงเป็นข้อพิจารณาสำคัญต่อการออกกฎระเบียบ หรือมาตรการระบบเฝ้าระวังที่เหมาะสมไม่ควรเป็นการสร้างภาระอย่างไม่เป็นธรรมต่อทั้งผู้ให้บริการและผู้ใช้งาน ซึ่งอาจส่งผลต่อสภาพคล่องในการทำธุรกรรมเงินสกุลเข้ารหัสกับผู้ให้บริการในประเทศ จนเป็นเหตุให้ผู้ใช้งานในประเทศอาจเลือกใช้บริการกับผู้ให้บริการต่างประเทศ ซึ่งอยู่นอกเขตอำนาจในการกำกับดูแลของประเทศไทย เนื่องจากธุรกรรมเงินสกุลเข้ารหัสมีมติของโลกาภิวัตรที่ ผู้ใช้งานสามารถทำธุรกรรมเชื่อมต่อกันได้ทั่วโลกโดยไม่มีข้อจำกัดทางเทคโนโลยี่ ดังนั้นการออกระเบียบมาตรการใดจึงควรคำนึงถึงความสมดุลดังกล่าวข้างต้น อีกทั้งธุรกรรมเงินสกุลเข้ารหัสสามารถดำเนินการได้ด้วยความรวดเร็ว อีกทั้งการจะนำมาตรการใดออกมาประกาศบังคับใช้ ควรมีการรับฟังความคิดเห็นจากผู้อาจได้รับผลกระทบ และผู้มีหน้าที่บังคับใช้ให้เป็นไปตามมาตรการ โดยสร้างความเข้าใจเจตนารมย์และแนวปฏิบัติที่ชัดเจนก่อนการประกาศบังคับใช้ เนื่องจากธุรกรรมเงินสกุลเข้ารหัสมีความไวต่อการดำเนินการ และสามารถดำเนินการข้ามประเทศได้รวดเร็ว จนอาจส่งผลให้การปฏิบัติตามมาตรการระบบเฝ้าระวังไม่ปรากฏผลในการรักษาความเป็นระเบียบเรียบร้อยของระบบได้ตามความคาดหวัง

5.2.2.3 การปรับปรุงกฎระเบียบหรือแนวปฏิบัติในการสืบสวนหาพยานหลักฐานที่เกี่ยวข้องกับการกระทำธุรกรรมฟอกเงินโดยเงินสกุลเข้ารหัส รวมถึงกระบวนการดำเนินคดีที่เกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัสได้อย่างมีประสิทธิภาพโดยมีกฎหมายรองรับการปฏิบัติหน้าที่ เช่น

(1) ระเบียบว่าด้วย การรวบรวมพยานหลักฐานดิจิทัลที่ได้จากตรวจสอบเส้นทางธุรกรรมเงินสกุลเข้ารหัสต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสดำเนินการบนระบบปฏิบัติการบล็อกเชน ซึ่งเป็นฐานข้อมูลสาธารณะในระบบเปิดที่ผู้ใช้งานทั่วไปสามารถเข้าถึงได้ และรายการธุรกรรมจะถูกบันทึกในระบบบัญชีแบบกระจายศูนย์ ที่ไม่สามารถแปลงเปลี่ยนแก้ไขข้อมูลได้หลังจากระบบได้พิสูจน์ยืนยันรายการแล้ว ดังนั้นจึงควรพิจารณาระเบียบว่าด้วยพยานหลักฐานดิจิทัลที่พิสูจน์โดยระบบปฏิบัติการบล็อกเชนในการดำเนินคดี

(2) ระเบียบว่าด้วย การยึดอายัดเงินสกุลเข้ารหัสของผู้กระทำผิดหรือผู้ต้องสงสัยในความผิดมูลฐานเกี่ยวกับการฟอกเงิน เนื่องจากมาตรการยึดอายัดผลประโยชน์จากการกระทำผิดของอาชญากร เป็นเครื่องมือสำคัญในจำกัดแหล่งเงินทุนและตัดวงจรการนำผลประโยชน์ดังกล่าวไปใช้ในการก่ออาชญากรรมต่อไปอีก แต่การทำการยึดอายัดเงินสกุลเข้ารหัสของผู้กระทำผิดหรือผู้ต้องสงสัยจะต้องได้มาซึ่งรหัสเปิดส่วนบุคคลซึ่งเป็นข้อมูลลับของเจ้าของกระเป๋าเงิน แม้ว่าในการสืบสวนจะ

ทราบถึงเส้นทางธุรกรรมต้องสงสัยและกระเป๋าเงินเป้าหมายแล้วก็ตาม ดังนั้นจึงควรมีมาตรการในการให้ได้มาซึ่งรหัสเปิดส่วนบุคคลจากอุปกรณ์คอมพิวเตอร์ที่จัดเก็บ ระบบฐานข้อมูลอิเล็กทรอนิกส์ หรือจากตัวผู้กระทำผิดหรือผู้ต้องสงสัยเองโดยชอบด้วยกฎหมาย ภายใต้หลักการปกป้องและรักษาสิทธิการเข้าถึงและการใช้ข้อมูลส่วนบุคคล (Privacy) นอกจากนี้ควรพิจารณาถึงระเบียบว่าด้วยการจัดการเก็บรักษาเงินสกุลเข้ารหัสที่ยึด หรืออายัดด้วยการโอนเงินสกุลเข้ารหัสดังกล่าวเข้าจัดเก็บในกระเป๋าเงินกลางของรัฐ (State Wallet) เพื่อให้มั่นใจได้ว่าเงินสกุลเข้ารหัสในกระเป๋าเงินของตัวผู้กระทำผิดหรือผู้ต้อสงสัยจะไม่ถูกยักย้ายออกไปโดยมิชอบ ด้วยการใช้ช่องทางเทคโนโลยีอื่นใดในการเข้าถึงกระเป๋าเงินเหล่านั้นได้จากบุคคลภายนอก

(3) ระเบียบว่าด้วย การปฏิบัติงานในการระงับการทำธุรกรรมเงินสกุลเข้ารหัสของผู้กระทำผิดหรือผู้ต้องสงสัยอย่างเร่งด่วนเป็นการชั่วคราว เนื่องจากธุรกรรมเงินสกุลเข้ารหัสสามารถดำเนินการได้โดยไม่มีข้อจำกัดด้านเวลาและสถานที่ ดังนั้นมาตรการระงับการทำธุรกรรมอย่างเร่งด่วนเป็นการชั่วคราว จึงเป็นเครื่องมือที่สำคัญต่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ทั้งนี้ถ้าสามารถการดำเนินมาตรการได้รวดเร็วเท่าใดก็จะส่งผลต่อประสิทธิภาพในการระงับยับยั้งความเสียหายได้เพิ่มมากขึ้นเท่านั้น แต่มาตรการนี้ย่อมต้องคำนึงถึงความโปร่งใสในการปฏิบัติงานและความเป็นธรรมให้แก่ผู้ต้องสงสัย โดยมีแนวปฏิบัติที่ทำให้เชื่อได้ว่ามาตรการนี้จะไม่ถูกนำไปบังคับใช้ในทางมิชอบ จึงควรพิจารณากำหนดอำนาจในการอนุมัติดำเนินมาตรการโดยผู้บริหารระดับสูงของหน่วยงานบังคับใช้กฎหมาย และต้องมีมาตรการตรวจสอบเพื่อความโปร่งใสของการปฏิบัติหน้าที่ ทั้งนี้การระงับธุรกรรมต้องอยู่บนพื้นฐานของความจำเป็นเร่งด่วนและใช้ช่วงเวลาสั้นที่สุดเพื่อให้ผู้ปฏิบัติงานเร่งดำเนินการให้เป็นตามกฎระเบียบทั่วไปในขั้นตอนต่อไปโดยมิชักช้า

(4) ระเบียบว่าด้วย การใช้เทคนิควิธีการสอบสวนพิเศษโดยใช้ทรัพยากรของรัฐ เพื่อการแฝงตัวเข้าร่วมทำธุรกรรมเงินสกุลเข้ารหัสที่เกี่ยวข้องกับกระบวนการฟอกเงินของผู้ต้องสงสัย โดยมีเป้าหมาย เพื่อรวบรวมพยานหลักฐานในการตรวจสอบเชื่อมโยงเส้นทางธุรกรรมเงินสกุลเข้ารหัสกับกระเป๋าเงินต่างๆที่เกี่ยวข้องให้เข้าถึงตัวผู้ต้องสงสัย

5.2.2.4 การปฏิบัติตามกรอบแนวปฏิบัติสากล เพื่อการป้องกันและปราบปรามการฟอกเงินในระดับสากลนั้น เป็นหลักการหรือแนวปฏิบัติที่ประเทศสมควรต้องเคารพตามพันธะสัญญาระหว่างประเทศ อย่างไรก็ตามประเทศก็ควรมีมาตรการทางกฎหมายภายในประเทศเพื่อการป้องกันอาชญากรรมตามแนวทางที่เหมาะสมต่อบริบทของประเทศอีกชั้นหนึ่ง (กมล สุปรียาสุนทรา, ข้อมูลสัมภาษณ์, มิถุนายน 2021)

เนื่องจาก FATF เป็นองค์ระหว่างประเทศที่มีวัตถุประสงค์ในการศึกษากลไกการฟอกเงินจากการใช้เครื่องมือทางการเงินระหว่างประเทศ รวมถึงจัดทำแนวปฏิบัติเพื่อปรับปรุงมาตรการป้องกันและปราบปรามการฟอกเงิน โดยนำเสนอกรอบข้อแนะนำและแนวปฏิบัติมาตรฐานเพื่อการ

ต่อต้านการฟอกเงินและการสนับสนุนทางการเงินต่อการก่อการร้าย ให้แก่ประเทศสมาชิกได้นำไปดำเนินการออกมาตรการทางกฎหมายหรือปรับแก้ไขกฎหมายภายในของแต่ละประเทศให้มีผลบังคับใช้ในทางปฏิบัติเพื่อการต่อต้านการฟอกเงิน และประเทศไทยก็เป็นประเทศมาชิกในกลุ่มพันธมิตรกับ FATF จึงมีพันธะที่จะต้องปรับปรุงมาตรการทางกฎหมายให้สอดคล้องกับแนวปฏิบัติตามข้อแนะนำของ FATF ซึ่งเป็นข้อแนะนำที่เปิดเผยเป็นข้อมูลสาธารณะให้ได้รับทราบแก่บุคคลโดยทั่วไปอย่างเป็นสากล รวมถึงกลุ่มผู้กระทำผิด หรืออาชญากร และองค์กรอาชญากรรมข้ามชาติก็มีโอกาสเข้าถึงและได้รับทราบมาตรการเฝ้าระวังการฟอกเงินเช่นกัน ดังนั้นประเทศไทยจึงควรพิจารณาออกมาตรการทางกฎหมายภายในประเทศที่มีลักษณะการบังคับใช้เป็นการเฉพาะ และปฏิบัติต่อการกระทำผิดในการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เกิดขึ้นภายในขอบเขตอำนาจของอธิปไตยไทย โดยการกำหนดแนวปฏิบัติเพื่อการปรับใช้ประมวลกฎหมายอาญา ที่บังคับใช้อยู่ในปัจจุบันให้ครอบคลุมการกระทำผิดในกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส หรือการแก้ไขเพิ่มเติมบทบัญญัติความผิดขึ้นเป็นการเฉพาะ

(1) ประมวลกฎหมายอาญา ส่วนที่ 2 วิธีการเพื่อความปลอดภัย มาตรา 50 *“เมื่อศาลพิพากษาให้ลงโทษผู้ใด ถ้าศาลเห็นว่าผู้นั้นกระทำความผิดโดยอาศัยโอกาสจากการประกอบอาชีพหรือวิชาชีพ หรือเนื่องจากการประกอบอาชีพหรือวิชาชีพ และเห็นว่าหากผู้นั้นประกอบอาชีพหรือวิชาชีพนั้นต่อไปอาจกระทำความผิดเช่นนั้นขึ้นอีก ศาลจะสั่งไว้ในคำพิพากษาห้ามการประกอบอาชีพหรือวิชาชีพนั้นมีกำหนดเวลาไม่เกินห้าปีนับแต่วันพ้นโทษไปแล้วก็ได้”* ซึ่งเป็นข้อบัญญัติของกฎหมายภายในที่อาจนำมาปรับใช้กับผู้กระทำผิดที่อาจกระทำการในประเทศไทย และมีเครือข่ายในต่างประเทศร่วมกันกระทำการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยจัดทำแนวปฏิบัติเพื่อการพิจารณากำหนดบทลงโทษเพิ่ม จากบทลงโทษในการกระทำผิดต่อฐานความผิดตามบทบัญญัติของกฎหมายอื่น ด้วยการสั่งห้ามผู้กระทำผิดนั้นทำการประกอบอาชีพหรือวิชาชีพที่เกี่ยวข้องซึ่งอาจเป็นกิจการบังหน้าเพื่อเป็นอีกหนึ่งมาตรการทางกฎหมายที่มีโอกาสใช้บังคับในการระงับ หรือยับยั้งกระบวนการฟอกเงินที่มีความเชื่อมโยงอย่างโลกาภิวัตรของเงินสกุลเข้ารหัส

(2) การแก้ไขเพิ่มเติม บทบัญญัติลักษณะความผิดทางอาญาขึ้นเป็นการเฉพาะสำหรับการกระทำความผิดที่เกี่ยวข้องกับกระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ในประมวลกฎหมายอาญา ลักษณะ 1 ความผิดเกี่ยวกับความมั่นคงแห่งราชอาณาจักร ด้วยการเพิ่มเติม *“หมวดความผิดต่อความมั่นคงทางเศรษฐกิจของรัฐ”* เนื่องจากผลร้ายที่เกิดจากการกระทำความผิดในลักษณะนี้อาจส่งผลต่อระบบการเงิน ระบบการค้าที่มีแนวโน้มพัฒนารูปแบบการทำธุรกรรมในระบบออนไลน์มากขึ้นตามบริบทของการเปลี่ยนแปลงทางสังคมโลก ในอนาคตระบบนิเวศเงินสกุลเข้ารหัสบนระบบปฏิบัติการบล็อกเชน อาจมีโอกาสเชื่อมโยงเครือข่ายกับระบบนิเวศเงินสกุลดิจิทัลของรัฐในหลายประเทศ (Central Bank Digital Currency - CBDC) รวมถึงโครงการอินทนนท์ของธนาคารแห่ง

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ประเทศไทย อีกทั้งการพัฒนาเทคโนโลยีบนระบบอินเตอร์เน็ตมีความซับซ้อนมากขึ้นเพื่ออำนวยความสะดวกแก่ผู้ใช้งาน และพร้อมให้การสนับสนุนธุรกรรมที่เชื่อมโยงข้ามเครือข่ายของระบบนิเวศด้วยความรวดเร็วแบบไร้พรมแดนประเทศ ดังนั้นผู้ใช้งานทั้งในประเทศและนอกประเทศมีโอกาสทำการแลกเปลี่ยนมูลค่าไปมาระหว่างเงินสกุลเข้ารหัสกับเงินสกุลดิจิทัลของไทยและของประเทศต่างๆได้ด้วยความรวดเร็วในระบบนิเวศของโลกเสมือน ซึ่งยากต่อการระงับ ยับยั้ง และติดตามผู้กระทำผิด อันอาจก่อให้เกิดผลกระทบอย่างร้ายแรงต่อระบบการเงิน ระบบการค้า และความมั่นคงทางเศรษฐกิจของประเทศ

