วารสารบริหารธุรกิจและสังคมศาสตร์ มหาวิทยาลัยรามคำแหง
ปีที่ 4 ฉบับที่ 2 พฤษภาคม – สิงหาคม 2564

การฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

Money Laundering by Cryptocurrency Transaction

Received: March 25, 2021
Revised: July 07, 2021
Accepted: August 30, 2021

วิสูต กัจฉมาภรณ์[1]
Visoot Kajchamaporn

บทคัดย่อ

การฟอกเงินเป็นกระบวนการที่อาชญากรสร้างความชอบธรรมให้แก่ผลตอบแทนที่ได้จากการกระทำผิด ให้เป็นเงินที่ชอบด้วยกฎหมายและเป็นแหล่งเงินทุนสนับสนุนการก่ออาชญากรรมต่อไป โดยอาชญากรมักแสวงหาช่องโอกาสจากเครื่องมือทางการเงินรูปแบบใหม่ตลอดเวลา เพื่อการหลีกหนีกฎระเบียบและข้อจำกัดในการฟอกผลประโยชน์ โดย “เงินสกุลเข้ารหัส” เป็นนวัตกรรมทางการเงินที่ผู้ใช้งานสามารถทำธุรกรรมการโอนมูลค่าระหว่างกันโดยตรงแบบไร้พรมแดนได้อย่างรวดเร็ว และไม่มีหน่วยงานกลางใดกำกับ และอาจถูกนำไปใช้เป็นเครื่องมือในการฟอกเงิน

อาชญากรรมที่มีโอกาสใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน ส่วนใหญ่เป็นอาชญากรรมทางเศรษฐกิจ หรืออาชญากรรมไซเบอร์ ซึ่งมักก่อความเสียหายแก่เหยื่อในวงกว้าง และสร้างผลประโยชน์แก่อาชญากรด้วยมูลค่าสูง เนื่องด้วยกลไกการทำงานของเงินสกุลเข้ารหัสมีศักยภาพในการลดความเชื่อมโยงของเส้นทางธุรกรรมระหว่างต้นทางและปลายทาง จึงสามารถหลีกเลี่ยงหรือหลุดพ้นจากการติดตาม การอายัด และการจับกุมจากเจ้าหน้าที่ มาตรการป้องกันที่เหมาะสม คือ ควรเพิ่มประสิทธิภาพการพิสูจน์ตัวตนของผู้ใช้งานโดยจัดทำระบบจัดการฐานข้อมูลกลางของประเทศ เฝ้าระวังการทำธุรกรรมแปรสภาพระหว่างเงินสกุลเข้ารหัสเป็นเงินตราทั่วไป เสริมสร้างทักษะความรู้เกี่ยวกับเงินสกุลเข้ารหัสที่ถูกต้องให้แก่เจ้าหน้าที่และประชาชน ปรับปรุงกฎระเบียบในการดำเนินคดีเกี่ยวกับธุรกรรมเงินสกุลเข้ารหัส รวมถึงใช้โปรแกรมการตรวจสอบธุรกรรมต้องสงสัยบนบล็อกเชนเทคโนโลยี

คำสำคัญ: เงินสกุลเข้ารหัส, บิตคอยน์, การฟอกเงิน, การป้องกันอาชญากรรม

---

[1] นิสิตปริญญาเอก หลักสูตรศิลปศาสตรดุษฎีบัณฑิต สาขาอาชญาวิทยาและงานยุติธรรม ภาควิชาสังคมวิทยาและมานุษยวิทยา คณะรัฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย; Graduate Student of Doctor of Philosophy Program in Criminology and Criminal Justice, Department of Sociology and Anthropology, Faculty of Political Science, Chulalongkorn University; Email: visootk@hotmail.com

---

ABSTRACT

Money laundering is a process that criminals can use to legitimatize their illegal money and fund crimes. Criminals usually seek for opportunities from modern money laundering tools to avoid rules, regulations, and limitations in laundering their interests. 'Cryptocurrency' is a financial innovation that enables users to conduct peer-to-peer transactions globally in a speedy manner without any central controlling agency. It may be used as a tool for money laundering.

Crimes with an opportunity to use cryptocurrency as a tool for money laundering are mostly economic crimes or cybercrimes. These crimes usually create wide damages to victims and foster great benefits to criminals. The mechanism of cryptocurrency has the potential to reduce the connection of the transaction path between the source and the destination. It can avoid or be free from being tracked, confiscated, or having the users arrested by officers. Appropriate preventive measures are as follows. Increase the efficiency of user verification by making a national Know Your Customer (KYC) data center. Closely monitor swapping transactions between cryptocurrency and legal currency. Foster skills and knowledge about cryptocurrency correctly to officers and members of the general public. Improve the rules and regulations for the prosecution of cases related to cryptocurrency. Utilize a program to detect suspicious transactions on blockchain technology.

Keywords: Cryptocurrency, Bitcoin, Money Laundering, Crime Prevention

บทนำ

การฟอกเงินเป็นกระบวนการจัดการซ่อนเร้นผลประโยชน์ที่อาชญากรได้รับจากการกระทำผิด 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) หรืออาจกล่าวโดยสรุปได้ว่า เป็นกระบวนการที่อาชญากรใช้เพื่อการสร้างความชอบธรรมด้วยกฎหมายให้แก่เงินจากการกระทำผิด ซึ่งส่วนใหญ่มักเกี่ยวข้องกับอาชญากรรมองค์กรที่สามารถสร้างผลประโยชน์มหาศาลจากการค้ายาเสพติด การค้าอาวุธ การค้ามนุษย์ รวมถึงการฉ้อโกง (European Commission, 2020) ดังนั้น

เกือบทุกประเทศรวมถึงประเทศไทยได้มีการบัญญัติให้การฟอกเงินเป็นความผิดตามกฎหมาย เพื่อให้สามารถดำเนินมาตรการป้องกันและปราบปรามการฟอกเงินได้อย่างมีประสิทธิภาพ เพื่อเป็นการตัดวงจรการนำเงินหรือทรัพย์สินที่เกี่ยวข้องกับการกระทำผิดไปทำการฟอกเงิน และนำไปใช้ในการกระทำผิดต่อไปได้อีก (สำนักงานป้องกันและปราบปรามการฟอกเงิน, 2560) ทั้งนี้อาชญากรอาจจัดการซ่อนเร้นผลประโยชน์ด้วยวิธีการกลบเกลื่อนร่องรอยเส้นทางการเงิน เพื่อไม่ให้สามารถตรวจพิสูจน์แหล่งที่มาของแหล่งผลประโยชน์รวมถึงการตรวจสอบย้อนกลับไปถึงตัวอาชญากรได้ เช่น การนำเงินจากการกระทำผิดไปซื้อเพชรพลอย ทองคำ รถยนต์หรู งานศิลปะ หรือวัตถุโบราณ โดยไม่ระบุแหล่งที่มาของเงินในการซื้อทรัพย์สินดังกล่าว รวมถึงการถ่ายโอนทรัพย์ กระจายการถือครองไปหลายลำดับชั้น การให้กู้ยืมเงินแก่บุคคลรายย่อย การทยอยโอนเงินระหว่างประเทศ จนในที่สุดไม่สามารถตรวจสอบย้อนกลับไปยังแหล่งที่มาของเส้นทางการเงินตั้งต้นได้ (Baath & Zellhorn, 2016) อย่างไรก็ตาม อาชญากรก็มักจะมีพัฒนาการแสวงหาช่องโอกาสจากเครื่องมือทางการเงินรูปแบบใหม่ตลอดเวลา เพื่อหลีกหนีกฎระเบียบและข้อจำกัดของหน่วยงานที่บังคับใช้กฎหมายในการจัดการกับผลประโยชน์จากการฟอกเงิน และเงินสกุลเข้ารหัสถือเป็นนวัตกรรมเทคโนโลยีทางการเงินซึ่งมีคุณลักษณะเฉพาะหลายประการที่เอื้อประโยชน์ต่อการฟอกเงิน

