หมวดหมู่ของอาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซี
Categories of Cryptocurrency-Related Crimes

เจษฎาพงษ์ ค้ำชู
คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล

Chetsadaphong Khamchu
Faculty of Social Sciences and Humanities, Mahidol University

Received January 20, 2022 | Revised May 30, 2022 | Accepted June 9, 2022

บทความวิชาการ (Academic Article)

บทคัดย่อ

ผลกระทบจากการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรน่า 2019 (COVID – 19) ในช่วงปี 2563 ที่ผ่านมานั้น ทำให้ทั่วโลกต้องปรับตัวกับการควบคุมและป้องกันการแพร่ระบาดของโรคติดเชื้อไวรัสชนิดนี้ด้วยการปรับตัวให้เข้ากับชีวิตประจำวันตามแนวคิดความปกติใหม่ (New Normal) และเมื่อเป็นเช่นนั้นการดำเนินการทางธุรกรรมการเงินผ่านโทรศัพท์มือถือก็มีการใช้งานที่แพร่หลายขึ้นอย่างมีนัยสำคัญ รูปแบบการใช้เทคโนโลยีทางการเงินที่เปลี่ยนไปให้สอดรับการชีวิตตามความปกติใหม่ การใช้คริปโทเคอร์เรนซีก็เป็นอีกทางเลือกหนึ่งที่ได้รับความนิยมแพร่หลายมากขึ้น ในขณะเดียวกันผู้กระทำผิดได้เล็งเห็นช่องทางในการก่ออาชญากรรมหลายประเภทที่เกี่ยวข้องกับคริปโทเคอร์เรนซี บทความนี้จึงมีวัตถุประสงค์เพื่อรวบรวมอาชญากรรมที่เกี่ยวข้องการใช้คริปโทเคอร์เรนซี แล้วจัดหมวดหมู่ในการกระทำความผิดตามแนวคิดและทฤษฎีทางด้านอาชญาวิทยา จากการจัดหมวดหมู่ในการกระทำผิดสามารถจำแนกอาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซี 3 ประเภท คือ 1) อาชญากรรมที่มีคริปโทเคอร์เรนซีเป็นเป้าหมาย คือ หมวดหมู่อาชญากรรมที่ต้องการขโมยคริปโทเคอร์เรนซีจากกระเป๋าเงินดิจิทัลของผู้ใช้งานหรือผู้ให้บริการแต่ละระดับ อีกทั้งรูปแบบวิธีการในการขโมยก็จะแตกต่างกันออกไปตามรูปแบบของกระเป๋าเงินดิจิทัล 2) อาชญากรรมที่ใช้คริปโทเคอร์เรนซีเป็นอาวุธ คือ หมวดหมู่อาชญากรรมที่มุ่งทำลายระบบบล็อกเชน และการแทรกแซงอุปกรณ์ในระบบบล็อกเชน และ 3) อาชญากรรมที่ใช้คริปโทเคอร์เรนซีเครื่องมือ คือ อาชญากรรมที่การใช้คริปโทเคอร์เรนซีก่ออาชญากรรมทั่วไป โดยการใช้ประโยชน์จากคุณสมบัติเฉพาะของคริปโทเคอร์เรนซีในการปกปิดตัวตนเพื่อก่ออาชญากรรมทางคอมพิวเตอร์ทั้งอาชญากรรมทางคอมพิวเตอร์และอาชญากรรมแบบดั้งเดิม ในบทความนี้ได้สรุปและเสนอแนะแนวทางป้องกันอาชญากรรมตามแนวคิดทฤษฎีทางอาชญาวิทยาที่เกี่ยวข้องกับการใช้คริปโทเคอร์เรนซีในทางที่ผิดอีกด้วย

คำสำคัญ: หมวดหมู่อาชญากรรม, คริปโทเคอร์เรนซี, ปรากฏการณ์ล้มทั้งยืน, การหลอกลวง, การลักลอบขุดเหรียญ

Abstract

Since early 2020, the COVID-19 pandemic has globally affected people in many dimensions, such as health, economics, and lifestyle. According to the infectious disease prevention, a new living lifestyle called "New Normal" has been launched. In other words, communication technology has rapidly changed the new normal lifestyle. It refers to the financial transactions through online systems or online banking, which have increasingly become more accessible. Besides, the alternative online financial transactions are made by cryptocurrency as well. On the other hand, offenders can find ways to commit crimes related to cryptocurrency. Additionally, this article aims to compile and categorize cryptocurrency-related crimes by applying criminological concepts and theories to clarify them. In this case, cryptocurrency-related crimes are classified into three types. Firstly, the crime with cryptocurrency as a target consists of an attempt to steal coins from users' digital wallets, ICO Exchanges, or Miners. In addition, the stealing technique may be altered by the types of digital wallets and cryptocurrency holders. Secondly, the crime that cryptocurrency is defined as a weapon that aims to break the blockchain network and disrupt the blockchain devices. Lastly, the crime that cryptocurrency is defined as a tool. To illustrate, offenders can take advantage of the particularities of cryptocurrency in terms of anonymity to commit a variety of crimes, both of cybercrimes and traditional crimes. In conclusion, this article summarizes and proposes cryptocurrency-related crime prevention strategies based on relevant criminological theories.

Keywords: Categories of Crimes, Cryptocurrency, Rug Pull, Fraud, Cryptojacking

บทนำ

จากการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรน่า 2019 (COVID – 19) ในช่วงปี 2563 ที่ผ่านมา ทำให้สังคมโลกต้องปรับตัวกับการควบคุมและป้องกันการแพร่ระบาดของโรคติดเชื้อไวรัสชนิดนี้ โดยการปรับวิถีชีวิตที่เป็นความปกติใหม่ (New Normal) ซึ่งมีการปฏิบัติที่หลากหลายแนวทางร่วมกัน ประกอบด้วย การเว้นระยะห่างทางสังคม (Social Distancing) การทำงานที่บ้าน (Work From Home) การดำเนินการทางธุรกรรมอิเล็กทรอนิกส์ (Online Business) (Thailand Institute of Occupational Safety and Health (Public Organization), 2022) เมื่อวิถีชีวิตเปลี่ยนไป ลักษณะการใช้เงินในชีวิตประจำวันก็เปลี่ยนแปลงตามไปด้วย ดังปรากฏในสถิติการเปรียบเทียบการทำธุรกรรมการชำระเงินผ่านบริการ Mobile Bank และ Internet Banking รายไตรมาส ระหว่างปี พ.ศ.2563 และ 2562 (Bank of Thailand, 2021) พบว่า เมื่อเปรียบเทียบการทำธุรกรรมผ่านโทรศัพท์ (Mobile Banking) ในช่วงไตรมาสที่ 1 ของปี 2562 ที่ยังไม่มีการแพร่ระบาดของเชื้อไวรัสโคโรน่า 2019 (COVID – 19) กับไตรมาสที่ 1 ของ ปี 2563 ที่เริ่มมีการแพร่ระบาดของเชื้อไวรัสโคโรน่า 2019 (COVID – 19) จะเห็นได้ว่า จำนวนบัญชีลูกค้าที่ใช้บริการ Mobile Banking เพิ่มขึ้นอย่างก้าวกระโดด ราว 12 ล้านบัญชีผู้ใช้งาน และ เพิ่มอีก 10 ล้านบัญชีผู้ใช้งานในไตรมาส 1 ของ ปี 2564 รวมเป็น 72 ล้านบัญชีผู้ใช้งาน มีปริมาณ

รายการเพิ่มขึ้นในช่วงปีเดียวกันถึง 7 ร้อยล้านรายการของช่วงเดียวกันในปี 2562 กับ 2563 และเมื่อพิจารณามูลค่าของการทำธุรกรรมการชำระเงินผ่าน Mobile Banking ในช่วงไตรมาสที่ 4 ปี 2562 ก่อนการระบาดของโรคติดเชื้อไวรัสโคโรน่า 2019 (COVID – 19) และ ไตรมาสที่ 3 ปี 2563 ช่วงที่มีการกลับมาแพร่ระบาดของโรคติดเชื้อไวรัสโคโรน่า 2019 (COVID – 19) ระลอกใหม่ในประเทศไทย (Bank of Thailand, 2021) พบว่า มีมูลค่าการทำธุรกรรมเพิ่มขึ้นถึง 300 ล้านล้านบาท รายละเอียดเพิ่มเติมในตารางที่ 1