5.2.2.5 จากผลการศึกษา รูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและใช้กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสนั้น ปรากฏว่า การกระทำผิดจากการเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิสเตอร์ ซึ่งอาชญากรรมไซเบอร์เป็นอาชญากรรมรูปแบบหนึ่งที่ไม่ได้ถูกบัญญัติเป็นความผิดมูลฐานโดยตรงในกฎหมายป้องกันและปราบปรามการฟอกเงิน โดยมีเพียงการเทียบเคียงความผิดมูลฐานอื่น เช่น ความผิดมูลฐานมาตรา 3(6) การกรรโชก รีดเอาทรัพย์ที่มีลักษณะช่องโจร ความผิดมูลฐานมาตรา 3(18) การกรรโชก รีดเอาทรัพย์ที่มีลักษณะเป็นปกติธุระ และความผิดมูลฐานมาตรา 3(24) การมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ในขณะที่แนวโน้มของอาชญากรรมลักษณะดังกล่าวมีโอกาสเพิ่มจำนวนมากขึ้นในต่างประเทศ และมีโอกาสที่ผู้กระทำผิดขยายพื้นที่กระทำผิดเข้ามาในประเทศไทย ดังนั้นการบัญญัติความผิดมูลฐานให้ชัดเจนโดยตรงก็จะเป็นประโยชน์ต่อการดำเนินคดี และการขอความร่วมมือในการดำเนินคดีระหว่างประเทศที่ควรมีมูลฐานความผิดที่บัญญัติไว้ในลักษณะทำนองเดียวกัน นอกจากนี้ประเทศไทยได้มีการตราพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัลตั้งแต่ปี 2018 โดยมีสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์เป็นหน่วยงานบังคับใช้กฎหมาย จึงควรพิจารณาบัญญัติความผิดมูลฐานที่เกี่ยวข้องกับสินทรัพย์ดิจิทัลเพิ่มเติม ในลักษณะทำนองเดียวกับ ความผิดมูลฐานมาตรา 3(20) การกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหลักทรัพย์ ดังเช่น *“การกระทำอันไม่เป็นธรรมเกี่ยวกับการประกอบธุรกิจและการซื้อขายสินทรัพย์ดิจิทัล”*

5.2.2.6 อาชญากรรมการค้าสิ่งผิดกฎหมายบนระบบออนไลน์ (Dark Web) รวมถึงการค้ายาเสพติด เป็นอาชญากรรมรูปแบบหนึ่งที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการก่ออาชญากรรม แม้ว่าในปัจจุบันอาชญากรรมรูปแบบนี้ยังไม่ปรากฏชัดเจนในไทย เนื่องจากผู้กระทำผิดมักใช้ประเทศ ที่มีศักยภาพและมีประสิทธิภาพทางเทคโนโลยีการสื่อสารขั้นสูงเป็นฐานในการก่ออาชญากรรม อย่างไรก็ตามด้วยระบบเครือข่ายการค้าสิ่งผิดกฎหมายสามารถติดต่อเชื่อมโยงกันได้ในระบบออนไลน์แบบไร้พรมแดนกับผู้ทำการค้ายาเสพติดได้ทุกประเทศ ซึ่งอาจหมายรวมถึงผู้ค้ายาเสพติดในประเทศไทย ประกอบกับคุณลักษณะเฉพาะของเงินสกุลเข้ารหัสที่สามารถปกปิดตัวตนผู้ใช้งานและมีระบบการสร้างเงื่อนไขตรรกะการปฏิบัติงาน (Smart Contract) เพื่อเป็นเครื่องมืออำนวยความ

สะดวกต่อระบบการชำระเงิน ซึ่งผู้ใช้งานให้การยอมรับและมีความเชื่อถือได้ในความโปร่งใสของระบบปฏิบัติการบล็อกเชน ดังนั้นหน่วยงานบังคับใช้กฎหมายจึงควรทำการศึกษาเสริมสร้างองค์ความรู้เกี่ยวกับกลไกการดำเนินงานของกระบวนการค้าสิ่งผิดกฎหมายบนระบบอนนไลน์ และแนวทางการป้องและปราบปรามอาชญากรรมในลักษณะดังกล่าว เพื่อสร้างความพร้อมแก่หน่วยงานและผู้บังคับใช้กฎหมายในกรณีที่อาชญากรอาจขยายขอบเขตและเครือข่ายการค้าสิ่งผิดกฎหมายบนระบบออนไลน์เข้าสู่การปฏิบัติการในเขตพื้นที่ประเทศไทย

5.2.3 ข้อเสนอแนะสำหรับการวิจัยครั้งต่อไป

5.2.3.1 เนื่องด้วยมาตรการทางกฎหมายของแต่ละประเทศที่มีต่อสถานภาพเงินสกุลเข้ารหัสยังมีความแตกต่างกัน และโดยหลักกฎหมายภาษีอากรที่มีผลบังคับใช้ต่อเงินสกุลเข้ารหัสในบริบทของแต่ละสถานภาพย่อมมีความแตกต่างกัน กล่าวคือ ถ้าสถานภาพของเงินสกุลเข้ารหัสเป็น “เงินตรา” ซึ่งมีหน้าที่เป็นสื่อกลางในการชำระหนี้ตามกฎหมาย จึงไม่มีทางภาระภาษีอากรในลักษณะใด แต่ถ้ากำหนดสถานภาพเป็น “สินค้า” ที่สามารถซื้อขายแลกเปลี่ยนทางการค้า ก็อาจมีภาระภาษีมูลค่าเพิ่ม และภาษีเงินได้จากการประกอบการค้า และในกรณีที่กำหนดสภานภาพเป็น “หลักทรัพย์” ซึ่งเป็นทรัพย์สินเพื่อการลงทุน ก็อาจมีภาระภาษีธุรกิจเฉพาะ และภาษีเงินได้จากกำไรจากส่วนเกิน ดังนั้นเงินสกุลเข้ารหัสจึงอาจถูกนำไปใช้เป็นเครื่องมือในการหลีกเลี่ยงภาษีขององค์กรธุรกิจ และการตกแต่งมูลค่าทางบัญชีให้แก่กิจการเพิ่มขึ้นโดยเฉพาะอย่างยิ่งกิจการที่อยู่ในตลาดหลักทรัพย์ซึ่งอาจส่งผลกระทบต่อประชาชนในวงกว้าง อันเป็นอีกรูปแบบหนึ่งของอาชญากรรมทางเศรษฐกิจ

ทั้งนี้จึงเป็นการสมควรที่จะทำการศึกษากลไกการใช้ธุรกรรมเงินสกุลเข้ารหัสในระบบนิเวศที่มีขอบเขตการให้บริการแบบไร้พรมแดน รวมถึงความแตกต่างของมาตราการทางกฎหมายต่อสถานภาพเงินสกุลเข้ารหัสและการกำกับดูแลการทำธุรกรรมเงินสกุลเข้ารหัส อาจเป็นโอกาสแก่ผู้กระทำผิดในการใช้ช่องว่างทางมาตรการทางกฎหมายของระบบการจัดเก็บภาษีอากรที่มีความแตกต่างกัน เป็นช่องทางในการหลีกเลี่ยงภาษีขององค์กรธุรกิจ และการตกแต่งเพิ่มมูลค่าทางบัญชีให้แก่กิจการ เพื่อศึกษาค้นหาแนวทางการป้องกันและปราบปรามการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือกระทำผิดในลักษณะดังกล่าว

5.2.3.2 ปัจจุบันการพัฒนานวัตกรรมทางเทคโนโลยีการเงินมีความก้าวหน้าอย่างต่อเนื่อง ตั้งแต่สังคมโลกเริ่มรู้จักกับบิตคอยน์ซึ่งเป็นเงินสกุลเข้ารหัสแรกที่มีระบบปฏิบัตงานแบบกระจายศูนย์โดยไร้การควบคุมจากหน่วยงานกลางใด จนเกิดเป็นระบบบริการทางการเงินแบบไร้ตัวกลางในการกำกับขึ้น (Decentralized Finance - DeFi) ซึ่งเป็นระบบที่ให้บริการทางการเงินที่ได้พัฒนาขึ้นบนระบบปฏิบัติการบล็อกเชน โดยสามารถทำธุรกรรมทางการเงินระหว่างกันโดยตรงแบบ

Peer-to-Peer เช่น การกู้ยืม การให้กู้ การชำระเงิน เป็นต้น ภายใต้การดำเนินงานตามเงื่อนไขข้อตกลงที่ถูกกำหนดขึ้นและระบุตรรกะปฏิบัติงานไว้ล่วงหน้าใน Smart Contract ซึ่งระบบจะดำเนินการโดยอัตโนมัติอย่างอิสระไร้การกำกับควบคุม และดำเนินการติดต่อกันระหว่างผู้ใช้งานผ่านโปรแกรมแบบกระจายอำนาจ (Decentralized Applications – dApps) ด้วยระบบนิเวศแบบเปิดบนฐานข้อมูลสาธารณะแบบกระจายศูนย์ที่สร้างความน่าเชื่อถือและโปร่งใส ในการตรวจสอบติดตามเส้นทางธุรกรรม แต่ยังคงหลักการสำคัญ คือการรักษาความลับข้อมูลส่วนบุคคลของผู้ใช้งานในระบบนิเวศลักษณะ Zero-Knowledge-Proof (ZKP) อันเป็นโอกาสที่ก่อให้เกิดช่องทางการก่ออาชญากรรมและสร้างความเสี่ยงแก่เหยื่อได้ในวงกว้างเข้าข่ายรูปแบบของอาชญากรรมทางเศรษฐกิจ และอาชญากรรมไซเบอร์ จึงเป็นประเด็นที่น่าจะนำไปศึกษาวิจัยต่อยอดในเชิงลึกเกี่ยวกับพัฒนาการของรูปแบบการให้บริการทางการเงินแบบไร้ตัวกลาง และแนวทางการป้องกันอาชญากรรมในลักษณะดังกล่าว

5.2.3.3 จากผลการศึกษาปรากฏว่า มีความเห็นเชิงเสนอแนะในบางมาตรการไม่ได้รับฉันทามติจากผู้ให้ข้อมูลสำคัญสรุปให้เป็นแนวทางหรือแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม แต่ผู้วิจัยมีความเห็นว่าหากได้นำประเด็นดังกล่าวมาศึกษาขยายการวิจัยเพิ่มเติมก็น่าจะเป็นประโยชน์ยิ่งขึ้น กล่าวคือ แนวทางการออกระเบียบหรือมาตรการในการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัส และผู้ให้บริการที่เกี่ยวข้องนั้น ควรคำนึงถึงดุลยภาพของแนวทางการกำกับดูแลธุรกรรมเงินสกุลเข้ารหัส โดยไม่ถึงกับปิดกั้นประโยชน์ของสาธารณะที่จะได้รับจากนวัตกรรมทางการเงินควรเป็นอย่างไรจึงเหมาะสม เนื่องจากผลการศึกษานี้ไม่ได้ข้อยุติอย่างเป็นแนทามติต่อข้อเสนอแนวทางส่งเสริมศักยภาพการแข่งขันให้แก่ผู้ให้บริการรับอนุญาตตามกฎหมาย ให้สามารถอำนวยความสะดวกในการทำธุรกรรมเงินสกุลเข้ารหัสแก่ผู้ใช้งาน เพื่อสร้างแรงจูงใจแก่ผู้ใช้งานให้เลือกใช้บริการกับผู้ให้บริการรับอนุญาตมากกว่าการใช้บริการกับผู้ให้บริการนอกระบบ หรือผู้ให้บริการต่างประเทศ ซึ่งเป็นมาตรการที่ช่วยลดฐานจำนวนผู้ใช้งานนอกระบบการกำกับของหน่วยงานบังคับใช้กฎหมาย และต่อข้อเสนอแนวปฏิบัติในการบังคับใช้มาตรการทางกฎหมายอย่างจริงจัง แม้ว่าธุรกรรมเงินสกุลเข้ารหัสจะเป็นนวัตกรรมใหม่ทางเทคโนโลยี่การเงิน แต่ก็ควรนำมาตรการทางกฎหมายที่บังคับใช้อยู่มาตีความปรับใช้เชิงปฏิบัติการให้ได้อย่างรวดเร็ว มีความชัดเจนแน่นอน และใช้บทลงโทษระดับรุนแรง เพื่อให้สังคมได้รับรู้และตระหนักถึงผลร้ายของการกระทำผิด

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

บรรณานุกรม

Alvarez, M. (2018). Comparative Analysis of Cryptocurrency Regulation in the United State, Nigeria and China; The Potential Influence of illicit Activities on Regulatory Evolution. *ILSA Journal of International and Comparative Law,, 25*(1), 33-56.

Andrew, L., & Douglas, A. (2018). Bitcoin Investigations: Evolving Methodologies and Case Studies. *Journal of Forensic Research, 09*(03). doi:10.4172/2157-7145.1000420

Awataguchi, T., Edited by, & Dewey, J. (2019). Japan: Global Legal Insights – Blockchain & Cryptocurrency Regulation 2019 (Frist Edition). *Global Legal Group*, 349-358. Retrieved from https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

Baath, D., & Zellhorn, F. (2016). *How to combat money laundering in Bitcoin? – An institutional and game theoretic approach to anti-money laundering prevention measures aimed at Bitcoin.* Institutioen for Ekonomisk och Industriell Utveckling (IEI), Linkopings Universitet, Retrieved from https://www.diva-portal.org/smash/get/diva2:1039181/FULLTEXT01.pdf

Braga, R. R. P., & Luna, A. A. B. (2018). Dark Web and Bitcoin: An Analysis of the impact of digital Anonymate and cryptocurrencies in the Practice of Money Laundering Crime. *Direito Desenvolvimento, 9*(2), 270-285. Retrieved from https://heinonline.org/HOL/LandingPage?handle=hein.journals/ddesnvol9&div=38&id=&page=

Breing, C., Accorsi, R., & Muller, G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. *ECIS2015 Completed Research Papers,*(20). Retrieved from http://aisel.aisnet.org/ecis2015_cr/20

Burniske, C., & Tara, J. (2017). *Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond*: McGraw-Hill.