นับตั้งแต่ปี 2008 ซาโตชิ นากาโมโต (Satoshi Nakamoto) ได้นำเสนอนวัตกรรมทางการเงินบนบล็อกเชนเทคโนโลยี เพื่อการโอนเงินทางอิเล็กทรอนิกส์ระหว่างบุคคลต่อบุคคลโดยตรงภายใต้ระบบนิเวศเงินสกุลเข้ารหัสที่สามารถพิสูจน์ยืนยันรายการกันเอง โดยไม่ผ่านการกำกับของหน่วยงานกลางใดๆ ในนามเรียกขานว่า “บิตคอยน์ (Bitcoin)” ซึ่งถือเป็นเงินสกุลเข้ารหัส (Cryptocurrency) สกุลแรกของโลก (Nakamoto, 2008) และเนื่องด้วยคุณลักษณะเฉพาะที่สำคัญของเงินสกุลเข้ารหัสคือ ผู้ใช้งานไม่ต้องเปิดเผยตัวตน การโอนมูลค่าสามารถดำเนินการข้ามประเทศแบบไร้พรมแดนด้วยความรวดเร็วไร้หน่วยงานตัวกลางในการกำกับ ด้วยต้นทุนดำเนินงานต่ำ จึงเป็นคุณลักษณะที่ท้าท้ายสถาบันการเงินและระบบการเงินโลกอย่างมาก (FATF, 2019) อีกทั้งกลุ่มอาชญากรทางเศรษฐกิจให้ความสนใจนำเงินสกุลเข้ารหัสไปใช้เป็นเครื่องมือในการโอนผลประโยชน์ระหว่างประเทศ เพื่อส่งต่อผลตอบแทนจากการกระทำผิดกฎหมาย เช่น การค้ายาเสพติด การค้าสิ่งผิดกฎหมายในระบบออนไลน์ การเรียกค่าไถ่ การคอรัปชั่น รวมถึงการฟอกเงิน ส่งผลให้ราคาของบิตคอยน์แรกเริ่มในปี 2009 มีมูลค่า 1 บิตคอยน์ต่ำกว่า 1 เซนต์ ได้ปรับตัวจนมีมูลค่าสูงขึ้นเป็นประมาณ 20,000 เหรียญสหรัฐต่อ 1 บิตคอยน์ ในปี 2017 ก่อนที่มูลค่าจะลดลงอย่างต่อเนื่องหลังจากกลุ่มอาชญากรรมค้าสิ่งผิดกฎหมายทางระบบออนไลน์ (Dark Web) รายใหญ่ถูกกวาดล้างจับกุม ทำให้ราคาบิตคอยน์ลดลงมาเคลื่อนไหวอยู่ในระดับ 5,000 – 7,000 เหรียญสหรัฐต่อ 1 ต่อบิตคอยน์ สอดคล้องกับเหตุการณ์จับกุมและสั่งปิด Silk Road กลุ่มค้าสิ่งผิดกฎหมายทางออนไลน์ในปี 2013 และอีกเหตุการณ์หนึ่งคือ AlphaBay กลุ่มค้าสิ่งผิดกฎหมายทางออนไลน์อีกรายซึ่งถูกจับกุมและสั่งปิดในปี 2017 เช่นกัน (Fanusie & Robinson, 2018)

นอกจากนี้ ในปี 2013 กระทรวงยุติธรรมของสหรัฐอเมริกาได้ดำเนินคดีฟอกเงินกับธุรกิจบริการแลกเปลี่ยนเงินรายใหญ่ “Liberty Reserve” ที่ให้บริการแลกเปลี่ยนเงินตราและการโอนเงินอิเล็กทรอนิกส์ระหว่างประเทศ เข้าข่ายการฟอกเงินอย่างผิดกฎหมายด้วยเงินสกุลเข้ารหัสที่ชื่อ “Liberty Dollars หรือ LD” โดยมีจำนวนผู้ใช้บริการในเครือข่ายทั่วโลกหลายล้านราย โดยเฉพาะในประเทศสหรัฐอเมริกามีผู้ใช้บริการจำนวนมากกว่า 2 แสนราย ด้วยจำนวนธุรกรรมรายการโอนเงินผิดกฎหมายประมาณ 55 ล้านรายการ และเป็นการสนับสนุนการฟอกเงินไม่น้อยกว่า 6 พันล้านเหรียญสหรัฐ (Dyntu & Dykyi, 2019) ในขณะที่นายรอป เวียนไรท์ (Rob Wainwright) ผู้อำนวยการยูโรพอล ได้รายงานว่ามีปริมาณเงินของผู้กระทำผิดกฎหมายในยุโรปจำนวนมากประมาณ 3 ถึง 4 พันล้านปอนด์ที่ทำการฟอกเงินโดยเงินสกุลเข้ารหัส (Kepli & Zulhuda, 2019)

สำหรับกรณีอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและการฟอกเงินในประเทศไทยมีปรากฏไม่มากนัก แต่เมื่อเกิดเหตุขึ้นมักจะมีมูลค่าความเสียหายสูง เช่น กรณีการหลอกนักลงทุนชาวฟินแลนด์ ซึ่งประกอบธุรกิจซื้อขายแลกเปลี่ยนเงินสกุลเข้ารหัส ได้รับการชักชวนให้เข้าลงทุนในประเทศไทยจากผู้บริหารบริษัทหลักทรัพย์แห่งหนึ่งร่วมกับนักธุรกิจและพวกซึ่งมีความสัมพันธ์กับนักแสดงรายหนึ่งเพื่อการสร้างความน่าเชื่อถือให้แก่เหยื่อ ตั้งแต่กลางปี 2018 ด้วยข้อเสนอการลงทุนในบริษัท Expay Group เพื่อเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ในนาม Dragon Coin ด้วยการสร้างความคาดหวังในการเพิ่มมูลค่าเงินลงทุนจำนวนมหาศาล จากนั้นกลุ่มผู้กระทำผิดกลับฉ้อโกงเหยื่อด้วยการนำเงินที่ได้รับเหยื่อจำนวนประมาณ 800 ล้านบาทไปกระจายให้แก่เครือญาติและบุคคลใกล้ชิดในลักษณะของการฟอกเงิน (ข่าวการเงิน, 2561) และอีกกรณีตัวอย่างคือ การหลอกลวงในปี 2019 ด้วยการโฆษณาในเว็บไซต์ Cryptominingfarm ซึ่งเป็นบริษัทผู้ให้เช่าเครื่องมือในการขุดบิตคอยน์ โดยเสนอการลงทุนต่อผู้สนใจเพื่อเข้าเชื่อมต่อระบบนิเวศเงินสกุลเข้ารหัสและทำหน้าที่ยืนยันธุรกรรมบิตคอยน์ โดยได้รับค่าตอบแทนเป็นบิตคอยน์ แต่ผู้กระทำผิดได้นำเงินที่ได้รับจากผู้ลงทุนไปแลกเปลี่ยนเป็นบิตคอยน์และนำไปกระจายส่งมอบเป็นค่าตอบแทนให้แก่นักลงทุนในช่วงแรก เพื่อสร้างแรงจูงใจให้เหยื่อขยายการลงทุนและสามารถขยายฐานจำนวนนักลงทุน จนในที่สุดเวปไซต์นี้ได้ปิดตัวลงโดยสร้างความเสียหายให้แก่นักลงทุนที่หลงเชื่อการหลอกลวงจำนวนรวมสูงถึงประมาณ 500 ล้านบาท (ข่าวอาชญากรรม, 2562)

อีกทั้งในปัจจุบัน แต่ละประเทศมีบทบัญญัติทางกฎหมายที่ใช้บังคับต่อการดำเนินธุรกรรมเงินสกุลเข้ารหัสที่แตกต่างกันอย่างเห็นได้ชัด กล่าวคือ บางประเทศไม่ให้การยอมรับเงินสกุลเข้ารหัสและถือว่าธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสเป็นสิ่งต้องห้ามและผิดกฎหมาย ในขณะที่บางประเทศยอมรับเงินสกุลเข้ารหัสเป็นสิ่งถูกต้องตามกฎหมายและส่งเสริมการดำเนินงานของธุรกิจที่เกี่ยวข้อง จึงเกิดเป็นช่องโอกาสทางกฎหมายที่ส่งผลให้อาชญากรอาจเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการถ่ายโอนผลประโยชน์มากขึ้น

ทฤษฎีทางอาชญาวิทยากับการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

เงินสกุลเข้ารหัสมีคุณลักษณะเฉพาะหลายประการที่เป็นปัจจัยที่อาจส่งผลต่อการเลือกใช้เครื่องมือในการฟอกเงินของอาชญากร โดยวิเคราะห์การก่ออาชญากรรมด้วยทฤษฎีปกตินิสัย (Routine Activity Theory) จะเกิดขึ้นได้เมื่อสถานการณ์ครบ 3 องค์ประกอบ กล่าวคือ อาชญากรซึ่งเป็นองค์ประกอบแรกมีแรงจูงใจที่มากพอให้เลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน เนื่องด้วยได้ประเมินโอกาสการฟอกเงินน่าจะประสบความสำเร็จมากกว่าความเสี่ยงที่อาจเกิดการถูกอายัดจับกุม ตามแนวคิดของทฤษฎีการเลือกกระทำอย่างมีเหตุผล (Rational Choice Theory) และเนื่องจากพื้นฐานทางเทคโนโลยีของระบบนิเวศเงินสกุลเข้ารหัสมีความโน้มเอียงที่จะสามารถหลีกเลี่ยงหรือหลุดพ้นการติดตามอายัดจับกุมได้ ในขณะที่มาตรการทางกฎหมายในการกำกับ ป้องกัน ปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสของหลายประเทศในปัจจุบันยังมีความแตกต่างกัน ตั้งแต่ประเทศที่มีกฎระเบียบในการกำกับอย่างเคร่งครัด ประเทศที่มีมาตรการไม่เคร่งครัด จนถึงขั้นประเทศที่ไม่มีมาตรการใดกำกับ จึงถือว่าเป็นการขาดประสิทธิภาพการพิทักษ์ปกป้องอันเป็นองค์ประกอบที่สอง อีกทั้งศักยภาพของเงินสกุลเข้ารหัสที่สามารถโอนมูลค่าอย่างโลกภิวัตน์ ดังนั้นความอ่อนแอในการกำกับธุรกรรมเงินสกุลเข้ารหัส ณ ประเทศใดเพียงแหล่งเดียวก็ถือเป็นการขาดประสิทธิภาพการกำกับของบริบทโดยรวม เนื่องจากเป็นช่องโอกาสที่อาชญากรอาจเลือกใช้พื้นที่นั้นเป็นแหล่งในการฟอกเงินได้โดยง่าย และองค์ประกอบประการสุดท้ายคือเหยื่อ หรือในที่นี้หมายถึงรัฐและผลประโยชน์แห่งรัฐ หากรัฐไม่สามารถดำเนินนโยบายหรือกำหนดมาตรการป้องกันและปราบปรามการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสอย่างมีประสิทธิภาพเพียงพอก็อาจส่งผลร้ายต่อรัฐและประโยชน์สาธารณะแห่งรัฐ จากการขาดศักยภาพในการทำลายแหล่งผลประโยชน์ของอาชญากรและการตัดวงจรการประกอบอาชญากรรมลงได้