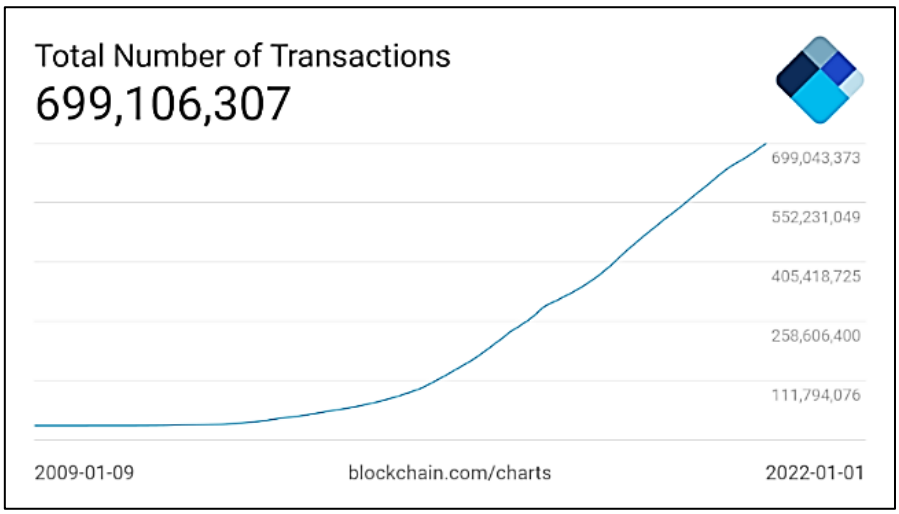
ตารางที่ 1 แสดงจำนวนธุรกรรมการชำระเงินผ่านบริการ Mobile Banking และ Internet Banking* เปรียบเทียบรายไตรมาสตั้งแต่ปี พ.ศ.2562 – 2564

	รายการ	ไตรมาส 4	ไตรมาส 3	ไตรมาส 2	ไตรมาส 1
1 ธุรกรรมการชำระเงินผ่าน Internet Banking					
1.1	จำนวนบัญชีลูกค้าที่ใช้บริการ**	[n/a] 34,946,211 (29,404,466)	[36,638,170] 34,213,563 (27,614,364)	[35,857,161] 30,976,384 (26,549,841)	[35,498,415] 29,850,113 (25,004,793)
1.2	ปริมาณรายการ (พันรายการ)	[n/a] 120,964 (82,180)	[156,483] 114,512 (139,249)	[137,916] 105,130 (127,449)	[127,800] 88,843 (109,339)
1.3	มูลค่ารายการ (พันล้านบาท)	[n/a] 6,162 (5,319)	[6,721] 5,530 (5,672)	[6,513] 5,336 (6,633)	[6,562] 5,810 (6,002)
	รายการ	ไตรมาส 4	ไตรมาส 3	ไตรมาส 2	ไตรมาส 1
2 ธุรกรรมการชำระเงินผ่าน Mobile Banking					
2.1	จำนวนบัญชีลูกค้าที่ใช้บริการ**	[n/a] 68,697,059 (60,084,145)	[78,824,825] 65,160,583 (56,300,671)	[74,982,583] 62,913,603 (55,153,004)	[72,081,849] 62,788,691 (49,756,353)
2.2	ปริมาณรายการ (พันรายการ)	[n/a] 2,958,200 (1,701,511)	[4,274,184] 2,557,189 (1,412,802)	[3,515,348] 2,202,528 (1,155,912)	[3,284,376] 1,870,805 (1,028,807)
	2.2.1 การโอนเงินและชำระเงิน	[n/a] 2,830,986 (1,616,797)	[4,139,734] 2,444,093 (1,343,268)	[3,384,329] 2,114,950 (1,104,042)	[3,155,563] 1,776,949 (988,821)
	2.2.2 การถอนเงินสด	[n/a] 127,215 (84,713)	[134,450] 113,098 (69,535)	[131,019] 87,580 (51,870)	[128,812] 93,858 (39,986)
3 ธุรกรรมการชำระเงินผ่าน Mobile Banking					
3.1	มูลค่ารายการ	[n/a]	[14,325]	[13,739]	[12,755]

รายการ	ไตรมาส 4	ไตรมาส 3	ไตรมาส 2	ไตรมาส 1
(พันล้านบาท)	11,715	10,651	8,867	8,967
	(8,706)	(7,578)	(5,782)	(5,562)
3.1.1 การโอนเงินและชำระเงิน	[n/a]	[14,066]	[13,478]	[12,501]
	11,480	10,449	8,705	8,790
	(8,546)	(7,452)	(5,685)	(5,488)
3.1.2 การถอนเงินสด	[n/a]	[259]	[260]	[254]
	237	203	162	175
	(160)	(126)	(97)	(75)

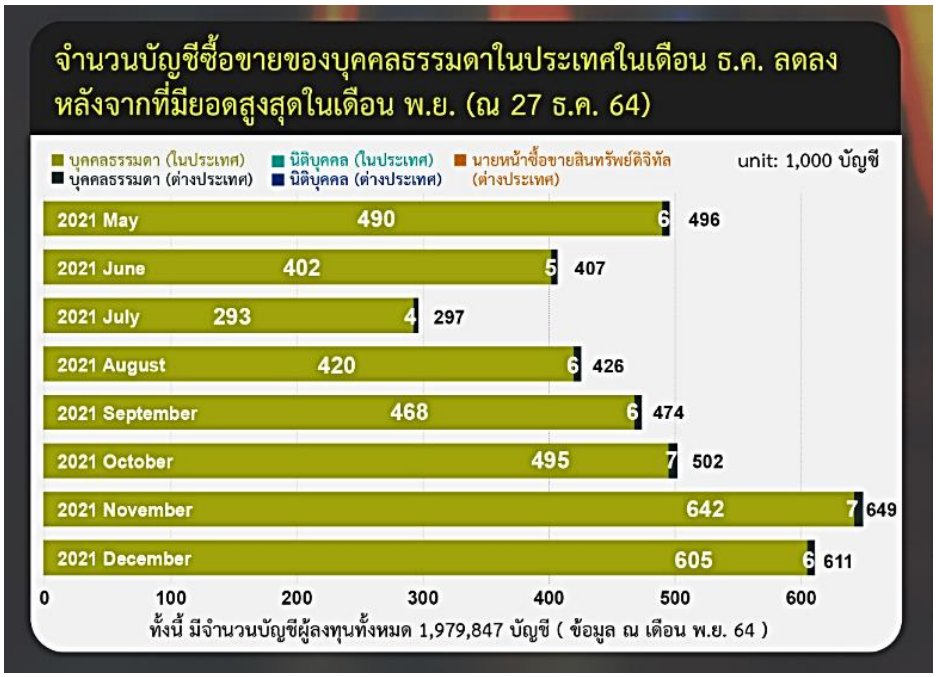
แหล่งที่มา: Bank of Thailand (2021)
หมายเหตุ: ข้อมูลปี พ.ศ.2564 ในเครื่องหมาย [ ], ข้อมูลปี พ.ศ.2563 ไม่มีเครื่องหมาย และ ข้อมูลปี พ.ศ.2562 ในเครื่องหมาย ( )
* ครอบคลุมรายการโอนภายในธนาคารเดียวกัน ต่างธนาคาร, ชำระค่าสินค้าและบริการ และการถอนเงินสด
** จำนวนบัญชีสะสมทั้งหมดที่ทำสัญญาขอใช้บริการจนถึงงวดปัจจุบัน ภายใต้บริการประเภทต่าง ๆ ของธนาคาร

