

มาตรการในการควบคุมการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล



คู่มือฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตร

นิติศาสตรดุษฎีบัณฑิต

คณะนิติศาสตร์

สถาบันบัณฑิตพัฒนบริหารศาสตร์

2565

มาตรการในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล

พงศ์จิรา เชิดชู

คณะนิติศาสตร์

..... อาจารย์ที่ปรึกษาวิทยานิพนธ์หลัก  
(อาจารย์ ดร.อัญธิกา ณ พิบูลย์)

คณะกรรมการสอบวิทยานิพนธ์ ได้พิจารณาแล้วเห็นสมควรอนุมัติให้เป็นส่วนหนึ่งของ  
การศึกษาตามหลักสูตรนิติศาสตรดุษฎีบัณฑิต

..... ประธานกรรมการ  
(ศาสตราจารย์ณรงค์ ใจหาญ)

..... กรรมการ  
(ศาสตราจารย์ ดร.พินัย ณ นคร)

..... กรรมการ  
(รองศาสตราจารย์ ดร.ปกป้อง ศรีสนิท)

..... กรรมการ  
(อาจารย์ ดร.อัญธิกา ณ พิบูลย์)

..... กรรมการ  
(อาจารย์ ดร.ธนัทเทพ เขียรประสิทธิ์)

## บทคัดย่อ

ชื่อคุณิพนธ์	มาตรการในการควบคุมการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล
ชื่อผู้เขียน	นางสาวพงศ์จิรา เขตชู
ชื่อปริญญา	นิติศาสตรคุณิบัณฑิต
ปีการศึกษา	2565

คุณิพนธ์นี้มีวัตถุประสงค์เพื่อแสวงหามาตรการที่เหมาะสมในการควบคุมการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัล สืบเนื่องจากปัจจุบันการใช้หรือการถือครองสกุลเงินดิจิทัลในภาคประชาชนยังปราศจากกลไกการควบคุมทางกฎหมาย หากมีการนำไปใช้หรือได้มาโดยมิชอบอาจส่งผลเสียหายต่อระบบเศรษฐกิจและสังคมโดยรวมได้ จากการศึกษาถึงกฎหมายและมาตรการทางอาญาที่เกี่ยวข้องพบประเด็นปัญหาที่สำคัญ คือ ปัญหาความไม่ชัดเจนเกี่ยวกับสถานะทางกฎหมายของสกุลเงินดิจิทัล ปัญหาฐานความผิดตามกฎหมายที่มีอยู่ไม่ครอบคลุมถึงกรณีการขโมยสกุลเงินดิจิทัลและกรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นโดยมิชอบ และปัญหาความร่วมมือทางอาญาระหว่างประเทศ จึงนำมาสู่การแสวงหามาตรการที่เหมาะสมโดยการมีกฎหมายสารบัญญัติที่ชัดเจน เพื่อให้การบังคับใช้กฎหมายเป็นไปอย่างมีประสิทธิภาพ ควบคู่ไปกับการใช้มาตรการความร่วมมือทางอาญาระหว่างประเทศได้อย่างมีประสิทธิภาพและสอดคล้องกับหลักสากล โดยวิเคราะห์กฎหมายภายใน กฎหมายต่างประเทศ มาตรการความร่วมมือทางอาญาระหว่างประเทศ และใช้วิธีดำเนินการวิจัยเชิงคุณภาพ ด้วยการวิจัยเอกสารและรวบรวมข้อมูลที่เกี่ยวข้องจากหนังสือ งานวิจัย ตัวอย่างกฎหมาย ตำรา วารสาร บทความ คำพิพากษาฎีกา

ข้อเสนอแนะของคุณิพนธ์นี้ ประกอบด้วยข้อเสนอแนะทางกฎหมาย คือ ควรกำหนดสถานะทางกฎหมายให้กับสกุลเงินดิจิทัลไว้เป็นการเฉพาะ และเพิ่มเติมบทบัญญัติกรณีที่ยังเป็นช่องว่างทางกฎหมายให้เป็นความผิดอาญา ส่วนข้อเสนอแนะอื่น ๆ ผู้เขียนได้เสนอให้ควรมีการส่งเสริมการแลกเปลี่ยนความรู้ ทักษะที่จำเป็นในการป้องกันและปราบปรามอาชญากรรมเกี่ยวกับสกุลเงินดิจิทัลให้แก่เจ้าหน้าที่ที่เกี่ยวข้อง และควรให้ความรู้แก่ประชาชนในการใช้งานและการถือครองสกุลเงินดิจิทัลอย่างปลอดภัย รวมถึงควรมีการรวบรวมแนวปฏิบัติความร่วมมือทางอาญาระหว่างประเทศทั้งรูปแบบที่เป็นทางการและไม่เป็นทางการ เพื่อให้การควบคุมการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลภายใต้กรอบของกฎหมายอาญาเป็นไปอย่างมีประสิทธิภาพ



## ABSTRACT

<b>Title of Dissertation</b>	Legal Measures Controlling Crimes Against Cryptocurrency
<b>Author</b>	Miss Pongjira Cherdchoo
<b>Degree</b>	Doctor of Laws
<b>Year</b>	2022

---

The purpose of this thesis is to explore and find appropriate measures to control crimes relating to cryptocurrencies. At present, the use or possession of cryptocurrencies among the general public are, yet, without any legal control mechanisms, and as such the abuse or illegal acquisition of such currencies could lead to catastrophic ramifications of the overall economic system and the society. According to the study of the relevant legislation and criminal measures, key issues on this topic include: the ambiguity of the legal status of cryptocurrencies, incomprehensible offences under the law which does not cover theft of cryptocurrencies and abuse of another person's computer resources, as well as the issue relating to international cooperation. As a result, the appropriate measures in response to those issues have been explored and concluded that there should be explicit substantive legislation on the matter to ensure standardized enforcement of the laws, along with the effective implementation of mutual legal assistance in criminal matters consistent with international principles. Internal laws, domestic laws, instrument of mutual legal assistance in criminal matters will be analyzed. Also, qualitative research will be conducted by various means i.e., documentary research and gathering of information from different literature, including books, researches, statutes, textbooks, magazines, articles, and the Supreme Court decisions.

The proposal of this thesis consists of legal suggestions i.e., the legal status of cryptocurrencies should be specifically given, with enactment of additional statutory provisions to fulfill the current loopholes of the law so that certain acts are criminalized. Also, as for other suggestions, it is proposed that there should be

activities for relevant officers to promote the exchange of knowledge and expertise required to prevent and suppress crimes relating to cryptocurrencies. In addition, there should be outreach activities for the general public on how to securely use and own cryptocurrencies. Practical guidelines on mutual legal assistance in criminal matters via both formal and informal channels should also be gathered. This is to ensure effective control of crimes relating to cryptocurrencies under the scope of criminal law.



## กิตติกรรมประกาศ

ดุชฎินิพนธ์ฉบับนี้จะเกิดขึ้นมิได้หากไม่ได้รับคำแนะนำจากศาสตราจารย์ณรงค์ ใจหาญ ขอขอบพระคุณท่านเป็นอย่างสูงที่กรุณาให้คำแนะนำมาตั้งแต่ต้นจนสำเร็จลุล่วงและกรุณารับเป็น ประธานกรรมการสอบดุชฎินิพนธ์ ขอขอบพระคุณศาสตราจารย์พินัย ณ นคร และรองศาสตราจารย์ ดร.ปกป้อง ศรีสนิท เป็นอย่างยิ่งที่กรุณารับเป็นกรรมการสอบดุชฎินิพนธ์และได้ให้คำแนะนำ ข้อคิดเห็น ทางวิชาการด้วยความเมตตาเป็นอย่างยิ่ง ขอขอบพระคุณอาจารย์ ดร.ธนัทเทพ เสียรประสิทธิ์ ที่กรุณา รับเป็นกรรมการสอบและตรวจสอบแก้ไขเนื้อหาให้มีความสมบูรณ์ยิ่งขึ้น

ขอขอบพระคุณ อาจารย์ ดร.อัญธิกา ณ พิบูลย์ อาจารย์ที่ปรึกษา ที่ได้สละเวลาอันมีค่าให้ คำปรึกษา ตลอดจนได้ตรวจสอบและแก้ไขข้อบกพร่องต่าง ๆ ที่เป็นประโยชน์ในการศึกษา ยิ่ง และทำให้ ดุชฎินิพนธ์ฉบับนี้สำเร็จลงได้ด้วยดี

ขอขอบคุณรองศาสตราจารย์ ดร.ปวีณี ไพรทอง ผู้ช่วยศาสตราจารย์ ดร.สุพัชรา แผนวิจิต ผู้ช่วยศาสตราจารย์ ดร.ธีรเดช มโนลีหกุล ผู้ช่วยศาสตราจารย์ ดร.วรรณวิภา เมืองถ้ำ ผู้ช่วย ศาสตราจารย์ ดร.สาธิตา วิมลคุณารักษ์ ผู้ช่วยศาสตราจารย์ ดร.สิริกานต์ อยู่เรือง คุณศิวดี เกิดเจริญ ที่ คอยช่วยเหลือและเป็นกำลังใจในการทำดุชฎินิพนธ์เล่มนี้ตลอดมา

ขอขอบพระคุณคุณพ่อ คุณแม่ พี่อ๊อฟ ที่ให้กำลังใจ ให้ความคิดและสติปัญญาหล่อหลอมมาเป็น ผู้เขียนได้ถึงทุกวันนี้ ท้ายที่สุดขอขอบคุณคุณภรรยา อนันตชัย ที่เข้าใจ เป็นกำลังใจทุกช่วงเวลาในการทำ ดุชฎินิพนธ์ และคอยช่วยเหลือทุก ๆ ด้าน ตลอดมา

พงศ์จิรา เขตชู

มกราคม 2566

## สารบัญ

	หน้า
บทคัดย่อ.....	ค
ABSTRACT.....	จ
กิตติกรรมประกาศ.....	ช
สารบัญ.....	ช
สารบัญตาราง.....	ฐ
สารบัญภาพ.....	ท
บทที่ 1 บทนำ.....	1
1.1 ที่มาและความสำคัญ.....	1
1.2 วัตถุประสงค์งานวิจัย.....	5
1.3 ขอบเขตงานวิจัย.....	6
1.4 คำถามงานวิจัย.....	6
1.5 สมมติฐานงานวิจัย.....	7
1.6 ระเบียบวิธีวิจัย.....	7
1.7 ประโยชน์ที่คาดว่าจะได้รับ.....	8
บทที่ 2 แนวคิด ลักษณะ และการควบคุมเงินตราและสกุลเงินดิจิทัล.....	9
2.1 แนวคิด ความเป็นมาและลักษณะทั่วไปของเงินตรา.....	9
2.1.1 แนวคิดพื้นฐานและลักษณะทั่วไปของเงินตรา.....	10
2.1.1.1 วิวัฒนาการของเงินตราในประเทศไทย.....	10
2.1.1.2 ความหมายของเงินตรา.....	12
2.1.1.3 คุณสมบัติและหน้าที่ของเงินตรา.....	13
2.1.1.4 รูปแบบของเงินตรา.....	15

2.1.2 แนวคิดในการควบคุมเงินตรา.....	18
2.1.2.1 หน่วยงานที่เกี่ยวข้องกับการควบคุมเงินตรา .....	18
2.1.2.2 กฎหมายที่เกี่ยวข้องกับการควบคุมเงินตรา.....	19
2.2 แนวคิด ความเป็นมาและลักษณะของสกุลเงินดิจิทัล (Virtual Currency/ Cryptocurrency).....	25
2.2.1 แนวคิดพื้นฐานและลักษณะทั่วไปของสกุลเงินดิจิทัล .....	25
2.2.1.1 ประวัติ ความเป็นมาของสกุลเงินดิจิทัล.....	25
2.2.1.2 ความหมายของสกุลเงินดิจิทัล.....	27
2.2.1.3 การยอมรับและสถานะของสกุลเงินดิจิทัล.....	29
2.2.1.4 แนวคิดเกี่ยวกับบล็อกเชน .....	33
2.2.1.5 สกุลเงินดิจิทัลในปัจจุบัน .....	36
2.2.1.6 แนวโน้มการใช้สกุลเงินดิจิทัล.....	42
2.2.1.7 ประโยชน์และข้อจำกัดของสกุลเงินดิจิทัล.....	43
2.2.2 แนวคิดในการควบคุมสกุลเงินดิจิทัล.....	49
2.2.2.1 หน่วยงานที่เกี่ยวข้องกับการควบคุมสกุลเงินดิจิทัล .....	49
2.2.2.2 กฎหมายที่เกี่ยวข้องกับสกุลเงินดิจิทัล.....	51
2.2.2.3 ประเด็นปัญหาสถานะทางกฎหมายอาญาของสกุลเงินดิจิทัลในประเทศไทย.....	57
2.3 แนวคิดในการควบคุมการกระทำความผิดทางอาญาเกี่ยวกับสกุลเงินดิจิทัล .....	60
2.3.1 ความหมายและวัตถุประสงค์ของกฎหมายอาญา.....	61
2.3.1.1 ความหมายของกฎหมายอาญา .....	61
2.3.1.2 วัตถุประสงค์ของกฎหมายอาญา .....	62
2.3.2 หลักเกณฑ์การบัญญัติความผิดทางอาญา.....	64
2.3.2.1 หลักเกณฑ์ตามนโยบายในการบัญญัติกฎหมายอาญาของรัฐ.....	65
2.3.2.2 หลักเกณฑ์การคุ้มครองนิติสมบัติในวิธีทางสุดท้าย .....	65

2.3.2.3	หลักเกณฑ์การบัญญัติความผิดอาญาของ Nigel Walker.....	66
2.3.2.4	หลักเกณฑ์การบัญญัติความผิดอาญาของ Herbert L. Packer.....	69
2.3.2.5	หลักเกณฑ์การบัญญัติความผิดอาญาของ Lon Fuller.....	71
2.3.2.6	หลักเกณฑ์การบัญญัติความผิดอาญาของ Douglas Husak.....	71
2.4	รูปแบบการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล .....	73
2.4.1	การเจาะข้อมูล/การโจรกรรม (Hack/Theft).....	73
2.4.2	การใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล (Cryptojacking).....	76
บทที่ 3	หลักกฎหมายต่างประเทศและหลักกฎหมายประเทศไทยเกี่ยวกับการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล .....	79
3.1	หลักกฎหมายในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลของสหรัฐอเมริกา.....	80
3.1.1	สถานะของสกุลเงินดิจิทัล .....	80
3.1.1.1	คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (Security and Exchange Commission).....	80
3.1.1.2	สำนักงานคณะกรรมการกำกับการซื้อขายสินค้าโภคภัณฑ์ (Commodity Futures Trading Commission) .....	81
3.1.1.3	เครือข่ายการบังคับใช้กฎหมายอาชญากรรมทางการเงิน (Financial Crime Enforcement Network) .....	82
3.1.1.4	กรมสรรพากร (The Internal Revenue Service) .....	82
3.1.2	ความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล .....	83
3.1.3	กฎหมายเกี่ยวกับการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล.....	84
3.2	หลักกฎหมายในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลของสหราชอาณาจักร (อังกฤษ).....	89
3.2.1	สถานะของสกุลเงินดิจิทัล .....	89
3.2.2	ความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล .....	91

3.2.3 กฎหมายเกี่ยวกับการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล	93
3.2.3.1 Theft Act 1968.....	93
3.2.3.2 The Computer Misuse Act 1990.....	97
3.3 หลักกฎหมายในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลของประเทศไทย.....	102
3.3.1 สถานะทางกฎหมายของสกุลเงินดิจิทัล.....	102
3.3.2 ความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล.....	103
3.3.3 กฎหมายเกี่ยวกับการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล.....	104
3.3.3.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550.....	104
3.3.3.2 ประมวลกฎหมายอาญา.....	116
3.4 ความร่วมมือทางอาญาระหว่างประเทศเกี่ยวกับสกุลเงินดิจิทัล.....	124
3.4.1 ความร่วมมือทางอาญาระหว่างประเทศรูปแบบอนุสัญญา.....	124
3.4.1.1 อนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ (Convention on Cybercrime).....	124
3.4.2 ความร่วมมือทางอาญาระหว่างประเทศรูปแบบองค์กร.....	131
3.4.2.1 สำนักงานป้องกันยาเสพติดและปราบปรามอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime (UNODC)).....	131
3.4.2.2 คณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน Financial Action Task Force (FATF).....	136
3.4.2.3 ตำรวจสากล (Interpol).....	140
บทที่ 4 วิเคราะห์ปัญหาทางกฎหมายเกี่ยวกับการกระทำความผิดอาญา ที่เกี่ยวกับสกุลเงินดิจิทัล	146
4.1 ปัญหาเกี่ยวกับสถานะของสกุลเงินดิจิทัล.....	146
4.2 ปัญหาฐานความผิดเกี่ยวกับสกุลเงินดิจิทัล.....	156