ในขณะที่รูปแบบอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและใช้เพื่อการฟอกเงินเข้าข่ายเป็นอาชญากรรมทางเศรษฐกิจ ดังนั้น เมื่อนำแนวคิดอาชญากรรมคอปกขาว (White Collar Crime) ของ เอ็ดวิน เฮช ซัตเธอร์แลนด์ (Edwin H. Sutherland, 1961) มาวิเคราะห์ จะเห็นได้ว่าอาชญากรรมข้างต้นมักมีผู้กระทำผิดเป็นบุคคลที่มีฐานะทางเศรษฐกิจมั่งคั่ง หรือมีความสัมพันธ์เชิงอำนาจกับผู้มีอิทธิพลโดยตำแหน่งหน้าที่การงานในการสนับสนุนการกระทำผิด (Siegel, 2013) อีกทั้งการกระทำความผิดมักเป็นความร่วมมือกันของกลุ่มบุคคลหรือกลุ่มองค์กรจากหลายประเทศ เพื่อร่วมกันจัดเตรียมวางแผนการก่ออาชญากรรม และนำไปปฏิบัติการก่อเหตุกระทำความผิดต่างเขตประเทศ ซึ่งมีโครงสร้างการดำเนินงานซับซ้อน สร้างความยากต่อการสืบสวนจับกุม เข้าลักษณะเป็นอาชญากรรมองค์กรข้ามชาติ รวมถึงการกระทำต่อระบบปฏิบัติการและอุปกรณ์เครื่องคอมพิวเตอร์เป้าหมายที่เป็นแหล่งผลประโยชน์ขององค์กรเอกชน หรือภาครัฐนั้น เข้าลักษณะเป็นอาชญากรรมทางไซเบอร์ ซึ่งสร้างผลกระทบให้เกิดความเสียหายทางเศรษฐกิจในวงกว้าง ในขณะที่ผู้กระทำผิดได้รับผลประโยชน์จำนวนมหาศาล อีกทั้งได้ใช้

ความพยายามในการฟอกเงิน เพื่อนำไปเป็นแหล่งเงินทุนสนับสนุนการกระทำผิดต่อไป เป็นวงจรการก่ออาชญากรรมอย่างต่อเนื่องไม่รู้จบ

นอกจากนี้เมื่อนำทฤษฎีป้องกันอาชญากรรม (Crime Prevention Theory) ประกอบการศึกษาแนวทางการป้องกันการฟอกเงินโดยเงินสกุลเข้ารหัสที่เหมาะสม อาศัยหลักการสำคัญ คือ การป้องปรามเพื่อลดโอกาสการก่อเหตุกระทำผิดได้สำเร็จอย่างมีประสิทธิภาพมากขึ้นเท่าไร ก็จะส่งผลในทิศทางให้การเกิดอาชญากรรมลดลงยิ่งขึ้นเช่นเดียวกัน (Lilly, Cullen, & Ball, 2015) และหลักการลดทอนประโยชน์ที่พึงได้รับจากการกระทำผิด หรือก่อภาระเพิ่มแก่ต้นทุนการสูญเสียจากการก่อเหตุ ทั้งนี้ไม่จำกัดเฉพาะโอกาสที่พึงได้รับประโยชน์หรือภาระการสูญเสียทางเศรษฐกิจ แต่ยังหมายรวมถึงโอกาสการสร้างสะสมประสบการณ์ และการเรียนรู้กระบวนการกระทำผิด รวมถึงการพัฒนาองค์ความรู้เทคนิคการก่อเหตุอาชญากรรมอย่างเป็นระเบียบแบบแผน (Siegel, 2013) ซึ่งเป็นกรอบแนวคิดในการป้องกันอาชญากรรม ดังนี้ คือ การเพิ่มภาระความยากลำบากแก่ผู้กระทำผิด การเพิ่มความเสี่ยงต่อการถูกตรวจพบจับกุม การลดผลประโยชน์ตอบแทนที่ได้รับ การสร้างสำนึกต่อการกระทำผิด และการลดเหตุข้ออ้างที่จะใช้แก้ตัว (Lilly et al., 2015; Siegel, 2013)

รูปแบบอาชญากรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสและใช้การฟอกเงินโดยเงินสกุลเข้ารหัส

จากการศึกษา พบว่า การก่ออาชญากรรมที่มีโอกาสเกิดขึ้นในรูปแบบที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือ และดำเนินการฟอกผลประโยชน์ที่ได้รับจากการกระทำผิดโดยเงินสกุลเข้ารหัสนั้น ส่วนใหญ่เป็นรูปแบบอาชญากรรมที่มีแนวโน้มในทิศทางเดียวกับสถิติอาชญากรรมทางคดีการจับกุมยึดอายัดทรัพย์สินจากการกระทำความผิดมูลฐาน ของกฎหมายป้องกันและปราบปรามการฟอกเงิน (สำนักงานป้องกันและปราบปรามการฟอกเงิน, 2562) จัดลำดับตามความสำคัญ ดังนี้

1. การหลอกลวงประชาชนแบบแชร์ลูกโซ่ เนื่องจากเงินสกุลเข้ารหัสเป็นนวัตกรรมเทคโนโลยีทางการเงินที่เป็นองค์ความรู้ใหม่ บุคคลที่รู้และเข้าใจกลไกการทำงาน คุณลักษณะ ความเสี่ยง และการประยุกต์ใช้งานอย่างเหมาะสมยังมีจำนวนอยู่ในวงจำกัด แต่ความรู้ที่เผยแพร่ต่อสาธารณะซึ่งประชาชนส่วนใหญ่ได้รับรู้ คือ การลงทุนที่มีแนวโน้มให้อัตราผลตอบแทนสูงอย่างต่อเนื่อง จึงเป็นสิ่งจูงใจสำคัญต่ออาชญากรในการใช้เป็นกิจการบังหน้าเพื่อการหลอกลวงให้ร่วมลงทุน โดยนำเงินลงทุนจากเหยื่อรายใหม่ไปหมุนเวียนให้ผลตอบแทนแก่เหยื่อรายเดิม อาชญากรรมแชร์ลูกโซ่ลักษณะนี้มักสร้างเงินทุนหมุนเวียนจำนวนมาก และได้รับผลประโยชน์ในรูปของเงินสกุลเข้ารหัสอยู่แล้ว จึงสามารถฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสในระหว่างกิจการบังหน้ายังดำเนินอยู่ได้ด้วยความรวดเร็ว

2. การค้ายาเสพติด มักเป็นการกระทำความผิดลักษณะอาชญากรรมองค์กรหรืออาชญากรรมองค์กรข้ามชาติที่มีแหล่งเงินทุนสนับสนุนการดำเนินงาน และมีเครือข่ายบุคลากรในหลายระดับ รวมถึงบุคลากร

ที่มีความเชี่ยวชาญด้านการเงินและเทคโนโลยีในการดูแลจัดการผลประโยชน์ ทั้งนี้เงินสกุลเข้ารหัสจึงไม่ถือเป็นสิ่งใหม่ของกระบวนการค้ายาเสพติดข้ามชาติ ที่ค้ายาเสพติดทางระบบออนไลน์ (Dark Web) เช่น Silk Road และ AlphaBay ที่ถูกจับกุมและสั่งปิดไป แต่อาชญากรก็ได้พัฒนาผู้ค้ายาเสพติดทางระบบออนไลน์รายใหม่ได้แก่ Hydra ซึ่งเป็นกิจการขนาดใหญ่ตั้งอยู่ในประเทศรัสเซีย (Chainalysis, 2021) นอกจากนี้ยังมีการประยุกต์ใช้ระบบ Smart Contract ของเงินสกุลเข้ารหัสเป็นเครื่องมือในการค้ายาเสพติดโดยการจัดส่งทางไปรษณีย์ ด้วยการตั้งเงื่อนไขในการโอนชำระค่าซื้อขายยาเสพติดกันโดยอัตโนมัติเมื่อรหัส URL บนพัสดุไปรษณีย์แสดงสถานะว่าปลายทางได้รับแล้ว

3. การเรียกค่าไถ่ด้วยการส่งไวรัสคอมพิวเตอร์นั้น ผู้กระทำความผิดจะทำการส่งชุดคำสั่งจากระบบงานที่ตั้งอยู่ในต่างประเทศเข้าสู่ระบบงานเป้าหมายโดยมุ่งหวังที่เข้าทำลายระบบปฏิบัติการหรือระบบจัดการฐานข้อมูล โดยการตั้งเงื่อนไขการทำงานผ่านการเปิดจดหมายอิเล็กทรอนิกส์ การเปิดเว็บไซต์หรือการตั้งค่าเวลาล่วงหน้า เพื่อเป็นการข่มขู่ระบบงานเป้าหมาย ด้วยปฏิบัติการก่อกวนระบบงานให้เกิดความขัดข้อง ประมวลผลข้อมูลผิดพลาด หรือทำลายฐานข้อมูลให้เสียหาย และเรียกร้องผลประโยชน์เป็นค่าไถ่เพื่อแลกกับการถอนชุดคำสั่งที่เข้าก่อกวนระบบงานให้กลับสู่สภาพเดิม หรือให้เกิดความเสียหายน้อยที่สุด โดยระบบนิเวศเงินสกุลเข้ารหัสสามารถช่วยสนับสนุนการโอนค่าไถ่โดยตรงไปยังกระเป๋าเงินที่ไม่ต้องระบุตัวตน ทั้งนี้ได้ปรากฏกรณีการเรียกค่าไถ่ในประเทศไทยเมื่อปี 2020 ด้วยมูลค่า 20,000 บิตคอยน์ (ราว 6.3 หมื่นล้านบาทในขณะนั้น) จากการส่งไวรัสคอมพิวเตอร์เข้าระบบปฏิบัติการคอมพิวเตอร์ของโรงพยาบาลสระบุรี เพื่อเข้าปิดระบบฐานข้อมูล ทำให้ทั้งโรงพยาบาลไม่สามารถเข้าใช้งานและให้บริการแก่คนไข้ได้ (The Reporter Asia Online, 2020)