จากตารางที่ 1 แสดงให้เห็นถึงการขยายตัวของผู้ใช้งาน การเข้าถึงการดำเนินการธุรกรรมทางการเงินผ่านโทรศัพท์มือถือ ในห้วงเวลาที่มีการแพร่ระบาดของโรคติดเชื้อไวรัสโคโรน่า 2019 (COVID – 19) ที่ผ่านมาที่เป็นตัวกระตุ้นให้เกิดการใช้เทคโนโลยีทางการเงินเพื่อให้สอดรับกับการใช้ชีวิตตามความปกติใหม่ (New Normal) การใช้คริปโทเคอร์เรนซีเป็นอีกทางเลือกหนึ่งที่ได้รับความนิยมแพร่หลายมากขึ้น ตามภาพที่ 1 พบว่าในช่วงเวลาที่ผ่านมา จำนวนธุรกรรมในบล็อกเชนเพิ่มขึ้นอย่างเห็นได้ชัด โดยพิจารณาจากจำนวนของการทำธุรกรรมของบล็อกเชน ซึ่งเป็นเทคโนโลยีหนึ่งของคริปโทเคอร์เรนซี ถึง 699 ล้านธุรกรรมทั่วโลก ตั้งแต่ ปี 2009 – 2022



ภาพที่ 1 จำนวนธุรกรรมในบล็อกเชน
แหล่งที่มา Blockchain.com (2022)

จำนวนของธุรกรรมของบล็อกเชนทั่วโลกที่มีปริมาณเพิ่มมากขึ้นนั้น สอดรับกับจำนวนของบัญชีซื้อขายคริปโทเคอร์เรนซีของบุคคลธรรมดาในประเทศไทย เดือน ธันวาคม 2564 ที่มีจำนวนสูงถึง 605,000 บัญชี รวมจำนวนบัญชีผู้ลงทุน ณ เดือน พฤศจิกายน ทั้งหมด 1,979,847 บัญชี (The Securities and Exchange Commission (Thailand), 2022) รายละเอียดเพิ่มเติมใน ภาพที่ 2



ภาพที่ 2 จำนวนบัญชีซื้อขายของบุคคลธรรมดาในประเทศในเดือน ธันวาคม 2564
แหล่งที่มา The Securities and Exchange Commission (Thailand) (2022)

ด้วยเทคโนโลยีทางการเงินเปลี่ยนแปลงไปอย่างรวดเร็ว ทำให้การแลกเปลี่ยนคริปโทเคอร์เรนซีที่มีลักษณะเป็นอิสระจากการควบคุมของหน่วยงานภาครัฐ (Decentralize) ไม่ต้องเสียค่าธรรมเนียมในการทำธุรกรรม มีคุณสมบัติโดดเด่นในการปกปิดตัวตนของผู้ทำธุรกรรมซึ่งสนองตอบความต้องการของผู้ใช้งานที่ไม่ต้องการระบุตัวตน (Anonymous) สามารถใช้อำพรางการกระทำความผิดได้ อีกทั้งยังมีความรวดเร็วในการทำธุรกรรมระหว่างประเทศ (Supervision and Examination Division, 2021) ทำให้ผู้กระทำผิดเล็งเห็นโอกาสจากการใช้ประโยชน์ของคริปโทเคอร์เรนซีในการก่ออาชญากรรมที่อาจจะก่อให้เกิดความเสียต่อทรัพย์สินของประชาชนและระบบเศรษฐกิจของประเทศไทยเป็นอย่างมาก โดยบทความนี้มีวัตถุประสงค์เพื่อรวบรวมอาชญากรรมที่เกี่ยวข้องการใช้คริปโทเคอร์เรนซี แล้วทำการ จัดหมวดหมู่ในการกระทำผิดตามแนวคิดและทฤษฎีทางด้านอาชญาวิทยา เพื่อให้เกิดความเข้าใจเกี่ยวกับอาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซีมากยิ่งขึ้น

คริปโทเคอร์เรนซี

1) ความหมายของ คริปโทเคอร์เรนซี

ตาม มาตรา 3 แห่ง พระราชกำหนด การประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ได้กำหนดความหมายของ “คริปโทเคอร์เรนซี” ไว้ว่า หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้าและบริการ

Siam Commercial Bank (2022) ได้ให้ความหมายของ คริปโทเคอร์เรนซี ไว้ว่าสินทรัพย์ดิจิทัลประเภทหนึ่งที่มีการเข้ารหัส มีราคากลางในการซื้อขายแปรผันตามกลไกตลาด จึงสามารถทำหน้าที่เป็นสื่อกลางในการแลกเปลี่ยนมูลค่าผ่านอินเทอร์เน็ตได้ แต่ด้วยไม่ได้มีลักษณะทางกายภาพเหมือนเช่นสกุลเงินทั่วไป (Fiat Currency) ของแต่ละประเทศที่มีการตีพิมพ์ธนบัตรหรือเหรียญกษาปณ์ออกมาทำให้ถูกเรียกว่าเป็น สกุลเงินเสมือน (Virtual Currency)

Binance (2022) ซึ่งเป็นผู้ประกอบธุรกิจเป็นศูนย์ซื้อขายทรัพย์สินดิจิทัล (Digital Asset Exchange) ได้ให้ความหมายของ คริปโทเคอร์เรนซี ไว้ว่า เป็นรูปแบบของเงินสดดิจิทัล (Digital Cash) ที่ช่วยให้บุคคลสามารถส่งต่อมูลค่าในสภาพแวดล้อมดิจิทัล (Digital Setting)

ปัจจุบันคริปโทเคอร์เรนซียังไม่ใช่เงินที่ธนาคารกลางใดในโลกรับรองว่าสามารถใช้ชำระหนี้ได้ตามกฎหมาย (Legal Tender) คริปโทเคอร์เรนซีที่รู้จักกันแพร่หลาย เช่น Bitcoin, Ethereum และ Bitkub Coin เป็นต้น (The Securities and Exchange Commission (Thailand), 2021)

สรุปแล้ว คริปโทเคอร์เรนซี คือ หน่วยข้อมูลทางดิจิทัลที่ถูกสร้างขึ้น ใช้งานผ่านช่องทางอินเตอร์เน็ตโดยเทคโนโลยีบล็อกเชน (Blockchain) โดยการส่งผ่านข้อมูล รับรองและสอบทานความถูกต้องร่วมกันโดยไม่มีตัวกลาง โดยมีการใช้เทคโนโลยีการเข้ารหัส (Cryptography) เพื่อความปลอดภัยของข้อมูล ซึ่งสามารถใช้เป็นตัวกลางในการแลกเปลี่ยนสินค้าและบริการได้ โดยมีราคากลางในการซื้อขายแปรผันตามกลไกตลาด

2) รูปแบบการจัดเก็บคริปโทเคอร์เรนซี

กระเป๋าเงินดิจิทัล (Digital Wallets) คือ เครื่องมือที่ใช้เข้าถึงเครือข่ายบล็อกเชนที่ใช้เป็นเทคโนโลยีในการจัดเก็บข้อมูลของคริปโทเคอร์เรนซี โดยกระเป๋าเงินดิจิทัลมีหลายรูปแบบสามารถจำแนกเป็นกลุ่มใหญ่ ๆ ได้ 3 กลุ่ม คือ ซอฟท์แวร์ ฮาร์ดแวร์ และ กระดาษ (Binance, 2022) กระเป๋าเงินดิจิทัลสามารถสร้างข้อมูลสำคัญเพื่อรับและส่งข้อมูลคริปโทเคอร์เรนซีผ่านเทคโนโลยีบล็อกเชนที่เรียกว่า Public Keys หรือ Private Keys แล้วแต่ชนิดประเป๋าเงินดิจิทัล โดยแต่ละกระเป๋าเงินดิจิทัลจะมี Address ที่ถูกสร้างขึ้นแบบสุ่มด้วยระบบคอมพิวเตอร์ และประกอบด้วยตัวเลขกับตัวอักษร 26 - 34 ตัว ตัวอย่างเช่น“1F1tAaz5x1HUXrCNLbtMDqcw6o5GNn4xqX” ซึ่งเปรียบเสมือน เลขบัญชีเงินฝากของแต่ละธนาคารสำหรับโอนหรือรับโอนเท่านั้น โดยผู้ทำธุรกรรมทั้ง 2 ฝ่าย จะรับรู้เพียง Address ของแต่ละฝ่ายเท่านั้น จึงไม่สามารถเข้าถึงข้อมูลส่วนตัวของแต่ละฝ่ายได้ หลังจากการทำธุรกรรมเสร็จสิ้นเรียบร้อยแล้ว Address จะเปลี่ยนไปทุกครั้งที่มีการเปลี่ยนแปลงยอดเงินในเกระเป๋าเงินดิจิทัล ทั้งผู้โอนและผู้รับโอนด้วยการเข้ารหัสข้อมูลด้วยการแฮช (Hash Function) (Supervision and Examination Division, 2022) ประเภทของกระเป๋าเงินดิจิทัล ตามตารางที่ 2 มีรายละเอียดดังนี้