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Campbell-Verduyn, M. (2018). Bitcoin, crypto-coins, and global anti-money laundering governance. *Crime, Law and Social Change, 69*(2), 283-305. doi:10.1007/s10611-017-9756-5

Carlisle, D. (2017). Virtual Currencies and Financial Crime: Challenges and Opportunities. *The Royal United Services Institute for Defence and Security Studies,*. Retrieved from https://rusi.org/sites/default/files/rusi_op_virtual_currencies_and_financial_crime.pdf

Chainalysis. (2019). *Crypto Crime Report: Decoding increasingly sophisticated hacks, darknet markets, and scams*. Retrieved from https://go.chainalysis.com/2019-Crypto-Crime-Report.html

Chainalysis. (2021). The 2021 Crypto Crime Report; Everytheing yoi need to know about ransome, darknet markets and more. Retrieved from https://go.chainalysis.com/2021-Crypto-Crime-Report.html

Choo, K.-K. R. (2015). Cryptocurrency and Virtual Currency. In *Handbook of Digital Currency* (pp. 283-307).

Ciphertrace. (2019). *Cryptocurrency Anti-Money Laundering Report, 2018 Q4*. Retrieved from https://ciphertrace.com/cryptocurrency-anti-money-laundering-report-q4-2018/

Crawford, J. B. (2019). *Knowing Your Bitcoin Customer: A Survey of Bitcoin Money Laundering Services and Techincal Solutions For Anti-money Laundering Compliance.* (Graduate Theses and Dissertations). Iowa State University, Iowa State University, Digital Repository. Retrieved from https://lid.dr.iastate.edu/etd/17661 (17661)

Cvetkova, I. (2018). Cryptocurrencies Legal Regulation. *BRICS Law Journal, 5*(2), 128-153. doi:10.21684/2412-2343-2018-5-2-128-153

Dewey, J. (2018). Global Legal Insights – Blockchain & Cryptocurrency Regulation. *Global Legal Group,, 2019 Frist Edition*. Retrieved from https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Dillion, M. (2014). *Conflict, Power and Dependency in Macro-Societal Process: Introduction to Sociological Theory: Theorists, Concepts, and Their Applicability to the Twenty-First Century* (Second ed.): John Wiley & Son Ltd.

Dyntu, V., & Dykyi, O. (2019). Cryptocurrency in the System of Money Laundering. *Baltic Journal of Economic Studies, 4*(5). doi:10.30525/2256-0742/2018-4-5-75-81

Dyson, S., Buchanan, W. J., & Bell, L. (2018). The Challenges of Investigating Cryptocurrencies and Blockchain Related Crime. *The JBBA,, 1*(2). Retrieved from https://www.researchgate.net/publication/334760145_The_Challenges_of_Investigating_Cryptocurrencies_and_Blockchain_Related_Crime

European Commission. (2020). Money Laundering, An official website of the European Union, Organised Crime and Human Trafficking Retrieved from https://ec.europa.eu/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/money-laundering_en#:~:text=Money%20laundering%20is%20the%20process,beings%20as%20well%20as%20fraud.

Fanusie, Y. J., & Robinson, T. (2018). Bitcoin Laundering : An Analysis of Illicit Flows into Digital Currency Services. *Center of Sanctions & Illictic Finance and ELLIPTIC*. Retrieved from https://www.fdd.org/wp-content/uploads/2018/01/MEMO_Bitcoin_Laundering.pdf

FATF. (2019). *Financial Action Task Froce – 30 years*. Retrieved from www.fatf-gafi.org/publications/fatfgeneraldocuments/FATF-30.html

Federico Paesano. (2019). Working Paper 28: Regulating Cryptocurrencies: Challenges and Considerations. *Basel Institute on Governance,*. Retrieved from https://baselgovernance.org/sites/default/files/2019-06/190628%20Working%20Paper%20Cryptocurrency%20Regulations.pdf

Frick, T. A. (2019). Virtual and cryptocurrencies—regulatory and anti-money laundering approaches in the European Union and in Switzerland. *ERA Forum, 20*(1), 99-112. doi:10.1007/s12027-019-00561-1

Girasa, R. (2018). *Regulation of Cryptocurrencies and Blockchain Technologies ; National and International Perspectives*. In Palgrave Studies in Financial Services Technology (Ed.). doi:https://doi.org/10.1007/978-3-319-78509-7

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Gitlitz, M. A., Buerstetta, G. E., Edited by, & Dewey, J. (2019). An Introduction to virtual currency money transmission regulation: Global, Legal Insights – Blockchain & Cryptocurrency Regulation 2019 (Frist Edition)

Global Legal Group, 132-148. Retrieved from https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

Gong, L., Yu, L., Edit by, & Dewey, J. (2019). China: Global, Legal Insights – Blockchain & Cryptocurrency Regulation 2019 (Frist Edition),. *Global Legal Group*, 262-267. Retrieved from https://www.acc.com/sites/default/files/resources/vl/membersonly/Article/1489775_1.pdf

Goriacheva, A., Jakubenko, N., Pogodina, O., & Silnov, D. (2018). Anonymization Technologies of Cryptocurrency Transactions as Money Laundering Instrument. *KnE Social Sciences, 3*(2). doi:10.18502/kss.v3i2.1523

Hazar, H. B. (2019). The Imortance of Regulations on Cryptocurrency Transactions. *Social Sceinces, Management and Economics Journal,, 1*(2), 28-34.

Homeland Security Enterprise. (2014). Risk and Threats of Cryptocurrencies. *Homeland Security Studies and Analysis Institute (HSSAI),*. Retrieved from https://www.anser.org/docs/reports/RP14-01.03.03-02_Cryptocurrencies%20508_31Dec2014.pdf

HouBen, R., & Snyers, A. (2018). Cryptocurencies and blockchain – Legal context and implications for financial crime, money laundering and tax evasion. *Policy Department for Economic, Scientific and Qualities of Life Policies : European Parliament,*. Retrieved from http://www.europarl.europea.eu/supporting-analysis

Hu, Y., Seneviratne, S., Thilakaratha, K., Fukuda, K., & Seneviratne, A. (2019). Characterizing and Detecting Money Laundering Activities on the Bitcoin Network. *Social and Information Networks,*. Retrieved from https://arxiv.org/abs/1912.12060

Hughes, S. D. (2017). Cryptocurrency Regulations and Enforcement in the U.S. *Western State Law Review,, 45*(1), 1-28. Retrieved from

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

https://heinonline.org/HOL/LandingPage?handle=hein.journals/wsulr45&div=4&id=&page=&t=1558818783

Jacquez, T. (2016). Cryptocurrency the New Money Laundering Problem for Banking, Law Enforcement, and the Legal System. *ProQuest Dissertations Publishing,, Master of Science in Cybersecurity*(10251759). Retrieved from https://search.proquest.com/openview/daa0d91607166b4d9e3a0accbca6cc09/1?pq-origsite=gscholar&cbl=18750&diss=y

Jonge, M. d., & Jonge, D. d. (2018). A Brief Overview on China and CryptoCurrency. *Ningbo Economic Review, University of Nottingham UK,*(1), 33-35.

Kawai, K., Nagase, T., Edited by, Sachheim, M. S., & Howell, N. A. (2019). Japan. *The Virtual Currency Regulation Review (Second Edition),*, 170-179. Retrieved from https://thelawreviews.co.uk/digital_assets/079249ba-c1fd-43cb-b3ad-6c23efb53357/The-Virtual-Currency-Regulation-Review---Edition-2.pdf

Kepli, M. Y. b. Z., & Zulhuda, S. (2019). Cryptocurrencies and Anti-money Laundering Laws: The Need for an Integrated Approach. In *Emerging Issues in Islamic Finance Law and Practice in Malaysia* (pp. 247-263).

Kethineni, S., & Cao, Y. (2019). The Rise in Popularity of Cryptocurrency and Associated Criminal Activity. *International Criminal Justice Review, 30*(3), 325-344. doi:10.1177/1057567719827051

Lilly, J. R., Cullen, F. T., & Ball, R. A. (2015). *Criminological Theory : Context and Consequences* (6 ed.): USA : SAGE Publication Inc.

McQuade, S. C. (2006). *Understanding and Managing Cybercrime*: USA: Pearson Education.

Moser, M., Bohme, R., & Breuker, D. (2013). An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem. *eCrime Researcher Summit (eCrime), IEEE,*. Retrieved from https://maltemoeser.de/paper/money-laundering.pdf

Nakamoto, S. (2008). Bitcoin : A Peer-to-Peer Electronic Cash System. Retrieved from https://s3.amazonaws.com/academia.edu.documents/32413652/BitCoin_P2P_electronic_cash_system.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1543487245&Signature=vgVx%2BPi%2FU%2Bb3ku%2BPJY%2BKqUCw8%2FE%3D

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

&response-content-disposition=inline%3B%20filename%3DBitcoin_A_Peer-to-Peer_Electronic_Cash_S.pdf

Nian, L. P., & Chuen, D. L. E. E. K. (2015). Introduction to Bitcoin. In *Handbook of Digital Currency* (pp. 5-30).

Panova, O., Leheza, Y., Ivanytsia, A., Marchenko, V., & Oliukha, V. (2019). International Models of Legal Regulation and Ethics Cryptocurrency US: Country Review, Journal of Legal. *Ethical and Regulatory Issues,, 22*(2), 1-6. Retrieved from https://www.abacademies.org/articles/International-Models-of-legal-regulation-and-ethics-of-cryptocurrency-use-country-review-1544-0044-22-SI-2-374.pdf

Samanta, S., Mohanta, B. K., Pati, S. P., & Jena, D. (2019). *A Framework to Build User Profile on Cryptocurrency Data for Detection of Money Laundering Activities*. Paper presented at the 2019 International Conference on Information Technology (ICIT), Bhubaneswar, India, India. https://ieeexplore.ieee.org/document/9031941

Sapovadia, V. (2015). Legal Issues in Cryptocurrency. In *Handbook of Digital Currency* (pp. 253-266).

Seo, J., Park, M., Oh, H., & Lee, K. (2018). Money Laundering in the Bitcoin Network: Perspective of Mixing Services. *2018 International Conference on Information and Communication Technology Convergence (ICTC),*. doi:10.1109/ICTC.2018.8539548

Sheller, M. (2017). From spatial turn to mobilities turn. *Current Sociology, 65*(4), 623-639. doi:10.1177/0011392117697463

Sheller, M., & Urry, J. (2006). The New Mobility Paradigm. *Environment and Planning A 2006, 38*, 207-226. doi:https://doi.org/10.1068/a37268

Siegel, L. J. (2013). *Criminology: Theories, Patterns and Typologies* (11th ed.): USA: Linda Ganster.

Tax Justic Network. (2020). Financial Secrecy Index 2020 reports progress on global transparency – but backsliding from US, Cayman and UK prompts call for sanctions [Press release]. Retrieved from https://www.taxjustice.net/press/financial-secrecy-index-2020-reports-progress-

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

on-global-transparency-but-backsliding-from-us-cayman-and-uk-prompts-call-for-sanctions/

The Law Library of Congress. (2018). Regulations of Cryptocurrency Around the world. *Global Legal Research Center,*. Retrieved from https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf

The Reporter Asia Online. (2020). ตามรอย โรงพยาบาลสระบุรี โดน Ransomware เรียกค่าไถ่. Retrieved from https://www.thereporter.asia/th/2020/09/10/ransomware-hospital/

Unite Nations Office on Drugs and Crime. (2020). The Money Laundering Cycle. Retrieved from https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html

University of Minnesota Libraries. (2018). Principles of Economics. *Edition 2016 adapted from a work originally produced in 2012, Minneapolis, MN,*, 817-818. Retrieved from https://open.lib.umn.edu/principleseconomics/chapter/24-1-what-is-money/

Urry, J. (2005). The Complexity Turn. *Theory, Culture & Society 2005 (SAGE),, 22*(5), 1-14. doi:https://doi.org/10.1177/0263276405057188

Van Wegberg, R., Oerlemans, J.-J., van Deventer, O., & Futter, A. (2018). Bitcoin money laundering: mixed results? An explorative study on money laundering of cybercrime proceeds using bitcoin. *Journal of Financial Crime*, 00-00. doi:10.1108/jfc-11-2016-0067

Vandezande, N. (2017). Virtual currencies under EU anti-money laundering law. *Computer Law & Security Review, 33*(3), 341-353. doi:10.1016/j.clsr.2017.03.011

Walby, S. (2007). Complexity Theory, System Theory, and Multiple Intersecting Social Inequalities. *Philosophy of the Social Sciences,, 37*(4), 449-470. doi:https://doi.org/10.1177/0048393107307663

Yang, M. (2016). Cryptocurrency in China: Light-Touch Regulation in Demand. *Georgetown University Law Center,*.

Yermack, D. (2015). Is Bitcoin a Real Currency? An Economic Appraisal. In *Handbook of Digital Currency* (pp. 31-43).

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

Zareian, A. (2019). Arch Woodside, The Complexity Turn (2017). *Markets, Globalization & Development Review, 4*(4). doi:10.23860/mgdr-2019-04-04-05

เกาะกระแส. (2019, 7 กรกฎาคม 2562). “โจเซฟ สติกลิทซ์” นักเศรษฐศาตร์รางวัลโนเบล วิพากษ์ Libra - เฟซบุ๊กเปิดสมุดปกขาวแจงข้อมูล คริปโตเคอร์เรนซี. ไทยพับลิก้า Retrieved from https://thaipublica.org/2019/07/joseph-stiglitz-noble-laureate-opinion-on-libra-criptocurrency-facebook/

ไชยยศ เหมาะรัชตะ. (1997). มาตรการทางกฎหมายในการป้องกันและปราบปรามการฟอกเงิน. (การป้องกันราชอาณาจักรภาครัฐร่วมเอกชน รุ่นที่ 9). วิทยาลัยป้องกันราชอาญาจักร,

กิจชัยยะ สุรารักษ์. (2020). แนวทางการป้องกันอาชญากรรมที่เกี่ยวกับสกุลเงินเข้ารหัสในประเทศไทย: กรณีศึกษาบิตคอยน์. (ศิลปศาสตร์ดุษฎีบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม). จุฬาลงกรณ์มหาวิทยาลัย,

ข่าวการเงิน. (2018, 12 สิงหาคม 2561). เปิด 3 ขั้นตอนโกง “บิตคอยน์” 797 ล้านบาท. กรุงเทพธุรกิจออนไลน์ Retrieved from https://www.bangkokbiznews.com/news/detail/810106

ข่าวอาชญากรรม. (2019, 18 กุมภาพันธ์ 2562). ผู้เสียหายร้อง ตำรวจหลังถูกหลอกลงทุน "บิทคอยน์" สูญกว่า 500 ล้าน. ข่าวไทยพีบีเอสออนไลน์. Retrieved from https://news.thaipbs.or.th/content/277818

ธนาคารแห่งประเทศไทย. (2014). ข้อมูลเกี่ยวกับบิตคอยน์และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่นๆที่มีลักษณะใกล้เคียง [Press release]. Retrieved from https://www.bot.or.th/Thai/PressAndSpeeches/Press/News2557/n0857t.pdf