4.3 ปัญหาความร่วมมือทางอาญาระหว่างประเทศเกี่ยวกับการกระทำความผิดอาญาที่เกี่ยวข้อง  
กับสกุลเงินดิจิทัล ..... 168

บทที่ 5 บทสรุปและข้อเสนอแนะ ..... 172

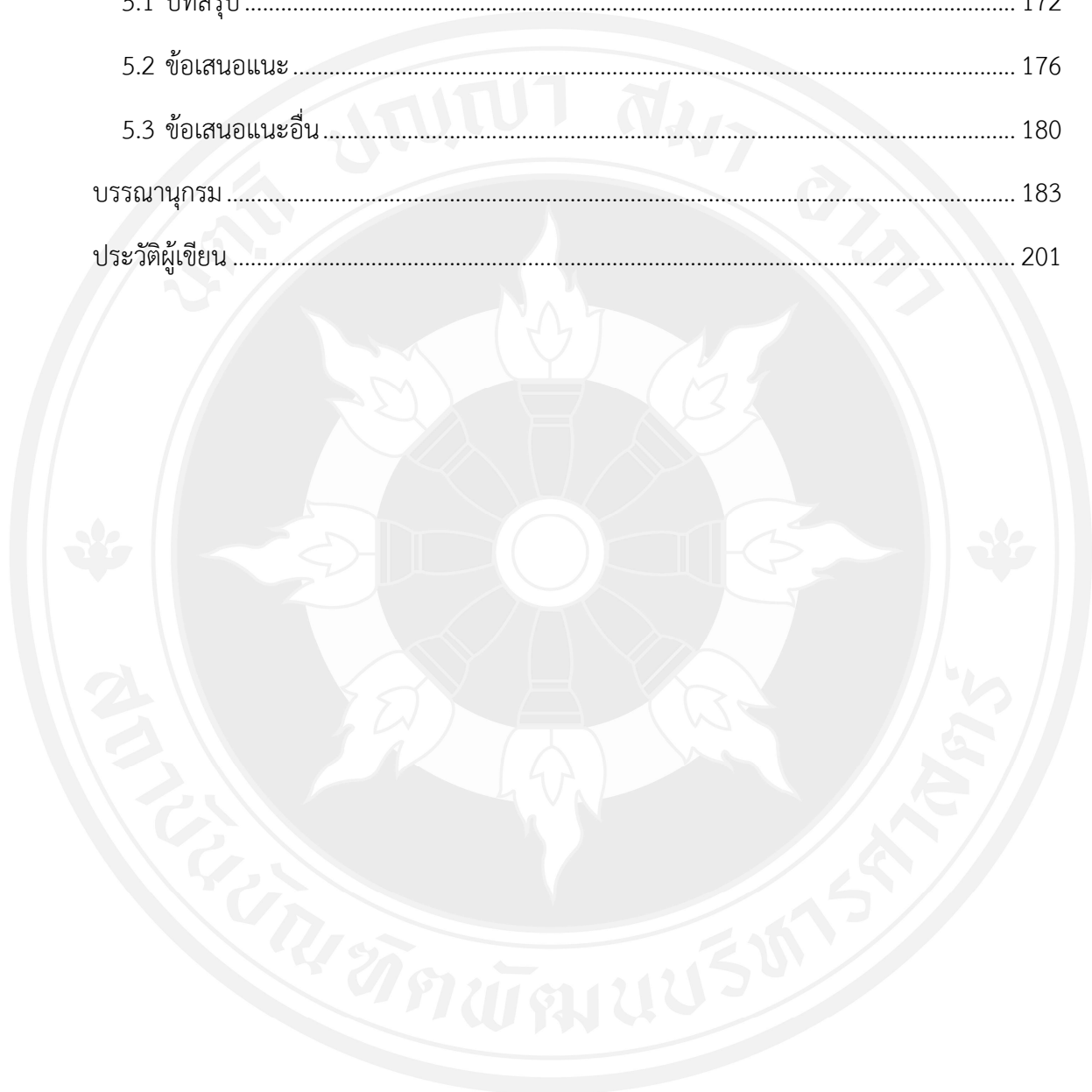
5.1 บทสรุป ..... 172

5.2 ข้อเสนอแนะ ..... 176

5.3 ข้อเสนอแนะอื่น ..... 180

บรรณานุกรม ..... 183

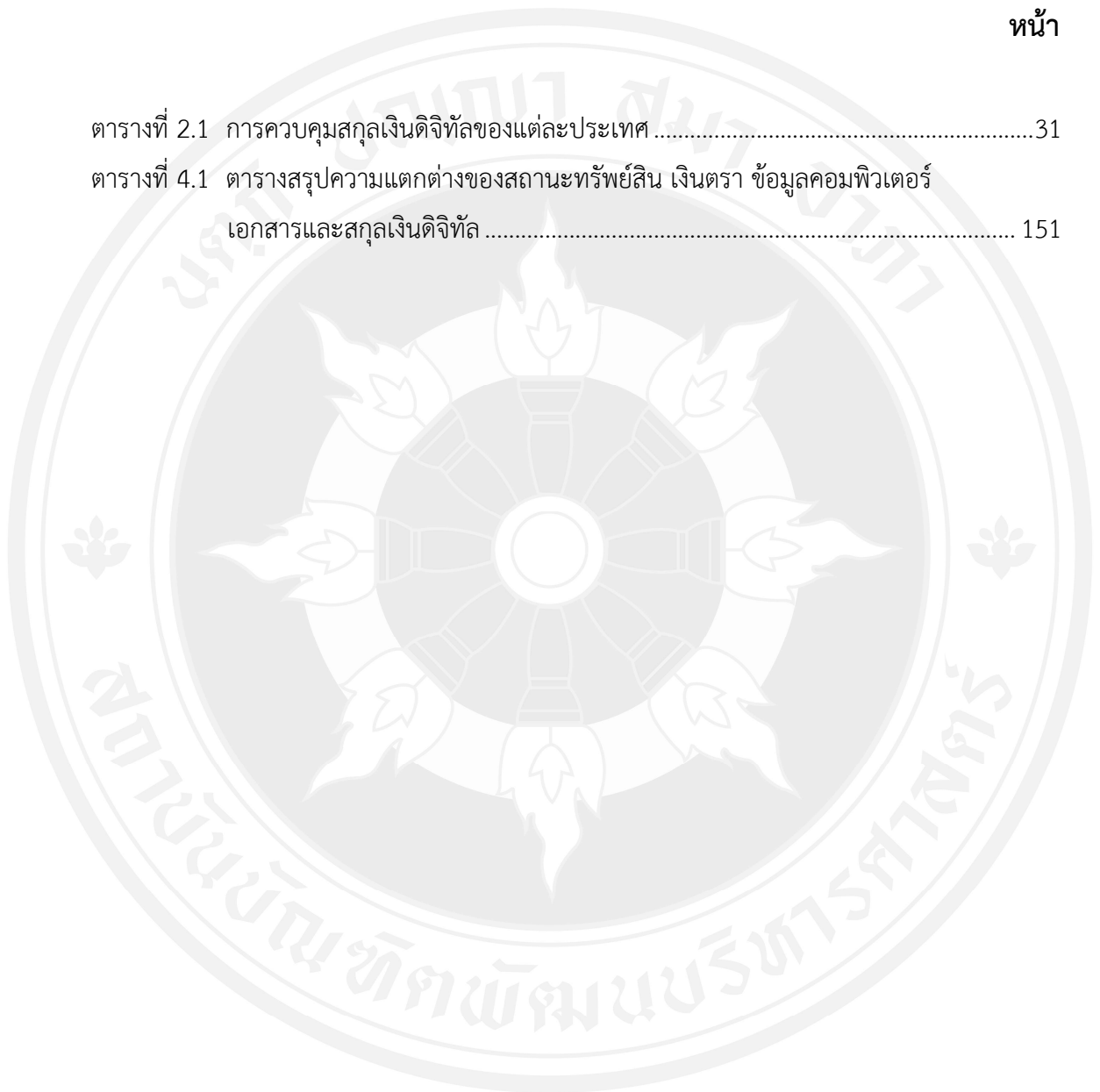
ประวัติผู้เขียน ..... 201



## สารบัญตาราง

หน้า

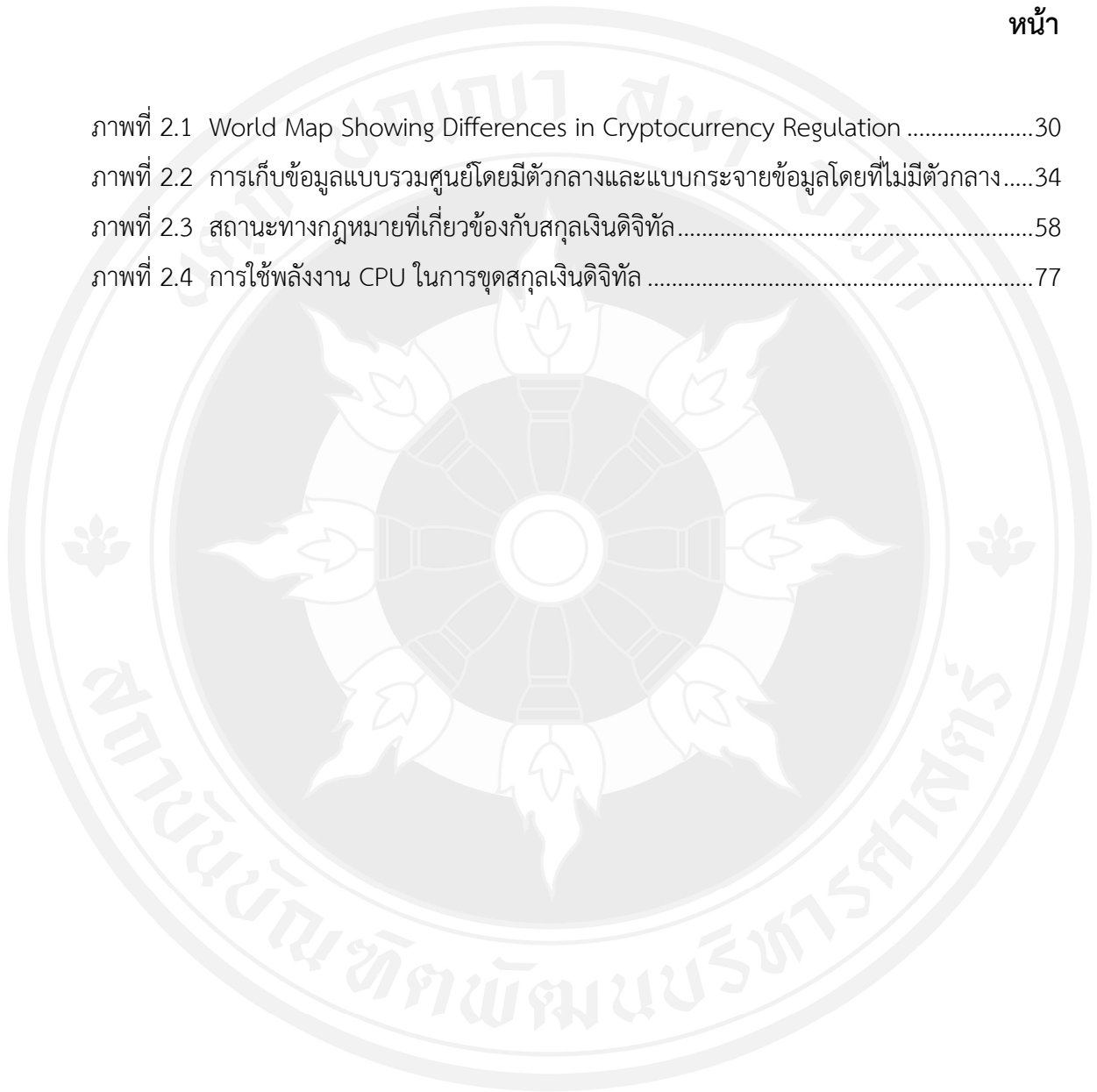
ตารางที่ 2.1 การควบคุมสกุลเงินดิจิทัลของแต่ละประเทศ.....	31
ตารางที่ 4.1 ตารางสรุปความแตกต่างของสถานะทรัพย์สิน เงินตรา ข้อมูลคอมพิวเตอร์ เอกสารและสกุลเงินดิจิทัล .....	151



## สารบัญภาพ

หน้า

ภาพที่ 2.1	World Map Showing Differences in Cryptocurrency Regulation .....	30
ภาพที่ 2.2	การเก็บข้อมูลแบบรวมศูนย์โดยมีตัวกลางและแบบกระจายข้อมูลโดยที่ไม่มีตัวกลาง.....	34
ภาพที่ 2.3	สถานะทางกฎหมายที่เกี่ยวข้องกับสกุลเงินดิจิทัล.....	58
ภาพที่ 2.4	การใช้พลังงาน CPU ในการขุดสกุลเงินดิจิทัล .....	77



# บทที่ 1

## บทนำ

### 1.1 ที่มาและความสำคัญ

เงินตราเป็นสิ่งที่มนุษย์สมมติให้มีมูลค่าเพื่อใช้เป็นสื่อกลางในการซื้อขายแลกเปลี่ยนสินค้าและบริการต่าง ๆ โดยเริ่มตั้งแต่ในอดีตมีการนำเปลือกหอย แร่โลหะต่าง ๆ ที่หายากมาใช้เป็นเงินตรา แต่เนื่องจากวัสดุที่นำมาผสมเป็นเงินตรานั้นมีน้ำหนักมาก ไม่เหมาะแก่การพกพาในการทำธุรกรรม จึงได้มีการพัฒนาเงินตราให้อยู่ในรูปของกระดาษที่เรียกว่าธนบัตรและโลหะที่มีน้ำหนักเบาเรียกว่าเหรียญกษาปณ์ ทั้งนี้ไม่ว่าเงินตราจะอยู่ในรูปแบบหรือลักษณะใด แต่คุณค่าที่สำคัญของเงินตราคือ เป็นสิ่งที่รัฐกำหนดสถานะให้เป็นเงินตราและสามารถใช้เพื่อชำระหนี้ได้ตามกฎหมาย อย่างไรก็ตาม วิวัฒนาการของเงินตรายังคงดำเนินอยู่อย่างต่อเนื่องประกอบปัจจุบันเศรษฐกิจและสังคมถูกขับเคลื่อนด้วยเทคโนโลยี ทำให้สังคมเปลี่ยนแปลงไปเป็นสังคมดิจิทัลที่มีการใช้เทคโนโลยีเพื่อพัฒนาประเทศในด้านต่าง ๆ รวมถึงด้านการเงินที่ได้มีการนำเทคโนโลยีดิจิทัลผนวกกัน เพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าบริการต่าง ๆ ในโลกออนไลน์ นอกเหนือไปจากธนบัตรหรือเหรียญกษาปณ์ที่ใช้กันในชีวิตประจำวัน สิ่งดังกล่าวเรียกว่า “สกุลเงินดิจิทัล” หรือ “เงินเสมือน” (Virtual Currency)

สกุลเงินดิจิทัลหรือเงินเสมือนมีลักษณะที่สำคัญ คือ เป็นสกุลเงินที่ถูกสร้างขึ้นในรูปแบบสถาปัตยกรรมระบบคอมพิวเตอร์ มูลค่าของสกุลเงินดิจิทัลนั้นขึ้นอยู่กับความต้องการของผู้ใช้ในระหว่างผู้ใช้ด้วยกันสามารถทำธุรกรรมได้โดยตรง (Peer to Peer) ในช่องทางออนไลน์ โดยไม่ผ่านตัวกลางหรือธนาคารจึงไม่อยู่ภายใต้การกำกับดูแลของรัฐบาลประเทศใด และไม่ได้มีทุนสำรองเป็นสินทรัพย์หรือทองคำไว้สำหรับเป็นหลักประกันมูลค่าแต่อย่างใด การทำธุรกรรมนั้นไม่ต้องระบุตัวตนที่แท้จริง จึงมีความเป็นส่วนตัวสูง สะดวก รวดเร็วสามารถเข้าถึงได้ทั่วโลก และยังสามารถติดตามความเคลื่อนไหวของธุรกรรมที่เกิดขึ้นได้ภายใต้ระบบที่เรียกว่า Distributed Ledger Technology (DLT) ที่มีการแยกข้อมูลแต่ละประเภทเป็นส่วน ๆ โดยให้ผู้ที่อยู่ในเครือข่ายเก็บไว้ในโหนด (Node) ซึ่งแต่ละธุรกรรมจะแบ่งเป็นบล็อกที่สามารถเชื่อมต่อกันได้ (Blockchain) ผู้ใช้สามารถตรวจสอบข้อมูลได้ตั้งแต่อดีตจนถึงปัจจุบัน ระบบดังกล่าวจึงมีความปลอดภัยในการจัดเก็บข้อมูลสูง ยากต่อแฮ็กหรือการแก้ไขข้อมูลที่ไม่ได้ผ่านระบบอย่างถูกต้อง อีกทั้งยังเสียค่าธรรมเนียมน้อยกว่าการเงินในระบบเงินตรา