ตารางที่ 2 แสดงประเภท ลักษณะของกระเป๋าเงินดิจิทัล

ประเภท	ลักษณะ	ตัวอย่างการให้บริการ
(A) Software wallet : ใช้งานผ่านซอฟท์แวร์บนอุปกรณ์ หรือ เว็ปไซต์ มีทั้งรูปแบบที่ผู้ให้บริการเก็บ PK (Pirate key) (Custodial) และ User เก็บเอง (Non-custodial) หลายรายมีบริการทำธุรกรรม เช่น รับฝาก แลกเปลี่ยน โอน เป็นธุรกิจหลัก		
A1) web-based wallet	• เข้าใช้งานผ่านเว็บไซต์ ของผู้ให้บริการ • นิยมใช้กับการซื้อขายแลกเปลี่ยน หรือการใช้จ่าย	• Exchange Wallet • Blockchain.com • Mycryptowallet
(A2) desktop /mobile wallet	• ใช้งานโดยติดตั้งโปรแกรมบนอุปกรณ์ เช่น มือถือ หรือ คอมพิวเตอร์ • ส่วนใหญ่ User เก็บ PK เอง	• JAXX.io • Mycelium
(B) Hardware wallet User ใช้อุปกรณ์ในการสร้าง/เก็บ PK Offline (user เก็บเอง)	• ผู้ใช้งานซื้ออุปกรณ์ (Hardware) เพื่อนำไปใช้งาน และ PK จะถูกสร้างและเก็บบน Hardware • ใช้งานผ่าน Hardware โดยตรง หรือต่อเชื่อมกับ อุปกรณ์อื่น	• Trezor • Ledger • KeepKey
(C) Paper wallet User บันทึก PK ลงในกระดาษ เก็บเอง	• เป็นการบันทึก address และ PK ลงบนกระดาษ • ใช้งานโดยนำไปเข้าระบบ (ส่วนมากใช้ครั้งเดียวทิ้ง เหตุผลด้านความปลอดภัย • นิยมเก็บทรัพย์สินที่มีมูลค่าสูงที่ต้องการเก็บเป็นเวลานาน	• Bitcoinpaperwallet.com • Bitaddress.org (open source)

แหล่งที่มา Supervision and Examination Division, 2021

3) คุณลักษณะพิเศษของคริปโทเคอร์เรนซีที่นำไปสู่ปัญหาในการใช้งาน

อภินพ อติพิบูลย์ ได้กว่าถึงปัญหาของบิทคอยน์ในประเด็นที่เกี่ยวกับปัญหาของบิทคอยน์ ซึ่งเป็นคริปโทเคอร์เรนซีหลักที่มีส่วนแบ่งของมูลค่าตลาดถึงร้อยละ 40 (Supervision and Examination Division, 2022) ไว้ว่า 1) ไม่มีคนกลางที่บริหารจัดการระบบเงิน การปรับปรุงบิทคอยน์ จึงขาดวิธีป้องกันการโจรกรรมข้อมูลจากเครื่องคอมพิวเตอร์ของเจ้าของบัญชีทำให้ต้องแบกรับความเสี่ยงจากการเก็บรักษา

บิทคอยน์ด้วยตนเอง ไม่มีหน่วยงานใดรับประกันเงินบิทคอยน์เหมือนการรับประกันเงินฝากในธนาคาร 2) ไม่มีการระบุตัวตนของเจ้าของเงินบิทคอยน์ การทำธุรกรรมทางการเงินของบิทคอยน์ ผู้ใช้งานทั่วไปจะไม่ถูกบังคับให้แสดงข้อมูลส่วนบุคคลเพื่อระบุตัวตนก่อนเข้าทำธุรกรรมเหมือนกับการทำธุรกรรมกับสถาบันทางการเงิน 3) มูลค่าหรือราคาของบิทคอยน์ถูกกำหนดจากต้องการของผู้ใช้เท่านั้น ซึ่งทำให้มูลค่าของบิทคอยน์เกิดความผันผวนอยู่ตลอดเวลา 4) การทำธุรกรรมของบิทคอยน์ไม่มีการเก็บข้อมูลส่วนบุคคลของผู้ทำธุรกรรมและสามารถโอนรับเงินได้หลายทอดโดยเสียค่าธรรมเนียมน้อยมาก จึงเป็นช่องทางในการหลบเลี่ยงภาษีได้ (Pimthunya Kongsanor, 2018) และกระทำผิดอื่นได้

แนวคิด ทฤษฎีทางด้านอาชญาวิทยาที่เกี่ยวข้อง

1) ทฤษฎีทางอาชญาวิทยา

ทฤษฎีปกติวิสัย (Routine Activity Theory) เป็นทฤษฎีของ Lawrence E. Cohen และ Marcus Felson ที่ถูกนำมาใช้อธิบายอาชญากรรมพื้นฐาน (Street Crime) โดยทฤษฎีนี้ถูกพัฒนามาจากทฤษฎีการเลือกอย่างมีเหตุผล (Rational Choice Theory) โดยได้ทำการศึกษาอาชญากรรมที่เกี่ยวข้องกับชีวิตและทรัพย์ ซึ่งหลักการสำคัญของทฤษฎีนี้อธิบายอาชญากรรมจะเกิดขึ้นได้ ต่อเมื่อมีองค์ประกอบสำคัญ 3 องค์ประกอบ คือ ผู้ที่จะกระทำผิด (Motivated Offender), เป้าหมายที่เหมาะสม (Suitable Target) และการขาดการคุ้มครองที่ดี (Lack of Capable Guardian) เกิดขึ้นพร้อมกัน (Seksan Khruakham, 2015) ในช่วงเวลา และสถานที่ที่เดียวกัน

การอธิบายองค์ประกอบของอาชากรรมทางคอมพิวเตอร์สามารถการประยุกต์ใช้ทฤษฎีปกติวิสัย (Routine Activity Theory) อธิบายองค์ประกอบ ได้ดังนี้

(1) ผู้ที่จะกระทำผิด (Motivated Offender) คือ ผู้ที่จะกระทำผิดที่มีแรงจูงใจในการก่ออาชญากรรมทางคอมพิวเตอร์ หลายประเภท ทั้งการหลอกลวง (Phishing) การใช้มัลแวร์ (Malware) การเจาะระบบ (Hacking) เป็นต้น

(2) เป้าหมายที่เหมาะสม (Suitable Target) ไม่ใช่เฉพาะ ผู้ใช้งานในระบบคอมพิวเตอร์เท่านั้น แต่รวมถึง อุปกรณ์คอมพิวเตอร์ ซอฟท์แวร์ ชุดข้อมูล และเครือข่ายข้อมูล อีกด้วย

(3) การขาดการคุ้มครองที่ดี (Lack of Capable Guardian) คือ สภาวะการขาดการคุ้มครองป้องกันที่ดีจากสภาพแวดล้อม แบ่งออกเป็น 2 ส่วนคือ 1) สภาพแวดล้อมในระบบคอมพิวเตอร์ที่ประกอบด้วย Hardware, Software และ Peopleware (ผู้ใช้งาน) 2) สภาพแวดล้อมนอกระบบคอมพิวเตอร์ ได้แก่ กฎหมาย ความรู้ และความสามารถของผู้บังคับใช้กฎหมาย ที่ไม่อยู่ในสภาวะคุ้มครองป้องกันเหยื่อจากผู้ที่จะกระทำผิดที่มีแรงจูงใจในการก่ออาชญากรรมทางคอมพิวเตอร์ได้