ธนาคารแห่งประเทศไทย. (2019a). แนวทางการประกอบธุรกิจสินทรัพย์ดิจิทัลของสถาบันการเงินและบริษัทในกลุ่มธุรกิจทางการเงินและสถาบันการเงิน. หนังสือเวียนธนาคารแห่งประเทศไทย ธปท.ฝนส.*(23)*ว.*1759/2561* (1 สิงหาคม 2561). Retrieved from https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/ThaiPDF/25610186.pdf

ธนาคารแห่งประเทศไทย. (2019b). ขอความร่วมมือสถาบันการเงินไม่ให้ทำธุรกรรมที่เกี่ยวข้องกับคริปโตเคอเรนซี่. หนังสือเวียนธนาคารแห่งประเทศไทย ธปท.ฝนส.*(23)*ว. *276/2561* (12 กุมภาพันธ์ 2561). Retrieved from https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/ThaiPDF/25610039.pdf

ธรรมรักษ์ หมื่นจักร รัชพร วงศาโรจน์ กษิดิศ ตันสงวน และเกวลี สันตโย. (2018). Digital Currency Series Vol.2: Cryptocurrencies and Friends: นวัตกรรม พัฒนากร ความเสี่ยง และการกำกับดูแล, ธนาคารแห่งประเทศไทย. *FAQ Focused and Quick,*(126). Retrieved from https://www.bot.or.th/Thai/MonetaryPolicy/ArticleAndResearch/FAQ/FAQ_126.pdf

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ธรรมรักษ์ หมื่นจักร รัชพร วงศาโรจน์ กษิดิศ ตันสงวน และเกวลี สันตโยดม. (2018). Digital Currency Series Vol.1: Central Bank Digital Currency อีกหนึ่งวิวัฒนาการของเงิน, ธนาคารแห่งประเทศไทย. *FAQ Focused and Quick*,(124). Retrieved from https://www.bot.or.th/Thai/MonetaryPolicy/ArticleAndResearch/FAQ/FAQ_124.pdf

พงศภัค รจนา. (2021, 15 มิถุนายน 2021). รู้จัก "เอลซัลวาดอร์" ประเทศแรกที่ยอมรับ Bitcoin เป็นค่าเงินตามกฎหมาย. สำนักข่าวอีไฟแนนซ์ไทย. Retrieved from https://www.efinancethai.com/LastestNews/LatestNewsMain.aspx?id=cGE4cDFxL1FRM2s9

พรชัย ขันตรี และคณะ. (2015). ทฤษฎีอาชญาวิทยา : หลักการ งานวิจัย และนโยบายประยุกต์: กรุงเทพฯ : ส.เจริญการพิมพ์.

พระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19) พ.ศ.2561 (2018), ราชกิจจานุเบกษา เล่มที่ 135 ตอนที่ 33 ก (13 พฤษภาคม 2561):71

พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 (2018), ราชกิจจานุเบกษา เล่มที่ 135 ตอนที่ 33 ก (13 พฤษภาคม 2561):43

พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ.2542 (2017), ราชกิจจานุเบกษา เล่มที่ 134 ตอนพิเศษ 201ง (8 สิงหาคม 2560):75

พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556 (2013), ราชกิจกานุเบกษา เล่มที่ 130 ตอนที่ 55ก (26 มิถุนายน 2556):1

วรสิทธิ์ เจริญพุฒ, & ศิรินัง, เ. (2015). การวิจัยเชิงอนาคตด้วยเทคนิคเดลฟาย. วารสารวิจัยมหาวิทยาลัยเวสเทิร์น มนุษยศาสตร์และสังคมศาสตร์, *Vol1, No.3 ,September-December 2015*(No.3 ,September-December 2015), 15. Retrieved from https://www.western.ac.th/westernnew/admin/uploaded/journal_human/files/34.pdf

วสันต์ เทียนหอม. (2018). สรุปสาระสำคัญของพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 [Press release]. Retrieved from https://www.sec.or.th/TH/Documents/ActandRoyalEnactment/LawReform/summary-decree-digitalasset2561.pdf

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. (2018). รายงานฉบับสมบูรณ์โครงการศึกษาเรื่องการบังคับคดีกับสินทรัพย์ดิจิทัล Retrieved from

http://www.led.go.th/articles/pdf/uO5ivavpioXiwe0zVD7ZS4DVtO0m3M27shbWXJzP2933110119024416.pdf

สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (2018, 30 สิงหาคม 2561). Re: ความก้าวหน้าทางเศรษฐกิจและการต่อต้านอาชญากรรมในยุคดิจิทัล: อาชญากรรมกับคริปโตเคอร์เรนซี่

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. (2018). สรุปสาระสำคัญของพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 [Press release]

สำนักงานป้องกันและปราบปรามการฟอกเงิน. (2017). รวมกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงินและกฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้าย และการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง (พิมพ์ครั้งที่14 ed.): กรุงเทพฯ: แจ็ส เพอ-พริ้น

สำนักงานป้องกันและปราบปรามการฟอกเงิน. (2019). ผลการปฏิบัติงานด้านการป้องกันการฟอกเงิน. รายงานประจำปี *2562*

สำนักงานป้องกันและปราบปรามการฟอกเงิน. Retrieved from file:///C:/Users/User/Downloads/annualYreportY2562_3013%20(1).pdf

สุทธมาศ จันทร์แดง. (2013). แนะนำกฎหมายใหม่และกฎหมายที่น่าสนใจ : พระราชบัญญัติป้องกันและปราบปรามการมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ พ.ศ.2556. จุลนิติ รัฐสภา,, ฉบับที่ *2* (กย.-ตค.56), 89-100.

สุพัตรา แผนวิชิต. (2019). การมีส่วนร่วมในองค์กรอาชญากรรมข้ามชาติ ในชุดวิชากฎหมายกระบวนการยุติธรรมเกี่ยวกับการควบคุมและปราบปรามอาชญากรรมในประเทศและข้ามชาติที่สำคัญ. มหาวิทยาลัยสุโขทัยธรรมาธิราช,. Retrieved from https://www.stou.ac.th/schoolsweb/law/UploadedFile/%E0%B8%AB%E0%B8%99%E0%B9%88%E0%B8%A7%E0%B8%A2%E0%B8%97%E0%B8%B5%E0%B9%88%205%20.pdf

สุภางค์ จันทวานิช. (2016). ทฤษฎีสังคมวิทยา (พิมพ์ครั้งที่ 7 ed.): สำนักพิมพ์แห่งจุฬาลงกรณ์มหาวิทยาลัย

สุมนทิพย์ จิตสว่าง. (2019). ปัญหาอาชญากรรมองค์การและปัญหาอาชญากรรมธุรกิจ. In ภาควิชาสังคมวิทยาและมานุษยวิยา คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย (Ed.).

ภาคผนวก

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ก. การรับรองจริยธรรมการวิจัยในคนของโครงการวิจัย

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2
สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย
อาคารจามจุรี 1 ชั้น 1 ห้อง 114 ถนนพญาไท แขวงวังใหม่ เขตปทุมวัน กรุงเทพมหานคร 10330
โทรศัพท์ : 0 2218 3210-11 E-mail: curec2.ch1@chula.ac.th

COA No. 058/2564

ใบรับรองโครงการวิจัย

โครงการวิจัยที่ 027/64 แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

ผู้วิจัยหลัก นายวิสูต กัจฉมาภรณ์

หน่วยงาน คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน กลุ่มสหสถาบัน ชุดที่ 2 สังคมศาสตร์ มนุษยศาสตร์ และศิลปกรรมศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย พิจารณาจริยธรรมการวิจัยโดยยึดหลัก ของ Declaration of Helsinki, the Belmont report, CIOMS guidelines และ The international conference on harmonization – Good clinical practice (ICH-GCP) อนุมัติให้ดำเนินการศึกษาวิจัยเรื่องดังกล่าวได้

ลงนาม.....
(ศาสตราจารย์กิตติคุณ ดร.ธีระพันธ์ เหลืองทองคำ)
ประธานคณะกรรมการ

ลงนาม.....
(ผู้ช่วยศาสตราจารย์ ดร.หนึ่งหทัย แรงผลสัมฤทธิ์)
กรรมการและเลขานุการ

รูปแบบการพิจารณาทบทวน: แบบลดขั้นตอน

วันที่รับรอง: 24 มีนาคม 2564 **วันหมดอายุ:** 23 มีนาคม 2565

เอกสารที่คณะกรรมการรับรอง

1. ข้อเสนอโครงการวิจัย
2. ประวัติและผลงานของผู้วิจัย
3. เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย
4. หนังสือยินยอมเข้าร่วมในการวิจัย
5. แนวคำถามสำหรับการสัมภาษณ์

คณะกรรมการพิจารณาจริยธรรมการวิจัยในคน สังคมศาสตร์ มนุษยศาสตร์ กลุ่มสหสถาบัน ชุดที่ 2 และศิลปกรรมศาสตร์

เลขที่โครงการ 027/64
วันที่รับรอง 24 มี.ค. 2564
วันหมดอายุ 23 มี.ค. 2565

เงื่อนไข

1. ผู้วิจัยรับทราบว่าเป็นการผิดจริยธรรม หากดำเนินการเก็บข้อมูลการวิจัยก่อนได้รับการอนุมัติจากคณะกรรมการพิจารณาจริยธรรมการวิจัยฯ
2. หากใบรับรองโครงการวิจัยหมดอายุ การดำเนินการวิจัยต้องยุติ เมื่อต้องการต่ออายุต้องขออนุมัติใหม่ล่วงหน้าไม่ต่ำกว่า 1 เดือน พร้อมส่งรายงานความก้าวหน้าการวิจัย
3. ต้องดำเนินการวิจัยตามที่ระบุไว้ในโครงการวิจัยอย่างเคร่งครัด
*4. ใช้เอกสารข้อมูลสำหรับกลุ่มตัวอย่าง/ผู้มีส่วนร่วมในการวิจัย ใบยินยอมของกลุ่มตัวอย่างหรือผู้มีส่วนร่วมในการวิจัย และเอกสารเชิญเข้าร่วมวิจัย (ถ้ามี) **เฉพาะที่ประทับตราคณะกรรมการเท่านั้น***
5. หากเกิดเหตุการณ์ไม่พึงประสงค์ร้ายแรงในสถานที่เก็บข้อมูลที่ขออนุมัติจากคณะกรรมการ ต้องรายงานคณะกรรมการภายใน 5 วันทำการ
6. หากมีการเปลี่ยนแปลงการดำเนินการวิจัย ให้ส่งคณะกรรมการพิจารณารับรองก่อนดำเนินการ
7. โครงการวิจัยไม่เกิน 1 ปี ส่งแบบรายงานสิ้นสุดโครงการวิจัย (AF 03-13) และบทคัดย่อผลการวิจัยภายใน 30 วัน เมื่อโครงการวิจัยเสร็จสิ้น สำหรับโครงการวิจัยที่เป็นวิทยานิพนธ์ให้ส่งบทคัดย่อผลการวิจัย ภายใน 30 วัน เมื่อโครงการวิจัยเสร็จสิ้น ทั้งนี้เพื่อเป็นหลักฐานในการปิดโครงการ
8. โครงการวิจัยที่ได้รับการอนุมัติโครงการโดยการพิจารณาทบทวนแบบกรณียกเว้น (Exemption review) ปฏิบัติตามเงื่อนไข ข้อ 1,6 และ 7 เท่านั้น

ข. แนวคำถามเบื้องต้นวิธีการสัมภาษณ์เชิงลึก

แนวคำถามการสัมภาษณ์ในการวิจัยเพื่อการจัดทำวิทยานิพนธ์

“แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส”

ชื่อผู้วิจัย **นายวิสูต กัจฉมาภรณ์** (นิสิตระดับดุษฎีบัณฑิต สาขาวิชาอาชญาวิทยาและงานยุติธรรม คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย) โทร 081-6172838 email: visootk@hotmail.com

วัตถุประสงค์การศึกษา :

1. เพื่อศึกษารูปแบบ คุณลักษณะเฉพาะ กลไกการทำงาน และสถานภาพทางกฎหมายของเงินสกุลเข้ารหัส รวมถึงบริบทของเงินสกุล้เข้ารหัสที่เป็นปัจจัยที่มีอิทธิพลต่อการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส
2. เพื่อศึกษารูปแบบของอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและใช้กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสสำหรับผลประโยชน์ที่ได้จากการกระทำผิด
3. เพื่อศึกษาแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อการปรับใช้กับบริบทของประเทศไทยและสากล

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

แนวคำถามการสัมภาษณ์เบื้องต้นกับ ผู้เชี่ยวชาญซึ่งเป็นผู้บริหารของหน่วยงานภาครัฐ และ/หรือหน่วยงานภาคเอกชนซึ่งเป็นผู้เชี่ยวชาญสายงานปฏิบัติการ และ/หรือสายงานกำกับนโยบายซึ่งมีหน้าที่รับผิดชอบเกี่ยวข้องกับการดำเนินกิจกรรมและธุรกรรมการเงินอิเลคทรอนิค และ/หรือการป้องกันและปราบปรามการฟอกเงิน ได้แก่

1. ท่านคิดว่าปัจจัยสำคัญอะไรบ้าง ในกลไกการทำงานของระบบนิเวศของเงินสกุลเข้ารหัส (Cryptocurrency Ecosystem) ที่อาจมีอิทธิพลต่ออาชญากรในการตัดสินใจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องในการทำธุรกรรมฟอกเงิน (กรุณาให้ข้อมูลตัวอย่างที่เป็นปัจจัยส่งเสริม)

2. ท่านคิดว่ารูปแบบของอาชญากรรมประเภทใดบ้าง ที่อาชญากรมีโอกาสเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการทำธุรกรรมฟอกเงิน และเพราะเหตุใด (กรุณาให้ข้อมูลตัวอย่างของรูปแบบอาชญากรรม)

3. ท่านทราบถึงเทคนิควิธีการ หรือกระบวนการติดตามสืบค้นผู้ต้องสงสัยที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงินในระบบนิเวศของเงินสกุลเข้ารหัสมีลักษณะการดำเนินงานอย่างไรบ้าง (กรุณาให้ข้อมูลกรณีตัวอย่างของพฤติการณ์และวิธีดำเนินการคร่าวๆ)

4. ท่านมีข้อเสนอแนะ หรือความคิดเห็นต่อการกำหนดนโยบายหรือแนวทางเพื่อป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส อย่างไรจึงจะเหมาะสมต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน (ทั้งนี้ขอความกรุณาให้ข้อเสนอแนะหรือแสดงความคิดเห็นต่อมาตรการที่คิดว่าเหมาะสมประมาณ 3 – 5 มาตรการ)

5. ท่านมีข้อเสนอแนะ หรือความคิดเห็นอย่างไร ต่อแนวทางปฏิบัติเพื่อการบังคับใช้เชิงปฏิบัติการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมและสามารถเพิ่มประสิทธิภาพการดำเนินงานตามนโยบายที่กำหนด (ทั้งนี้ขอความกรุณาให้ข้อเสนอแนะหรือแสดงความคิดเห็นต่อแนวทางปฏิบัติที่คิดว่าเหมาะสมประมาณ 3 – 5 แนวทาง)