4. การพนัน เป็นลักษณะความผิดที่กฎหมายบัญญัติให้การจัดให้มีการพนันเสี่ยงโชคเป็นการกระทำที่ผิดกฎหมาย ซึ่งบ่อนการพนันเป็นอีกแหล่งสำคัญที่เอื้ออำนวยต่อกระบวนการฟอกเงิน เนื่องจากความยากต่อการพิสูจน์เส้นทางการเงินที่ผู้เล่นพนันได้รับรางวัลชนะพนัน หรือสูญเสียจากการเสี่ยงโชคพนันอันเป็นการหลีกเลี่ยงความเชื่อมโยงของแหล่งเงินที่ไม่ชอบด้วยกฎหมาย และปัจจุบันการพนันได้พัฒนาสู่ระบบออนไลน์ทำให้สามารถขยายฐานผู้เข้าร่วมกิจกรรมได้ง่ายและกว้างขึ้น รวมถึงไม่มีข้อจำกัดด้านเวลาและสถานที่ในการเข้าร่วมกิจกรรม นอกจากนี้การใช้เงินสกุลเข้ารหัสเป็นสื่อกลางในการชำระหนี้พนันออนไลน์ ส่งผลให้ผู้กระทำผิดไม่ต้องแปลงค่าเป็นเงินตราสกุลท้องถิ่นของแต่ละประเทศ และสามารถถ่ายเทผลประโยชน์ในรูปแบบเงินสกุลเข้ารหัสบนระบบออนไลน์ได้ทุกขณะ

กล่าวโดยสรุป รูปแบบอาชญากรรมข้างต้นเข้าข่ายเป็นอาชญากรรมทางเศรษฐกิจ อาชญากรรมไซเบอร์ และส่วนใหญ่มีแนวโน้มการกระทำความผิดในลักษณะร่วมกันเป็นกลุ่มบุคคล หรือองค์กรทั้งภายในประเทศและต่างประเทศ โดยอาศัยเครือข่ายในหลายประเทศ เพื่อการโอนย้ายถ่ายเทผลประโยชน์ข้ามประเทศภายในเครือข่ายได้อย่างรวดเร็วอันมีลักษณะเป็นอาชญากรรมองค์กรข้ามชาติ

อีกทั้งอาชญากรรมดังกล่าวมักก่อให้เกิดความเสียหายทางเศรษฐกิจแก่เหยื่อจำนวนมากรายในวงกว้าง มีขนาดของผลประโยชน์ที่ได้รับจากการกระทำผิดมูลค่าสูงในระยะเวลาสั้น โดยมีข้อจำกัดด้านเวลาจำเป็นต้องกระจายผลประโยชน์และทำการฟอกเงินเป็นเงินที่ชอบด้วยกฎหมายในระยะสั้นให้เร็วที่สุด

การใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน

1. บริบทกลไกการทำงานของธุรกรรมเงินสกุลเข้ารหัส

กลไกการทำงานของเงินสกุลเข้ารหัสส่วนใหญ่มีคุณลักษณะเฉพาะทางเทคโนโลยีบนพื้นฐานเดียวกัน แต่อาจมีลักษณะเงื่อนไขเฉพาะบางประการของแต่ละสกุลที่แตกต่างกัน ดังเช่น บิตคอยน์ (Bitcoin) ซึ่งเป็นเงินสกุลเข้ารหัสสกุลแรกของโลก ได้เสนอกลไกการทำงานของระบบนิเวศด้วยการโอนเงินทางรหัสข้อมูลอิเล็กทรอนิกส์โดยตรงระหว่างผู้ใช้งาน (Peer-to-Peer หรือ P2P) แบบไร้การควบคุมจากหน่วยงานใด และระบบได้เปิดกว้างต่อผู้ใช้งานให้สามารถติดต่อเข้าสู่ระบบได้อย่างไม่มีเงื่อนไขโดยไม่จำเป็นต้องลงทะเบียนอัตลักษณ์ตัวตนแท้จริงของผู้ใช้งานก่อนเข้าสู่ระบบ (Girasa, 2018) ทั้งนี้ธุรกรรมการโอนมูลค่าเงินสกุลเข้ารหัสจะถูกบันทึกเป็นรหัสข้อมูล (Cryptographic) ในลักษณะคล้ายสมุดบัญชีเรียงลำดับข้อมูลเป็นชุด (Block) ซึ่งแต่ละชุดข้อมูลจะมีรหัสความสัมพันธ์กับชุดข้อมูลในลำดับถัดไปอย่างต่อเนื่องคล้ายห่วงโซ่ (Chain) หรือที่เรียกว่า Blockchain พร้อมทั้งส่งรหัสเปิดสาธารณะ (Public Key) ซึ่งกำกับชุดข้อมูลที่ถูกบันทึกไว้นั้นไปยังรหัสที่ตั้ง (IP Address) ปลายทาง โดยผู้รับโอนปลายทางจะใช้รหัสเปิดส่วนบุคคล (Private Key) เสมือนเป็นลายมือดิจิทัลของเจ้าของบัญชี ร่วมกับรหัสเปิดสาธารณะในการเปิดรายการข้อมูลที่ถูกจัดส่งมา และด้วยกลไกการทำงานในรูปแบบกระจายศูนย์ (Distributed) ผู้ใช้งานทุกคนจึงสามารถเข้าถึงฐานข้อมูลสาธารณะที่ถูกบันทึกในสมุดบัญชีอิเล็กทรอนิกส์ของระบบนิเวศเงินสกุลเข้ารหัสได้อย่างไม่มีข้อจำกัด สามารถติดตามความเคลื่อนไหวของเส้นทางธุรกรรมระหว่างผู้ใช้งานต่างๆ ได้ หรือที่เรียกระบบบันทึกบัญชีนี้ว่า Distributed Ledger Technology – DLT (Burniske & Tara, 2017)

นอกจากนี้ระบบการตรวจพิสูจน์ยืนยันรายการ (Proof of Work – PoW) ถือเป็นหัวใจสำคัญของกลไกในการสร้างความน่าเชื่อถือต่อระบบการโอนมูลค่าเงินสกุลเข้ารหัสระหว่างผู้โอนและผู้รับโอนที่อาจไม่มีประวัติความสัมพันธ์ต่อกัน และเป็นการโอนมูลค่าข้ามเขตประเทศซึ่งไม่มีหน่วยงานกลางใดเข้ามารับรอง (Nakamoto, 2008) โดยระบบมีกลไกสร้างแรงจูงใจให้ผู้ใช้งานที่กระจายอยู่ทั่วไปเข้าสู่ระบบแข่งขันเป็นผู้ตรวจพิสูจน์ ที่เรียกว่า นักขุด (Miner) ในการแก้โจทย์รหัสทางคณิตศาสตร์ประจำชุดข้อมูลก่อนการยืนยันด้วยฉันทามติของผู้ร่วมดำเนินการ ซึ่งนักขุดจะได้รับค่าตอบแทนเป็นเงินสกุลเข้ารหัสที่ถูกกำหนดไว้ล่วงหน้า (Burniske & Tara, 2017) อย่างไรก็ตาม ระบบการตรวจพิสูจน์ยืนยันรายการได้ถูกพัฒนาขึ้นอีกหลายวิธีการสำหรับเงินสกุลเข้ารหัสอื่นที่เกิดขึ้นในภายหลัง ดังเช่นระบบ Proof-of-Stake

หรือ PoS ที่ได้รับการยอมรับอันดับรองลงมาจาก PoW โดยวิธีการพิสูจน์ยืนยันรายการจะใช้ฉันทามติของผู้ร่วมดำเนินการตามสัดส่วนได้เสียจากการถือครองเงินสกุลเข้ารหัสนั้น (Girasa, 2018) ดังนั้นชุดข้อมูลเมื่อได้รับการพิสูจน์ยืนยันแล้ว จะไม่สามารถแก้ไขเปลี่ยนแปลงได้ (Immutable) เนื่องจากรหัสที่ได้รับการพิสูจน์ในส่วนท้ายของชุดข้อมูลจะมีความสัมพันธ์ทางคณิตศาสตร์กับรหัสส่วนต้นของชุดข้อมูลถัดไป จึงเป็นการให้ความเชื่อมั่นแก่ผู้ใช้งานได้ อีกทั้งเงินสกุลเข้ารหัสจะดำเนินการบนบล็อกเชนเทคโนโลยี (Blockchain) ซึ่งเป็นระบบงานแบบเปิด (Open Source) ซึ่งนักพัฒนาระบบงานสามารถเข้าถึง และนำไปพัฒนาโปรแกรมประยุกต์ที่เชื่อมต่อเข้ากับบล็อกเชนเทคโนโลยีต่อไปได้ (Burniske & Tara, 2017) ต่อมาในปี ค.ศ. 2014 Vitalik Buterin นักพัฒนาระบบได้นำเสนอเงินสกุลเข้ารหัสใหม่ที่สามารถสร้างชุดคำสั่งร่วมในการทำธุรกรรมภายใต้ตรรกะอย่างมีเงื่อนไข (Smart Contract) บนบล็อกเชนเทคโนโลยีเช่นกัน ในนาม อีเทอเรียม หรือ อีเทอ (Ethereum or Ether) (Girasa, 2018)

2. กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

กระบวนการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัสมีขั้นตอนการดำเนินงานทำนองเดียวกับการฟอกเงินทั่วไป เพียงแต่เป็นทรัพย์สินลักษณะไร้รูปร่างที่เป็นรหัสข้อมูลอิเล็กทรอนิกส์ในบล็อกเชนเทคโนโลยี โดยขั้นตอนแรกผู้กระทำผิดจะโอนผลประโยชน์ในรูปเงินสกุลเข้ารหัสที่ได้จากการกระทำผิดกฎหมาย หรือในรูปเงินตราทั่วไปที่ได้แลกเปลี่ยนเป็นเงินสกุลเข้ารหัส เข้าสู่ระบบนิเวศเงินสกุลเข้ารหัส โดยอาจจะโอนจากผู้โอนต้นทางที่ไม่ระบุตัวตนหรือระบุตัวตนผู้ใช้งาน ถือเป็นการนำเงินสกปรกเข้าสู่ระบบ (Placement Stage) (Jacquez, 2016) แต่ด้วยระบบฐานข้อมูลสาธารณะของเงินสกุลเข้ารหัส ส่งผลให้ผู้ใช้งานทั่วไปสามารถเข้าถึง และสืบค้นติดตามเส้นทางธุรกรรมระหว่างผู้ใช้งานบนบล็อกเชนเทคโนโลยีได้ และหากผู้กระทำผิดโอนไปยังบุคคลอื่นต่อไป ก็จะถูกบันทึกรายการในระบบฐานข้อมูลสาธารณะ ซึ่งสามารถติดตามเส้นทางธุรกรรมจากรหัสที่ตั้งประจำเครื่องมือสื่อสารหรืออุปกรณ์คอมพิวเตอร์ของผู้ใช้งานได้อย่างต่อเนื่อง

ขั้นตอนต่อไป ผู้กระทำผิดจะดำเนินการกลบเกลื่อนร่องรอย (Layering) โดยมีเป้าหมายที่จะไม่ให้ผู้ใดสามารถติดตามเชื่อมโยงเส้นทางธุรกรรมเงินสกุลเข้ารหัสที่ไม่ชอบด้วยกฎหมายกับเงินสกุลเข้ารหัสที่ได้รับปลายทางได้ เช่น การโอนเงินสกุลเข้ารหัสจากกระเป๋าเงินอิเล็กทรอนิกส์ที่ไม่ระบุตัวตน พร้อมทั้งแลกเปลี่ยนกระจายเป็นเงินสกุลเข้ารหัสอื่นหลายสกุลเพื่อโอนเข้าหลายกระเป๋าเงิน และการโอนไขว้กันไปมาหลายรอบ เนื่องจากสามารถดำเนินการได้อย่างรวดเร็ว รวมถึงการกระจายข้ามหลายประเทศ เพื่อให้เกิดความซับซ้อนยากต่อการติดตาม (Jacquez, 2016) หรือโอนเงินสกุลเข้ารหัสดังกล่าวผ่านศูนย์บริการแปรสภาพเงินสกุลเข้ารหัส (Cryptocurrency Mixer or Tumbler) ซึ่งจะให้บริการรับแลกเปลี่ยนเป็นเงินตราปกติและเงินสกุลเข้ารหัสทั้งผู้ใช้บริการทั่วไปและผู้กระทำผิด เพื่อปนเงินสกุล

เข้ารหัสเข้าด้วยกัน พร้อมกับทยอยส่งมอบให้ในหลายช่วงเวลา และกระจายธุรกรรมไปหลายกระเป๋าเงิน จนกระทั่งถึงผู้รับโอนปลายทางตามคำสั่งของผู้กระทำผิด ซึ่งผู้รับปลายทางจะได้รับเป็นเงินสกุลเข้ารหัสที่สามารถระบุตัวตนผู้โอนที่ชอบด้วยกฎหมาย และไม่สามารถเชื่อมโยงเส้นทางธุรกรรมย้อนกลับไปถึงผู้โอนต้นทางได้ (Jacquez, 2016; Samanta, Mohanta, Pati, & Jena, 2019) นอกจากนี้ ผู้กระทำผิดส่วนหนึ่งอาจเลือกใช้ระบบปฏิบัติการเฉพาะเพื่อปิดบังตัวตนเพิ่มขึ้นอีกชั้นหนึ่ง ที่เรียกว่าระบบปฏิบัติการ The Onion Router (TOR) ซึ่งเป็นระบบที่พัฒนาขึ้นเพื่อการป้องกันการเข้าถึงข้อมูลใช้งานส่วนบุคคล หรือการตรวจสอบสืบค้นรหัสที่ตั้งของผู้ใช้งาน โดยในขณะใช้งาน ระบบจะหมุนเวียนเคลื่อนย้ายรหัสที่ตั้งในแต่ละช่วงเวลาไปอย่างต่อเนื่อง อีกทั้งรหัสที่ตั้งนั้นก็อาจเป็นรหัสที่ตั้งลวงโดยระบบสร้างขึ้น พร้อมสร้างเส้นทางการเคลื่อนย้ายรหัสที่ตั้งลวงที่ไม่มีผู้ใดทราบข้อมูลที่ชัดเจน และเมื่อเสร็จสิ้นการใช้งาน รหัสที่ตั้งจะเคลื่อนกลับไปยังรหัสที่ตั้งต้นทาง ทำให้หน่วยงานตรวจสอบไม่สามารถสืบค้นประวัติการใช้งานเว็บไซต์ของผู้ใช้งานได้ (Homeland Security Enterprise, 2014)

จากนั้น ขั้นตอนสุดท้ายผู้กระทำผิดก็สามารถนำเงินสกุลเข้ารหัสที่สามารถระบุแหล่งที่มาได้ชัดเจนไปผ่านกระบวนการใช้ประโยชน์หมุนเวียนธุรกรรมในระบบนิเวศเงินสกุลเข้ารหัส หรือการเก็บรักษาไว้ในกระเป๋าเงินประเภท Cold Wallet ซึ่งไม่ได้เชื่อมต่อกับระบบอินเทอร์เน็ต เช่น USB Drive หรือซื้อทรัพย์สินอื่นด้วยเงินสกุลเข้ารหัสโดยตรง หรือแลกเปลี่ยนเป็นเงินตราที่ชอบด้วยกฎหมายผ่านระบบเครือข่ายที่เชื่อมต่อกับระบบสถาบันการเงิน ซึ่งเรียกขั้นตอนนี้ว่า “Cash Out Strategy” เช่น การใช้ศูนย์บริการแลกเปลี่ยนเงินสกุลเข้ารหัส (Cryptocurrency Exchangers) ที่ให้บริการแลกเปลี่ยนเป็นเงินสกุลเข้ารหัสอื่น หรือเงินตราทั่วไป รวมถึงการใช้บริการกับศูนย์บริการโอนเงิน Paypal ซึ่งไม่ต้องระบุตัวตนของผู้โอนเป็นต้น (Choo, 2015)

3. มาตรการทางกฎหมายของนานาชาติที่มีต่อเงินสกุลเข้ารหัส

ในปี 2018 The Law Library of Congress (2018) ได้เสนอผลสำรวจมาตรการทางกฎหมายที่เกี่ยวกับการกำกับดูแลเงินสกุลเข้ารหัสทั่วโลกจำนวน 130 ประเทศ เนื่องจากเงินสกุลเข้ารหัสมีอัตราเติบโตในมูลค่าทางเศรษฐกิจอย่างรวดเร็ว และการให้ความหมายของแต่ละประเทศแตกต่างกันโดยยังไม่มีข้อสรุปอย่างเป็นสากล เช่น “Digital Currency” สำหรับประเทศอาร์เจนตินา ไทย และออสเตรเลีย หรือ “Virtual Commodity” สำหรับประเทศแคนาดา จีน และไต้หวัน หรือ “Crypto-Token” สำหรับประเทศเยอรมัน หรือ “Payment Token” สำหรับประเทศสวิตเซอร์แลนด์ หรือ “Cyber Currency” สำหรับประเทศอิตาลี หรือ “Electronic Currency” สำหรับประเทศกัมพูชา และเลบานอน หรือ “Virtual Assets” สำหรับประเทศฮอนดูรัส และเม็กซิโก เป็นต้น โดยแต่ละประเทศให้ความสำคัญต่อการสร้างความเข้าใจให้ประชาชนได้ทราบถึงความเสี่ยงของเงินสกุลเข้ารหัสที่ไม่มีหน่วยงานใดให้การคุ้มครองทางกฎหมาย