2) แนวคิดด้านการจำแนกอาชญากรรมทางคอมพิวเตอร์

จากคู่มืออาชญากรรมทางคอมพิวเตอร์ (Computer Crime) ของกระทรวงยุติธรรมแห่งประเทศสหรัฐอเมริกา (U.S. Department of Justice: DOJ) ได้นิยามอาชญากรรมทางคอมพิวเตอร์ไว้ว่า “การละเมิดกฎหมายอาญาใด ๆ ที่เกี่ยวข้องกับความรู้ด้านเทคโนโลยีคอมพิวเตอร์ในการกระทำความผิด รวมการสอบสวนหรือการดำเนินคดี” โดยได้จำแนกอาชญากรรมทางคอมพิวเตอร์เป็น 3 ประเภท คือ 1) อาชญากรรมที่คอมพิวเตอร์คือ "เป้าหมาย" เป็นการขโมย ฮาร์ดแวร์ ซอฟต์แวร์ หรืออุปกรณ์ต่อพ่วงของคอมพิวเตอร์เป็นหลัก 2) อาชญากรรมที่มีคอมพิวเตอร์เป็น “อาวุธ” เป็นการโจมตีเครือข่ายคอมพิวเตอร์ หรือระบบปฏิบัติการ รวมไปถึงการทำลายหรือขัดขวางการทำงานของระบบ

คอมพิวเตอร์ซึ่งทำให้เกิดความเสียหายขึ้น และ 3) อาชญากรรมที่คอมพิวเตอร์และระบบที่เกี่ยวข้องเป็นวิธีการหรือ "เครื่องมือ" ใช้ก่ออาชญากรรมทั่วไป เช่น การขโมยข้อมูลประจำตัว ข้อมูล หรือเงิน หรือการครอบครองและการแจกจ่ายภาพอนาจารเด็ก (U.S. Department of Justice, 2012)

การจัดหมวดหมู่อาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซี

การวิเคราะห์อาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซี ผ่านการจำแนกประเภทของอาชญากรรมประเภทต่าง ๆ ตามแนวคิดการจำแนกอาชญากรรมทางคอมพิวเตอร์ตามแนวคิดข้างต้น สามารถจำแนกอาชญากรรมที่เกี่ยวขึ้นกับคริปโทเคอร์เรนซี ได้ดังนี้

1) อาชญากรรมที่มีคริปโทเคอร์เรนซีเป็นเป้าหมาย

อาชญากรรมทางคอมพิวเตอร์ที่มีคอมพิวเตอร์คือ "เป้าหมาย" คือ การขโมย ฮาร์ดแวร์ ซอฟต์แวร์ หรืออุปกรณ์ต่อพ่วงของคอมพิวเตอร์เป็นหลัก ในหลักการของการจัดกลุ่มของอาชญากรรมทางคอมพิวเตอร์ที่มีของคริปโทเคอร์เรนซีเป็นเป้าหมาย การขโมยคริปโทเคอร์เรนซี ที่สะสมอยู่ในกระเป๋าเงินดิจิทัล (Digital Wallet) โดยรูปแบบอาชญากรรมที่เกิดขึ้น จะมีการก่ออาชญากรรมคอมพิวเตอร์ประเภทอื่นร่วมด้วย เพื่อให้ผู้กระทำผิดได้มาซึ่งคริปโทเคอร์เรนซีของเหยื่อที่แบ่งออกเป็น 3 ประเภท คือ 1) เหยื่อที่เป็นบุคคลผู้ใช้งาน 2) เหยื่อที่เป็นศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Exchange) โดยทำหน้าที่เป็นศูนย์กลางหรือเครือข่ายในการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัล (The Securities and Exchange Commission (Thailand), 2021) และ 3) เหยื่อที่เป็นผู้ขุดเหมือง (Miner) อีกทั้งยังต้องคำนึงถึงรูปแบบการจัดเก็บคริปโทเคอร์เรนซีที่สะสมอยู่ในกระเป๋าเงินดิจิทัล (Digital Wallet) ในรูปแบบที่แตกต่างกัน ก็จะมีรูปแบบอาชญากรรมคอมพิวเตอร์ที่แตกต่างกันออกไป อาชญากรรมที่มีคริปโทเคอร์เรนซีเป็นเป้าหมาย จะมีให้เห็นอยู่บ่อยครั้ง ทั้งในรูปแบบการหลอกลวง (Phishing) การใช้มัลแวร์ (Malware) การเจาะระบบ (Hacking) เป็นต้น แต่การก่ออาชญากรรมทั้งหมดเพื่อให้ได้มาซึ่งคริปโทเคอร์เรนซีที่อยู่ในกระเป๋าเงินดิจิทัลของเหยื่อ

2) อาชญากรรมที่มีคริปโทเคอร์เรนซีเป็นอาวุธ

อาชญากรรมที่ใช้คอมพิวเตอร์เป็นอาวุธนั้น คือ อาชญากรรมที่มีเป้าหมายของการก่ออาชญากรรมมุ่งไปที่การทำลายเครื่องคอมพิวเตอร์ หรือระบบปฏิบัติการของคอมพิวเตอร์ แต่ในกรณีการจัดกลุ่มอาชญากรรมที่เกี่ยวข้องกับการใช้คริปโทเคอร์เรนซีเป็นอาวุธ ใช้รูปแบบการกระทำผิดที่คล้ายคลึงกัน คือ 1) แทรกแซงเปลี่ยนแปลงข้อมูลของระบบบล็อกเชน หรือ 2) ทำลายอุปกรณ์ในระบบบล็อกเชน โดยสามารถอธิบายในรายละเอียด ดังนี้

(1) การแทรกแซงระบบบล็อกเชน การออกแบบระบบบล็อกเชนให้เป็นระบบที่โปร่งใส ไร้ตัวกลาง มีการรับส่ง ข้อมูลระหว่างผู้ใช้กัน (Peer to Peer) (Binance, 2022) มีการรองรับความถูกต้องของข้อมูล และมีการทำสำเนาไว้ซึ่งกันและกัน ทำให้เป็นการยากหากจะแทรงแซงข้อมูล จาก 1 – 2 หน่วย (Node) ของบล็อกข้อมูล เพื่อแก้ไข ดัดแปลง ปรับปรุงข้อมูลในบล็อกเชนได้ตามใจชอบ แต่ในทางทฤษฎีบล็อกเชนสามารถถูกแทรกแซงได้ การจะเข้าแทรกแซงบล็อกเชนได้จำเป็นต้องใช้การดัดแปลงบล็อกข้อมูลกว่า 51% ของทั้งระบบเพื่อทำให้เกิดการรับรองข้อมูลเป็นเอกฉันท์ (Consensus) ในระบบบล็อกเชน ข้อจำกัดของบล็อกเชนที่มีจำนวนโหนดหรือผู้ใช้น้อยจึงมีความเป็นไปได้ที่จะถูกโจมตีได้ง่าย อย่างไรก็ตามแทบจะเป็นไปไม่ได้เลยในทางปฏิบัติ โดยเฉพาะเครือข่ายที่มีการกระจายตัวสูงอย่างบิทคอยน์ยิ่งมีผู้มีส่วนร่วมมากยิ่งทำให้เครือข่ายมีความแข็งแกร่ง ปลอดภัย และโปร่งใสมากเท่านั้น (bitkub, 2022)