6. ท่านมีความคิดเห็น หรือข้อเสนอแนะอื่นเพิ่มเติม (ถ้ามี)

ในการนี้ใคร่ขอขอบคุณผู้มีส่วนร่วมในการวิจัยทุกท่านที่ให้ข้อมูลสัมภาษณ์อันเป็นประโยชน์ต่อการวิจัย ทั้งนี้ผู้วิจัยจะได้ดำเนินการประมวลผลข้อเสนอแนะต่อแนวทางการกำหนดนโยบาย และแนวทางปฏิบัติในการป้องกันและปราบปราบการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่ได้รับ พร้อมสรุปผลข้อเสนอแนะนำเสนอต่อท่านในรูปแบบการสำรวจความเห็นเพื่อขอรับฟังเพิ่มเติมหลังการสัมภาษณ์ประมาณอีก 2-3 รอบ หรือจนกว่าข้อมูลจะเสถียร ซึ่งจะใช้เวลาในการอ่านและตอบแบบสำรวจความเห็นแต่ละรอบประมาณ 15-20 นาที โดยผู้วิจัยจะส่งแบบสำรวจความคิดเห็นให้ท่านตอบกลับทางอีเมล visootk@hotmail.com ในระหว่างช่วงเดือนมีนาคม – เมษายน พ.ศ. 2564

ค. แบบสำรวจความเห็นตามเทคนิควิธีเดลฟายรอบแรก

แบบสำรวจความเห็นต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินเข้ารหัส

การศึกษาวิจัยนี้ได้ใช้เทคนิควิธีเดลฟายรูปแบบปรับปรุง (Modified Delphi Technique) ในการสำรวจความเห็นตามเทคนิควิธีเดลฟายรอบแรก โดยปรับใช้วิธีการสัมภาษณ์เชิงลึกกับผู้ให้ข้อมูลสำคัญด้วยคำถามปลายเปิดแทนการสำรวจความเห็นอิสระโดยตรงแบบเปิดกว้าง ดังนี้

“ท่านมีข้อเสนอแนะ หรือความคิดเห็นต่อการกำหนดนโยบายหรือแนวทางเพื่อป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส อย่างไรจึงจะเหมาะสมต่อบริบทของประเทศไทย และสากลในสถานการณ์ปัจจุบัน (ทั้งนี้ขอความกรุณาให้ข้อเสนอแนะหรือแสดงความคิดเห็นต่อมาตรการที่คิดว่าเหมาะสมประมาณ 3 – 5 มาตรการ)”

และได้ทำการสังเคราะห์ผลสำรวจความคิดเห็นและทัศนะเชิงเสนอแนะต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน โดยได้สรุปเป็นข้อเสนอจำนวน 13 แนวทาง ซึ่งได้แสดงตามลำดับสัดส่วนความเห็นจากผู้ให้สัมภาษณ์ เพื่อจัดทำแบบสำรวจความเห็นตามเทคนิควิธีเดลฟายรอบที่ 2 ต่อไป

แนวทางป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	สัดส่วนความเห็น
1. ในการวางหลักเกณฑ์มาตรฐานสำหรับการบันทึกข้อมูลเพื่อการตรวจพิสูจน์ตัวตนของผู้ใช้งาน[1] (KYC) ควรมีการกำหนดข้อมูลจำเป็นอย่างเพียงพอ และทำตรวจสอบทบทวนข้อมูลบุคคลให้ทันสมัยอย่างสม่ำเสมอ	57.89%
2. ควรส่งเสริมความรู้ให้แก่ประชาชนถึงลักษณะ กลไกการทำงานของเงินสกุลเข้ารหัส[2] และความเสี่ยงของธุรกรรมเงินสกุลเข้ารหัส รวมถึงโอกาสการตรวจสอบและเข้าถึงเส้นทางการทำธุรกรรมในระบบปฏิบัติการบล็อกเชน	52.63%
3. ควรสร้างกรอบความร่วมมือระหว่างประเทศเพื่อการต่อต้านการฟอกเงิน[3] โดยการแลกเปลี่ยนข้อมูล และประสบการณ์ของแต่ละประเทศเกี่ยวกับการทำอาชญากรรมธุรกรรมเงินสกุลเข้ารหัส รวมถึงการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	47.37%
4. ควรส่งเสริมศักยภาพการแข่งขันให้แก่ผู้ให้บริการรับอนุญาต[4] เพื่ออำนวยความสะดวกในการทำธุรกรรมเงินสกุลเข้ารหัสให้แก่ผู้ใช้งาน และสร้างแรงจูงใจแก่ผู้ใช้งานให้เลือกใช้บริการกับผู้ให้บริการรับอนุญาต มากกว่าการใช้บริการกับผู้ให้บริการนอกระบบ หรือผู้ให้บริการต่างประเทศ	42.11%
5. ในกระบวนการออกกฎระเบียบเพื่อการกำกับธุรกรรมและผู้ให้บริการรับอนุญาตควรคำนึงถึงความคล่องตัวของธุรกิจ เพื่อสร้างความสมดุลระหว่างประโยชน์สาธารณะที่จะได้รับ กับข้อจำกัดในการดำเนินธุรกิจ	31.58%
6. ในการกำหนดแนวทางการกำกับธุรกรรมและผู้ให้บริการเงินสกุลเข้ารหัสควรอ้างอิงกับแนวทางหรือข้อแนะนำตามหลักมาตรฐานการปฏิบัติสากล เช่น FATF Recommendations	26.32%
7. ควรสร้างระบบเครือข่ายความร่วมมือในการแบ่งปันความช่วยเหลือระหว่างหน่วยงานบังคับใช้กฎหมาย[5] ในการเข้าถึงข้อมูลส่วนบุคคลของผู้ต้องสงสัย รวมถึงเส้นทางการทำธุรกรรมต้องสงสัย	21.05%

แนวทางป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	สัดส่วนความเห็น
8. ควรบรูณาการหน่วยงานหลักที่รับผิดชอบร่วมทำงานแบบองค์รวมเพื่อร่วมกันกำหนดแผนปฏิบัติงานตามลำดับขั้นตอนปฏิบัติการ ลดการทับซ้อนของขอบเขตงาน และเพิ่มประสิทธิภาพการปฏิบัติงาน โดยอาจมีคณะทำงานเฉพาะกิจหรือผู้เชี่ยวชาญเป็นที่ปรึกษาให้การสนับสนุนเชิงเทคนิคและแนวทาง	21.05%
9. ควรส่งเสริมให้สามารถสร้างกรอบความร่วมมือขององค์กรภาคเอกชนที่เกี่ยวข้องกับธุรกิจเงินสกุลเข้ารหัส เพื่อการสนับสนุนการดำเนินงานกำกับดูแลกันเองภายในอุตสาหกรรม และประสานงานกับหน่วยงานรัฐ	21.05%
10. ควรออกมาตรการกำหนดให้ผู้ใช้งานที่จะต้องการทำธุรกรรมจะต้องดำเนินการกับผู้ให้บริการที่ได้รับอนุญาต และหากเป็นธุรกรรมข้ามประเทศก็ให้ดำเนินกับผู้ให้บริการที่ได้รับอนุญาตของประเทศนั้นๆ	21.05%
11. ควรออกระเบียบปฏิบัติที่ชัดเจนที่เกี่ยวข้องกับการปฏิบัติหน้าที่ต่อการสืบสวน หาหลักฐานในลักษณะดิจิทัล และการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย โดยมีกฎหมายรองรับ หรือปรับแก้ไขกฎหมายให้สามารถดำเนินการได้	15.79%
12. ควรสร้างระบบจัดการฐานข้อมูลกลางของการแสดงตัวตนผู้ใช้งาน (KYC Bureau) ที่รวบรวมข้อมูลส่วนบุคคลจากผู้ให้บริการทางการเงินทุกประเภท[6] เพื่อสามารถเชื่อมโยงข้อมูลทั้งในส่วนธุรกรรมเงินสกุลเข้ารหัส และธุรกรรมทางการเงินทั่วไป	15.79%
13. ควรออกมาตรการต้องห้ามผู้ให้บริการรับอนุญาตทำธุรกรรมใดๆที่เกี่ยวข้องกับเงินสกุลเข้ารหัสซึ่งมีความเสี่ยงทางเทคโนโลยีสูงต่อการใช้เป็นเครื่องมือในการฟอกเงิน เช่น Privacy Coin[7] สกุลเงินต่างๆ	10.53%

(1) ผู้ใช้งาน หมายถึง บุคคลที่ประสงค์จะทำธุรกรรมเงินสกุลเข้ารหัส หรือใช้บริการกับผู้ให้บริการเกี่ยวกับเงินสกุลเข้ารหัส

(2) เงินสกุลเข้ารหัส หรือคริปโตเคอเรนซี (Cryptocurrency)

(3) องค์กรระหว่างประเทศ และหน่วยงานของแต่ละประเทศที่รับผิดชอบงานด้านการต่อต้านการฟอกเงิน

(4) ผู้ให้บริการรับอนุญาต หมายถึง Exchanger, Broker, Portal, Wallet Provider ที่ได้รับอนุญาตตามกฎหมาย เป็นต้น

(5) สำนักงาน ปปง. สำนักงาน กลต. ธปท. สำนักงานตำรวจ กรมสอบสวนคดีพิเศษ สำนักงานอัยการ กรมสรรพากร กรมบังคับคดี สำนักงาน กสทช. เป็นต้น

(6) เช่น ธนาคาร บริษัทเงินทุน บริษัทหลักทรัพย์ บริษัทบัตรเครดิต บริษัทการเงินนอกระบบธนาคาร บริษัทบริการการเงินอิเล็กทรอนิกส์

(7) Privacy coin มีคุณสมบัติที่สามารถปกปิดร่องรอยผู้ทำธุรกรรม เส้นทางธุรกรรม และมูลค่าในกระเป๋าเงิน (Wallet)

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

คำถามปลายเปิดในการสัมภาษณ์เชิงลึกเพื่อสำรวจความคิดเห็นจากผู้ให้ข้อมูลสำคัญ

“ท่านมีข้อเสนอแนะ หรือความคิดเห็นอย่างไร ต่อแนวทางปฏิบัติเพื่อการบังคับใช้เชิงปฏิบัติการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมและสามารถเพิ่มประสิทธิภาพการดำเนินงานตามนโยบายที่กำหนด (ทั้งนี้ขอความกรุณาให้ข้อเสนอแนะหรือแสดงความคิดเห็นต่อแนวทางปฏิบัติที่คิดว่าเหมาะสมประมาณ 3 – 5 แนวทาง)”

ทั้งนี้ได้ทำการสังเคราะห์ผลสำรวจความคิดเห็นและทัศนะเชิงเสนอแนะต่อแนวแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสม โดยได้สรุปเป็นข้อเสนอจำนวน 10 แนวปฏิบัติ ซึ่งได้แสดงตามลำดับสัดส่วนความเห็นจากผู้ให้สัมภาษณ์ เพื่อจัดทำแบบสำรวจความเห็นตามเทคนิควิธีเดลฟายรอบที่ 2 ต่อไป

แนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	สัดส่วนความเห็น
1. ควรพัฒนาองค์ความรู้เกี่ยวกับลักษณะ กลไกการทำงานของธุรกรรมเงินสกุลเข้ารหัสให้แก่เจ้าหน้าที่ผู้รับผิดชอบ รวมถึงการแลกเปลี่ยนประสบการณ์ กรณีศึกษาระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง	52.63%
2. ควรสร้างระบบประสานความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง เพื่อลดความทับซ้อนของการทำงาน และแบ่งปันข้อมูลความเชื่อมโยงธุรกรรมต้องสงสัย	36.84%
3. หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องควรร่วมกันประมวลขั้นตอนการปฏิบัติงาน เพื่อจัดทำคู่มือมาตรฐานการปฏิบัติงานตั้งแต่การกำกับดูแลต้นทางเพื่อการป้องกัน จนถึงขั้นตอนการบังคับคดีปลายทางของกระบวนการ	31.58%
4. ควรสร้างเครือข่ายความร่วมมือกับองค์กรด้านการสืบสวนคดีระหว่างประเทศ เพื่อช่วยเหลือสนับสนุนการปฏิบัติการข้ามประเทศ	31.58%
5. ควรสร้างระบบการทำงานในลักษณะคณะทำงานเฉพาะกิจ หรือศูนย์ปฏิบัติการประสานงานที่บูรณาการหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง เพื่อให้การทำงานเคลื่อนตัวไปในทิศทางเดียวกัน โดยไม่จำเป็นต้องจัดตั้งเป็นองค์ถาวร	26.32%
6. ควรออกระเบียบเกี่ยวกับกระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย ในลักษณะกำหนดหน่วยงานกลางที่รับผิดชอบดูแลกระเป๋าเงินอิเล็กทรอนิกส์กลาง (Bureau Wallet) เพื่อเก็บรักษา และจัดการเงินสกุลเข้ารหัสของกลางในคดี	26.32%
7. ควรจัดให้มีกระบวนการรับฟังความคิดเห็นจากหน่วยงานปฏิบัติการ เพื่อร่วมให้ความเห็นเพื่อร่วมปรับแก้วิธีการดำเนินงานให้เหมาะสมต่อการปฏิบัติงานก่อนการออกประกาศมาตรการที่เกี่ยวข้องกับการกำกับเงินสกุลเข้ารหัส	21.05%
8. ควรปรับปรุงแนวปฏิบัติเพื่อการแสวงหาหลักฐานทางเทคโนโลยี และเส้นทางร่องรอยธุรกรรมบนระบบปฏิบัติการบล็อกเชนที่ยอมรับโดยกฎหมายเพื่อใช้เป็นพยานในวิธีการพิจารณาคดีได้โดยชอบ	15.79%
9. ควรใช้เครื่องมือทางเทคโนโลยี[1] ในการวิเคราะห์ธุรกรรมเพื่อสืบค้นธุรกรรมต้องสงสัยโดยการเชื่อมต่อกับฐานข้อมูลในระบบปฏิบัติการบล็อกเชนของเงินสกุลเข้ารหัสเป้าหมาย	10.53%
10. ควรมีมาตรการบังคับใช้กฎหมายที่รวดเร็ว ชัดเจนแน่นอน และมีบทลงโทษระดับรุนแรง เพื่อให้สังคมได้รับรู้และตระหนักถึงผลร้ายของการกระทำผิด	10.53%

(1) เครื่องมือทางเทคโนโลยี รวมถึงการจัดหาเครื่องมือเอง พัฒนาขึ้นเอง และการว่าจ้างบริษัทตรวจสอบทางเทคนิค

ง. แบบสำรวจความเห็นตามเทคนิควิธีเดลฟายรอบที่ 2

แบบสำรวจความเห็นต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินเข้ารหัส

ผู้มีส่วนร่วมในการวิจัย 000 (รหัสผู้ให้ข้อมูลสำคัญ) ชื่อผู้ให้ข้อมูลสำคัญ .....