ที่ต้องทำธุรกรรมผ่านธนาคาร ด้วยเหตุนี้จึงทำให้คนทั่วไปนิยมใช้สกุลเงินดิจิทัลเป็นสื่อกลางในการแลกเปลี่ยนสินค้า บริการและสะสมเพื่อเก็งกำไร<sup>1</sup> เพิ่มมากขึ้น สกุลเงินดิจิทัลจึงเปรียบเสมือนเป็นอีกทางเลือกหนึ่งในการใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการในระบบเศรษฐกิจ สกุลเงินดิจิทัลที่เป็นที่รู้จักได้แก่ บิตคอยน์ (Bitcoin) อีเทอร์เรียม (Ethereum) ริพเพิล (Ripple) เป็นต้น และยังมีสกุลเงินดิจิทัลที่เกิดขึ้นใหม่และหมุนเวียนอยู่ในตลาดอีกกว่า 10,000 สกุล<sup>2</sup>

อย่างไรก็ตามความนิยมในการใช้ที่เพิ่มมากขึ้นนี้กลับพบว่ามีผลกระทบต่อความผิดทางอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลมีมากขึ้นด้วยเช่นกัน เนื่องจากคุณสมบัติของสกุลเงินดิจิทัลที่รักษาความเป็นส่วนตัวสูงสามารถใช้งานในระบบออนไลน์ได้ จึงสะดวก รวดเร็วและสามารถทำธุรกรรมข้ามพรมแดนได้ ทำให้ยากต่อการติดตามตัวผู้กระทำความผิด อาชญากรจึงมักใช้สกุลเงินดิจิทัลเป็นช่องทางและใช้เป็นเครื่องมือในการกระทำความผิดหลากหลายรูปแบบ เช่น การค้ายาเสพติด การค้าอาวุธสิ่งผิดกฎหมายต่าง ๆ การสนับสนุนองค์กรก่อการร้าย การโจรกรรม การหลอกลวง การข่มขู่โดยเรียกค่าไถ่ เป็นสกุลเงินดิจิทัล การกระทำความผิดกล่าวลวงแล้วแต่สร้างความเสียหายเป็นจำนวนเงินมหาศาล ส่งผลกระทบต่อความเชื่อมั่นของผู้ใช้หรือผู้ที่ถือครองในระบบเศรษฐกิจอย่างยิ่ง<sup>3</sup>

ปัจจุบันประเทศไทยแม้จะยังมิได้ยอมรับให้สกุลเงินดิจิทัลมีสถานะเป็นเงินตราที่สามารถชำระหนี้ได้ตามกฎหมาย แต่ก็ไม่ได้ห้ามมิให้ใช้สกุลเงินดิจิทัล ทำให้ประชาชนทั่วไปสามารถใช้ ถือครอง แลกเปลี่ยนเสมือนเป็นสื่อกลางและเก็งกำไรได้ ดังนั้นหากมีการนำไปใช้ในทางที่มีขอบอาจก่อให้เกิดความเสียหายแก่บุคคล เศรษฐกิจและสังคมได้ จึงจำเป็นต้องมีการควบคุมการกระทำความผิดที่เกี่ยวกับสกุลเงินดิจิทัล ทั้งนี้ผู้เขียนได้แบ่งประเด็นปัญหาในการศึกษาไว้ดังนี้

1) ปัญหาสถานะทางกฎหมายของสกุลเงินดิจิทัล ปัจจุบันกฎหมายอาญาของประเทศไทยยังไม่ได้มีการกำหนดสถานะที่ชัดเจนให้กับสกุลเงินดิจิทัล ทำให้เกิดความไม่ชัดเจนว่าหากมีการกระทำความผิดที่เกี่ยวกับสกุลเงินดิจิทัลเกิดขึ้นแล้ว จะนำกฎหมายของสถานะใดมาบังคับใช้

<sup>1</sup> Edward Castronova, **The Price of 'Man' and 'Woman': A Hedonic Pricing Model of Avatar Attributes in a Synthetic World**, Retrieved November 26, 2020 from <https://ssrn.com/abstract=415043>

<sup>2</sup> Statista, **Number of Cryptocurrencies Worldwide from 2013 to 2022**, Retrieved January 5, 2023 from <https://www.statista.com/statistics/863917/number-crypto-coins-tokens/>

<sup>3</sup> United States Department of Justice, **Attorney General's Cyber-Digital Task Force: Cryptocurrency: An Enforcement Framework 2020**, Retrieved November 28, 2020 from <https://www.justice.gov/archives/ag/page/file/1326061>

ทั้งนี้ต้องพิจารณาถึงลักษณะทางกายภาพและลักษณะการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลว่ามีความเหมาะสมจะเป็นสถานะใด ซึ่งมีข้อพิจารณา ดังนี้

(1) สกุลเงินดิจิทัลเป็นวัตถุไม่มีรูปร่างที่มีมูลค่า เมื่อพิจารณาจากลักษณะทางกายภาพแล้วอาจมีสถานะเป็น “ทรัพย์สิน” ได้ จึงต้องนำบทบัญญัติความผิดอาญาเกี่ยวกับทรัพย์สินในประมวลกฎหมายอาญาลักษณะ 12 มาปรับใช้ แต่ความผิดในลักษณะ 12 นี้ ได้กำหนดองค์ประกอบความผิดให้มีทั้ง “ทรัพย์” และ “ทรัพย์สิน” ปะปนแตกต่างกันไปตามแต่ละฐานความผิดคือ ความผิดที่มีองค์ประกอบเป็นทรัพย์สิน ได้แก่ ความผิดฐานกรรโชก ความผิดฐานฉ้อโกง ส่วนความผิดที่มีองค์ประกอบความผิดเป็น “ทรัพย์” ได้แก่ ลักทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ จึงมีปัญหว่าหากสกุลเงินดิจิทัลมีสถานะเป็นทรัพย์สินแล้ว จะนำฐานความผิดที่มีองค์ประกอบเป็นทรัพย์สินไปใช้ได้เท่านั้น ส่วนฐานความผิดที่มีองค์ประกอบเป็นทรัพย์ ไม่อาจนำมาใช้ได้ ทั้งที่ความผิดที่ทรัพย์เป็นองค์ประกอบสามารถเกิดขึ้นกับสกุลเงินดิจิทัลได้เช่นกัน

(2) สกุลเงินดิจิทัลมีคุณสมบัติในการใช้เป็นสื่อกลางในการแลกเปลี่ยนได้เสมือนกับเงินตรา จึงมีสถานะใกล้เคียงกับ “เงินตรา” แต่เนื่องจากประเทศไทยยังไม่ยอมรับให้สกุลเงินดิจิทัลมีสถานะเป็นเงินตราที่สามารถชำระหนี้ได้ตามกฎหมาย (Legal Tender) และกฎหมายยังกำหนดให้เงินตราต้องมีลักษณะเป็นธนบัตรหรือเหรียญกษาปณ์ ในขณะที่สกุลเงินดิจิทัลเป็นวัตถุที่ไม่มีรูปร่างไม่มีลักษณะเป็นธนบัตรหรือเหรียญกษาปณ์ จึงไม่ใช่เงินตราตามกฎหมาย อีกทั้งการกระทำความผิดอาญาที่เกี่ยวกับเงินตราที่บัญญัติไว้ในหมวด 7 แห่งประมวลกฎหมายอาญา เช่นความผิดฐานปลอมแปลง ทำให้น้ำหนักของเหรียญกษาปณ์ลดลง ฯลฯ เป็นความผิดที่ไม่สามารถเกิดขึ้นกับสกุลเงินดิจิทัล สถานะเงินตราจึงไม่สามารถนำมาปรับใช้กับความผิดเกี่ยวกับสกุลเงินดิจิทัลได้

(3) สกุลเงินดิจิทัลเป็นสิ่งที่ประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์และสามารถรับรู้โดยผ่านอุปกรณ์ที่เชื่อมต่อกับระบบอินเทอร์เน็ตจึงอาจมีสถานะเป็น “ข้อมูลคอมพิวเตอร์”<sup>4</sup> จึงต้องนำพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์มาปรับใช้กับความผิดที่กระทำต่อข้อมูลคอมพิวเตอร์ แต่การกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลนั้นเป็นความผิดที่มีลักษณะเฉพาะซึ่งมีความแตกต่างจากความผิดเกี่ยวกับคอมพิวเตอร์ จึงไม่อาจนำความผิดเกี่ยวกับคอมพิวเตอร์มาปรับใช้ได้ทุกกรณี

(4) สกุลเงินดิจิทัลอาจมีสถานะเป็น “เอกสาร”<sup>5</sup> ซึ่งมีที่มาจากคำพิพากษาศาลฎีกา<sup>6</sup> ได้วินิจฉัยรับรองว่าข้อมูลคอมพิวเตอร์มีสถานะเท่ากับเอกสาร แต่เมื่อพิจารณาถึงลักษณะ

<sup>4</sup> มาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

<sup>5</sup> มาตรา 1 (7) แห่งประมวลกฎหมายอาญา

<sup>6</sup> คำพิพากษาศาลฎีกาที่ 4311/2557

ความผิดเกี่ยวกับเอกสารนั้นต้องเป็นการกระทำต่อวัตถุที่มีรูปร่าง ในขณะที่สกุลเงินดิจิทัลเป็นสิ่งที่ไม่มีรูปร่าง ดังนั้นความผิดเกี่ยวกับเอกสารจึงไม่อาจนำมาปรับใช้กับสกุลเงินดิจิทัลได้อย่างเหมาะสม

จากปัญหาข้างต้นจะเห็นได้ว่าสกุลเงินดิจิทัลเกี่ยวข้องกับหลายสถานะและแต่ละสถานะต่างมีข้อจำกัดทางกฎหมายในการนำมาปรับใช้กับสกุลเงินดิจิทัล ซึ่งการที่ไม่กำหนดสถานะที่ชัดเจนให้แก่สกุลเงินดิจิทัลยังส่งผลต่อการวินิจฉัยความรับผิดทางอาญาของบุคคลตามหลักกฎหมายอาญากล่าวคือ เมื่อไม่มีกฎหมายบัญญัติว่าการกระทำใดเป็นความผิดและไม่ได้กำหนดโทษไว้ จะลงโทษทางอาญาแก่บุคคลนั้นมิได้ (Nullum Crimen, Nulla Poena Sine Lege)<sup>7</sup> เมื่อไม่มีกฎหมายกำหนดสถานะไว้ อาจมีการนำบทกฎหมายของสถานะที่ใกล้เคียงมาปรับใช้แตกต่างกันออกไป ปัญหาดังกล่าวก่อให้เกิดการตีความและการบังคับใช้กฎหมายที่ขาดเอกภาพและขัดต่อหลักความแน่นอนอันเป็นหลักประกันของกฎหมายอาญา

2) ปัญหาฐานความผิดตามกฎหมายที่มีอยู่ไม่ครอบคลุมถึงการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลสองกรณีด้วยกัน คือ การขโมยสกุลเงินดิจิทัลและการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นโดยมิชอบ กล่าวคือ ฐานความผิดที่มีอยู่ อันได้แก่ ความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 334 ความผิดฐานเอาไปซึ่งเอกสาร ตามประมวลกฎหมายอาญา มาตรา 188 และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 7 ไม่สามารถนำมาปรับใช้กับการขโมยสกุลเงินดิจิทัลได้อย่างเหมาะสม เนื่องจากวัตถุประสงค์แห่งการกระทำและเจตนาซึ่งเป็นองค์ประกอบความผิดมีความแตกต่างกัน ส่วนความผิดฐานลักทรัพย์ก็ไม่อาจนำมาปรับใช้กับกรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นโดยมิชอบได้ เนื่องจากการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นไม่ได้มีลักษณะของการเอาไป กรณีดังกล่าวจึงขาดองค์ประกอบความผิดในส่วนของการกระทำ ทั้งสองกรณีจึงยังเป็นช่องว่างทางกฎหมายที่ผู้กระทำไม่ต้องรับผิด และนอกจากนี้ยังส่งผลกระทบต่อผู้เสียหายอาจไม่ได้รับการเยียวยาและคุ้มครองตามหลักประกันสิทธิขั้นพื้นฐานอันเกิดจากการกระทำความผิดอาญาของบุคคลอื่นตามที่กำหนดไว้ในรัฐธรรมนูญ<sup>8</sup>

อย่างไรก็ตามแม้การขโมยสกุลเงินดิจิทัลและการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นโดยมิชอบจะยังไม่มีกฎหมายบัญญัติให้การกระทำนั้นเป็นความผิด แต่การกระทำดังกล่าวมีลักษณะเป็นการแสวงหาผลประโยชน์โดยมิชอบ จึงเป็นการกระทำที่น่าตำหนิ สมควรกำหนดให้เป็นความผิดอาญาขึ้นมาใหม่ตามหลักเกณฑ์การบัญญัติความผิดอาญา

<sup>7</sup> มาตรา 2 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

<sup>8</sup> มาตรา 25 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

3) ปัญหาความร่วมมือทางอาญาระหว่างประเทศ การกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลนั้นผู้ใช้งานไม่ต้องระบุตัวตนที่แท้จริงและเป็นความผิดที่กระทำบนเครือข่ายอินเทอร์เน็ตซึ่งสามารถเชื่อมโยงธุรกรรมได้จากทั่วทุกมุมโลก จึงเป็นความผิดที่ไร้พรมแดน ความเสียหายไม่ได้จำกัดอยู่ในประเทศใดประเทศหนึ่งเท่านั้น ด้วยเหตุนี้การปราบปรามการกระทำความผิดจึงต้องอาศัยความร่วมมือระหว่างประเทศ ซึ่งอุปสรรคที่สำคัญคือมุมมองในการกำกับดูแลและกฎหมายภายในของแต่ละประเทศที่มีความแตกต่างกัน ซึ่งปัจจุบันมีการประสานความร่วมมือในลักษณะที่ไม่เป็นทางการมากขึ้น โดยให้ความสำคัญกับการถ่ายทอดองค์ความรู้และเทคนิคที่จำเป็นในค้นหาพยานหลักฐานดิจิทัลและการตรวจสอบเส้นทางการเงินเพื่อติดตามตัวผู้กระทำความผิดมาลงโทษ

ดังนั้นการควบคุมการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลจึงจำเป็นต้องกำหนดสถานะที่ชัดเจนให้กับสกุลเงินดิจิทัล และกำหนดให้การกระทำที่ยังเป็นช่องว่างทางกฎหมายเป็นความผิดอาญาไว้เป็นการเฉพาะ เพื่อให้การป้องกันและปราบปรามเป็นไปอย่างมีประสิทธิภาพ ไม่ก่อให้เกิดความสับสนในการบังคับใช้กฎหมาย ทั้งนี้ผู้เขียนจึงได้ทำการศึกษาสภาพปัญหา ความหมาย สถานะทางกฎหมายของสกุลเงินดิจิทัล และสถานะใกล้เคียง เพื่อนำมาวิเคราะห์หาสถานะทางกฎหมายอาญาที่เหมาะสมกับสกุลเงินดิจิทัล และทำการศึกษากฎหมายเกี่ยวกับการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลของไทยและต่างประเทศ รวมถึงรูปแบบการกระทำความผิดทางอาญาที่ยังมีช่องว่างทางกฎหมาย และข้อจำกัดของกฎหมายในการนำมาปรับใช้กับสกุลเงินดิจิทัล เพื่อวิเคราะห์แสวงหามาตรการที่เหมาะสมกับประเทศไทย

## 1.2 วัตถุประสงค์งานวิจัย

- 1) เพื่อศึกษาประวัติความเป็นมาและแนวคิดเกี่ยวกับเงินตราและสกุลเงินดิจิทัล
- 2) เพื่อศึกษาหลักกฎหมายของประเทศไทย หลักกฎหมายต่างประเทศและความร่วมมือทางอาญาระหว่างประเทศเกี่ยวกับการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล
- 3) เพื่อศึกษาและวิเคราะห์ปัญหาทางกฎหมายของประเทศไทยและมาตรการความร่วมมือทางอาญาระหว่างประเทศเกี่ยวกับการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล
- 4) เพื่อเสนอแนะแนวทางการกำหนดสถานะของสกุลเงินดิจิทัลที่เหมาะสม รวมถึงกฎหมายและมาตรการในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลในประเทศไทย

### 1.3 ขอบเขตงานวิจัย

การศึกษานี้มุ่งศึกษาแนวคิด หลักเกณฑ์การบัญญัติความผิดอาญา สถานะของสกุลเงินดิจิทัล รูปแบบความผิดที่ยังเป็นช่องว่างทางกฎหมายสองกรณี คือ กรณีการขโมยสกุลเงินดิจิทัล และกรณีการใช้พลังงานคอมพิวเตอร์ของผู้อื่นโดยมิชอบเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล ไม่รวมถึงการนำสกุลเงินดิจิทัลมาใช้เป็นเครื่องมือในการกระทำความผิดภายใต้กฎหมายฟอกเงิน โดยทำการศึกษาบทบัญญัติของกฎหมายไทยที่เกี่ยวข้อง ได้แก่ ประมวลกฎหมายอาญา พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 พระราชบัญญัติเงินตรา พ.ศ. 2501 และพระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

ในส่วนของแต่ละประเทศได้ทำการศึกษากฎหมายของสหรัฐอเมริกา และสหราชอาณาจักร (อังกฤษ) เนื่องจากทั้งสองประเทศนี้มีนโยบาย และกรอบของกฎหมายในการควบคุมสกุลเงินดิจิทัลไว้อย่างชัดเจน ดังจะเห็นได้จากสหรัฐอเมริกาเมืองค์กรต่าง ๆ ทำหน้าที่กำกับดูแลสกุลเงินดิจิทัลไว้หลากหลายมุมมอง ส่วนประเทศอังกฤษมีหน่วยงานทางการเงินจัดทำแนวปฏิบัติการกำกับดูแลสกุลเงินดิจิทัลไว้เป็นการเฉพาะ กฎหมายของทั้งสองประเทศนี้จึงมีหลักเกณฑ์ในการควบคุมสกุลเงินดิจิทัลที่ชัดเจน นอกจากนี้ยังได้ทำการศึกษามาตรการความร่วมมือทางอาญาระหว่างประเทศเพื่อนำมาเป็นแนวทางในการควบคุมสกุลเงินดิจิทัลให้มีประสิทธิภาพและสอดคล้องกับหลักสากล

### 1.4 คำถามงานวิจัย

คำถามหลัก

- 1) ประเทศไทยมีความจำเป็นต้องมีกฎหมายที่ใช้ในการควบคุมการกระทำความผิดทางอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลหรือไม่
- 2) ปัจจุบันมีกฎหมายที่ใช้ในการควบคุมการกระทำความผิดทางอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลแล้วหรือไม่ ถ้ามี มีเพียงพอหรือครอบคลุมกับความผิดที่เกิดหรืออาจเกิดขึ้นหรือไม่
- 3) การกำหนดมาตรการทางกฎหมายในการควบคุมเงินสกุลดิจิทัลควรมีรูปแบบและเนื้อหาสาระสำคัญอย่างไร

## 1.5 สมมติฐานงานวิจัย

การใช้สกุลเงินดิจิทัลมีแนวโน้มเพิ่มมากขึ้น ปัจจุบันยังไม่มีกฎหมายควบคุมการกระทำ ความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลไว้เป็นการเฉพาะ เช่นกรณีการขโมยสกุลเงินดิจิทัลและกรณีการ ใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล หากมีการกระทำความผิดเกิดขึ้น จะต้องนำบทกฎหมายที่ใกล้เคียงมาปรับใช้ ซึ่งการนำบทกฎหมายที่ใกล้เคียงมาใช้อาจไม่เหมาะสมจะ นำมาลงโทษผู้กระทำผิด เนื่องจากการปรับใช้กฎหมายที่ใกล้เคียงก่อให้เกิดการตีความที่แตกต่างกัน และขาดมาตรฐานในการบังคับใช้ไปในทิศทางเดียวกัน อีกทั้งการกระทำดังกล่าวขัดกับหลักความ ชัดเจนแน่นอนของกฎหมายอาญา นอกจากนี้การกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลยังมี ลักษณะเฉพาะทางเทคนิค การกระทำความผิดบางกรณีอาจก่อให้เกิดช่องว่างทางกฎหมายไทย จึงจำเป็นต้องมีกฎหมายสารบัญญัติกำหนดความผิดฐานขโมยสกุลเงินดิจิทัลและความผิดฐานนำ พลังงานไฟฟ้าหรือพลังงานของผู้อื่นไปใช้โดยมิชอบไว้ในประมวลกฎหมายอาญาให้ชัดเจน เพื่อให้ สอดคล้องและครอบคลุมกับกรณีความผิดที่อาจเกิดขึ้นได้อย่างเหมาะสม ควบคู่ไปกับความร่วมมือ ทางอาญาระหว่างประเทศ และสามารถบังคับใช้ในการป้องกันและปราบปรามการกระทำความผิด เกี่ยวกับสกุลเงินดิจิทัลได้อย่างมีประสิทธิภาพ

## 1.6 ระเบียบวิธีวิจัย

การวิจัยเชิงคุณภาพ ประกอบด้วย การวิจัยเอกสาร (Documentary Research) ศึกษาและ รวบรวมข้อมูลที่เกี่ยวข้องจากหนังสือ งานวิจัย ตั๋วบทกฎหมาย ตำรา วารสาร บทความ คำพิพากษา ฎีกาที่เกี่ยวข้อง รวมถึงข้อมูลจากเครือข่ายอินเทอร์เน็ต โดยข้อมูลที่ได้จากการวิจัยเอกสาร มาเป็น ข้อมูลที่ใช้ในการวิเคราะห์ และสังเคราะห์เป็นมาตรการทางกฎหมายในการควบคุมการกระทำ ความผิดต่อสกุลเงินดิจิทัลที่เหมาะสมสำหรับประเทศไทย

## 1.7 ประโยชน์ที่คาดว่าจะได้รับ

- 1) ทำให้ทราบถึงวิวัฒนาการของสื่อในการแลกเปลี่ยนและความเชื่อมโยงของเงินตรา กับสกุลเงินดิจิทัลตั้งแต่อดีตจนถึงปัจจุบัน
- 2) ทำให้ทราบถึงหลักกฎหมายของประเทศไทย หลักกฎหมายของต่างประเทศและมาตรการความร่วมมือทางอาญาระหว่างประเทศเกี่ยวกับการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล
- 3) ทำให้ทราบถึงปัญหาทางกฎหมายของประเทศไทยและมาตรการความร่วมมือทางอาญาระหว่างประเทศในการควบคุมการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล
- 4) ทำให้ทราบข้อเสนอแนะเพื่อนำไปเป็นแนวทางในการกำหนดสถานะของสกุลเงินดิจิทัลและปรับปรุงกฎหมายรวมถึงมาตรการที่เหมาะสมในการควบคุมการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลในประเทศไทย

## บทที่ 2

### แนวคิด ลักษณะ และการควบคุมเงินตราและสกุลเงินดิจิทัล

ปัจจุบันสื่อกลางในการแลกเปลี่ยนสินค้าและบริการต่าง ๆ ไม่ได้มีเพียงแค่งเงินตราเท่านั้น แต่ยังมีสกุลเงินดิจิทัลเป็นอีกช่องทางหนึ่งในการใช้เป็นสื่อกลางในการทำธุรกรรมต่าง ๆ ในบทนี้จึงได้ศึกษาถึงแนวคิด ประวัติความเป็นมา พัฒนาการของสิ่งที่ใช้เป็นสื่อกลางในการทำธุรกรรมตั้งแต่เป็นเงินตราจนถึงสกุลเงินดิจิทัล ลักษณะ ความหมาย สถานะของเงินตราและสกุลเงินดิจิทัล รวมถึงแนวคิดในการควบคุมเงินตราและสกุลเงินดิจิทัลโดยใช้กลไกทางกฎหมาย เพื่อนำหลักการดังกล่าวมาวิเคราะห์ปัญหาและเสนอแนวทางที่เหมาะสมในการควบคุมการกระทำความผิดทางอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลต่อไป

#### 2.1 แนวคิด ความเป็นมาและลักษณะทั่วไปของเงินตรา

มนุษย์มีความต้องการในการใช้ทรัพยากรที่แตกต่างกัน ความสามารถของมนุษย์แต่ละคนในการแสวงหาทรัพยากรรวมถึงทรัพยากรในแต่ละถิ่นฐานย่อมมีขีดจำกัดและมีความแตกต่างกันออกไป ความแตกต่างดังกล่าวนี้ก่อให้เกิดการแลกเปลี่ยนกันสินค้าระหว่างกันเพื่อตอบสนองความต้องการของมนุษย์ให้มากที่สุด ซึ่งหากทั้งสองฝ่ายมีความต้องการสินค้าที่ต้องตรงกันแล้วก็สามารถทำการแลกเปลี่ยนกันได้ แต่ความต้องการของมนุษย์มีความหลากหลายและซับซ้อนจึงเกิดกรณีที่ความต้องการไม่ตรงกับสินค้าที่มี ดังนั้นเพื่อเป็นการแก้ไขปัญหาดังกล่าว จึงเกิดแนวคิดในการหาหน่วยมาตรฐานกลางที่คนทั่วไปยอมรับเพื่อทำหน้าที่ในการเป็นสื่อกลางการแลกเปลี่ยนสินค้า<sup>9</sup> โดยนำวัตถุหรือสิ่งของต่าง ๆ มาเป็นสื่อกลางจนกระทั่งพัฒนามาเป็น “เงินตรา” ที่ใช้กันอยู่ในทุกสังคมจนถึงปัจจุบัน

---

<sup>9</sup> Chirs Diamond, “The History of Money and Banking No One Ever Told You,” **Economic History Report**, Retrieved May 8, 2020 from <https://www.scribd.com/book/229908625/The-History-Of-Money-and-Banking-No-One-Ever-Told-You-Economic-History-Report>

เงินจึงเป็นสิ่งที่มีความสำคัญ เป็นที่ยอมรับของคนทั่วไปและใช้อย่างกว้างขวางในระบบเศรษฐกิจ ดังนั้นจึงจำเป็นต้องมีการควบคุมเงินตราเพื่อให้เกิดเสถียรภาพและความปลอดภัยต่อระบบเศรษฐกิจ และการเงิน ในหัวข้อนี้จึงได้แบ่งการศึกษาที่เกี่ยวข้องกับเงินตราออกเป็นสองส่วนคือ แนวคิดพื้นฐาน ลักษณะทั่วไปของเงินตรา และการควบคุมเงินตรา

## 2.1.1 แนวคิดพื้นฐานและลักษณะทั่วไปของเงินตรา

### 2.1.1.1 วิวัฒนาการของเงินตราในประเทศไทย

เงินตราที่ใช้เป็นสื่อกลางในการแลกเปลี่ยนและการซื้อขายสินค้าและบริการต่าง ๆ ในประเทศไทยได้สันนิษฐานว่ามีมาตั้งแต่ก่อนสมัยสุโขทัย ซึ่งสามารถแบ่งออกเป็น 5 สมัย<sup>10</sup> ดังนี้

#### 1) เงินตราสมัยก่อนสุโขทัย

สมัยก่อนสุโขทัยมีการค้นพบหลักฐานว่าประเทศไทยมีการใช้เงินที่ลักษณะเป็นเหรียญแบนมาตั้งแต่สมัยอาณาจักรพูนัน ด้านหนึ่งเป็นรูปครึ่งวงกลมมีลวดลายเป็นเส้นรัศมีกระจายรอบเหรียญ ส่วนอีกด้านเป็นรูปคล้ายหอกพระนารายณ์ ในสมัยอาณาจักรทวารวดี ลักษณะเงินที่พบยังคงมีสัญลักษณ์เกี่ยวกับกษัตริย์ อำนาจการปกครอง ความอุดมสมบูรณ์ ศาสนา<sup>11</sup>

#### 2) เงินตราสมัยสุโขทัย

มีการติดต่อค้าขายกับต่างชาติโดยเฉพาะทางทะเล ได้แก่ ประเทศจีน อินเดีย ยุโรป และยังติดต่อกับกลุ่มชนทางตอนเหนือของไทย เช่น ล้านช้าง ยูนาน น่านเจ้า ไปจนถึงแถบตะวันออกเฉียงใต้ โดยในสมัยสุโขทัยนี้ได้ผลิตเงินตราขึ้นใช้ในระบบเศรษฐกิจ คือ เงินพดด้วง โดยทำขึ้นจากแท่งเงินทุบปลายงอเข้าหากันแล้วตอกประทับตราประจำแผ่นดินและตราประจำรัชกาลลงไป ด้วยเหตุที่มีสัญญาณกลมคล้ายตัวดั่ง คนไทยจึงเรียกว่าเงินพดด้วง ในระยะแรกมีขนาด และรูปร่างไม่ได้มาตรฐาน ต่อมาได้มีการเปลี่ยนมาใช้เงินเป็นวัสดุและปรับปรุงน้ำหนักให้เป็นมาตรฐานเดียวกัน โดยใช้หน่วยเป็น ตำลึง บาท สลึง ส่วนตราที่ประทับลงบนเหรียญ ได้แก่ ตราช้าง และราชวัติ<sup>12</sup>นอกจากนี้ยังใช้ “เบี้ย” เป็นเงินปลีกสำหรับแลกเปลี่ยนสินค้าราคาต่ำ

<sup>10</sup> อัจฉรา หล่อตระกูล, Money: Meaning and Importance, วารสารวิจัยราชภัฏกรุงเทพฯ สาขามนุษยศาสตร์และสังคมศาสตร์ 2, 1 (มกราคม 2558): 67.

<sup>11</sup> กองกษาปณ์, เงินตรา, ค้นวันที่ 22 กันยายน 2563 จาก [www.royalthaimint.net/ewtadmin/ewt/mint\\_web/ewt\\_news.php?nid=46&filename=index](http://www.royalthaimint.net/ewtadmin/ewt/mint_web/ewt_news.php?nid=46&filename=index)

<sup>12</sup> กองกษาปณ์, เงินตรา, ค้นวันที่ 22 กันยายน 2562 จาก [www.royalthaimint.net/ewtadmin/ewt/mint\\_web/ewt\\_news.php?nid=46&filename=index](http://www.royalthaimint.net/ewtadmin/ewt/mint_web/ewt_news.php?nid=46&filename=index)

### 3) เงินตราสมัยกรุงศรีอยุธยา

เงินตราในสมัยกรุงศรีอยุธยายังคงเป็นเช่นเดียวกับสมัยสุโขทัย มีเงินตรา 3 ชนิด คือ เงินเบี้ย เงินพดด้วง และเงินประทับ มีลักษณะเป็นเงินที่ทำจากดินเผา ส่วนเงินเบี้ยที่ใช้สมัยนั้นมักทำมาจากเปลือกหอย ได้แก่ เบี้ยโพล้ง เบี้ยแก้ว เบี้ยหมู เบี้ยจั่น เบี้ยนาง เบี้ยบัว เบี้ยพองลม และเบี้ยตุ้ม ซึ่งเบี้ยจั่นเป็นเบี้ยที่นิยมใช้กันมากที่สุด มูลค่าของเบี้ยไม่ได้กำหนดไว้แน่นอนขึ้นอยู่กับกลไกของตลาดหากเบี้ยในตลาดมีปริมาณมาก ราคาเบี้ยจะต่ำ แต่หากเบี้ยมีปริมาณน้อย ราคาเบี้ยจะสูง วิวัฒนาการอีกประการหนึ่งที่ได้เห็นได้ชัดคือพดด้วงในสมัยนี้มีประทับตราเพียง 2 แบบ โดยประทับตราที่อยู่ส่วนบน คือตราจักรซึ่งเป็นตราประจำแผ่นดิน และส่วนด้านหน้าเป็นตราประจำรัชกาลลักษณะต่าง ๆ กัน แต่ยังไม่พบหลักฐานชัดเจนว่าเป็นตราของรัชกาลใด แต่ตราพุ่มข้าวบิณฑ์มีการสันนิษฐานว่าเป็นตราประจำรัชกาลของสมเด็จพระนารายณ์มหาราช<sup>13</sup>

### 4) เงินตราสมัยกรุงธนบุรี

เงินและเหรียญที่ใช้ในตอนต้นรัชกาลสมเด็จพระเจ้าตากสินมหาราชยังโปรดฯ ให้ใช้เงินพดด้วงของกรุงศรีอยุธยาต่อมาอีกระยะหนึ่ง จากนั้นได้โปรดฯ ให้ผลิตเงินพดด้วงประจำรัชกาลเพื่อใช้ในระบบเศรษฐกิจ โดยมีลักษณะเช่นเดียวกับเงินพดด้วงในสมัยกรุงศรีอยุธยาประทับตราจักรเป็นตราประจำแผ่นดินและให้ใช้ตราทิวชุกและตราตรีเป็นตราประจำรัชกาล<sup>14</sup>

### 5) เงินตราสมัยกรุงรัตนโกสินทร์

เงินตราที่ออกใช้ในสมัยกรุงธนบุรี และกรุงสมัยกรุงรัตนโกสินทร์ มี 3 ชนิด คือ เงินพดด้วง เงินเหรียญ เงินธนบัตรเงินพดด้วง<sup>15</sup> นับตั้งแต่สมัยกรุงสุโขทัย สมัยกรุงศรีอยุธยา สมัยกรุงธนบุรี มาจนถึงสมัยกรุงรัตนโกสินทร์ตอนกลาง เงินตราที่ใช้ยังคงใช้เงินพดด้วงเรื่อยมาจนกระทั่งปี พ.ศ. 2447 ในรัชกาลที่ 5 พระบาทสมเด็จพระจุลจอมเกล้าเจ้าอยู่หัวได้ประกาศยกเลิกการใช้เงินเหรียญที่เคยใช้มาตั้งแต่สมัยรัชกาลที่ 4 และมีการใช้เงินธนบัตรที่เป็นเงินกระดาษในประเทศไทยเริ่มผลิตขึ้นใช้ครั้งแรกในสมัยพระบาทสมเด็จพระจอมเกล้าและได้มีพระบรมราชโองการให้ตราพระราชบัญญัติธนบัตรสยาม รัตนโกสินทรศก 121 โดยมีวัตถุประสงค์ให้ธนบัตรตาม

<sup>13</sup> อัญญา ชันธวิทย์, กลไกตลาดการเงินในระบบเศรษฐกิจไทย: ตลาดหลักทรัพย์แห่งประเทศไทย พ.ศ. 2546, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: ตลาดหลักทรัพย์แห่งประเทศไทย, 2546), หน้า 42.