จึงยังไม่เคยปรากฏการโจมตีในลักษณะดังกล่าวเป็นข่าวสู่สาธารณะชน แต่ในอนาคตเมื่อมีการพัฒนาเทคโนโลยีควอนตัมคอมพิวเตอร์ (Quantum Computer) ให้สามารถประยุกต์ใช้ได้อย่างเต็มประสิทธิภาพ ก็จะสามารถถอดรหัส Public-Key ที่ใช้กับระบบการเงินของคริปโทเคอร์เรนซี (NIST, 2021) จึงมีความจำเป็นต้องทบทวนระบบรักษาความปลอดภัยใหม่ โดย NIST ซึ่งเป็นหน่วยงานกำหนดมาตรฐานทางเทคโนโลยี ของสหรัฐอเมริกากำลังเร่งดำเนินการเกี่ยวกับการสร้างมาตรฐานความปลอดภัยใหม่ในรูปแบบของการเข้ารหัสหลังยุคควอนตัมคอมพิวเตอร์ (Post-Quantum Cryptography (PQC)) เพื่อกำหนดมาตรฐานความปลอดภัยใหม่สำหรับเทคโนโลยีควอนตัมคอมพิวเตอร์

(2) การลักลอบขุดเหรียญ (Cryptojacking) เป็นรูปแบบหนึ่งของอาชญากรรมที่ผู้กระทำผิดเข้ามาแอบใช้ทรัพยากร รวมไปถึงพลังงานในการประมวลผลของเครื่องคอมพิวเตอร์ของเหยื่อเพื่อใช้ในการสร้างข้อมูลดิจิทัลในระบบบล็อกเชนของคริปโทเคอร์เรนซีแต่ละชนิดหรือใช้เครื่องคอมพิวเตอร์ของเหยื่อเป็นหนึ่งหน่วย (Node) ที่ใช้ในการขุดคริปโทเคอร์เรนซี เหตุการณ์นี้มักเกิดขึ้นเมื่อเหยื่อติดตั้งมัลแวร์ (Malware) ที่เปิดโอกาสให้ผู้กระทำผิดเข้าถึงคอมพิวเตอร์ รวมไปถึงทรัพยากรในกระมวลผลของเครื่องคอมพิวเตอร์เหยื่อ หรืออุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ตอื่น ๆ โดยรูปแบบการคลิกลิงก์ที่ไม่รู้จักในอีเมลหรือการเข้าถึงเว็บไซต์ที่ซ่อนไวรัสไว้ จะถูกใช้โดยอาชญากรเพื่อสร้างหรือขุดคริปโทเคอร์เรนซี (Interpol, 2022) ผลกระทบของอาชญากรรมที่มีต่อเหยื่ออาจจะดูไม่น่ากลัว แต่จะอาชญากรรมประเภทนี้จะส่งผลให้เป็นการเพิ่มรายจ่ายค่าไฟฟ้าให้กับเหยื่อ หรือในกรณีร้ายแรงอาจจะเกิดความเสียหายต่ออุปกรณ์คอมพิวเตอร์เลยก็ได้ (Interpol, 2022) ข้อสังเกตในการตกเป็นเหยื่ออาชญากรรมประเภทนี้คือ 1) คอมพิวเตอร์ หรืออุปกรณ์อื่น ๆ มีความเร็วในการประมวลผลช้าลง 2) แบตเตอร์รี่ของอุปกรณ์ร้อนเกินความจำเป็น 3) อุปกรณ์ปิดตัวเองเนื่องจากพบข้อบกพร่องเกี่ยวกับประสิทธิภาพในการประมวลผล 4) ค่าไฟฟ้าเพิ่มขึ้นอย่างชัดเจน

3) อาชญากรรมที่มีคริปโทเคอร์เรนซีเป็นเครื่องมือ

อาชญากรรมที่ใช้คอมพิวเตอร์เป็นเครื่องมือ คือ อาชญากรรมที่คอมพิวเตอร์และระบบที่เกี่ยวข้องถูกใช้เป็นวิธีการหรือเครื่องมือในการก่ออาชญากรรมทั่วไป โดยอาชญากรรมที่ใช้คริปโทเคอร์เรนซีเป็นเครื่องมือจะมุ่งเน้นการทำเงิน โดยการใช้ประโยชน์จากคุณสมบัติเฉพาะของคริปโทเคอร์เรนซีในการทำธุรกรรมเพื่อปกปิดตัวตน หรือการใช้ชื่อของคริปโทเคอร์เรนซีเพื่อการหลอกลวงเพื่อระดมทุน อาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซี มีรายละเอียดดังนี้

3.1 การหลอกลวง (Scam) หรือ การหลอกลวงทางอินเตอร์เน็ต ซึ่งสามารถรวบรวมรูปแบบการหลอกลวงที่มีความเกี่ยวข้องกับคริปโทเคอร์เรนซี (FBI, 2020) ดังนี้

1) การข่มขู่ (Blackmail) มีทั้งรูปแบบของอีเมลและจดหมาย โดยผู้กระทำผิดจะอ้างว่าเข้าถึงข้อมูลส่วนบุคคลของคุณหรือข้อมูลลับ (Dirty Secret) ของผู้เสียหายและเรียกร้องให้ชำระเงินเป็นคริปโทเคอร์เรนซีเพื่อป้องกันการเปิดเผยข้อมูล

2) หลอกสมัครงาน (Work from Home Scams) ผู้กระทำผิดจะสวมบทบาทเป็นนายจ้างที่จะหลอกให้ผู้เสียหายยอมรับเงินบริจาคของผู้กระทำผิดเข้าบัญชีธนาคารของผู้เสียหายและจะให้ผู้เสียหายฝากเงินบริจาคดังกล่าวเข้าตู้คริปโทเคอร์เรนซี (Crypto Kiosks) โดยสิ่งที่เรียกว่าเงินบริจาคนี้ มีแนวโน้มว่าเงินจะถูกขโมยจากผู้อื่น

3) การหลอกขายสินค้าหรือบริการ โดยผู้กระทำผิดจะหลอกให้โอนเงินที่เป็นคริปโท-เคอร์เรนซีเพื่อใช้ในการปกปิดตัวตนของผู้กับทำผิด แล้วไม่ส่งของหรือบริการให้ผู้เสียหาย

4) การหลอกให้ลงทุน (Investment Scams) โดยผู้กระทำผิดใช้เครื่องมือการลงทุนด้วยรูปแบบไอซีโอ (Initial Coin Offering (ICO)) คือการระดมทุนแบบดิจิทัลด้วยการเสนอขายโทเคนดิจิทัลผ่านระบบบล็อกเชนต่อสาธารณชน โดยผู้ระดมทุนจะเป็นผู้ออกโทเคนดิจิทัล มาแลกกับเงินดิจิทัล(Cryptocurrency) การระดมทุนด้วย ICO (The Securities and Exchange Commission (Thailand), 2021) ในอาชญากรรมที่เกิดขึ้นเป็นการหลอกผู้เสียหายให้ลงทุน โดยให้ความสำคัญว่าสถานการณ์ที่ดูเหมือน "ดีเกินกว่าจะเป็นจริง" ซึ่งให้ผลตอบแทนทางการเงินจำนวนมากสำหรับการลงทุนระยะสั้นในระยะสั้น ความจริงก็คือผู้กระทำผิดขโมยเงินลงทุนไปใช้งานส่วนตัวแล้วใช้ความซับซ้อนของเทคโนโลยี เพื่อซ่อนปลายทางที่แท้จริงของกองทุนที่ถูกขโมยไป

3.2 ปรากฏการณ์ล้มทั้งยืน (Rug Pull) ความหมายสแลงคือ “การดึงพรมที่มีคนยืนอยู่ซึ่งนั่นทำให้คนหัวทิ่ม” ภาษาอังกฤษ คือ to pull the rug out from under someone. (Angkurlee, 2021) โดย Rug pull เป็นการหลอกลวงอีกรูปแบบหนึ่ง ที่มีการใช้นวัตกรรมล่าสุดใหม่ล่าสุด (Chainalysis, 2021) โดยมีกลไกเกี่ยวข้องกับการหลอกลวงด้วยการใช้ DeFi (Decentralized Financial) ซึ่งเป็นบริการทางการเงินแบบกระจายศูนย์กลางที่ผ่านระบบบล็อกเชน โดยใช้กลไกควบคุมการดำเนินการให้เป็นไปตามเงื่อนไขที่กำหนดผ่านสัญญาอัจฉริยะ (Smart Contract) กับคริปโทเคอร์เรนซี จุดสำคัญของโครงการ DeFi อยู่ที่ความน่าเชื่อถือ ระบบทำงานอย่างถูกต้อง ความน่าเชื่อถือ และความปลอดภัยของเทคโนโลยีเป็นหลัก แตกต่างจากบริการทางการเงินรูปแบบดั้งเดิมที่ความสำคัญจะอยู่ที่การปฏิบัติงานของสถาบันการเงิน (Phawasan, 2022) หลังการระดมเงินลงทุนผู้พัฒนาก็จะละทิ้งโครงการแล้วหนีไปพร้อมกับเงินลงทุนของเหยื่อที่ถูกหลอกให้ลงทุน ซึ่งมักเกิดกับกลุ่มเหยื่อที่ชอบลงทุนในอะไรที่เป็นสิ่งแปลกใหม่และดูน่าจะทำกำไรได้จำนวนมากในระยะเวลาอันสั้น สามารถแบ่งเป็น 2 รูปแบบ คือ 1) กลโกงในด้านสภาพคล่อง (Liquidity Scam) และ 2) การจัดการทางเทคนิค (Technical Manipulation) มีรายละเอียด ดังนี้