ตามที่ผู้วิจัยได้รับความอนุเคราะห์จากท่านในการสละเวลาให้ข้อมูลการสัมภาษณ์ เพื่อการวิจัยในการจัดทำวิทยานิพนธ์เรื่อง "แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส (Cryptocurrency)" ผู้วิจัยใคร่ขอขอบคุณท่านอย่างสูงมา ณ โอกาสนี้ ในขณะเดียวกันผู้วิจัยได้ประมวลความคิดเห็นจากผู้ให้ข้อมูลการสัมภาษณ์ทุกท่านต่อการกำหนดนโยบายหรือแนวทางเพื่อป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมต่อบริบทของประเทศไทยและสากลในสถานการณ์ปัจจุบัน รวมถึงความคิดเห็นต่อแนวทางปฏิบัติเพื่อการบังคับใช้ในการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมและสามารถเพิ่มประสิทธิภาพการดำเนินงานตามนโยบายที่กำหนด

ผู้วิจัยใคร่ขอความอนุเคราะห์จากท่านอีกครั้ง ในการให้ความคิดเห็นต่อแนวทางเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสซึ่งเป็นการประมวลผลจากข้อมูลการสัมภาษณ์ โดยขอให้ท่านได้ระบุความคิดเห็นต่อแต่ละแนวทางที่นำเสนอด้วยระดับความเห็นตั้งแต่ 1 ถึง 5 ทั้งนี้ **ระดับ 1** หมายถึง แนวทางที่นำเสนอเหมาะสมต่อการนำไปบังคับใช้ได้**น้อยที่สุด** และ **ระดับ 5** หมายถึงแนวทางที่นำเสนอเหมาะสมต่อการนำไปบังคับใช้ได้**มากที่สุด**

แนวทางป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	สัดส่วนความเห็นจากผู้ให้สัมภาษณ์	ระดับความเห็น					ความเห็นเพิ่มเติม
		1	2	3	4	5	
1. ในการวางหลักเกณฑ์มาตรฐานสำหรับการบันทึกข้อมูลเพื่อการตรวจพิสูจน์ตัวตนของผู้ใช้งาน* (KYC) ควรมีการกำหนดข้อมูลจำเป็นอย่างเพียงพอ และทำตรวจสอบทบทวนข้อมูลบุคคลให้ทันสมัยอย่างสม่ำเสมอ	57.89%						*ผู้ใช้งาน หมายถึง บุคคลที่ประสงค์จะทำธุรกรรมเงินสกุลเข้ารหัส หรือใช้บริการกับผู้ให้บริการเกี่ยวกับเงินสกุลเข้ารหัส
2. ควรส่งเสริมความรู้ให้แก่ประชาชนถึงลักษณะ กลไกการทำงานของเงินสกุลเข้ารหัส* และความเสี่ยงของธุรกรรมเงินสกุลเข้ารหัส รวมถึงโอกาสการตรวจสอบและเข้าถึงเส้นทางการทำธุรกรรมในระบบปฏิบัติการบล็อกเชน	52.63%						*เงินสกุลเข้ารหัส หรือคริปโตเคอเรนซี (Cryptocurrency)
3. ควรสร้างกรอบความร่วมมือระหว่างประเทศเพื่อการต่อต้านการฟอกเงิน* โดยการแลกเปลี่ยนข้อมูล และประสบการณ์ของแต่ละประเทศเกี่ยวกับการทำอาชญากรรมธุรกรรมเงินสกุลเข้ารหัส รวมถึงการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	47.37%						*องค์กรระหว่างประเทศ และหน่วยงานของแต่ละประเทศที่รับผิดชอบงานด้านการต่อต้านการฟอกเงิน

แนวทางป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	สัดส่วน	ระดับความเห็น					ความเห็นเพิ่มเติม
		1	2	3	4	5	
4. ควรส่งเสริมศักยภาพการแข่งขันให้แก่ผู้ให้บริการรับอนุญาต* เพื่ออำนวยความสะดวกในการทำธุรกรรมเงินสกุลเข้ารหัสให้แก่ผู้ใช้งาน และสร้างแรงจูงใจแก่ผู้ใช้งานให้เลือกใช้บริการกับผู้ให้บริการรับอนุญาต มากกว่าการใช้บริการกับผู้ให้บริการนอกระบบ หรือผู้ให้บริการต่างประเทศ	42.11%						*ผู้ให้บริการรับอนุญาต หมายถึง Exchanger, Broker, Portal, Wallet Provider ที่ได้รับอนุญาตตามกฎหมาย เป็นต้น
5. ในกระบวนการออกกฎระเบียบเพื่อการกำกับธุรกรรมและผู้ให้บริการรับอนุญาตควรคำนึงถึงความคล่องตัวของธุรกิจ เพื่อสร้างความสมดุลระหว่างประโยชน์สาธารณะที่จะได้รับ กับข้อจำกัดในการดำเนินธุรกิจ	31.58%						
6. ในการกำหนดแนวทางการกำกับธุรกรรมและผู้ให้บริการเงินสกุลเข้ารหัสควรอ้างอิงกับแนวทางหรือข้อแนะนำตามหลักมาตรฐานการปฏิบัติสากล เช่น FATF Recommendations	26.32%						
7. ควรสร้างระบบเครือข่ายความร่วมมือในการแบ่งปันความช่วยเหลือระหว่างหน่วยงานบังคับใช้กฎหมาย* ในการเข้าถึงข้อมูลส่วนบุคคลของผู้ต้องสงสัย รวมถึงเส้นทางการทำธุรกรรมต้องสงสัย	21.05%						*สำนักงาน ปปง. สำนักงาน กลต. ธปท. สำนักงานตำรวจ กรมสอบสวนคดีพิเศษ สำนักงานอัยการ กรมสรรพากร กรมบังคับคดี สำนักงาน กสทช. เป็นต้น
8. ควรบูรณาการหน่วยงานหลักที่รับผิดชอบร่วมทำงานแบบองค์รวมเพื่อร่วมกันกำหนดแผนปฏิบัติงานตามลำดับขั้นตอนปฏิบัติการ ลดการทับซ้อนของขอบเขตงาน และเพิ่มประสิทธิภาพการปฏิบัติงาน โดยอาจมีคณะทำงานเฉพาะกิจหรือผู้เชี่ยวชาญเป็นที่ปรึกษาให้การสนับสนุนเชิงเทคนิคและแนวทาง	21.05%						
9. ควรส่งเสริมให้สามารถสร้างกรอบความร่วมมือขององค์กรภาคเอกชนที่เกี่ยวข้องกับธุรกิจเงินสกุลเข้ารหัส เพื่อการสนับสนุนการดำเนินงานกำกับดูแลกันเองภายในอุตสาหกรรม และประสานงานกับหน่วยงานรัฐ	21.05%						
10. ควรออกมาตรการกำหนดให้ผู้ใช้งานที่จะต้องการทำธุรกรรมจะต้องดำเนินการกับผู้ให้บริการที่ได้รับอนุญาต และหากเป็นธุรกรรมข้ามประเทศก็ให้ดำเนินกับผู้ให้บริการที่ได้รับอนุญาตของประเทศนั้นๆ	21.05%						

แนวทางป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	สัดส่วน	ระดับความเห็น					ความเห็นเพิ่มเติม
		1	2	3	4	5	
11. ควรออกระเบียบปฏิบัติที่ชัดเจนที่เกี่ยวข้องกับการปฏิบัติหน้าที่ต่อการสืบสวน หาหลักฐานในลักษณะดิจิทัล และการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย โดยมีกฎหมายรองรับ หรือปรับแก้ไขกฎหมายให้สามารถดำเนินการได้	15.79%						
12. ควรสร้างระบบจัดการฐานข้อมูลกลางของการแสดงตัวตนผู้ใช้งาน (KYC Bureau) ที่รวบรวมข้อมูลส่วนบุคคลจากผู้ให้บริการทางการเงินทุกประเภท* เพื่อสามารถเชื่อมโยงข้อมูลทั้งในส่วนธุรกรรมเงินสกุลเข้ารหัส และธุรกรรมทางการเงินทั่วไป	15.79%						*เช่น ธนาคาร บริษัทเงินทุน บริษัทหลักทรัพย์ บริษัทบัตรเครดิต บริษัทการเงินนอกระบบธนาคาร บริษัทบริการการเงินดิเล็กทรอนิกส์
13. ควรออกมาตรการต้องห้ามผู้ให้บริการรับอนุญาตทำธุรกรรมใดๆที่เกี่ยวข้องกับเงินสกุลเข้ารหัสซึ่งมีความเสี่ยงทางเทคโนโลยีสูงต่อการใช้เป็นเครื่องมือในการฟอกเงิน เช่น Privacy Coin* สกุลเงินต่างๆ	10.53%						*Privacy coin มีคุณสมบัติที่สามารถปกปิดร่องรอยผู้ทำธุรกรรม เส้นทางธุรกรรม และมูลค่าในกระเป๋าเงิน (Wallet)

และความคิดเห็นต่อแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมและสามารถเพิ่มประสิทธิภาพในการปฏิบัติงานได้ ซึ่งเป็นการประมวลผลจากข้อมูลการสัมภาษณ์ โดยขอให้ท่านได้ระบุความคิดเห็นต่อแต่ละแนวปฏิบัติที่นำเสนอด้วยระดับความเห็นตั้งแต่ 1 ถึง 5 ทั้งนี้ ระดับ 1 หมายถึง แนวปฏิบัติที่นำเสนอน่าจะมีโอกาสเพิ่มประสิทธิภาพในการปฏิบัติงานได้**น้อยที่สุด** และ ระดับ 5 หมายถึงแนวปฏิบัติที่นำเสนอน่าจะมีโอกาสเพิ่มประสิทธิภาพในการปฏิบัติงานได้มากที่สุด

แนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	สัดส่วนความเห็นจากการสัมภาษณ์	ระดับความเห็น					ความเห็นเพิ่มเติม
		1	2	3	4	5	
1. ควรพัฒนาองค์ความรู้เกี่ยวกับลักษณะ กลไกการทำงานของธุรกรรมเงินสกุลเข้ารหัสให้แก่เจ้าหน้าที่ผู้รับผิดชอบ รวมถึงการแลกเปลี่ยนประสบการณ์ กรณีศึกษาระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง	52.63%						
2. ควรสร้างระบบประสานความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องเพื่อลดความทับซ้อนของการทำงาน และแบ่งปันข้อมูลความเชื่อมโยงธุรกรรมต้องสงสัย	36.84%						

แนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	สัดส่วน	ระดับความเห็น					ความเห็นเพิ่มเติม
		1	2	3	4	5	
3. หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องควรร่วมกันประมวลขั้นตอนการปฏิบัติงานเพื่อจัดทำคู่มือมาตรฐานการปฏิบัติงานตั้งแต่การกำกับดูแลต้นทางเพื่อการป้องกันจนถึงขั้นตอนการบังคับคดีปลายทางของกระบวนการ	31.58%						
4. ควรสร้างเครือข่ายความร่วมมือกับองค์กรด้านการสืบสวนคดีระหว่างประเทศ เพื่อช่วยเหลือสนับสนุนการปฏิบัติการข้ามประเทศ	31.58%						
5. ควรสร้างระบบการทำงานในลักษณะคณะทำงานเฉพาะกิจ หรือศูนย์ปฏิบัติการประสานงานที่บูรณาการหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง เพื่อให้การทำงานเคลื่อนตัวไปในทิศทางเดียวกัน โดยไม่จำเป็นต้องจัดตั้งเป็นองค์กรถาวร	26.32%						
6. ควรออกระเบียบเกี่ยวกับกระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย ในลักษณะกำหนดหน่วยงานกลางที่รับผิดชอบดูแลกระเป๋าเงินอิลีกทรอนิกส์กลาง (Bureau Wallet) เพื่อเก็บรักษา และจัดการเงินสกุลเข้ารหัสของกลางในคดี	26.32%						
7. ควรจัดให้มีกระบวนการรับฟังความคิดเห็นจากหน่วยงานปฏิบัติการ เพื่อร่วมให้ความเห็นเพื่อร่วมปรับแก้วิธีการดำเนินงานให้เหมาะสมต่อการปฏิบัติงานก่อนการออกประกาศมาตรการที่เกี่ยวข้องกับการกำกับเงินสกุลเข้ารหัส	21.05%						
8. ควรปรับปรุงแนวปฏิบัติเพื่อการแสวงหาหลักฐานทางเทคโนโลยี และเส้นทางร่องรอยธุรกรรมบนระบบปฏิบัติการบล็อกเชนที่ยอมรับโดยกฎหมายเพื่อใช้เป็นพยานในวิธีการพิจารณาคดีได้โดยชอบ	15.79%						
9. ควรใช้เครื่องมือทางเทคโนโลยี* ในการวิเคราะห์ธุรกรรมเพื่อสืบค้นธุรกรรมต้องสงสัยโดยการเชื่อมต่อกับฐานข้อมูลในระบบปฏิบัติการบล็อกเชนของเงินสกุลเข้ารหัสเป้าหมาย	10.53%						*เครื่องมือทางเทคโนโลยี รวมถึงการจัดหาเครื่องมือเอง พัฒนาขึ้นเอง และการว่าจ้างบริษัทตรวจสอบทางเทคนิค
10. ควรมีมาตรการบังคับใช้กฎหมายที่รวดเร็ว ชัดเจนแน่นอน และมีบทลงโทษระดับรุนแรง เพื่อให้สังคมได้รับรู้และตระหนักถึงผลร้ายของการกระทำผิด	10.53%						

จ. แบบสำรวจความเห็นตามเทคนิควิธีเดลฟายรอบที่ 3

แบบสำรวจความเห็นต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินเข้ารหัส(ฉบับทบทวนหรือยืนยันความเห็น)

ผู้มีส่วนร่วมในการวิจัย 000 (รหัสผู้ให้ข้อมูลสำคัญ) ชื่อผู้ให้ข้อมูลสำคัญ .....