<sup>14</sup> มูลนิธิอนุรักษ์โบราณสถานในพระราชวังเดิม, เงินตราโบราณของไทย, ค้นวันที่ 22 กันยายน 2563 จาก [http://www.wangdermpalace.org/Pod%20Duang%20Money\\_th.html](http://www.wangdermpalace.org/Pod%20Duang%20Money_th.html)

<sup>15</sup> อัจฉรา หล่อตระกูล, เรื่องเดิม, หน้า 67.

พระราชบัญญัตินี้มีลักษณะเป็นตัวสัญญาใช้เงินที่รัฐบาลสัญญาว่าจะจ่ายเงินตราให้แก่ผู้นำธนบัตรมา ยื่น ธนบัตรจึงเข้ามามีบทบาทในระบบเศรษฐกิจของไทยอย่างเป็นทางการ<sup>16</sup>

ต่อมาในรัชกาลพระบาทสมเด็จพระปกเกล้าเจ้าอยู่หัว มีการประกาศใช้พระราชบัญญัติเงินตรา พ.ศ. 2471 มีผลยกเลิกพระราชบัญญัติธนบัตร ร.ศ. 121<sup>17</sup> ที่มีการบังคับใช้มาตั้งแต่สมัยรัชกาลที่ 5 และได้กำหนดให้เงินตราของประเทศ ได้แก่ ธนบัตรและเหรียญกษาปณ์ เป็นเงินที่ชำระหนี้ได้ตามกฎหมาย ซึ่งหลักการดังกล่าวยังคงมีอยู่ในพระราชบัญญัติเงินตราเรื่อยมาจนถึงปัจจุบัน

#### 2.1.1.2 ความหมายของเงินตรา

เงินตรา คือ “สื่อกลางในการแลกเปลี่ยนและใช้วัดมูลค่าของสินค้าและบริการได้ทุกชนิด”<sup>18</sup> เงินตราในอดีตเริ่มจากการใช้เปลือกหอย อัญมณี พัฒนามาเป็นโลหะ ปัจจุบันมีลักษณะเป็นเหรียญกษาปณ์และธนบัตร<sup>19</sup> ซึ่งรัฐกำหนดขึ้นไว้เพื่อใช้ชำระหนี้ตามกฎหมาย<sup>20</sup> นอกจากนี้เงินตรายังหมายถึงความถึงสินทรัพย์ที่มีคุณสมบัติพิเศษในการเป็นสื่อกลางการแลกเปลี่ยนในระบบเศรษฐกิจ เป็นหน่วยในทางบัญชีและเป็นยังเป็นเครื่องรักษามูลค่า<sup>21</sup>

ทั้งนี้ความหมายของคำว่าเงินตรา เมื่อพิจารณาจาก พระราชบัญญัติเงินตรา พ.ศ. 2501 มาตรา 6 บัญญัติว่า “เงินตราได้แก่เหรียญกษาปณ์และธนบัตร” ซึ่งคำว่าเหรียญกษาปณ์และธนบัตรในพระราชบัญญัติเงินตราดังกล่าวไม่ได้ให้นิยามไว้ แต่ได้กำหนดว่าเหรียญกษาปณ์เป็นสิ่งที่สามารถชำระหนี้ได้ตามกฎหมาย<sup>22</sup> โดยต้องทำขึ้นและออกใช้โดยกระทรวงการคลัง และต้องมีการกำหนดชนิด ราคา โลหะ อัตราเนื้อโลหะ น้ำหนัก ขนาด ลวดลาย และลักษณะอื่น ๆ ของเหรียญ

<sup>16</sup> ธนาคารแห่งประเทศไทย, **วิวัฒนาการเงินตราไทย**, ค้นวันที่ 22 กันยายน 2563 จาก [https://www.bot.or.th/Thai/Banknotes/HistoryAndSeriesOfBanknotes/Pages/Evolution\\_of\\_Thai\\_Banknotes.aspx](https://www.bot.or.th/Thai/Banknotes/HistoryAndSeriesOfBanknotes/Pages/Evolution_of_Thai_Banknotes.aspx)

<sup>17</sup> พระราชบัญญัติเงินตรา พ.ศ. 2471

<sup>18</sup> Paul A. Samuelson, **Economics**, 11<sup>st</sup> ed. (New York: McGraw-Hill, 1980), p. 10.

<sup>19</sup> กองกษาปณ์, **เรื่องเดิม**.

<sup>20</sup> ราชบัณฑิตยสถาน, **พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554**, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: นานมีบุ๊คส์, 2556), หน้า 18.

<sup>21</sup> Laurence M. Ball, **Money, Banking and Financial Markets** (New York: Worth Publishers, 2009), p. 49.

<sup>22</sup> มาตรา 11 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

กษาปณ์โดยกฎกระทรวง<sup>23</sup> ส่วนธนบัตรนั้นต้องสามารถชำระหนี้ได้ตามกฎหมาย<sup>24</sup> และต้องทำขึ้นและออกใช้โดยธนาคารแห่งประเทศไทยซึ่งรัฐมนตรีได้ประกาศ ชนิด ราคา สีขนาดและลักษณะอื่น ๆ ของธนบัตรที่จะออกใช้ในราชกิจจานุเบกษา<sup>25</sup>

### 2.1.1.3 คุณสมบัติและหน้าที่ของเงินตรา

คุณสมบัติของเงินตรา คือทำมาจากวัสดุที่คงทนถาวรพอสมควร เพื่อที่เวลาใช้เป็นประจำจะได้ไม่ชำรุดเสียหายได้ง่าย มูลค่าของวัสดุที่นำมาทำเป็นเงินต้องเท่ากัน สามารถพกพาได้สะดวก มีน้ำหนักเบา สามารถแบ่งออกเป็นหน่วยย่อยได้ มีเสถียรภาพ ที่สำคัญคือเป็นยอมรับในการนำมาใช้เป็นสื่อกลางการแลกเปลี่ยนเงินตราที่ทำมาจากกระดาษจึงเป็นวัสดุที่ทั่วโลกนิยมใช้มากที่สุด<sup>26</sup>

นอกจากเงินตราจะมีคุณสมบัติดังที่ได้กล่าวมาแล้ว จะต้องทำหน้าที่ที่สำคัญต่อระบบเศรษฐกิจ ดังนี้

1) หน้าที่เป็นสื่อกลางในการแลกเปลี่ยน (Medium of Exchange) การใช้เงินเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการทำให้ผู้ทำธุรกรรมการค้าได้รับความสะดวกมากขึ้นทางการซื้อขายสินค้าและบริการ เนื่องจากเงินเข้ามาทำหน้าที่แก้ปัญหาการแลกเปลี่ยนสินค้ากับสินค้าโดยตรง (Barter) ที่ทั้งสองฝ่ายมีความต้องการสอดคล้องกันทุกประการเท่านั้น จึงจะทำการแลกเปลี่ยนกันได้ การที่คู่ค้าต้องมีความต้องการสอดคล้องกันทุกประการ ส่งผลให้คู่ค้าที่มีความต้องการสอดคล้องกันทุกประการอาจต้องใช้เวลามาก ธุรกิจหยุดชะงัก นอกจากนั้นการแลกเปลี่ยนสินค้าจะต้องมีสถานที่เก็บสินค้าเพื่อเตรียมไว้นำมาแลกเปลี่ยน ซึ่งเป็นต้นทุนที่เพิ่มขึ้นรวมถึงค่าขนส่งในการแลกเปลี่ยน ดังนั้นการใช้เงินเป็นสื่อกลางการแลกเปลี่ยนจึงช่วยลดข้อจำกัดของการแลกเปลี่ยนดังกล่าว<sup>27</sup>

2) หน้าที่เป็นมาตรฐานในการวัดมูลค่าสินค้าและบริการ (Standard of Value or Unit of Account) หน่วยของเงินของประเทศถูกใช้เป็นมาตรฐานในการระบุมูลค่าของสินค้าและบริการ และยังใช้เป็นหน่วยนับสำหรับบันทึกบัญชีที่เกิดขึ้นในประเทศนั้น ในประเทศไทยราคาของสินค้าและบริการทุกประเภทจะถูกระบุในหน่วยของเงินบาท การระบุราคาของสินค้าแต่ละชิ้นทำให้ทั้งผู้ซื้อและผู้ขายมีความเข้าใจตรงกันถึงมูลค่าของสินค้าที่ต้องการซื้อขาย แต่หากไม่มีเงิน

<sup>23</sup> มาตรา 10 และมาตรา 11 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>24</sup> มาตรา 15 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>25</sup> มาตรา 14 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>26</sup> อัจฉรา หล่อตระกูล, *เรื่องเดิม*, หน้า 72.

<sup>27</sup> อัญญา ชันฉวีรักษ์, *เรื่องเดิม*, หน้า 60-63.

เป็นหน่วยมาตรฐานเดียวกันแล้ว ราคาของสินค้าและบริการจะถูกแสดงในรูปอัตราแลกเปลี่ยนระหว่างคู่สินค้าจะทำให้เกิดความยุ่งยาก

3) หน้าที่เป็นมาตรฐานในการชำระหนี้ในภายหลัง (Standard of Deferred Payments) เนื่องจากปัจจุบันเงินทำหน้าที่เป็นสื่อกลางในการแลกเปลี่ยนและเป็นมาตรฐานในการระบุมูลค่าสินค้าและบริการ เงินจึงมีความเหมาะสมที่จะทำหน้าที่เป็นมาตรฐานสำหรับการชำระราคาและภาระผูกพันที่จะเกิดขึ้นในอนาคต โดยเฉพาะอย่างยิ่งในการทำธุรกรรมที่มีการทำสัญญาเช่าซื้อสินค้าหรือบริการที่ทำกันไว้ในปัจจุบัน แต่จะมีการจ่ายชำระราคาในอนาคต การทำสัญญาเช่นนี้จะมีการระบุการชำระค่าเช่าหรือการส่งเงินต้นพร้อมดอกเบี้ยในอนาคตจนถึงวันที่สัญญานั้นสิ้นสุดลงเป็นหน่วยของเงิน การระบุภาระผูกพันที่จะเกิดขึ้นในอนาคตเป็นหน่วยของเงินทำให้การตกลงทำสัญญาสะดวกขึ้น เนื่องจากคู่สัญญาให้ความสนใจตรงกันถึงภาระผูกพัน ที่ฝ่ายหนึ่งจะต้องนำส่งในรูปของเงินในอนาคต

ดังนั้นหากไม่มีเงินเป็นมาตรฐานในการชำระราคาหรือภาระผูกพันในอนาคตแล้วการตกลงเงื่อนไขในการชำระค่าเช่าหรือชำระหนี้อื่นอาจต้องใช้สินค้าหรือสินทรัพย์ที่มีตัวตนเป็นมาตรฐานแทนซึ่งจะทำให้เกิดความยุ่งยาก ใช้เวลานาน และอาจเกิดการโต้แย้งเสียเปรียบกัน เนื่องจากต้องพิจารณาถึงลักษณะทางกายภาพของสินค้าหรือบริการที่จะนำมาใช้ชำระหนี้ทุกกรณีไป<sup>28</sup>

4) หน้าที่สะสมมูลค่า (Store of Value) สิ่งของทั่วไปมีทั้งแบบที่เน่าเสียง่ายและแบบที่เน่าเสียยาก ทำให้ผู้ที่มีสิ่งของที่เน่าเสียยากได้เปรียบกว่า เนื่องจากมีมูลค่าในตัวเองมากกว่า โดยเงินถือเป็นสิ่งของที่เน่าเสียยาก และหากเงินมีมูลค่าที่เสถียรหรืออยู่ในสภาวะที่มีอำนาจซื้อที่คงที่ ไม่เปลี่ยนแปลงบ่อยแล้ว เงินจึงเป็นเครื่องสะสมมูลค่าที่ดี เพราะเมื่อเวลาเปลี่ยนแปลงไปเงินก็ยังคงมีมูลค่าเสมอและสามารถนำไปบริหารจัดการให้เกิดดอกผลได้ ดังนั้นเงินจึงเป็นเครื่องมือหนึ่งที่มนุษย์นิยมใช้ในการสะสมมูลค่า<sup>29</sup>

อย่างไรก็ดีปัจจุบันเงินอาจไม่ใช่ทางเลือกเดียวที่บุคคลหรือผู้ประกอบการธุรกิจจะใช้สะสมกำลังซื้อสินทรัพย์อื่น ๆ สินทรัพย์ที่มีตัวตนและสินทรัพย์ทางการเงินสามารถทำหน้าที่นี้ได้ด้วยกันทั้งคู่ และยังมีข้อได้เปรียบมากกว่าเงินในเรื่องการให้ผลตอบแทนแก่ผู้ถือครอง แต่หากพิจารณาถึงความสะดวกในการใช้จ่ายแล้วเงินก็ยังเป็นสื่อกลางในการแลกเปลี่ยนที่สะดวกรวดเร็วใน

<sup>28</sup> John Kenneth Galbraith and James K. Galbraith, **Money: Whence it came, where it went** (Princeton: Princeton University Press, 2017), p. 24.

<sup>29</sup> ดลพร ประสงค์สุทธิพร, **แนวทางการกำกับดูแลการใช้เงินเสมือน: กรณีศึกษาบิตคอยน์** (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2557), หน้า 42.

ขณะที่ ในขณะที่ผู้ถือสินทรัพย์อื่น ๆ อาจต้องขายสินทรัพย์นั้นเพื่อแลกเปลี่ยนสภาพให้เป็นเงินสด ก่อนแล้วจึงค่อยใช้เงินจำนวนนั้นไปซื้อสินค้าหรือบริการ

#### 2.1.1.4 รูปแบบของเงินตรา

เงินตรายังคงมีวิวัฒนาการมาอย่างต่อเนื่องตั้งแต่อดีตที่มีการนำวัตถุ หรือโลหะ มาทำ เป็นเหรียญนำกระดาษมาทำเป็นธนบัตร จนปัจจุบันมีการพัฒนารูปลักษณะของเงินในรูปแบบที่ต่างไป จากเดิม โดยได้มีการนำเทคโนโลยีเข้ามาใช้ร่วมด้วย ซึ่งสามารถจำแนกรูปแบบของเงินตราได้ดังนี้

1) สิ่งของหรือสินค้า เงินที่เป็นสิ่งของหรือสินค้า (Commodity Money) เป็นสื่อกลางในการแลกเปลี่ยนชนิดแรกของมนุษย์ โดยเริ่มต้นจากการที่มนุษย์เริ่มหาสิ่งมีค่า ที่สังคม ยอมรับเป็นสื่อกลางในการแลกเปลี่ยนสิ่งของระหว่างกันในแต่ละสังคม จะมีลักษณะแตกต่างกันตาม สภาพภูมิศาสตร์และความจำเป็นของสินค้านั้น ๆ ได้แก่ ส่วนต่าง ๆ ของพืช กระจุกสัตว์ หนังสัตว์ เป็นต้น รวมไปถึงบรรดาเครื่องมือเครื่องใช้หรือเครื่องประดับ เช่น เสียม หม้อ เครื่องปั้นดินเผา เป็นต้น

2) เงินโลหะ (Metallic Money) เป็นเงินที่ทำจากโลหะอย่างใดอย่างหนึ่ง หรือโลหะผสม เช่น ทองคำ เงิน ทองแดง ดีบุก ตะกั่ว ฯลฯ ที่นำมาหลอมและแบ่งเป็นชิ้น ๆ โดยมี รูปร่างเป็นก้อน แท่ง หรือรูปทรงต่าง ๆ ตามที่สังคมนั้นกำหนดให้มีขนาดและความบริสุทธิ์ใกล้เคียง กันต่อมาจึงมีการประทับตราผู้จัดทำหรือออกใช้ เพื่อเป็นประกันว่าเงินที่ถูกตรานั้นได้รับการ ตรวจสอบว่ามีความเที่ยงตรง สามารถใช้เป็นสื่อกลางในการแลกเปลี่ยนได้<sup>30</sup>

3) เงินเหรียญหรือเหรียญกษาปณ์ (Coin Money) เป็นพัฒนาการที่มาจากเงินโลหะ โดยการนำโลหะมีค่ามาหลอมให้เป็นเหรียญซึ่งมีรูปร่าง ขนาด น้ำหนัก และ ส่วนประกอบตามที่กำหนดไว้ ส่วนใหญ่มีลักษณะแบน เหรียญกษาปณ์สามารถแบ่งย่อยได้อีกเป็น เหรียญกษาปณ์ที่มีมูลค่ากำหนดหน้าเหรียญเท่ากับค่าของโลหะที่นำมาทำเหรียญ เรียกว่า เหรียญมีค่า เต็มตัว (Full-bodied Coin) และเหรียญกษาปณ์ที่กำหนดมูลค่ามากกว่าโลหะที่นำมาทำเหรียญ เรียกว่า เหรียญที่มีค่าไม่เต็มตัว (Token Money)<sup>31</sup>

4) เงินกระดาษหรือธนบัตร เงินกระดาษ (Paper Money) หรือธนบัตร เป็นเงินที่มีลักษณะแผ่นกระดาษหรือแผ่นวัสดุขนาดเล็กซึ่งพิมพ์ชนิดราคาแล้ว และสามารถนำไปใช้ ชำระหนี้ได้ตามกฎหมายถือเป็นเงินตราที่เกิดจากความเชื่อถือในระบบการควบคุม การพิมพ์ และการ

<sup>30</sup> วิโรจน์ กลั่นเปา, เรื่องของเงินและธนาคาร (กรุงเทพมหานคร: เคล็ดไทย, 2517), หน้า 7.