1) กลโกงในด้านสภาพคล่อง (Liquidity Scam) เมื่อเหยื่อหลงกลเข้ามาลงทุนมากขึ้นเพราะเห็นว่าเป็นโอกาสดีที่ได้เข้ามาตั้งแต่ช่วงต้น และเมื่อโทเคน (Token) ได้รับความนิยมและมีมูลค่าเพิ่มขึ้น ผู้พัฒนาจะทำการทุ่มเงินเดิมพันทั้งหมดลงไปในคราวเดียวเพื่อทำกำไร จากนั้นจะทำการถ่ายโอนข้อมูลเหล่านี้ออกไป ทำให้โทเคนที่เหยื่อรายอื่น ๆ ถืออยู่ กลายเป็นสกุลเงินดิจิทัลที่ไร้ค่าและไม่มีทางที่จะได้รับเงินคืน (efinanceThai, 2021)

ภาพที่ 3 ตัวอย่างการ Rug Pull เหรียญ Squid Coin
แหล่งที่มา Nation TV (2021)

2) การจัดการทางเทคนิค (Technical Manipulation) เป็นการใช้ประโยชน์จาก Approve Function ของโทเคน ERC-20 บนเครือข่าย Ethereum ซึ่งนักพัฒนาจะดำเนินการแก้ไขฟังก์ชันนี้ให้ผู้ใช้งานสามารถซื้อโทเคนได้เท่านั้น ไม่สามารถขาย หรือ อนโทเคนที่ซื้อมาได้ (efinanceThai, 2021)

3.3 อาชญากรรมที่ใช้มูลค่าทางการเงินของคริปโทเคอร์เรนซีเป็นเครื่องมือในการเป็นตัวกลางแลกเปลี่ยนเงินหรือสิ่งของผิดกฎหมาย อาชญากรรมประเภทนี้จะเป็นอาชญากรรมที่มีความเกี่ยวข้องกับอาชญากรรม 3 ประเภท คือ

1) อาชญากรรมที่เกี่ยวข้องกับองค์กรอาชญากรรม (Organized Crime) ด้วยจุดเด่นของคริปโทเคอร์เรนซีที่สามารถปกปิดตัวตนของผู้ใช้งานได้เป็นอย่างดี ทำให้องค์กรอาชญากรรมใช้คริปโทเคอร์เรนซีเพื่อเป็นเงินทุนสำหรับกิจกรรมของตนตามวิธีการระดมทุนแบบดั้งเดิม (Shacheng Wang & Xixi Zhu, 2021)

2) อาชญากรรมที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ (Cybercrimes) ด้วยความรวดเร็วในการทำธุรกรรมและความสามารถปกปิดตัวตนของผู้กระทำผิดของคริปโทเคอร์เรนซีจึงถูกนำมาใช้เป็นตัวกลางในการเรียกค่าไถ่จาก มัลแวร์เรียกค่าไถ่ (Ransomware) การซื้อขายสิ่งของผิดกฎหมายในเว็บไซต์ตลาดมืด (Dark Web) หรือเพื่อการทำธุรกรรมเพื่อใช้ในการปกปิดตัวตน

3) อาชญากรรมที่เกี่ยวข้องกับการฟอกเงิน (Money Laundering) ผู้กระทำผิดจะทำเป็นขบวนการโดยทำธุรรรมที่มีขั้นตอนเดียวกับการฟอกเงินทั่วไป เพียงแต่เป็นทรัพย์สินที่แปรรูปมีลักษณะไร้รูปร่างที่เป็นรหัสข้อมูลอิเล็กทรอนิกส์ในบล็อกเชนเทคโนโลยี ขั้นตอนแรกผู้กระทำผิดจะแปรรูปเงินที่ได้จากการกระทำผิดเป็นคริปโทเคอร์เรนซี ขั้นตอนต่อมาผู้กระทำผิดจะเกลื่อนร่องรอย (Layering) โดยมีเป้าหมายที่จะไม่ให้ผู้ใดสามารถติดตามเชื่อมโยงเส้นทางธุรกรรมที่ไม่ชอบด้วยกฎหมายกับคริปโท-เคอร์เรนซีที่ได้รับปลายทางได้ เช่น การโอนเงินคริปโทเคอร์เรนซีจากกระเป๋าเงินอิเล็กทรอนิกส์จำนวนมากไขว้กันไปมาหลายรอบ เพราะสามารถดำเนินการได้อย่างรวดเร็ว (Kajchamaporn, 2021) ซึ่งการที่ผู้กระทำผิดใช้คริปโทเคอร์เรนซียังเป็นจุดได้เปรียบ

บทสรุป

การหมวดหมู่ของอาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซีแบ่งออกเป็น 3 ประเภท คือ 1) อาชญากรรมที่มีคริปโทเคอร์เรนซีเป็นเป้าหมาย คือ การขโมยคริปโทเคอร์เรนซีจากกระเป๋าเงินดิจิทัลของผู้ใช้งาน รูปแบบ ขั้นตอน และวิธีการขโมยคริปโทเคอร์เรนซีขึ้นอยู่กับ ผู้ให้บริการแต่ละระดับ และลักษณะของกระเป๋าเงินดิจิทัล 2) อาชญากรรมที่มีคริปโทเคอร์เรนซีเป็นอาวุธ คือ การมุ่งทำลายระบบบล็อกเชน และการแทรกแซงอุปกรณ์ในระบบบล็อกเชน และ 3) อาชญากรรมที่มีคริปโทเคอร์เรนซีเป็นเครื่องมือ คือ การใช้ประโยชน์จากคุณสมบัติเฉพาะของคริปโทเคอร์เรนซีในก่ออาชญากรรม

ในการป้องกันอาชญากรรม พบว่า อาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซีมีพื้นฐานจากอาชญากรรมคอมพิวเตอร์หลากหลายรูป ดังนั้นการป้องกันอาชญากรรมจะไม่แตกต่างจากเดิมมากเท่าใดนัก ในการป้องกันภัยอาชญากรรมโดยการอ้างอิงตามทฤษฎีปกติวิสัย (Routine Activity Theory) ควรเน้นไปที่ลดความเป็นเหยื่ออาชญากรรมที่เหมาะสม (Suitable Target) ให้กับผู้ใช้งานคริปโทเคอร์เรนซี เพราะด้วยการลงทุนในคริปโทเคอร์เรนซีเป็นเทคโนโลยีที่ใหม่ และมีผลตอบแทนที่สูงจึงควรส่งเสริมให้มีการสร้างการรับรู้ ความเข้าใจ ในเทคโนโลยีคริปโทเคอร์เรนซี และพฤติกรรมในการก่ออาชญากรรม และการป้องกันการหลอกให้ลงทุน ในรูปแบบต่าง ๆ เพื่อไม่ให้นักลงทุนเป็นเหยื่อ