ตามที่ผู้วิจัยได้รับความอนุเคราะห์จากท่านในการสละเวลาให้สัมภาษณ์และตอบแบบสำรวจ เพื่อการวิจัยในการจัดทำวิทยานิพนธ์เรื่อง “แนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส (Cryptocurrency)” นั้น ผู้วิจัยใคร่ขอขอบคุณท่านอย่างสูงมา ณ โอกาสนี้ ในขณะเดียวกันผู้วิจัยได้ประมวลความคิดเห็นจากการตอบแบบสำรวจความเห็นต่อแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินเข้ารหัสของผู้ให้ข้อมูลทุกท่าน โดยได้สรุปความเห็นต่อแต่ละแนวทางแสดงเป็นข้อมูลสถิติเบื้อง ประกอบด้วยสัดส่วนผู้ให้ความเห็นแต่ละระดับจาก 1 ถึง 5 เป็น %ของจำนวนผู้ตอบแบบสำรวจรวม ค่าเฉลี่ย และค่าเบี่ยงเบนมาตรฐาน รวมถึงคำตอบของท่านซึ่งได้ตอบไว้ในแบบสำรวจครั้งก่อน

ในการนี้ ผู้วิจัยใคร่ขอความอนุเคราะห์จากท่านอีกครั้ง ในการพิจารณาทบทวนหรือยืนยันความคิดเห็นของท่านต่อแนวทางเพื่อป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยขอให้ท่านระบุความคิดเห็นต่อแต่ละแนวทางที่นำเสนอ โดยระบุตัวเลขระดับความเห็นที่ท่านคิดว่าเหมาะสมตั้งแต่ 1 ถึง 5 ทั้งนี้ ระดับ 1 หมายถึง แนวทางที่นำเสนอเหมาะสมต่อการนำไปบังคับใช้ได้”น้อยที่สุด”, ระดับ 2 หมายถึง “น้อย”, ระดับ 3 หมายถึง “ปานกลาง”, ระดับ 4 หมายถึง “มาก” และ ระดับ 5 หมายถึง “มากที่สุด”

แนวทางป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	ความเห็นครั้งนี้	ความเห็นครั้งก่อนของท่าน	สรุปรวมความเห็นของผู้ให้ข้อมูลครั้งก่อน				
			1	2	3	4	5
1. ในการวางหลักเกณฑ์มาตรฐานสำหรับการบันทึกข้อมูลเพื่อการตรวจพิสูจน์ตัวตนของผู้ใช้งาน* (KYC) ควรมีการกำหนดข้อมูลจำเป็นอย่างเพียงพอ และทำตรวจสอบทบทวนข้อมูลบุคคลให้ทันสมัยอย่างสม่ำเสมอ			0.00%	0.00%	5.56%	22.22%	72.22%
		ค่าเฉลี่ย (Mean) = 4.67			ค่าเบี่ยงเบน (SD) = 0.58		
2. ควรส่งเสริมความรู้ให้แก่ประชาชนถึงลักษณะ กลไกการทำงานของเงินสกุลเข้ารหัส*และความเสี่ยงของธุรกรรมเงินสกุลเข้ารหัส รวมถึงโอกาสการตรวจสอบและเข้าถึงเส้นทางการทำธุรกรรมในระบบปฏิบัติการบล็อกเชน			5.56%	0.00%	0.00%	16.67%	77.78%
		ค่าเฉลี่ย (Mean) = 4.61			ค่าเบี่ยงเบน (SD) = 0.95		

แนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	ความเห็นครั้งนี้	ความเห็นครั้งก่อนของท่าน	สรุปรวมความเห็นของผู้ให้ข้อมูลครั้งก่อน				
			1	2	3	4	5
5. ควรสร้างระบบการทำงานในลักษณะคณะทำงานเฉพาะกิจ หรือศูนย์ปฏิบัติการประสานงานที่บูรณาการหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง เพื่อให้การทำงานเคลื่อนตัวไปในทิศทางเดียวกัน โดยไม่จำเป็นต้องจัดตั้งเป็นองค์กรวร			5.56%	11.11%	33.33%	38.89%	11.11%
		ค่าเฉลี่ย (Mean) = 3.39			ค่าเบี่ยงเบน (SD) = 1.01		
6. ควรออกระเบียบเกี่ยวกับกระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย ในลักษณะกำหนดหน่วยงานกลางที่รับผิดชอบดูแลกระเป๋าเงินอิลึกทรอนิกส์กลาง (Bureau Wallet) เพื่อเก็บรักษา และจัดการเงินสกุลเข้ารหัสของกลางในคดี			5.56%	0.00%	11.11%	44.44%	38.89%
		ค่าเฉลี่ย (Mean) = 4.11			ค่าเบี่ยงเบน (SD) = 0.99		
7. ควรจัดให้มีกระบวนการรับฟังความคิดเห็นจากหน่วยงานปฏิบัติการ เพื่อร่วมให้ความเห็นเพื่อร่วมปรับแก้วิธีการดำเนินงานให้เหมาะสมต่อการปฏิบัติงานก่อนการออกประกาศมาตรการที่เกี่ยวข้องกับการกำกับเงินสกุลเข้ารหัส			5.56%	0.00%	0.00%	38.89%	55.56%
		ค่าเฉลี่ย (Mean) = 4.39			ค่าเบี่ยงเบน (SD) = 0.95		
8. ควรปรับปรุงแนวปฏิบัติเพื่อการแสวงหาหลักฐานทางเทคโนโลยี และเส้นทางร่องรอยธุรกรรมบนระบบปฏิบัติการบล็อกเชนที่ยอมรับโดยกฎหมายเพื่อใช้เป็นพยานในวิธีการพิจารณาคดีได้โดยชอบ			5.56%	0.00%	5.56%	33.33%	55.56%
		ค่าเฉลี่ย (Mean) = 4.33			ค่าเบี่ยงเบน (SD) = 1.00		
9. ควรใช้เครื่องมือทางเทคโนโลยี* ในการวิเคราะห์ธุรกรรมเพื่อสืบค้นธุรกรรมต้องสงสัยโดยการเชื่อมต่อกับฐานข้อมูลในระบบปฏิบัติการบล็อกเชนของเงินสกุลเข้ารหัสเป้าหมาย			0.00%	0.00%	16.67%	22.22%	61.11%
		ค่าเฉลี่ย (Mean) = 4.40			ค่าเบี่ยงเบน (SD)= 0.76		
10. ควรมีมาตรการบังคับใช้กฎหมายที่รวดเร็ว ชัดเจนแน่นอน และมีบทลงโทษระดับรุนแรง เพื่อให้สังคมได้รับรู้และตระหนักถึงผลร้ายของการกระทำผิด			0.00%	11.11%	22.22%	33.33%	33.33%
		ค่าเฉลี่ย (Mean) = 3.89			ค่าเบี่ยงเบน (SD) = 0.99		

แนวทางป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	ความเห็นครั้งนี้	ความเห็นครั้งก่อนของท่าน	สรุปรวมความเห็นของผู้ให้ข้อมูลครั้งก่อน				
			1	2	3	4	5
9. ควรส่งเสริมให้สามารถสร้างกรอบความร่วมมือขององค์กรภาคเอกชนที่เกี่ยวข้องกับธุรกิจเงินสกุลเข้ารหัส เพื่อการสนับสนุนการดำเนินงานกำกับดูแลกันเองภายในอุตสาหกรรม และประสานงานกับหน่วยงานรัฐ			0.00%	5.56%	11.11%	33.33%	50.00%
		ค่าเฉลี่ย (Mean) = 4.28			ค่าเบี่ยงเบน (SD)= 0.87		
10. ควรออกมาตรการกำหนดให้ผู้ใช้งานที่จะต้องการทำธุรกรรมจะต้องดำเนินการกับผู้ให้บริการที่ได้รับอนุญาต และหากเป็นธุรกรรมข้ามประเทศก็ให้ดำเนินกับผู้ให้บริการที่ได้รับอนุญาตของประเทศนั้นๆ			16.67%	11.11%	27.78%	33.33%	11.11%
		ค่าเฉลี่ย (Mean) = 3.11			ค่าเบี่ยงเบน (SD) = 1.24		
11. ควรออกระเบียบปฏิบัติที่ชัดเจนที่เกี่ยวข้องกับการปฏิบัติหน้าที่ต่อการสืบสวน หาหลักฐานในลักษณะดิจิทัล และการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย โดยมีกฎหมายรองรับ หรือปรับแก้ไขกฎหมายให้สามารถดำเนินการได้			0.00%	5.56%	5.56%	38.89%	50.00%
		ค่าเฉลี่ย (Mean) = 4.33			ค่าเบี่ยงเบน (SD) = 0.82		
12. ควรสร้างระบบจัดการฐานข้อมูลกลางของการแสดงตัวตนผู้ใช้งาน (KYC Bureau) ที่รวบรวมข้อมูลส่วนบุคคลจากผู้ให้บริการทางการเงินทุกประเภท* เพื่อสามารถเชื่อมโยงข้อมูลทั้งในส่วนธุรกรรมเงินสกุลเข้ารหัส และธุรกรรมทางการเงินทั่วไป			5.56%	5.56%	16.67%	38.89%	33.33%
		ค่าเฉลี่ย (Mean) = 3.89			ค่าเบี่ยงเบน (SD) = 1.10		
13. ควรออกมาตรการต้องห้ามผู้ให้บริการรับอนุญาตทำธุรกรรมใดๆที่เกี่ยวข้องกับเงินสกุลเข้ารหัสซึ่งมีความเสี่ยงทางเทคโนโลยีสูงต่อการใช้เป็นเครื่องมือในการฟอกเงิน เช่น Privacy Coin* สกุลเงินต่างๆ			16.67%	5.56%	16.67%	27.78%	33.33%
		ค่าเฉลี่ย (Mean) = 3.56			ค่าเบี่ยงเบน (SD)= 1.42		

การพิจารณาทบทวนหรือยืนยันความคิดเห็นของท่านต่อแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสที่เหมาะสมและสามารถเพิ่มประสิทธิภาพในการปฏิบัติงานได้ โดยขอให้ท่านระบุความคิดเห็นต่อแต่ละแนวทางที่นำเสนอ โดยระบุตัวเลขระดับความเห็นที่ท่านคิดว่าเหมาะสมตั้งแต่ 1 ถึง 5 ทั้งนี้ ระดับ 1 หมายถึง แนวปฏิบัติที่นำเสนอน่าจะมีโอกาสเพิ่มประสิทธิภาพในการปฏิบัติงานได้"น้อยที่สุด", ระดับ 2 หมายถึง "น้อย", ระดับ 3 หมายถึง "ปานกลาง", ระดับ 4 หมายถึง "มาก" และ ระดับ 5 หมายถึง "มากที่สุด"

แนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	ความเห็นครั้งนี้	ความเห็นครั้งก่อนของท่าน	สรุปรวมความเห็นของผู้ให้ข้อมูลครั้งก่อน				
			1	2	3	4	5
1. ควรพัฒนาองค์ความรู้เกี่ยวกับลักษณะ กลไกการทำงานของธุรกรรมเงินสกุลเข้ารหัสให้แก่เจ้าหน้าที่ผู้รับผิดชอบ รวมถึงการแลกเปลี่ยนประสบการณ์กรณีศึกษาระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง			0.00%	0.00%	0.00%	5.56%	94.44%
		ค่าเฉลี่ย (Mean) = 4.94			ค่าเบี่ยงเบน (SD) = 0.23		
2. ควรสร้างระบบประสานความร่วมมือระหว่างหน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้อง เพื่อลดความทับซ้อนของการทำงาน และแบ่งปันข้อมูลความเชื่อมโยงธุรกรรมต้องสงสัย			0.00%	0.00%	11.11%	33.33%	55.56%
		ค่าเฉลี่ย (Mean) = 4.44			ค่าเบี่ยงเบน (SD) = 0.68		
3. หน่วยงานบังคับใช้กฎหมายที่เกี่ยวข้องควรร่วมกันประมวลขั้นตอนการปฏิบัติงาน เพื่อจัดทำคู่มือมาตรฐานการปฏิบัติงานตั้งแต่การกำกับดูแลต้นทางเพื่อการป้องกัน จนถึงขั้นตอนการบังคับคดีปลายทางของกระบวนการ			0.00%	0.00%	27.78%	27.78%	44.44%
		ค่าเฉลี่ย (Mean) = 4.17			ค่าเบี่ยงเบน (SD) = 0.83		
4. ควรสร้างเครือข่ายความร่วมมือกับองค์กรต้านการสืบสวนคดีระหว่างประเทศ เพื่อช่วยเหลือสนับสนุนการปฏิบัติการข้ามประเทศ			0.00%	0.00%	38.89%	16.67%	44.44%
		ค่าเฉลี่ย (Mean) = 4.06			ค่าเบี่ยงเบน (SD)= 0.91		

แนวปฏิบัติเพื่อการป้องกันและปราบปราม การฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส	ความเห็นครั้งนี้	ความเห็นครั้งก่อนของท่าน	สรุปรวมความเห็นของผู้ให้ข้อมูลครั้งก่อน				
			1	2	3	4	5
5. ควรสร้างระบบการทำงานในลักษณะคณะทำงานเฉพาะกิจ หรือศูนย์ปฏิบัติการประสานงานที่บูรณาการหน้าที่ความรับผิดชอบของหน่วยงานที่เกี่ยวข้อง เพื่อให้การทำงานเคลื่อนตัวไปในทิศทางเดียวกัน โดยไม่จำเป็นต้องจัดตั้งเป็นองค์กรวร			5.56%	11.11%	33.33%	38.89%	11.11%
		ค่าเฉลี่ย (Mean) = 3.39			ค่าเบี่ยงเบน (SD) = 1.01		
6. ควรออกระเบียบเกี่ยวกับกระบวนการยึดอายัดเงินสกุลเข้ารหัสต้องสงสัย ในลักษณะกำหนดหน่วยงานกลางที่รับผิดชอบดูแลกระเป๋าเงินอิลึกทรอนิกส์กลาง (Bureau Wallet) เพื่อเก็บรักษา และจัดการเงินสกุลเข้ารหัสของกลางในคดี			5.56%	0.00%	11.11%	44.44%	38.89%
		ค่าเฉลี่ย (Mean) = 4.11			ค่าเบี่ยงเบน (SD) = 0.99		
7. ควรจัดให้มีกระบวนการรับฟังความคิดเห็นจากหน่วยงานปฏิบัติการ เพื่อร่วมให้ความเห็นเพื่อร่วมปรับแก้วิธีการดำเนินงานให้เหมาะสมต่อการปฏิบัติงานก่อนการออกประกาศมาตรการที่เกี่ยวข้องกับการกำกับเงินสกุลเข้ารหัส			5.56%	0.00%	0.00%	38.89%	55.56%
		ค่าเฉลี่ย (Mean) = 4.39			ค่าเบี่ยงเบน (SD) = 0.95		
8. ควรปรับปรุงแนวปฏิบัติเพื่อการแสวงหาหลักฐานทางเทคโนโลยี และเส้นทางร่องรอยธุรกรรมบนระบบปฏิบัติการบล็อกเชนที่ยอมรับโดยกฎหมายเพื่อใช้เป็นพยานในวิธีการพิจารณาคดีได้โดยชอบ			5.56%	0.00%	5.56%	33.33%	55.56%
		ค่าเฉลี่ย (Mean) = 4.33			ค่าเบี่ยงเบน (SD) = 1.00		
9. ควรใช้เครื่องมือทางเทคโนโลยี* ในการวิเคราะห์ธุรกรรมเพื่อสืบค้นธุรกรรมต้องสงสัยโดยการเชื่อมต่อกับฐานข้อมูลในระบบปฏิบัติการบล็อกเชนของเงินสกุลเข้ารหัสเป้าหมาย			0.00%	0.00%	16.67%	22.22%	61.11%
		ค่าเฉลี่ย (Mean) = 4.40			ค่าเบี่ยงเบน (SD)= 0.76		
10. ควรมีมาตรการบังคับใช้กฎหมายที่รวดเร็ว ชัดเจนแน่นอน และมีบทลงโทษระดับรุนแรง เพื่อให้สังคมได้รับรู้และตระหนักถึงผลร้ายของการกระทำผิด			0.00%	11.11%	22.22%	33.33%	33.33%
		ค่าเฉลี่ย (Mean) = 3.89			ค่าเบี่ยงเบน (SD) = 0.99		