ผู้ใช้งานจะต้องรับความเสี่ยงภัยด้วยตนเอง รวมถึงการออกมาตรการกำกับดูแลป้องกันและปราบปรามการฟอกเงินโดยเงินสกุลเข้ารหัส และการออกมาตรการทางภาษีอากรดูแลผลประโยชน์ของประเทศจากผู้ทำธุรกรรมเงินสกุลเข้ารหัส นอกจากนี้ ยังรวมถึงมาตรการกำกับดูแลและกลั่นกรองการอนุญาตให้แก่บุคคลที่ประสงค์ทำธุรกิจเกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัส รวมถึงการระดมทุนด้วยการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ (Initial Coin Offering - ICO) โดยมีระดับการบังคับใช้กฎหมายที่แตกต่างกันตามบริบทของแต่ละประเทศ (The Law Library of Congress, 2018)

ทั้งนี้ แนวทางการออกมาตรการกำกับดูแลบริหารจัดการเงินสกุลเข้ารหัสตามบริบทของแต่ละประเทศสามารถจัดกลุ่มมาตรการทางกฎหมายตามลักษณะสภาพบังคับเชิงปฏิบัติได้ 3 กลุ่มประเทศ กล่าวคือ

1. กลุ่มแรก เป็นประเทศที่มีมาตรการทางกฎหมายรองรับสถานภาพเงินสกุลเข้ารหัส และยินยอมให้สามารถทำธุรกรรมที่เกี่ยวข้องกับเงินสกุลเข้ารหัสได้อย่างชอบด้วยกฎหมาย โดยประเทศญี่ปุ่นเป็นประเทศแรกที่ยอมรับสถานภาพทางกฎหมายของบิตคอยน์ในเดือนเมษายน 2017 จนกลายเป็นตลาดธุรกรรมเงินสกุลเข้ารหัสที่มีขนาดใหญ่ระดับโลกในปัจจุบัน และประเทศออสเตรียที่ให้การยอมรับบิตคอยน์ในปีเดียวกัน จากนั้นมีหลายประเทศได้ประกาศมาตรการทางกฎหมายให้การยอมรับเงินสกุลเข้ารหัสมากขึ้น เช่น ประเทศมอร์ต้าที่เป็นศูนย์กลางแลกเปลี่ยนเงินสกุลเข้ารหัสที่สำคัญของโลก และประเทศเยอรมัน บราซิล เป็นต้น (Kethineni & Cao, 2019)

2. กลุ่มที่สอง เป็นประเทศที่มีมาตรการต้องห้ามและไม่ยอมรับสถานภาพเงินสกุลเข้ารหัสถือเป็นสิ่งที่ไม่ชอบด้วยกฎหมาย ห้ามสถาบันการเงินดำเนินธุรกรรมใดๆที่เกี่ยวข้องรวมถึงการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ภายในขอบเขตประเทศของตน เช่น ประเทศแอลจิเรีย โบลีเวีย โมร็อกโก เนปาล ปากีสถาน และเวียดนาม เป็นต้น ส่วนประเทศการ์ตา และบาห์เรน จะยกเว้นไม่ห้ามสำหรับธุรกรรมเงินสกุลเข้ารหัสที่ดำเนินการในต่างประเทศ (The Law Library of Congress, 2018) รวมถึงประเทศที่มีเศรษฐกิจขนาดใหญ่ คือ ประเทศจีน เกาหลีใต้ และรัสเซีย เป็นต้น (Kethineni & Cao, 2019)

3. กลุ่มประเทศสุดท้าย เป็นประเทศที่มีมาตรการทางกฎหมายยอมรับสถานภาพเงินสกุลเข้ารหัส ในบางลักษณะ และอนุญาตให้ดำเนินธุรกรรมที่เกี่ยวข้องบางลักษณะภายใต้กรอบมาตรการกำกับดูแลที่เคร่งครัด รวมถึงการเสนอขายเงินสกุลเข้ารหัสสกุลใหม่ที่มีลักษณะเข้าข่ายหลักทรัพย์ หรือตราสารหนี้ เช่น นิวซีแลนด์ และเนเธอร์แลนด์ นอกจากนี้บางประเทศไม่ห้ามประชาชนในการถือครองเงินสกุลเข้ารหัส เพื่อการลงทุน แต่อาจจะมีข้อกำหนดในการกำกับการทำธุรกรรมของสถาบันการเงินที่เกี่ยวข้องกับเงินสกุลเข้ารหัส เช่น ประเทศบังกลาเทศ อิหร่าน ลิทัวเนีย กัมพูชา และไทย เป็นต้น (The Law Library of Congress, 2018)

---

4. ปัจจัยที่มีอิทธิพลต่อการเลือกใช้เงินสุกลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน

กล่าวโดยสรุป จากผลการศึกษาปรากฏว่าผู้เชี่ยวชาญมีความเห็นในทิศทางเดียวกับงานวิจัยต่างประเทศซึ่งแสดงถึงปัจจัยที่อาจเอื้อประโยชน์ต่อผู้กระทำผิดในการฟอกเงินโดยเงินสกุลเข้ารหัส (HouBen & Snyers, 2018) ดังนี้

1. กลไกการทำงานแบบกระจายศูนย์ไร้การควบคุมจากหน่วยงานใด โดยระบบนิเวศเงินสกุลเข้ารหัสเปิดกว้างต่อผู้ใช้งาน สามารถเข้าสู่ระบบและโอนมูลค่าให้แก่กันได้อย่างไม่มีเงื่อนไข ผู้ใช้งานไม่จำเป็นต้องแสดงตัวตนก่อนใช้งาน จึงเป็นการเปิดโอกาสให้แก่อาชญากรสามารถฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส โดยไม่อยู่ในกำกับของหน่วยงานใดที่จะรับรู้ตัวตนที่แท้จริงของผู้ใช้งาน

2. การอำพรางตัวตน และความยากต่อการสืบค้นเส้นทางธุรกรรม โดยผู้ใช้งานสามารถใช้นามแฝงและไม่ต้องระบุข้อมูลส่วนบุคคล ซึ่งเป็นปัจจัยทางธรรมชาติของระบบงานที่ป้องกันการตรวจสอบการเข้าถึงตัวตนของผู้ใช้งาน และการเข้าถึงรหัสเปิดส่วนบุคคลสำหรับการเปิดกระเป๋าเงิน อีกทั้งในกรณีที่อาชญากรดำเนินการบนระบบปฏิบัติการ TOR Browser เพื่อลวงรหัสที่ตั้งของผู้ใช้งานในขณะเข้าสู่ระบบ หรืออาจใช้บริการกับศูนย์บริการแปรสภาพเงินสกุลเข้ารหัส Crypto Mixer หรือ Tumbler ในการตัดความเชื่อมโยงเส้นทางธุรกรรมระหว่างต้นทางและปลายทาง ก็จะยิ่งเอื้อประโยชน์ต่อการใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน

3. ด้านความสะดวก รวดเร็ว และสามารถทำธุรกรรมข้ามประเทศแบบไร้พรมแดน เนื่องจากระบบนิเวศเงินสกุลเข้ารหัสเป็นการดำเนินการบนระบบอินเทอร์เน็ต ซึ่งปัจจุบันมีโครงข่ายการติดต่อสื่อสารเชื่อมโยงถึงกันทั้งในประเทศและระหว่างประเทศ จึงสามารถทำธุรกรรมการโอนมูลค่าจำนวนสูงในคราวเดียวโดยไร้ข้อจำกัดด้านขนาด มูลค่าและรายการ สามารถโอนย้ายข้ามประเทศได้อย่างเสรี รวดเร็วและไม่มีข้อจำกัดด้านเวลา ซึ่งมีความสะดวกรวดเร็วกว่าการฟอกเงินโดยเงินสด ที่อาจมีหลายขั้นตอนในการขนย้ายข้ามประเทศ และความเสี่ยงจากการโกงผลประโยชน์กันเอง

4. การรักษามูลค่าทรัพย์สินด้วยต้นทุนการดูแลต่ำ ทั้งนี้การทำธุรกรรมมีต้นทุนดำเนินการต่อรายการต่ำกว่ามาก ทำให้สามารถโอนย้ายไปมา สร้างความซับซ้อน และก่อให้เกิดภาระต่อการตรวจสอบสืบค้นของเจ้าหน้าที่ ทำให้ยากต่อการเข้าถึงธุรกรรมด้วยต้นทุนดำเนินการรวมไม่สูงมาก อีกทั้งในกรณีที่ต้องการแหล่งหลบซ่อนรักษาเงินสกุลเข้ารหัสในระบบนิเวศได้อย่างปลอดภัยและต้นทุนต่ำกว่าวิธีการอื่น ทั้งเงินสดที่ต้องมีตู้นิรภัย รถยนต์หรูที่ต้องมีโรงจอด สำหรับเงินสกุลเข้ารหัสสามารถจัดเก็บในกระเป๋าเงินประเภท Cold Wallet ซึ่งเป็นอุปกรณ์คอมพิวเตอร์ที่จัดเก็บข้อมูลและไม่เชื่อมต่อกับระบบอินเทอร์เน็ต เช่น USB Drive ซึ่งในปัจจุบันมีขนาดเล็กสามารถพกพาติดตัว เก็บซ่อนไว้ในพื้นที่เล็กขนาดเท่านิ้วหัวแม่มือเท่านั้น จึงมีโอกาสสูงที่จะรอดพ้นการตรวจสอบสืบค้นจากเจ้าหน้าที่หน่วยบังคับใช้กฎหมาย