ในส่วนของการเสริมสร้างการระวังป้องกันที่ดี (Capability of Guardian) มี 4 ส่วนที่เกี่ยวข้อง ได้แก่ 1) ทรัพยากรมนุษย์ (Human Resources) ในกระบวนการยุติธรรมมีความจำเป็นต้องเสริมสร้างความรู้ความเข้าใจ เพิ่มทักษะ และความสามารถให้กับเจ้าหน้าที่บังคับใช้กฎหมายให้เข้าใจถึงเทคโนโลยีที่เปลี่ยนแปลง 2) เทคโนโลยีในการป้องกันอาชญากรรมและควบคุมอาชญากรรม (Equipment) สร้างฐานข้อมูลกลาง (Big Data) สำหรับธุรกรรมจากผู้ใช้งานและผู้ให้บริการทุกประเภท รวมถึงการพัฒนาเทคโนโลยีในการพิสูจน์หลักฐานทางดิจิทัล เพื่อเพิ่มประสิทธิภาพในการบังคับใช้กฎหมาย 3) ตราหรือปรับปรุงกฎหมายให้มีสภาพบังคับใช้ในการป้องกันอาชญากรรมและในเวลาเดียวกันสามารถส่งเสริมการลงทุนเพื่อเพิ่มขีดความสามารถในการแข่งขันทางเศรษฐกิจของประเทศได้ด้วย และ 4) พัฒนาการบริหารจัดการ เสริมสร้างความร่วมมือกับภาคเอกชนและหน่วยงานบังคับใช้กฎหมายทั้งในและต่างประเทศ เพื่อให้เกิดการบูรณาการในการบังคับใช้กฎหมายอย่างมีประสิทธิภาพ ทั้งเป็นการป้องกันและควบคุมอาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซีที่จะเกิดขึ้นในอนาคต และประการสุดท้ายการบังคับใช้กฎหมายอย่างเข้มข้นเพื่อให้ผู้กระทำผิดที่มีแรงจูงใจ (Motivated Offender) เกิดความยำเกรงทำให้กฎหมายมีสภาพในการยับยั้งการกระทำผิด ผู้กระทำผิดรายใหม่ไม่กล้าจะทำผิดต่อไป

เอกสารอ้างอิง

Angkurlee C. (November 2, 2021). *Get to know `Rug pull`, a dark trick in the DeFi universe.* Retrieved January 3, 2022. From https://www.efinancethai.com/LastestNews/LatestNewsMain.aspx?release=y&ref=M&id=MW9lVHFRQ0d4Q2c9.

Bank of Thailand. (2021). *Payment transactions via Mobile Banking and Internet Banking.* Retrieved January 3, 2022. From https://www.bot.or.th/App/BTWS_STAT/statistics/ReportPage.aspx?reportID=949&language=th.

Binance Academy. (2022). Crypto Wallet Types Explained. Retrieved January 3, 2022. From https://academy.binance.com/en/articles/crypto-wallet-types-explained

Binance Academy. (2022). *What Is Cryptocurrency?.* Retrieved January 3, 2022. From https://academy. binance.com/en/articles/what-is-cryptocurrency.

Binance Academy. (2022. *What Are Nodes?.* Retrieved January 7, 2022. From https://academy. binance.com/en/articles/what-are-nodes.

Bitkub. (2022). *Limitation of Blockchain Technology.* Retrieved January 7, 2022. From https://www.bitkub.com/blog/blockchain-142baeb2db28.

Blockchain.com. (2022). *Total Number of Transactions.* Retrieved January 3, 2022. From https://www.blockchain.com/charts/n-transactions-total.

Chainalysis. (December 16, 2021). *The Biggest Threat to Trust in Cryptocurrency: Rug Pulls Put 2021 Scam Revenue Close to All-time Highs.* Retrieved January 3, 2022. From https://blog.chainalysis.com/reports/2021-crypto-scam-revenues/.

efinanceThai. (November 15, 2021). *Rug Pull Disasters that can happen unexpectedly.* Retrieved January 7, 2022. From https://www.efinancethai.com/Fintech/FintechMain.aspx?release=y&name=ft_202111151542.

Digital Assets Market Status Weekly Report. (2022). Retrieved January 3, 2022. From https://www.sec.or.th/TH/PublishingImages/Pages/DA-WeeklyReport/

Federal Bureau of Investigation (FBI). (April 13, 2020). *FBI Expects a Rise in Scams Involving Cryptocurrency Related to the COVID-19 Pandemic.* Retrieved January 8, 2022. From https://www.fbi.gov/news/pressrel/press-releases/fbi-expects-a-rise-in-scams-involving-cryptocurrency-related-to-the-covid-19-pandemic.

Interpol. (2022). *Cryptojacking.* Retrieved January 7, 2022. From https://www.interpol.int/Crimes/Cybercrime/Cryptojacking.

Kajchamaporn V.. (August 30, 2021). *Money Laundering by Cryptocurrency Transaction.* Retrieved January 7, 2022. From https://so02.tci-thaijo.org/index.php/ibas/article/view/248126.

Khruakham S.. (2015). *Criminology and Criminal Justice.* Nakhonprathom. Thailand.

Kongsanor P.. (2018). *Bitcoin, the virtual currency of the future.* Retrieved January 7, 2022. From https://www.parliament.go.th/ewtadmin/ewt/parliament_parcy/ewt_dl_link.php?nid=47266.

Nation TV. (December 7 2021). *Investigate the truth | "Rug pull" crime in the cryptocurrency world.* Retrieved January 7, 2022. https://www.nationtv.tv/hotclip/378855784.

National Institute of Standards and Technology (NIST) U.S. Department of Commerce. (December 02, 2021). *Post-Quantum Cryptography.* Retrieved January 5, 2022. From https://csrc.nist.gov/Projects/post-quantum-cryptography/post-quantum-cryptography-standardization/Call-for-Proposals.

Phawasun N.. (2022). *Decentralized Finance (DeFi) and Supervision.* Retrieved January 5, 2022. From https://www.sec.or.th/TH/Template3/Articles/2564/070664.pdf.

Siam Commercial Bank. (2021). *Cryptocurrency 101.* Retrieved October 24, 2022. From https://www.scb.co.th/th/personal-banking/stories/grow-your-wealth/cryptocurrency101.html.

Shacheng Wang, Xixi Zhu. (September 7, 2021). *Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing.* Retrieved January 7, 2022. From https://doi.org/10.1093/police/paab059.

Supervision and Examination Division. (2021). *Financial intelligence report on the risks of virtual money on the financial system, economy, investment and opportunity of crime and money laundering.* Retrieved January 7, 2022. From https://sed.amlo.go.th/uploads/content_attachfile/attach_202007210835_5f1646564f0b7.pdf

The Securities and Exchange Commission (Thailand). (2021). *Digital Assets.* Retrieved December 30, 2021. From https://www.sec.or.th/digitalasset.

Thailand Institute of Occupational Safety and Health (Public Organization). (2022). *New Normal Lifestyle.* Retrieved January 7, 2022. From http://www.tosh.or.th/covid-19/index.php/new-normal.

The Decree of the business of digital assets in 2561. (2019, May 13). *Royal Thai Government Gazette.* Volumes 135 Episodes 33 ก. Pages 43 – 70.

U.S. Department of Justice. (2012). *Computer Crimes.* Retrieved January 7, 2022. From https://www.ojp.gov/ncjrs/virtual-library/abstracts/computer-crimes-7.

ประวัติผู้เขียน

คำนำหน้า ชื่อ-สกุล **ว่าที่ร้อยตำรวจโท เจษฎาพงษ์ ค้ำชู ***
ตำแหน่ง/สถานะ นักศึกษาหลักสูตรปรัชญาดุษฎีบัณฑิต
สาขาอาชญาวิทยาการบริหารงานยุติธรรมและสังคม
ที่อยู่หน่วยงาน/สังกัด คณะสังคมศาสตร์และมนุษยศาสตร์ มหาวิทยาลัยมหิดล
25/25 หมู่ 5 ถนนพุทธมณฑล สาย 4 ตำบลศาลายา
อำเภอพุทธมณฑล จังหวัดนครปฐม 73170
ไปรษณีย์อิเล็กทรอนิกส์ chetsadaphong.d@gmail.com

* ผู้ประพันธ์บรรณกิจ (Corresponding Author)