<sup>31</sup> กฤษฎา สังขมณี, การเงินและการธนาคาร (กรุงเทพมหานคร: ศูนย์หนังสือมหาวิทยาลัย ราชภัฏสวนสุนันทา, 2550), หน้า 3.

นำออกใช้ที่มีกฎหมายรับรอง<sup>32</sup> ไม่ใช่มูลค่าของกระดาษหรือวัตถุที่นำมาจัดทำเป็นเงินอีกต่อไป เงินเป็นชนชาติแรกที่คิดหาเงินกระดาษขึ้นตั้งแต่สมัยก่อนคริสตกาล ซึ่งต่อมาได้แพร่หลายไปยังทวีปยุโรปในศตวรรษที่ 6<sup>33</sup> เงินกระดาษในสมัยนี้มีคุณสมบัติอยู่ระหว่างบัตรธนาคารกับตัวเงินของทางราชการ มีวัตถุประสงค์เพื่อใช้ชั่วคราวแทนเงินโลหะ แต่ในภายหลังเงินกระดาษทำให้เกิดปัญหาเงินเฟ้อ เนื่องจากการพิมพ์ธนบัตรออกมามากเกินไป ประชาชนบางส่วนจึงสูญเสียความเชื่อมั่นในเงินตราประเภทนี้<sup>34</sup>

5) เงินในบัญชีธนาคาร แม้ธนบัตรจะเป็นเงินที่ผู้คนนิยมใช้กันมากที่สุดก็ตาม แต่เมื่อความเจริญทางเศรษฐกิจเพิ่มมากขึ้น ทำให้การใช้ธนบัตรอาจไม่เหมาะสมในการดำเนินธุรกิจการค้า โดยเฉพาะอย่างยิ่งการค้าระหว่างประเทศ จึงมีผู้คิดค้นการใช้เงินในบัญชีธนาคารขึ้น (Book Money, Bank Money หรือ Scriptural Money) ลักษณะสำคัญของเงินประเภทนี้จะใช้วิธีการทางบัญชีแทนการส่งมอบธนบัตรหรือเหรียญกษาปณ์<sup>35</sup> คู่สัญญาอาจตกลงวิธีการชำระหนี้ตามสัญญาให้ใช้วิธีการหักบัญชีเงินฝากที่ต้นมืออยู่กับธนาคารพาณิชย์ ซึ่งธนาคารมีหน้าที่จะต้องจ่ายคืนเมื่อทวงถามโดยมีรูปแบบวิธีการที่หลากหลาย เช่น การใช้ตัวเงินหรือเช็ค การหักบัญชี เลตเตอร์ออฟเครดิต ฯลฯ เป็นต้น เหตุที่เงินในบัญชีธนาคารถือเป็นเงินในมุมมองหนึ่ง เนื่องจากความน่าเชื่อถือของธุรกรรมที่ทำผ่านธนาคารต้องแสดงตัวตนที่แท้จริงซึ่งมีเงินจริงฝากอยู่ในบัญชี สามารถตรวจสอบข้อมูลได้โดยมีธนาคารเป็นศูนย์กลางในการเก็บข้อมูล และยังมีวิธีที่ใช้จ่ายที่สะดวก สามารถหมุนเวียนเปลี่ยนมือได้สะดวกโดยผู้โอนเขียนรายการลงบนตัวลงในระบบคอมพิวเตอร์ และผู้รับโอนก็สามารถนำไปเปลี่ยนเป็นเงินได้ทันที แม้สิ่งเหล่านี้จะไม่ถือว่าเป็นเงินที่ใช้ชำระหนี้ได้ตามกฎหมายซึ่งเจ้าหนี้อาจปฏิเสธการชำระหนี้จากการใช้เงินในบัญชีธนาคารได้ก็ตาม<sup>36</sup>

6) ข้อมูลอิเล็กทรอนิกส์ พัฒนาการของวิทยาการคอมพิวเตอร์เป็นจุดเริ่มต้นในการเปลี่ยนสังคมมนุษย์จากยุคอุตสาหกรรมไปสู่ยุคสารสนเทศ เกิดการประยุกต์ใช้เทคโนโลยีสารสนเทศต่าง ๆ เข้ามาใช้เป็นเครื่องมือในการทำธุรกรรมทางการเงิน จึงทำให้เกิดความ

<sup>32</sup> นวรัตน์ เลขาภกุล, **เบี้ย บาท กษาปณ์ แบงก์** (กรุงเทพมหานคร: สารคดี, 2542), หน้า 52.

<sup>33</sup> วารีย์ พงษ์เวช, **การเงินและการธนาคาร** (กรุงเทพมหานคร: อุตสาหกรรมกรรมการพิมพ์, 2502), หน้า 13-15.

<sup>34</sup> เบอ์นาร์ดี ลีตาร์, **เงินตราแห่งอนาคต: วิธีใหม่สู่การรังสรรค์ความมั่งคั่ง งาน และโลกอันชาญฉลาด**, แปลโดย จินตลา วิเศษกุล (กรุงเทพมหานคร: สวนเงินมีมา, 2547), หน้า 46-47.

<sup>35</sup> เมธี ดุลยจินดา, **วิวัฒนาการของระบบธนาคารของโลก** (กรุงเทพมหานคร: ดวงกมล, 2519), หน้า 170.

<sup>36</sup> วิโรจน์ กลั่นเปา, **เรื่องเดิม**, หน้า 8.

สะดวก รวดเร็ว มีประสิทธิภาพมากขึ้นอีกทั้งยังส่งผลให้จำนวนธุรกรรมทางการเงินมีปริมาณและมูลค่าเพิ่มขึ้นด้วย<sup>37</sup> เช่น การโอนเงินในบัญชีผ่านระบบธนาคาร หรือการใช้บัตรเครดิตในการชำระค่าสินค้าและบริการไปก่อน แล้วจึงชำระเงินคืนให้แก่ธนาคารในอนาคตตามที่ตกลงกันไว้<sup>38</sup> เรียกว่า “เงินดิจิทัล” สิ่งเหล่านี้เป็นเงินซึ่งถูกใช้ในรูปของข้อมูลอิเล็กทรอนิกส์ โดยไม่ต้องส่งมอบเงินที่เป็นเหรียญหรือธนบัตรที่จับต้องได้ทางกายภาพ ซึ่งต่อมามีการพัฒนานวัตกรรมทางการเงินต่าง ๆ เพิ่มมากขึ้น เช่น เงินอิเล็กทรอนิกส์ (e-Money) กระเป๋าเงินอิเล็กทรอนิกส์ (e-Wallet) รวมไปถึงสกุลเงินดิจิทัลซึ่งเป็นวัตถุในการศึกษาของวิทยานิพนธ์ฉบับนี้

อย่างไรก็ตามเงินดิจิทัลกับสกุลเงินดิจิทัล มีความเหมือนและความแตกต่างกัน กล่าวคือ ทั้งสองมีสิ่งๆที่เหมือนกันคือคำว่า “ดิจิทัล” กล่าวคือ เป็นสิ่งๆที่ไม่มีรูปร่าง จับต้องไม่ได้ ถูกสร้างขึ้นให้อยู่ในรูปแบบของข้อมูลอิเล็กทรอนิกส์ ต้องทำธุรกรรมทางการเงินในระบบออนไลน์เช่นกัน ส่วนความต่างระหว่าง “เงินดิจิทัล” กับ “สกุลเงินดิจิทัล” คือ เงินดิจิทัลคือเงินที่มีเงินสกุลท้องถิ่นหนุนหลังซึ่งออกให้ใช้โดยรัฐบาลของประเทศนั้น ๆ เช่น สกุลเงินบาท สกุลเงินเยน เป็นต้น ผู้ใช้ต้องนำเงินมาชำระแก่ผู้ให้บริการ e-Money ซึ่งเงินที่นำมาชำระนั้นจะยึดโยงกับเงินที่มีอยู่จริงในบัญชีที่ผู้ใช้ได้เปิดบัญชีไว้กับธนาคาร จึงกล่าวได้ว่าเงินดิจิทัลแม้จะมีคำว่าเงินอยู่แต่เมื่อพิจารณาแล้วจะเห็นว่าไม่ได้มีลักษณะเป็นเงินตรารูปแบบใหม่ แต่เป็นเพียงช่องทางการชำระเงิน (Method of Payment) ที่ใช้เทคโนโลยีดิจิทัลเข้ามาทำให้ผู้ใช้สะดวกในการทำธุรกรรมยิ่งขึ้นเท่านั้น ส่วน “สกุลเงินดิจิทัล” เป็นคริปโทเคอร์เรนซี (Cryptocurrency) ประเภทหนึ่ง เช่น บิตคอยน์ (Bitcoin) เป็นสกุลเงินใหม่ที่ไม่ได้อิงกับสกุลเงินท้องถิ่นของประเทศใด และไม่ได้อิงกับมูลค่าทองคำ บุคคลธรรมดาสามารถออกสกุลเงินดิจิทัลขึ้นเองได้จึงมีความผันผวนไปตามความต้องการของกลุ่มคนที่ใช้เท่านั้น สกุลเงินดิจิทัลนี้สร้างขึ้นจากกลไกทางคณิตศาสตร์ และใช้เทคโนโลยีบล็อกเชน (Blockchain) ในการจัดเก็บข้อมูลและติดตามการเคลื่อนไหวของเงินแบบกระจายข้อมูลไว้กับผู้ใช้ทุกคนที่เกี่ยวข้อง โดยไม่จำเป็นต้องผ่านตัวกลาง<sup>39</sup> ที่เรียกว่า ธนาคาร อีกต่อไป

<sup>37</sup> วินัย แทนประเสริฐกุล, **ความสมบูรณ์ของระบบการชำระเงิน: ศึกษากรณีผลกระทบที่เกิดขึ้นจากหลักการนับเวลาที่ศูนย์นาฬิกา** (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2547), หน้า 1.

<sup>38</sup> กฤษณา สังขมณี, *เรื่องเดิม*, หน้า 3.

<sup>39</sup> ฐิติมา ชูเชิด, **สกุลเงินดิจิทัล ใกล้ตัวเราแค่ไหน?**, ค้นวันที่ 22 ตุลาคม 2562 จาก [https://www.bot.or.th/Thai/ResearchAndPublications/articles/Pages/Article\\_01Feb2019.aspx](https://www.bot.or.th/Thai/ResearchAndPublications/articles/Pages/Article_01Feb2019.aspx)

ดังนั้นรูปแบบของเงินตราตั้งแต่อดีตจนถึงปัจจุบันนั้นมีการเปลี่ยนแปลงไปตามสภาพ การค้า เศรษฐกิจ สังคม และเทคโนโลยี ซึ่งการเปลี่ยนแปลงนี้ไม่เพียงแต่เป็นการพัฒนาในเชิงวัตถุที่นำมาทำ เป็นเงินตราเท่านั้น แต่ยังมีการพัฒนาวิธีการชำระเงินโดยนำเทคโนโลยีเข้ามามีส่วนช่วยในการเพิ่ม ช่องทางการชำระเงินให้สะดวก รวดเร็ว และสามารถตอบสนองความต้องการของคนในยุคนี้ และยังมี การพัฒนารูปแบบของสื่อกลางในการแลกเปลี่ยนระหว่างบุคคลโดย ที่ไม่ถือเป็นเงินตราตามกฎหมาย อยู่ในรูปของวัตถุที่จับต้องไม่ได้และมีระบบจัดเก็บข้อมูลที่ไม่ต้องผ่านตัวกลางแต่อย่างใด

### 2.1.2 แนวคิดในการควบคุมเงินตรา

เงินตราเป็นสิ่งที่ออกใช้โดยรัฐบาล รัฐเป็นผู้มีเอกสิทธิ์ในการออกใช้เงินตราแต่เพียงผู้เดียว<sup>40</sup> และกำหนดทิศทางเศรษฐกิจของชาติโดยใช้อำนาจการควบคุมผ่านหน่วยงานต่าง ๆ ซึ่งมีหน้าที่กำกับ ดูแลการผลิตเงินและการหมุนเวียนของเงินในระบบ เช่น กระทรวงการคลัง หรือธนาคารกลาง อัน เป็นหน่วยงานที่มีบทบาทสำคัญต่อการเงินของประเทศในการทำให้ระบบเงินตราและเครดิตมี เสถียรภาพและทำให้การไหลเวียนของเงินในระบบเศรษฐกิจเป็นไปตามสภาพที่เหมาะสม ซึ่งมี หน่วยงานที่ทำหน้าที่ควบคุมเงินตราดังนี้

#### 2.1.2.1 หน่วยงานที่เกี่ยวข้องกับการควบคุมเงินตรา

1) กระทรวงการคลัง ทำหน้าที่เป็นเสาหลักทางการเงินเศรษฐกิจของประเทศ โดยให้คำแนะนำนโยบายการคลังในการบริหารการจัดเก็บรายได้ภาครัฐ การบริหารการเงิน และการจัดการทรัพย์สินของภาครัฐ ซึ่งมีการกิจหลักในด้านต่าง ๆ ดังนี้<sup>41</sup> ได้แก่ภารกิจด้านทรัพย์สิน และการกิจด้านรายได้ ซึ่งมีหน่วยงานในกำกับทำหน้าที่ในการควบคุมเงินตรา ดังนี้

(1) กรมธนารักษ์ มีหน้าที่ผลิตเหรียญ กษาปณ์ จัดทำ เครื่องราชอิสริยาภรณ์ อนุรักษ์ เก็บรักษา จัดแสดงและเผยแพร่ความรู้เกี่ยวกับทรัพย์สินอันมีค่าของ แผ่นดิน จัดให้ใช้ประโยชน์ในที่ราชพัสดุ นอกจากนี้ ยังมีหน้าที่เกี่ยวกับการควบคุมการรับ-จ่ายแลกเปลี่ยนรักษาเหรียญกษาปณ์ การเบิก-ส่งเงินคงคลังของจังหวัด และบริหารจัดการเหรียญกษาปณ์ให้ สอดคล้องกับความต้องการในระบบเศรษฐกิจและการควบคุมยอดเงินฝากของรัฐ รวมถึงดำเนินการ เกี่ยวกับการกำหนดราคาประเมินอสังหาริมทรัพย์และทรัพย์สินอื่น ตามกฎหมายที่เกี่ยวข้อง

<sup>40</sup> พงศ์บวร ควะชาติ, **สกุลเงินเสมือนจริงปลอดภัยการควบคุมบนเครือข่ายอินเทอร์เน็ต** (วิทยานิพนธ์ปริญญาโทมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558), หน้า 37.