5. ด้านมาตรการทางกฎหมายและการบังคับใช้เชิงปฏิบัติ ปัจจุบันแต่ละประเทศมีมาตรการภายในประเทศต่อเงินสกุลเข้ารหัสที่แตกต่างกัน ตั้งแต่ยอมรับสถานภาพทางกฎหมาย จนถึงขั้นต้องห้ามเป็นสิ่งผิดกฎหมาย จึงถือเป็นโอกาสของผู้ใช้งานที่จะอาศัยช่องว่างทางกฎหมายของแต่ละประเทศในการถ่ายโอนเพื่อการแปรสภาพเป็นเงินตราในประเทศที่ยอมรับสถานภาพทางกฎหมาย และหลีกเลี่ยงประเทศที่มีกฎหมายบังคับอย่างเข็มงวด

ทั้งนี้เมื่อวิเคราะห์โดยทฤษฎีการเลือกกระทำอย่างมีเหตุผล พบว่า คุณลักษณะเฉพาะและกลไกการทำงานของเงินสกุลเข้ารหัสสามารถทำธุรกรรมข้ามประเทศได้ด้วยความรวดเร็ว และปราศจากการควบคุมของหน่วยงานใด อีกทั้งมีระบบปฏิบัติการเฉพาะในการช่วยลดความเชื่อมโยงเส้นทางธุรกรรมระหว่างต้นทางและปลายทาง ดังนั้นการฟอกผลประโยชน์ที่ได้จากการกระทำผิดเป็นเงินที่ชอบด้วยกฎหมายโดยเงินสกุลเข้ารหัสจึงมีโอกาสสำเร็จสูง และคุ้มค่าเมื่อเปรียบเทียบกับความเสี่ยงที่อาจถูกตรวจสอบยึด อายัดและจับกุมโดยเจ้าหน้าที่ นอกจากนี้ด้วยมาตรการทางกฎหมายในการกำกับเงินสกุลเข้ารหัสของแต่ละประเทศมีความแตกต่างกัน เกิดเป็นช่องโอกาสทางกฎหมายต่อการฟอกเงินโดยเงินสกุลเข้ารหัส เข้าข่ายขาดการพิทักษ์ปกป้องอย่างมีประสิทธิภาพอันเป็นองค์ประกอบสำคัญโดยทฤษฎีปกตินิสัย จึงอาจเป็นเหตุสนับสนุนให้อาชญากรเลือกใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการฟอกเงิน

แนวทางการป้องกันการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส

ผู้เขียนได้สังเคราะห์ข้อเสนอแนะเกี่ยวกับแนวทางการป้องกันและปราบปรามการฟอกเงินโดยเงินสกุลเข้ารหัสที่เหมาะสม โดยอ้างอิงกรอบแนวคิดทฤษฎีป้องกันอาชญากรรม สามารถสรุปเป็นมาตรการได้ดังนี้

1. มาตรการสำคัญซึ่งเป็นที่ยอมรับสำหรับการป้องกันและปราบปรามการฟอกเงินทั้งในระดับประเทศและสากล คือ การตรวจสอบพิสูจน์ตัวตนของผู้ขอใช้บริการก่อนการเริ่มใช้ระบบงาน (Know Your Customer - KYC) และการตรวจประเมินธุรกรรมต้องสงสัย (Customer Due Diligent - CDD) โดยผู้ให้บริการรับอนุญาตจากหน่วยงานบังคับใช้กฎหมาย ซึ่งเป็นแนวทางเพิ่มภาระความยากลำบากแก่ผู้กระทำผิด แต่ฐานข้อมูลเพื่อการติดตามสืบค้นเข้าถึงตัวตนของผู้ต้องสงสัยจะมีประสิทธิภาพมากเท่าใด ย่อมขึ้นอยู่กับขอบเขตของข้อมูลที่จำเป็นและเพียงพอต่อการพิสูจน์ตัวตน และการประเมินความเป็นไปได้ของธุรกรรมต้องสงสัย รวมถึงการปรับปรุงฐานข้อมูลของผู้ใช้บริการให้มีความทันสมัยอยู่เสมอ ซึ่งเป็นแนวการดำเนินงานในการกำกับธุรกรรมทางการเงินของระบบสถาบันการเงินในปัจจุบัน อย่างไรก็ตาม ด้วยระบบนิเวศเงินสกุลเข้ารหัสมีโครงข่ายเชื่อมโยงแบบโลกภิวัตน์บนระบบอินเทอร์เน็ต ผู้ใช้งานทั่วโลกสามารถเข้าถึงและเชื่อมโยงธุรกรรมข้ามพรมแดนต่อกันได้ ดังนั้นการขยายฐานข้อมูลตัวตนผู้ใช้งานได้มากขึ้นเท่าไร ก็จะยิ่งเพิ่มประสิทธิภาพการพิสูจน์ตัวตนของผู้ต้องสงสัยได้มากขึ้นเท่านั้น

2. มาตรการเพิ่มศักยภาพของหน่วยงานบังคับใช้กฎหมายโดยใช้เครื่องมือทางเทคโนโลยีขั้นสูงในการเชื่อมต่อเข้ากับระบบฐานข้อมูลแบบกระจายศูนย์ของบล็อกเชนเทคโนโลยี ซึ่งสนับสนุนระบบนิเวศเงินสกุลเข้ารหัส (Application Programming Interface – API) เป็นแนวทางเพิ่มความเสี่ยงต่อการถูกตรวจพบจับกุมแก่ผู้กระทำผิดด้วยเครื่องมือทางเทคโนโลยีที่ทันสมัย ในการวิเคราะห์พฤติกรรมการทำธุรกรรมเงินสกุลเข้ารหัส ความเชื่อมโยงของการทำธุรกรรมระหว่างรหัสที่ตั้งของกระเป๋าเงิน เพื่อการวิเคราะห์และสังเคราะห์พฤติกรรมกลุ่มผู้ใช้งาน และเส้นทางธุรกรรมเพื่อนำไปสู่การบริหารจัดการธุรกรรมต้องสงสัยและช่วยติดตามสืบค้นผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส รวมถึงการเชื่อมโยงเปรียบเทียบกับธุรกรรมประจำวันบนรหัสที่ตั้งของผู้ต้องสงสัยในระบบงานอื่น เช่น Email, Facebook, Twitter และสื่อสังคมออนไลน์ เพื่อสืบค้นพิสูจน์ตัวตนของผู้ต้องสงสัย

3. มาตรการเฝ้าระวังการทำธุรกรรมแปรสภาพระหว่างเงินสกุลเข้ารหัสเป็นเงินตราทั่วไปหรือเป็นสินทรัพย์อื่นที่มีระบบทะเบียนกำกับสำหรับการติดตามสืบค้น ซึ่งเป็นแนวทางเพิ่มความเสี่ยงต่อการถูกตรวจพบและจับกุมผู้กระทำผิด แม้ว่าจะเป็นมาตรการเชิงตั้งรับก็ตาม แต่ก็เป็นมาตรการที่มีประสิทธิภาพหลายประเทศในกลุ่มสหภาพยุโรปใช้แนวทางนี้เป็นมาตรการขั้นพื้นฐานภายใต้สภาพแวดล้อมปัจจุบันอาชญากรย่อมประสงค์ที่จะยักย้ายถ่ายเทและแปรสภาพเงินที่ไม่ชอบด้วยกฎหมายให้เป็นเงินตราทั่วไปที่ชอบด้วยกฎหมาย เพื่อเป็นผลตอบแทนจากการก่ออาชญากรรมและใช้เป็นแหล่งเงินทุนสนับสนุนการก่ออาชญากรรมต่อไป โดยข้อจำกัดด้านสภาพคล่องของเงินสกุลเข้ารหัสที่ยังไม่ได้รับการยอมรับให้เป็นสื่อกลางในการชำระค่าสินค้าและบริการได้อย่างเป็นปกติธุระ ดังนั้นธุรกรรมเงินสกุลเข้ารหัสที่หมุนเวียนอยู่ในระบบนิเวศ จึงย่อมมีโอกาสที่ธุรกรรมส่วนหนึ่งอาจเชื่อมโยงเข้าสู่ระบบสถาบันการเงินทั่วไป ซึ่งเป็นระบบการกำกับที่รัดกุม ส่งผลให้สามารถเริ่มติดตามสืบค้นถึงบุคคลที่มีส่วนเกี่ยวข้องกับธุรกรรมเงินสกุลเข้ารหัสต้องสงสัยที่สัมพันธ์กันได้ แม้ว่ามาตรการนี้จะประหยัดทรัพยากรในการติดตามสืบค้นผู้ต้องสงสัยในระบบนิเวศเงินสกุลเข้ารหัส แต่ก็ยังมีประเด็นที่พึงพิจารณา คือ อาชญากรอาจใช้ช่องว่างของมาตรการทางกฎหมายที่แตกต่างกันของแต่ละประเทศเป็นแนวทางในการเลือกสถานที่ซึ่งเอื้ออำนวยต่อการแปรสภาพเป็นเงินที่ชอบด้วยกฎหมายได้เช่นกัน

4. มาตรการสร้างความร่วมมือกับองค์กรนานาชาติ และหน่วยงานบังคับใช้กฎหมายของต่างประเทศที่เกี่ยวข้องกับการต่อต้านการฟอกเงิน รวมถึงหน่วยงานเอกชนที่มีส่วนสนับสนุนการต่อต้านการฟอกเงินโดยธุรกรรมเงินสกุลเข้ารหัส ทั้งในด้านองค์ความรู้เกี่ยวกับบริบทเงินสกุลเข้ารหัส พัฒนาการทางเทคโนโลยีการทำธุรกรรมและการสืบสวน ประสบการณ์ทางคดีในกรณีศึกษาเชิงปฏิบัติการและการแลกเปลี่ยนข้อมูลเพื่อการสืบค้นติดตามตัวผู้ต้องสงสัยข้ามประเทศ ซึ่งเป็นแนวทางเพิ่มความเสี่ยงต่อการถูกตรวจพบและจับกุมแก่ผู้กระทำผิด แม้ว่าปัจจุบันจะมีแนวปฏิบัติมาตรฐานในการขอความร่วมมือทางคดีอาญาระหว่างประเทศอยู่แล้ว แต่การสร้างกรอบความร่วมมือเฉพาะบริบทที่เกี่ยวข้องกับการฟอก