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

ฉ. รายงานการวิเคราะห์ผลการศึกษาโดยเทคนิควิธีเดลฟาย

วิเคราะห์ผลการศึกษาโดยเทคนิควิธีเดลฟาย

ตารางที่ 1 : การวิเคราะห์ค่าสถิติของการสำรวจความเห็นรอบที่ 3

ข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุล **รอบที่ 2**

แนวทางป้องกัน	ค่าเฉลี่ย	ค่ามัธยฐาน	ค่าฐานนิยม	ค่าควอไทล์ที่ 1	ค่าควอไทล์ที่ 3	ค่าเบี่ยงเบนมาตรฐาน	ค่าความแปรปรวน	ค่าความแปรปรวน
1	4.72	5.00	5.00	5.00	5.00	0.575	0.330	0.353
2	4.61	5.00	5.00	5.00	5.00	0.979	0.958	0.958
3	4.44	5.00	5.00	4.00	5.00	0.856	0.732	0.732
4	4.17	4.00	5.00	3.25	5.00	0.857	0.735	1.242
5	4.44	5.00	5.00	4.00	5.00	0.784	0.614	0.840
6	4.39	4.00	4.00	4.00	5.00	0.608	0.369	0.379
7	4.56	5.00	5.00	4.00	5.00	0.616	0.379	1.075
8	4.33	5.00	5.00	4.00	5.00	0.907	0.824	0.918
9	4.28	4.00	5.00	4.00	5.00	0.752	0.565	0.801
10	3.17	3.50	4.00	2.00	4.00	1.383	1.912	1.634
11	4.33	4.50	5.00	4.00	5.00	0.840	0.706	0.706
12	3.83	4.00	4.00	3.25	4.75	1.098	1.206	1.281
13	3.50	4.00	4.00	3.00	4.75	1.425	2.029	2.144

ข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

แนวปฏิบัติเพื่อป้องกัน	ค่าเฉลี่ย	ค่ามัธยฐาน	ค่าฐานนิยม	ค่าควอไทล์ที่ 1	ค่าควอไทล์ที่ 3	ค่าเบี่ยงเบนมาตรฐาน	ค่าความแปรปรวน	ค่าความแปรปรวน
1	4.94	5.00	5.00	5.00	5.00	0.2357	0.0556	0.0556
2	4.61	5.00	5.00	4.00	5.00	0.6077	0.3693	0.4967
3	4.24	4.00	5.00	4.00	5.00	0.8314	0.6912	0.7353
4	4.17	4.50	5.00	3.00	5.00	0.9235	0.8529	0.8791
5	3.50	3.50	3.00	3.00	4.00	1.1504	1.3235	1.0752
6	4.17	4.00	5.00	4.00	5.00	1.0432	1.0882	1.0458
7	4.39	5.00	5.00	4.00	5.00	0.9785	0.9575	0.9575
8	4.61	5.00	5.00	4.00	5.00	0.6077	0.3693	1.0588
9	4.61	5.00	5.00	4.25	5.00	0.6978	0.4869	0.6144
10	4.00	4.00	5.00	3.25	5.00	1.0290	1.0588	1.0458

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

วิเคราะห์ผลการศึกษาโดยเทคนิควิธีเดลฟาย

ตารางที่ 2 : การตรวจสอบระดับความคงที่จากการสำรวจความเห็นรอบที่ 2 และรอบที่ 3

ข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุล

แนวทางป้องกัน	ความแตกต่างของระดับความเห็นรอบที่ 2 และ 3					ค่าสถิติ F-Test	นัยสำคัญทางสถิติ	ระดับความคงที่
	น้อยมาก	น้อย	ปานกลาง	มาก	มากที่สุด			
1	0.0%	0.0%	0.0%	5.6%	-5.6%	1.069	--	เข้าเกณฑ์
2	0.0%	0.0%	0.0%	0.0%	0.0%	1.000	--	เข้าเกณฑ์
3	0.0%	0.0%	0.0%	0.0%	0.0%	1.000	--	เข้าเกณฑ์
4	5.6%	0.0%	-11.1%	-5.6%	11.1%	1.689	--	เข้าเกณฑ์
5	0.0%	5.6%	-5.6%	0.0%	0.0%	1.367	--	เข้าเกณฑ์
6	0.0%	0.0%	0.0%	-5.6%	5.6%	1.027	--	เข้าเกณฑ์
7	5.6%	0.0%	0.0%	-5.6%	0.0%	2.836	**	ไม่เข้าเกณฑ์
8	0.0%	0.0%	5.6%	-5.6%	0.0%	1.115	--	เข้าเกณฑ์
9	0.0%	5.6%	-5.6%	-5.6%	5.6%	1.416	--	เข้าเกณฑ์
10	0.0%	-5.6%	11.1%	0.0%	-5.6%	0.855	--	เข้าเกณฑ์
11	0.0%	0.0%	0.0%	0.0%	0.0%	1.000	--	เข้าเกณฑ์
12	0.0%	0.0%	0.0%	-5.6%	5.6%	1.062	--	เข้าเกณฑ์
13	0.0%	0.0%	0.0%	-5.6%	5.6%	1.056	--	เข้าเกณฑ์

ข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

แนวปฏิบัติเพื่อป้องกัน	ความแตกต่างของระดับความเห็นรอบที่ 2 และ 3					ค่าสถิติ F-Test	นัยสำคัญทางสถิติ	สรุประดับความคงที่
	น้อยมาก	น้อย	ปานกลาง	มาก	มากที่สุด			
1	0.0%	0.0%	0.0%	0.0%	0.0%	1.000	--	เข้าเกณฑ์
2	0.0%	0.0%	5.6%	5.6%	-11.1%	1.345	--	เข้าเกณฑ์
3	0.0%	0.0%	5.6%	0.0%	0.0%	1.064	--	เข้าเกณฑ์
4	0.0%	0.0%	5.6%	0.0%	-5.6%	1.031	--	เข้าเกณฑ์
5	0.0%	0.0%	0.0%	11.1%	-11.1%	0.812	--	เข้าเกณฑ์
6	0.0%	0.0%	0.0%	5.6%	-5.6%	0.961	--	เข้าเกณฑ์
7	0.0%	0.0%	0.0%	0.0%	0.0%	1.000	--	เข้าเกณฑ์
8	5.6%	0.0%	0.0%	5.6%	-11.1%	2.867	**	ไม่เข้าเกณฑ์
9	0.0%	0.0%	5.6%	5.6%	-11.1%	1.262	--	เข้าเกณฑ์
10	0.0%	0.0%	5.6%	0.0%	-5.6%	0.988	--	เข้าเกณฑ์

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University

วิเคราะห์ผลการศึกษาโดยเทคนิควิธีเดลฟาย

ตารางที่ 3 : การตรวจสอบความเป็นฉันทามติ

ข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุล

แนวทางป้องกัน	ค่าสัมประสิทธิ์การกระจาย	ค่าสัมบูรณ์ของผลต่างค่ามัธยฐานกับค่าฐานนิยม	ค่าพิสัยระหว่างควอไทล์	ความเป็นฉันทามติ
1	0.122	0.00	0.00	เข้าเกณฑ์
2	0.212	0.00	0.00	เข้าเกณฑ์
3	0.193	0.00	1.00	เข้าเกณฑ์
4	0.206	1.00	1.75	ไม่เข้าเกณฑ์
5	0.176	0.00	1.00	เข้าเกณฑ์
6	0.138	0.00	1.00	เข้าเกณฑ์
7	0.135	0.00	1.00	เข้าเกณฑ์
8	0.209	0.00	1.00	เข้าเกณฑ์
9	0.176	1.00	1.00	เข้าเกณฑ์
10	0.437	0.50	2.00	ไม่เข้าเกณฑ์
11	0.194	0.50	1.00	เข้าเกณฑ์
12	0.286	0.00	1.50	ไม่เข้าเกณฑ์
13	0.407	0.00	1.75	ไม่เข้าเกณฑ์

ข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

แนวปฏิบัติเพื่อป้องกัน	ค่าสัมประสิทธิ์การกระจาย	ค่าสัมบูรณ์ของผลต่างค่ามัธยฐานกับค่าฐานนิยม	ค่าพิสัยระหว่างควอไทล์	ความเป็นฉันทามติ
1	0.048	0.00	0.00	เข้าเกณฑ์
2	0.132	0.00	1.00	เข้าเกณฑ์
3	0.196	1.00	1.00	เข้าเกณฑ์
4	0.222	0.50	2.00	ไม่เข้าเกณฑ์
5	0.329	0.50	1.00	เข้าเกณฑ์
6	0.250	1.00	1.00	เข้าเกณฑ์
7	0.223	0.00	1.00	เข้าเกณฑ์
8	0.132	0.00	1.00	เข้าเกณฑ์
9	0.151	0.00	0.75	เข้าเกณฑ์
10	0.257	1.00	1.75	ไม่เข้าเกณฑ์

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

วิเคราะห์ผลการศึกษาโดยเทคนิควิธีเดลฟาย

ตารางที่ 4 : การวิคราะห์ความเห็นต่อข้อเสนอเกณฑ์ฉันทามติเสียงข้างมาก

ข้อเสนอแนวทางการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุล

แนวทางป้องกัน	ค่าเฉลี่ย	ค่ามัธยฐาน	สัดส่วนร้อยละของระดับความเห็นจากการสำรวจ						ฉันทามติเสียงข้างมาก
			น้อยมาก	น้อย	ปานกลาง	มาก	มากที่สุด	มากและมากที่สุด	
1	4.72	5.00	0.0%	0.0%	5.6%	16.7%	77.8%	94.44%	เข้าเกณฑ์
2	4.61	5.00	5.6%	0.0%	0.0%	16.7%	77.8%	94.44%	เข้าเกณฑ์
3	4.44	5.00	0.0%	5.6%	5.6%	27.8%	61.1%	88.89%	เข้าเกณฑ์
4	4.17	4.00	0.0%	0.0%	27.8%	27.8%	44.4%	72.22%	ไม่เข้าเกณฑ์
5	4.44	5.00	0.0%	0.0%	16.7%	22.2%	61.1%	83.33%	เข้าเกณฑ์
6	4.39	4.00	0.0%	0.0%	5.6%	50.0%	44.4%	94.44%	เข้าเกณฑ์
7	4.56	5.00	0.0%	0.0%	5.6%	33.3%	61.1%	94.44%	เข้าเกณฑ์
8	4.33	5.00	0.0%	5.6%	11.1%	27.8%	55.6%	83.33%	เข้าเกณฑ์
9	4.28	4.00	0.0%	0.0%	16.7%	38.9%	44.4%	83.33%	เข้าเกณฑ์
10	3.17	3.50	16.7%	16.7%	16.7%	33.3%	16.7%	50.00%	ไม่เข้าเกณฑ์
11	4.33	4.50	0.0%	5.6%	5.6%	38.9%	50.0%	88.89%	เข้าเกณฑ์
12	3.83	4.00	5.6%	5.6%	16.7%	44.4%	27.8%	72.22%	ไม่เข้าเกณฑ์
13	3.50	4.00	16.7%	5.6%	16.7%	33.3%	27.8%	61.11%	ไม่เข้าเกณฑ์

ข้อเสนอแนวปฏิบัติเพื่อการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

แนวปฏิบัติเพื่อป้องกัน	ค่าเฉลี่ย	ค่ามัธยฐาน	สัดส่วนร้อยละของระดับความเห็นจากการสำรวจ						ฉันทามติเสียงข้างมาก
			น้อยมาก	น้อย	ปานกลาง	มาก	มากที่สุด	มากและมากที่สุด	
1	4.94	5.00	0.0%	0.0%	0.0%	5.6%	94.4%	100.00%	เข้าเกณฑ์
2	4.61	5.00	0.0%	0.0%	5.6%	27.8%	66.7%	94.44%	เข้าเกณฑ์
3	4.24	4.00	0.0%	0.0%	22.2%	27.8%	44.4%	72.22%	ไม่เข้าเกณฑ์
4	4.17	4.50	0.0%	0.0%	33.3%	16.7%	50.0%	66.67%	ไม่เข้าเกณฑ์
5	3.50	3.50	5.6%	11.1%	33.3%	27.8%	22.2%	50.00%	ไม่เข้าเกณฑ์
6	4.17	4.00	5.6%	0.0%	11.1%	38.9%	44.4%	83.33%	เข้าเกณฑ์
7	4.39	5.00	5.6%	0.0%	0.0%	38.9%	55.6%	94.44%	เข้าเกณฑ์
8	4.61	5.00	0.0%	0.0%	5.6%	27.8%	66.7%	94.44%	เข้าเกณฑ์
9	4.61	5.00	0.0%	0.0%	11.1%	16.7%	72.2%	88.89%	เข้าเกณฑ์
10	4.00	4.00	0.0%	11.1%	16.7%	33.3%	38.9%	72.22%	ไม่เข้าเกณฑ์

จุฬาลงกรณ์มหาวิทยาลัย
CHULALONGKORN UNIVERSITY

ประวัติผู้เขียน

ชื่อ-สกุล	นายวิสูต กัจฉมาภรณ์
วัน เดือน ปี เกิด	7 พฤษภาคม 2506
สถานที่เกิด	จังหวัดราชบุรี
วุฒิการศึกษา	- ประกาศนียบัตรบัณฑิตขั้นสูง (CAGS) สาขานวัตกรรมการจัดการ วิทยาลัยการจัดการหลักสูตรนานาชาติ มหาวิทยาลัยมหิดล - ศิลปศาสตรมหาบัณฑิต สาขากฎหมายเศรษฐกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย - บริหารธุรกิจมหาบัณฑิต (MBA) บัณฑิตวิทยาลัยหลักสูตรนานาชาติ มหาวิทยาลัยอัสสัมชัญ - ประกาศนียบัตรบัณฑิต (การภาษีอากร) คณะบริหารธุรกิจ มหาวิทยาลัยหอการค้าไทย - เศรษฐศาสตร์บัณฑิต สาขาการพัฒนาเศรษฐกิจ คณะเศรษฐศาสตร์ มหาวิทยาลัยรามคำแหง - สถิติศาสตร์บัณฑิต สาขาคณิตศาสตร์สถิติ คณะพาณิชยศาสตร์และการบัญชี จุฬาลงกรณ์มหาวิทยาลัย
ที่อยู่ปัจจุบัน	4/140 หมู่บ้านธารารมณ์ ซอยอนามัยงามเจริญ11 ถนนพระราม2 แขวงท่าข้าม เขตบางขุนเทียน กรุงเทพมหานคร 10150

จุฬาลงกรณ์มหาวิทยาลัย
Chulalongkorn University