<sup>41</sup> กระทรวงการคลัง, **ภารกิจ และหน้าที่รับผิดชอบของหน่วยงาน**, ค้นวันที่ 30 พฤษภาคม 2564 จาก <https://www.mof.go.th/th/detail/2018-12-21-15-00-10/2018-12-21-17-48-06>

(2) สำนักงานคณะกรรมการนโยบายรัฐวิสาหกิจ (สคร.) มีหน้าที่เสนอแนะนโยบาย การเงิน การบัญชี ค่าตอบแทน และสวัสดิการของรัฐวิสาหกิจ กำหนดการนำส่งเงินรายได้แผ่นดิน พัฒนาประสิทธิภาพของรัฐวิสาหกิจ จัดให้มีระบบประเมินผลการดำเนินงานและระบบการกำกับดูแลกิจการที่ดี รวมถึงการแปรรูปรัฐวิสาหกิจ

2) ธนาคารแห่งประเทศไทย เป็นสถาบันการเงินที่มีบทบาทสำคัญในการขับเคลื่อนเศรษฐกิจการเงินของประเทศ โดยทำหน้าที่ระดมและจัดสรรเงินทุนทั้งของภาคประชาชนและภาคธุรกิจ อีกทั้งยังเป็นตัวกลางในการทำธุรกรรมต่าง ๆ ให้กับภาคประชาชนและภาคเอกชน เช่น การฝากเงิน การถอนเงิน การให้สินเชื่อให้แก่ผู้กู้โดยธนาคารจะต้องบริหารความเสี่ยง รวมถึงการให้ข้อมูลทางการเงินแก่ประชาชนเพื่อการตัดสินใจในการลงทุน นอกจากนี้ธนาคารยังสามารถรับชำระค่าสินค้าและบริการต่าง ๆ ได้ ดังนั้นธุรกรรมต่าง ๆ ที่เกี่ยวข้องกับการเงินจะมีธนาคารเป็นตัวกลางในการทำธุรกรรมแทบทั้งสิ้น การดำเนินงานบริหารการเงินของธนาคารจึงต้องเป็นไปอย่างมีประสิทธิภาพ โปร่งใส รักษาสภาพคล่องทางการเงินและบริหารความเสี่ยงอย่างเหมาะสม<sup>42</sup>

ดังนั้นเศรษฐกิจและเสถียรภาพทางการเงินของประเทศจะเป็นไปในทิศทางใดย่อมขึ้นอยู่กับหลายปัจจัย แต่ปัจจัยหนึ่งที่สำคัญหนึ่งคือนโยบายทางการเงินของธนาคาร ธนาคารจึงมีบทบาทที่สำคัญในการควบคุม ดูแลการเงินของประเทศไทย อย่างไรก็ตามปัจจุบันเทคโนโลยีเข้ามามีบทบาททางการเงินมากขึ้น จนอาจนำมาใช้ทดแทนระบบการให้บริการของธนาคารได้ เช่น การโอนเงินระหว่างประเทศ หากโอนผ่านธนาคารจะมีค่าธรรมเนียมในการทำธุรกรรมค่อนข้างสูง เนื่องจากต้องผ่านตัวกลางที่อาจมีมากกว่าหนึ่งธนาคาร ยังมีตัวกลางมากยิ่งขึ้นทำให้เสียค่าธรรมเนียมมาก ในขณะที่การทำธุรกรรมผ่านเทคโนโลยีจะเสียค่าธรรมเนียมน้อยกว่าการโอนผ่านธนาคารเนื่องจากต้นทุนต่ำกว่าและโอนไปยังปลายทางได้โดยตรง ทำให้การทำธุรกรรมที่ผ่านธนาคารเริ่มมีความจำเป็นลดน้อยลง สถานการณ์ดังกล่าวจึงเป็นสิ่งที่ท้าทายความจำเป็นของธนาคารที่ต้องมีการปรับเปลี่ยนพัฒนาบทบาทการให้บริการของธนาคารให้คงอยู่เพื่อให้สอดคล้องกับยุคดิจิทัลทางการเงิน

#### 2.1.2.2 กฎหมายที่เกี่ยวข้องกับการควบคุมเงินตรา

##### 1) พระราชบัญญัติเงินตรา พ.ศ. 2501

พระราชบัญญัติเงินตรา พ.ศ. 2501 มีวัตถุประสงค์เพื่อต้องการให้ระบบการจัดการเงินตราของประเทศมีลักษณะเป็นสากล เอื้อประโยชน์ในการเศรษฐกิจทั้งภายในประเทศ

<sup>42</sup> ธนาคารแห่งประเทศไทย, **บทบาทหน้าที่ ธปท.**, ค้นวันที่ 8 กรกฎาคม 2563 จาก <https://www.bot.or.th/Thai/AboutBOT/RolesAndHistory/Pages/RolesAndResponsibility.aspx>

และการค้าระหว่างประเทศและกำหนดหลักเกณฑ์สำหรับการจัดการเกี่ยวกับการจัดทำและการใช้เงินตราของประเทศให้เหมาะสมกับสภาพเศรษฐกิจปัจจุบัน

พระราชบัญญัติเงินตรา พ.ศ. 2501 มีหลักเกณฑ์ที่สำคัญ ดังต่อไปนี้

- (1) เงินตรา หมายถึง เหรียญกษาปณ์และธนบัตร<sup>43</sup>
- (2) ห้ามมิให้ผู้ใด ทำ จำหน่าย ใช้ หรือนำออกใช้ซึ่งวัตถุหรือเครื่องหมายใด ๆ แทนเงินตราเว้นแต่จะได้รับอนุญาตจากรัฐมนตรี<sup>44</sup>
- (3) ให้กระทรวงการคลังจัดทำและนำออกใช้ซึ่งเหรียญกษาปณ์<sup>45</sup>
- (4) ให้ธนาคารแห่งประเทศไทยมีอำนาจจัดทำ จัดการ และนำออกใช้ซึ่งธนบัตรของรัฐบาลตามกฎหมายว่าด้วยธนาคารแห่งประเทศไทยได้ต่อไป ให้รัฐมนตรีประกาศ ชนิด ราคา สี ขนาด และลักษณะอื่น ๆ ของธนบัตรที่จะออกใช้ในราชกิจจานุเบกษาเว้นแต่กรณีที่จะนำออกใช้ซึ่งธนบัตรถอนคืน<sup>46</sup>
- (5) รัฐมนตรีโดยคำแนะนำของธนาคารแห่งประเทศไทยมีอำนาจประกาศกำหนดอัตราขึ้นสูงและอัตราขั้นต่ำสำหรับการซื้อหรือขายทันที ซึ่งเงินตราต่างประเทศโดยธนาคารพาณิชย์หรือบุคคลอื่นได้ และเมื่อมีประกาศของรัฐมนตริดังกล่าวแล้ว ธนาคารพาณิชย์หรือบุคคลอื่นที่ซื้อหรือขายทันทีซึ่งเงินตราต่างประเทศต้องซื้อหรือขายในอัตราที่ไม่สูงหรือต่ำกว่าอัตราที่กำหนดนั้นห้ามมิให้ธนาคารพาณิชย์หรือบุคคลอื่นรับเงินส่วนลด หรือเรียกเก็บเงินไม่ว่าประเภทใด เนื่องในการซื้อหรือขายทันทีซึ่งเงินตราต่างประเทศนอกจากค่าโทรเลข ทั้งนี้ไม่ว่าจะมีประกาศตามวรรคหนึ่งหรือไม่<sup>47</sup>
- (6) เงินตราจำต้องมีเงินทุนสำรอง โดยทรัพย์สินดังต่อไปนี้ เป็นทรัพย์สินที่ชอบด้วยกฎหมายที่จะประกอบขึ้นเป็นเงินทุนสำรองเงินตรา<sup>48</sup> คือ
  - (1) ทองคำ
  - (2) เงินตราต่างประเทศอันเป็นเงินตราที่พึงเปลี่ยนได้ หรือเงินตราต่างประเทศอื่นใดที่กำหนดโดยกฎกระทรวง ทั้งนี้ต้องเป็นรูปเงินฝากในธนาคารนอกราชอาณาจักรหรือในสถาบันการเงินระหว่างประเทศ

<sup>43</sup> มาตรา 6 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>44</sup> มาตรา 9 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>45</sup> มาตรา 10 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>46</sup> มาตรา 14 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>47</sup> มาตรา 25 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>48</sup> มาตรา 30 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

- (3) หลักทรัพย์ต่างประเทศที่จะมีการชำระหนี้เป็นเงินตราต่างประเทศที่ระบุไว้ใน (2)
- (4) ทองคำ สินทรัพย์ต่างประเทศ และสิทธิพิเศษถอนเงิน ทั้งนี้ที่นำส่งสมทบกองทุนการเงิน
- (5) ใบสำคัญสิทธิซื้อส่วนสำรอง
- (6) ใบสำคัญสิทธิพิเศษถอนเงิน
- (7) หลักทรัพย์รัฐบาลไทยที่จะมีการชำระหนี้เป็นเงินตราต่างประเทศที่ระบุไว้ใน (2) หรือเป็นบาท
- (8) ตัวเงินในประเทศที่ธนาคารแห่งประเทศไทยพึงซื้อหรือรับช่วงซื้อลดได้ แต่ต้องมีค่ารวมกันไม่เกินร้อยละสิบของจำนวนธนบัตรออกใช้สินทรัพย์ตาม (1) (2) (3) (4) (5) และ (6) นั้น ธนาคารแห่งประเทศไทยจะต้องจัดตารางไว้ให้มีค่ารวมกันทั้งสิ้นไม่ต่ำกว่าร้อยละหกสิบของจำนวนธนบัตรออกใช้

จากพระราชบัญญัติดังกล่าวจะเห็นได้ว่าระบบเงินตราของประเทศไทยประกอบด้วยสื่อกลางการแลกเปลี่ยนที่ใช้หมุนเวียนในระบบเศรษฐกิจ 2 ประเภท ได้แก่ เหรียญกษาปณ์และธนบัตรที่มีสกุลเงินบาทเป็นหน่วยบัญชี โดยที่กระทรวงการคลังรับผิดชอบในการจัดทำและนำออกใช้ซึ่งเหรียญกษาปณ์ และธนาคารแห่งประเทศไทยรับผิดชอบในการจัดการและนำออกใช้ซึ่งธนบัตรของรัฐบาล และยังมีบทบัญญัติที่กำหนดลักษณะ ผู้มีหน้าที่ออกใช้และจัดการเงินตรา<sup>49</sup> รวมถึงการกำหนดกองทุนสำรองเงินตราเพื่อรักษาเสถียรภาพและความน่าเชื่อถือของค่าเงินบาทไว้

## 2) พระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485

พระราชบัญญัติควบคุมการแลกเปลี่ยนเงินตรา พ.ศ. 2485 บัญญัติขึ้นโดยวัตถุประสงค์เพื่อรวบรวมเงินตราต่างประเทศไว้ในแหล่งกลาง เพื่อควบคุมการใช้จ่ายเงินตราต่างประเทศให้เป็นไปในทิศทางที่เป็นประโยชน์ต่อส่วนรวม เพื่อป้องกันการโอนทุนออกนอกประเทศ และเพื่อรักษาค่าภายนอกของเงินบาท หรืออัตราแลกเปลี่ยนให้มั่นคง

ตามพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485 มีการบัญญัติถึงความหมายของคำว่า เงินตรา และเงินตราต่างประเทศ ดังต่อไปนี้

“เงินตรา” หมายความว่า เงินที่ชำระหนี้ได้ตามกฎหมายในประเทศไทย<sup>50</sup>

<sup>49</sup> พงศ์บวร ควะชาติ, *เรื่องเดิม*, หน้า 139.

<sup>50</sup> มาตรา 3 แห่งพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485

“เงินตราต่างประเทศ” หมายความว่า เงินที่ชำระหนี้ได้ตามกฎหมายในประเทศอื่นใด นอกจากประเทศไทย และหมายความรวมถึงค่าแลกเปลี่ยนเงินตราต่างประเทศ<sup>51</sup>

พระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485 ยังบัญญัติถึงการให้รัฐมนตรีมีอำนาจออกกฎกระทรวงควบคุม กำกัดหรือห้ามการปฏิบัติกิจการทั้งปวงเกี่ยวกับการแลกเปลี่ยนเงินหรือการอื่นซึ่งมีเงินตราต่างประเทศเข้ามาเกี่ยวข้องไม่ว่ารูปแบบใด และให้มีอำนาจออกกฎกระทรวงดังต่อไปนี้<sup>52</sup>

- (1) การซื้อ การขาย การให้กู้ยืมเงินตราต่างประเทศหรือทองคำ
- (2) การส่งเงินตรา ธนาकारบัตร ธนาณัติ หลักทรัพย์ เงินตราต่างประเทศหรือ ทองคำออกไปนอกประเทศ
- (3) การโอนหลักทรัพย์จากประเทศไทยไปที่อื่น
- (4) การออกตั๋วแลกเงินหรือตั๋วสัญญาใช้เงิน การทำให้ตั๋วแลกเงินหรือตั๋วสัญญาใช้เงินเปลี่ยนมือ การโอนหลักทรัพย์ หรือการรับสภาพหนี้ อันเป็นการก่อให้เกิดหรือโอนไป ซึ่งสิทธิที่จะ ได้รับชำระเงินในประเทศไทยเป็นการตอบแทน
- (5) การกำหนดอัตราแลกเปลี่ยนเงิน โดยเฉพาะการนี้ถ้ารัฐมนตรีเห็นสมควรก็ให้กระทำ โดยประกาศได้
- (6) การอนุญาตให้ธนาคารหรือบุคคลอื่นใดทำการแลกเปลี่ยนเงิน
- (7) สั่งให้ขายของขาออกเป็นเงินตราต่างประเทศ หรือชำระเงินค่าของขาเข้าเป็นเงินตรา ต่างประเทศ ทั้งนี้ จะระบุชื่อเงินตราต่างประเทศนั้นด้วยก็ได้
- (8) สั่งให้ขายเงินตราต่างประเทศที่ได้มาจากของขาออก หรือซื้อเงินตราต่างประเทศ เพื่อชำระค่าของขาเข้า ให้แก่หรือจากบุคคลที่รัฐมนตรีกำหนดและกำหนดระยะเวลาวิธีการ และเงื่อนไขแห่งการขายและซื้อดังกล่าวนี้
- (9) กัก กำกัดหรือห้ามการส่งออกซึ่งของ เมื่อมิได้ขายเงินตราต่างประเทศที่ได้มาจากของนั้น หรือการนำเข้าซึ่งของ เมื่อมิได้ซื้อเงินตราต่างประเทศ เพื่อชำระค่าของนั้นตามระยะเวลา วิธีการ หรือเงื่อนไขที่กำหนดไว้
- (10) กำหนดวิธีการและเงื่อนไขในการรับหรือการใช้จ่ายเงินที่ส่งมาจากเมืองต่างประเทศ

<sup>51</sup> มาตรา 3 แห่งพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485

<sup>52</sup> มาตรา 4 แห่งพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485

(11) กำหนดให้ผู้ส่งของออกหรือผู้นำของเข้าแจ้งรายการเกี่ยวกับเงินที่ได้รับหรือได้ชำระเป็นค่าของที่ส่งออกหรือที่นำเข้า พร้อมทั้งแจ้งรายการแห่งของนั้นโดยหลักเกณฑ์และข้อกำหนดต่าง ๆ ของรัฐมนตรีที่มีอำนาจออกกฎกระทรวงควบคุม กำจัดหรือห้ามการปฏิบัติกิจการทั้งปวงเกี่ยวกับการแลกเปลี่ยนเงินหรือการอื่นซึ่งมีเงินตราต่างประเทศเข้ามาเกี่ยวข้องไม่ว่ารูปแบบใด มีการออกเป็นกฎกระทรวงฉบับที่ 13 พ.ศ. 2497 ออกตามความในพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2475 อาศัยอำนาจตามความในมาตรา 4 แห่งพระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2475

3) พระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485

พระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485 บัญญัติขึ้นโดยมีเหตุผลในการจัดตั้งธนาคารแห่งประเทศไทยขึ้นในราชอาณาจักร โดยให้มีธนาคารกลางเรียกว่า “ธนาคารแห่งประเทศไทย” (ธปท.) เป็นนิติบุคคล มีฐานะเป็นหน่วยงานของรัฐที่ไม่เป็นส่วนราชการหรือรัฐวิสาหกิจ โดยมีวัตถุประสงค์ในการดำเนินการกิจอันพึงเป็นงานของธนาคารกลางเพื่อดำรงไว้ซึ่งเสถียรภาพทางการเงิน และเสถียรภาพของระบบสถาบันการเงิน และระบบการชำระเงิน โดยต้องคำนึงถึงดำเนินนโยบายทางเศรษฐกิจของรัฐบาล ตามพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485 มีสาระสำคัญ ดังต่อไปนี้<sup>53</sup>