เงินโดยเงินสกุลเข้ารหัส จะเสริมประสิทธิภาพในการประสานงานได้เท่าทันต่อการเปลี่ยนแปลงทางเทคโนโลยี และการปรับเปลี่ยนรูปแบบพฤติกรรมของอาชญากร ทั้งนี้ขึ้นอยู่กับข้อจำกัดทางกฎหมายระหว่างประเทศ และของแต่ละประเทศที่เป็นคู่เจรจา

5. มาตรการประมวลองค์ความรู้และเผยแพร่ข้อมูลเกี่ยวกับกลไกการทำงานของระบบนิเวศเงินสกุลเข้ารหัสให้แก่สาธารณะ และประชาชนทั่วไปได้ทราบถึงประโยชน์ของธุรกรรมเงินสกุลเข้ารหัสและกระบวนการติดต่อผู้ให้บริการรับอนุญาตที่ถูกต้องตามกรอบของกฎหมาย รวมถึงความเสี่ยงที่อาจเกิดขึ้นทั้งด้านความไม่แน่นอนเชิงมูลค่า และโอกาสที่อาจตกเป็นเหยื่อแก่อาชญากรที่ใช้เงินสกุลเข้ารหัสเป็นเครื่องมือในการกระทำผิดและการฟอกเงิน เป็นแนวทางการลดเหตุข้ออ้างที่จะใช้แก้ตัวด้วยความไม่รู้ในการกระทำผิด นอกจากนี้การพัฒนาศักยภาพและทักษะของเจ้าหน้าที่ผู้รับผิดชอบทั้งในส่วนกลางและส่วนภูมิภาคประจำพื้นที่ก็มีความสำคัญยิ่ง เนื่องจากธุรกรรมเงินสกุลเข้ารหัสสามารถดำเนินการได้ทุกที่ในประเทศเท่าที่การให้บริการระบบอินเทอร์เน็ตครอบคลุมถึง มาตรการนี้เป็นการเสริมสร้างภูมิคุ้มกันให้แก่บุคคลที่อาจตกเป็นเหยื่อ และเสริมสร้างศักยภาพของเจ้าหน้าที่ซึ่งเป็นผู้พิทักษ์ป้องกันเหตุแห่งอาชญากรรม

ข้อเสนอแนะเชิงนโยบายและเชิงปฏิบัติการ

1. เนื่องจากกระบวนการพิสูจน์ตัวตนของผู้ใช้งานในระบบนิเวศเงินสกุลเข้ารหัสเป็นกลไกสำคัญที่จะทำให้ทราบถึงเจ้าของกระเป๋าเงินสกุลเข้ารหัสที่แท้จริง ดังนั้นจึงควรขยายฐานข้อมูลโดยการสร้างระบบจัดการฐานข้อมูลกลางของประเทศในลักษณะศูนย์ข้อมูลส่วนบุคคลกลาง (Big Data) สำหรับผู้ใช้บริการธุรกรรมการเงินทุกประเภท รวมถึงธุรกรรมเงินสกุลเข้ารหัส (KYC Bureau หรือ KYC Data Center) โดยจำกัดผู้เข้าถึงข้อมูลส่วนบุคคลนี้เฉพาะเจ้าหน้าที่ของหน่วยงานซึ่งมีกฎหมายรองรับการปฏิบัติงาน นอกจากนี้ยังเป็นการเตรียมความพร้อมรองรับความร่วมมือระหว่างประเทศในการแลกเปลี่ยนข้อมูลการตรวจสอบผู้ต้องสงสัยระหว่างกันต่อไปในอนาคต

2. เพื่อเสริมสร้างศักยภาพทางนวัตกรรมของประเทศ จึงควรส่งเสริมให้นักพัฒนาโปรแกรมในประเทศได้แข่งขันในการสร้างโปรแกรมเชื่อมต่อเข้ากับระบบฐานข้อมูลแบบกระจายศูนย์ของบล็อกเชนเทคโนโลยี (Application Programming Interface – API) เพื่อวิเคราะห์พฤติกรรมการทำธุรกรรมเงินสกุลเข้ารหัสของกลุ่มผู้ใช้งานต้องสงสัย และช่วยสืบค้นเชื่อมโยงธุรกรรมต้องสงสัยในระบบงานอื่นเพื่อให้สามารถเข้าถึงตัวตนของผู้ต้องสงสัย โดยกำหนดกรอบแนวคิดการพัฒนาโปรแกรมบนหลักการทำงานเช่นเดียวกับ Chainalysis, ChipherTrace หรือ Elliptic ซึ่งเป็นโปรแกรมสำเร็จรูประดับมาตรฐานสากล เพื่อลดภาระการพึ่งพิงโปรแกรมจากต่างประเทศ และอีกประการหนึ่งเป็นการสงวนปกป้องข้อมูลการสืบสวนให้อยู่ในอำนาจจัดการภายในประเทศ

3. ส่งเสริมแผนงานโครงการอินทนนท์ของธนาคารแห่งประเทศไทย ในการพัฒนาโครงสร้างพื้นฐานระบบการเงินแบบสังคมไร้เงินสด สู่การเป็นระบบการเงินดิจิทัลในรูปแบบเงินสกุลดิจิทัลที่ออกโดยธนาคารกลาง (Central Bank Digital Currency หรือ CBDC) ทั้งนี้เมื่อระบบการเงินดิจิทัลของหน่วยงานรัฐเชื่อมต่อกับระบบนิเวศเงินสกุลเข้ารหัสบนบล็อกเชนเทคโนโลยี ก็จะเป็นการขยายจุดเฝ้าระวังเพื่อการตรวจสอบธุรกรรมเงินสกุลเข้ารหัสต้องสงสัยได้อย่างกว้างขวางและทันทีเมื่อธุรกรรมข้ามมาสู่ระบบสื่อกลางชำระราคาโดยเงินสกุลดิจิทัลของรัฐ ย่อมส่งผลให้เกิดการจำกัดขอบเขตการใช้ผลประโยชน์ของอาชญากรที่ได้จากการกระทำผิดหรือการฟอกเงินมากขึ้น

4. ควรพิจารณาปรับปรุงกฎระเบียบหรือแนวปฏิบัติในกระบวนการดำเนินคดีที่เกี่ยวข้องกับธุรกรรมการฟอกเงินโดยเงินสกุลเข้ารหัสให้มีประสิทธิภาพมากขึ้น เช่น วิธีการรวบรวมพยานหลักฐานดิจิทัลที่ได้จากตรวจสอบเส้นทางธุรกรรมเงินสกุลเข้ารหัสต้องสงสัยในระบบบัญชีแบบกระจายศูนย์ การยึดอายัดเงินสกุลเข้ารหัสของผู้กระทำผิดเข้าจัดเก็บในกระเป๋าเงินกลางของรัฐ (State Wallet) เพื่อไม่ให้ถูกยักย้ายออกจากกระเป๋าเงินของผู้กระทำผิดไปโดยมิชอบ การระงับการทำธุรกรรมเงินสกุลเข้ารหัสของผู้กระทำผิดอย่างเร่งด่วนเป็นการชั่วคราว และการสอบสวนพิเศษด้วยการแฝงตัวเข้าร่วมทำธุรกรรมเงินสกุลเข้ารหัสกับผู้ต้องสงสัยเพื่อรวบรวมพยานหลักฐาน เป็นต้น

เอกสารอ้างอิง

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

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

สำนักงานป้องกันและปราบปรามการฟอกเงิน. (2560). *รวมกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน และกฎหมายว่าด้วยการป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายและการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง (พิมพ์ครั้งที่* 14). กรุงเทพฯ: แจ็ส เพอ-พริ้น

สำนักงานป้องกันและปราบปรามการฟอกเงิน. (2562). *ผลการปฏิบัติงานด้านการป้องกันการฟอกเงิน. (รายงานประจำปี 2562*). สืบค้นจาก https://www.amlo.go.th/index.php/th/strategy/annual-report/detail/11092

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

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

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: Corruption and money laundering/terrorism financing risks?. In *Handbook of digital currency* (pp. 283-307). Academic Press.

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

Edwin H. Sutherland, (1961). *White Collar Crime*, New York: Holt, Rinehart and Winston, p.9-10.

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

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

Girasa, R. (2018). *Regulation of cryptocurrencies and blockchain technologies: national and international perspectives*. Springer.

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). Cryptocurrencies 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

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*). Retrieved from https://search.proquest.com/openview/daa0d91607166b4d9e3a0accbca6cc09/1?pq-origsite=gscholar&cbl=18750&diss=y

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* (6th ed.) SAGE Publication Inc.

Nakamoto, S. (2008). *Bitcoin : A Peer-to-Peer Electronic Cash System*. Decentralized Business Review, 21260. 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&response-content-disposition=inline%3B%20filename%3DBitcoin_A_Peer-to-Peer_Electronic_Cash_S.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. Retrieved from https://ieeexplore.ieee.org/document/9031941

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

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). T*he Money Laundering Cycle*. Retrieved from https://www.unodc.org/unodc/en/money-laundering/laundrycycle.html