(1) มีวัตถุประสงค์ในการดำเนินงานของธนาคารแห่งประเทศไทยซึ่งต้องดำรงไว้ซึ่งเสถียรภาพ ทางการเงิน เสถียรภาพของระบบสถาบันการเงินและระบบการชำระเงิน<sup>54</sup> และอำนาจในการกระทำการกิจต่าง ๆ ของธนาคารแห่งประเทศไทยเพื่อให้บรรลุวัตถุประสงค์<sup>55</sup> และกำหนดข้อห้ามมิให้ธนาคารแห่งประเทศไทยกระทำการในเรื่องต่าง ๆ<sup>56</sup>

(2) กำหนดกระบวนการได้มา องค์ประกอบ คุณสมบัติและลักษณะต้องห้าม การประชุมและองค์ประชุม วาระในการดำรงตำแหน่งอำนาจหน้าที่และการพ้นจากตำแหน่งของคณะกรรมการชุดต่าง ๆ เพื่อทำหน้าที่ของธนาคารแห่งประเทศไทย (หมวด 4)

(3) กำหนดกระบวนการคัดเลือก คุณสมบัติและลักษณะต้องห้าม วาระการดำรงตำแหน่งและการพ้นจากตำแหน่งของผู้ว่าการ รวมทั้งกำหนดให้ผู้ว่าการมีความเป็น

<sup>53</sup> ธนาคารแห่งประเทศไทย, คำอธิบายสรุปสาระสำคัญของ พระราชบัญญัติธนาคารแห่งประเทศไทย พุทธศักราช 2485, ค้นวันที่ 3 พฤศจิกายน 2563 จาก <https://www.bot.or.th/Thai/AboutBOT/LawsAndRegulations/Documents/SUMLAW01.pdf>

<sup>54</sup> มาตรา 7 แห่งพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485

<sup>55</sup> มาตรา 8 แห่งพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485

<sup>56</sup> มาตรา 9 แห่งพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485

อิสระในการบริหารจัดการกิจการของธปท. รวมทั้งข้อห้ามมิให้ผู้ว่าการซึ่งพ้นจากตำแหน่งไปดำรงตำแหน่งใดในสถาบันการเงินใดภายในระยะเวลา 2 ปีนับแต่พ้นจากตำแหน่ง (หมวด 5)

(4) กำหนดสถานะ วัตถุประสงค์ ที่มาของแหล่งเงิน และอำนาจกระทำการต่าง ๆ ของกองทุนเพื่อการฟื้นฟูและพัฒนาระบบสถาบันการเงิน องค์ประกอบ วาระการดำรงตำแหน่ง การพ้นจากตำแหน่ง การประชุมและองค์ประชุม อำนาจหน้าที่ของคณะกรรมการจัดการกองทุน (หมวด 5 ทวิ)

(5) กำหนดหลักเกณฑ์เกี่ยวกับการดำเนินการตามอำนาจหน้าที่ของธนาคารแห่งประเทศไทยด้านต่าง ๆ ได้แก่ การออกธนบัตรของรัฐบาลและบัตรธนาคาร การดำเนินนโยบายการเงิน การบริหารจัดการสินทรัพย์ของ ธนาคารแห่งประเทศไทย การเป็นนายธนาคารและนายทะเบียนหลักทรัพย์ของรัฐบาล การเป็นนายธนาคารของสถาบันการเงิน การรักษาเสถียรภาพของระบบเศรษฐกิจและระบบการเงิน การจัดตั้งหรือสนับสนุนการจัดตั้งระบบการชำระเงิน (หมวด 6)

(6) กำหนดข้อห้ามมิให้ผู้ว่าการ กรรมการ พนักงานและลูกจ้างกระทำการอันใดที่ขัด หรือแย้งระหว่างผลประโยชน์ของตนและผลประโยชน์ของ ธปท. หรือขัดแย้งกับการปฏิบัติหน้าที่ของตนเอง รวมทั้งให้พนักงานหรือลูกจ้างเปิดเผยข้อมูลส่วนตัวได้เสียของตนในการปฏิบัติหน้าที่ และห้ามพนักงานหรือลูกจ้างที่มีส่วนได้เสียพิจารณาหรือเข้าร่วมการประชุมในเรื่องที่ตนมีส่วนได้เสีย และห้ามพนักงานและลูกจ้างดำรงตำแหน่ง รับจ้างหรือทำงานในสถาบันการเงิน เว้นแต่เป็นไปตามข้อบังคับของคณะกรรมการธนาคารแห่งประเทศไทย<sup>57</sup>

(7) กำหนดให้รัฐมนตรีว่าการกระทรวงการคลังมีอำนาจหน้าที่กำกับดูแลโดยทั่วไปซึ่งกิจการของธนาคารแห่งประเทศไทย และให้ธนาคารแห่งประเทศไทยหรือเป็นครั้งคราวร่วมกับรัฐมนตรีว่าการกระทรวงการคลังเพื่อประโยชน์ในการรักษาเสถียรภาพทางการเงิน หรือระบบสถาบันการเงิน (หมวด 8)

(8) กำหนดให้การบัญชีของธนาคารแห่งประเทศไทยจัดทำตามหลักการบัญชีที่รับรองทั่วไป เว้นแต่ คณะกรรมการธนาคารแห่งประเทศไทยจะกำหนดเฉพาะเรื่องเป็นอย่างอื่นเพื่อให้สอดคล้องกับการปฏิบัติของธนาคารกลางอื่นได้<sup>58</sup> และให้มีคณะกรรมการตรวจสอบเพื่อทำหน้าที่กำกับดูแลการตรวจสอบกิจการของธนาคารแห่งประเทศไทย<sup>59</sup>

(9) กำหนดโทษสำหรับบุคคล สถาบันการเงิน ที่ฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กฎหมายฉบับนี้กำหนดกระทำความผิด รวมถึงผู้ว่าการ กรรมการ พนักงานหรือ

<sup>57</sup> มาตรา 46 แห่งพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485

<sup>58</sup> มาตรา 54 แห่งพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485

<sup>59</sup> มาตรา 55 แห่งพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485

ลูกจ้างที่กระทำความผิดต่อตำแหน่งหน้าที่ หรือที่ฝ่าฝืนหรือไม่ปฏิบัติตามหลักเกณฑ์ที่กฎหมายฉบับนี้ กำหนด<sup>60</sup>

## 2.2 แนวคิด ความเป็นมาและลักษณะของสกุลเงินดิจิทัล (Virtual Currency/ Cryptocurrency)

สกุลเงินดิจิทัลเป็นสื่อกลางในการทำธุรกรรมทางการเงินอีกหนึ่งประเภทนอกเหนือจากเงินตราที่ใช้กันอยู่ โดยสกุลเงินดิจิทัลเกิดมาจากแนวคิดในการสร้างระบบการเงินที่ปราศจากการควบคุมโดยรัฐบาลของประเทศใด และผู้ใช้สามารถตรวจสอบความถูกต้องของธุรกรรมโดยใช้เทคโนโลยี ซึ่งเริ่มมีขึ้นในหมู่แฮกเกอร์และได้พัฒนามาเป็นระบบที่ใช้กับสกุลเงินดิจิทัลที่ได้รับการยอมรับมากขึ้นเนื่องจากสามารถใช้เป็นสื่อกลางได้เสมือนเป็นเงินตรา แต่เนื่องด้วยลักษณะ และวิธีการใช้สกุลเงินดิจิทัลมีข้อจำกัดจึงทำให้มีความแตกต่างจากเงินตรา ปัจจุบันการใช้สกุลเงินดิจิทัลถือเป็นทางเลือกหนึ่งของการทำธุรกรรมทางการเงินซึ่งได้รับยอมรับในสังคมออนไลน์ ที่มาพร้อมกับประโยชน์ในแง่ของความสะดวก รวดเร็ว ความเป็นส่วนตัว และค่าใช้จ่ายในการทำธุรกรรมต่ำ<sup>61</sup>

### 2.2.1 แนวคิดพื้นฐานและลักษณะทั่วไปของสกุลเงินดิจิทัล

#### 2.2.1.1 ประวัติ ความเป็นมาของสกุลเงินดิจิทัล

“สกุลเงินดิจิทัล” (Cryptocurrency) เป็นสกุลเงินใหม่ที่สร้างขึ้นจากกลไกทางคณิตศาสตร์ที่กำหนดจำนวนไว้จำกัด โดยใช้ระบบคอมพิวเตอร์ถอดรหัสเพื่อนำเงินออกจากกลไกสกุลเงินใหม่นี้ถูกออกแบบให้นำไปใช้เสมือนเป็นตัวกลางในการแลกเปลี่ยน (Medium of Exchange) สำหรับการทำธุรกรรมต่าง ๆ เพื่อลดการรวมศูนย์ของระบบการชำระเงินผ่านสถาบันการเงินให้สามารถกระจายไปยังผู้ใช้ในเครือข่ายสกุลเงินนั้น ๆ ได้โดยใช้เทคโนโลยีบล็อกเชน (Blockchain) ติดตามการเคลื่อนไหวของเงิน ซึ่งสามารถบันทึกและจัดเก็บด้วยวิธีการเข้ารหัส (Cryptographic) ซึ่งจะต้องมีการตรวจสอบความถูกต้องของรหัสก่อนที่ธุรกรรมสกุลเงินดิจิทัลจะเคลื่อนย้ายถ่ายโอน

<sup>60</sup> มาตรา 64, มาตรา 66 และมาตรา 75 แห่งพระราชบัญญัติธนาคารแห่งประเทศไทย พ.ศ. 2485

<sup>61</sup> ภัทรพร สหกิจพิจารณา, ปัญหาการจัดเก็บภาษีเงินได้บุคคลธรรมดาจากบิตคอยน์: การรับรู้เงินได้ (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2559), หน้า 9.

จากบุคคลหนึ่งไปอีกบุคคลหนึ่งจึงเป็นระบบที่สามารถป้องกันการปลอมแปลงได้ (Double Spending) นอกจากนี้วิธีการเก็บข้อมูลยังได้ออกแบบให้มีการกระจายรหัสการเข้าข้อมูลออกเป็น ส่วนย่อย ๆ (Distributed) เพื่อป้องกันไม่ให้มีศูนย์กลางอยู่ที่ใดที่หนึ่ง (Decentralized) ซึ่งการกระจายของข้อมูลนี้ทำให้ไม่สามารถเข้าถึงข้อมูลได้ง่าย และเป็นการป้องกันไม่ให้ข้อมูลถูกควบคุม หรือแทรกแซงจากบุคคลใดบุคคลหนึ่งหรือกลุ่มใดกลุ่มหนึ่ง<sup>62</sup> ระบบนี้จึงมีความปลอดภัยสูงและยาก ต่อการแฮ็กข้อมูล

ระบบการดำเนินการที่ใช้กับสกุลเงินดิจิทัลมีคุณสมบัติที่สำคัญ 6 ประการ ดังนี้<sup>63</sup>

- 1) สกุลเงินดิจิทัลมีระบบการดำเนินการที่ไม่ต้องการหน่วยงานกลางที่มีอำนาจ Central Authority ในการควบคุมหรือตรวจสอบ แต่ใช้ระบบกระจายอำนาจไปสู่การตัดสินใจร่วมกันของผู้ใช้ทั้งหมด โดยต้องเป็นผลจากมติของเสียงส่วนใหญ่
- 2) ใช้ระบบที่เก็บบันทึกภาพรวม ของหน่วยคริปโทเคอร์เรนซี และความ เป็นเจ้าของ
- 3) เป็นระบบที่กำหนดว่าจะสร้างคริปโทเคอร์เรนซีหน่วยใหม่ขึ้นหรือไม่ ถ้ามีการสร้างหน่วยใหม่ของคริปโทเคอร์เรนซีเกิดขึ้น ระบบก็จะกำหนดสถานะของสภาพเดิมของมันที่ ผ่านมา เพื่อใช้พัฒนาความเป็นเจ้าของของหน่วยที่ถูกสร้างขึ้น
- 4) ความเป็นเจ้าของคริปโทเคอร์เรนซีสามารถพิสูจน์ความเป็นเจ้าของได้ โดยการพิสูจน์การเข้ารหัส (Cryptographic)
- 5) ระบบดังกล่าวยอมให้ธุรกรรมถูกดำเนินการเปลี่ยนแปลงความเป็น เจ้าของของของหน่วยคริปโทเคอร์เรนซีรายการทางธุรกรรม (Transaction Statement) จะถูกสร้างขึ้น มาโดยใช้ความเป็นส่วนบุคคลใด ๆ (An Entity) ซึ่งจะมีไว้สำหรับผู้เป็นเจ้าของของหน่วยปัจจุบัน ของคริปโทเคอร์เรนซีเหล่านั้น
- 6) หากปรากฏว่ามีคำสั่งเพื่อเปลี่ยนแปลงความเป็นเจ้าของ ของหน่วย คริปโทเคอร์เรนซีหน่วยเดียวกัน เกิดขึ้นพร้อม ๆ กันแล้ว ระบบจะทำการเลือกคำสั่งดังกล่าวเพียง คำสั่งเดียว โดยใช้มติส่วนใหญ่ในเครือข่ายตัดสินใจเพียงคำสั่งเดียว

<sup>62</sup> Chris Burniske and Jack Tatar, **Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond** (New York: McGraw Hill, 2017), p. 87.

<sup>63</sup> Jan Lansky, "Possible State Approaches to Cryptocurrencies," **Journal of Systems Integration** 9, 1 (January 2018): 19-31.

### 2.2.1.2 ความหมายของสกุลเงินดิจิทัล

สกุลเงินดิจิทัลนี้อาจเรียกได้หลายคำแตกต่างกันไป เช่น เงินเสมือน สกุลเงินเข้ารหัส คริปโทเคอร์เรนซี เป็นต้น เนื่องจากสกุลเงินดิจิทัลเป็นการทำธุรกรรมด้วยระบบ Decentralise จึงไม่มีหน่วยงานกลางได้รับผิดชอบเป็นการเฉพาะ ดังนั้นการให้ความหมายจึงเป็นตามมุมมองของแต่ละหน่วยงานที่มีหน้าที่รับผิดชอบ

สกุลเงินดิจิทัล หมายถึง สกุลเงินซึ่งเป็นสกุลเงินดิจิทัลที่ไม่มีการควบคุมซึ่งมีเฉพาะในรูปแบบอิเล็กทรอนิกส์ ถูกจัดเก็บและทำธุรกรรมผ่านซอฟต์แวร์ที่กำหนดไว้ในแอปพลิเคชันมือถือหรือในคอมพิวเตอร์โดยผ่านกระเป๋าเงินดิจิทัลเฉพาะ ดังนั้นทุกธุรกรรมจึงเกิดขึ้นบนอินเทอร์เน็ตผ่านเครือข่ายที่ปลอดภัยและทำไว้เป็นการเฉพาะที่เรียกว่าบล็อกเชน<sup>64</sup>

Virtual Currency หรือเงินเสมือน คือ สิ่งใช้แทนมูลค่าซึ่งไม่ได้ออกหรือรับรองไม่ว่าจะโดยธนาคารกลางหรือโดยรัฐบาล ไม่จำเป็นต้องตราขึ้นเป็นสกุลเงินตามกฎหมายจึงไม่มีสถานะทางกฎหมายเป็นสกุลเงินหรือเงิน แต่อาจถูกยอมรับจากบุคคลได้โดยพฤตินัยหรือนิตินัย ไม่ว่าจะเป็นการแลกเปลี่ยน การโอนเปลี่ยนมือ การจัดเก็บและซื้อขายกันผ่านทางอิเล็กทรอนิกส์<sup>65</sup>

สื่อกลางในการแลกเปลี่ยนที่สามารถใช้ได้เหมือนเงินในสภาพแวดล้อมบางลักษณะ แต่ไม่มีสถานะเป็นตราสารที่ใช้ชำระหนี้ได้ตามกฎหมายในเขตอำนาจใด ๆ<sup>66</sup>

<sup>64</sup> Thailand-option Team, **สกุลเงินเสมือนคืออะไร?**, ค้นวันที่ 3 กุมภาพันธ์ 2563 จาก <https://thailand-option.com/cryptocurrency/>

<sup>65</sup> Tom Keatinge, David Carlisle and Florence Keen, **Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses** (Washington: European Parliament, 2018), Retrieved September 22, 2019 from [https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_STU\(2018\)604970\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf)

‘A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons as a means of exchange and which can be transferred, stored and traded electronically.’

<sup>66</sup> Treasury Financial Crimes Enforcement Network, **Application of Fincen’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies,**

Virtual Currency ทำหน้าที่เป็นตัวกลางในการแลกเปลี่ยน อยู่ในรูปแบบดิจิทัลที่ไม่ได้ออกใช้โดยหรือรับประกันโดยรัฐบาลใด จึงแตกต่างจากซึ่งเป็นเหรียญและเงินกระดาษของประเทศที่กำหนดเป็นเงินตราที่ถูกกฎหมาย<sup>67</sup>

Cryptocurrency หมายถึง “หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นตัวกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และให้หมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นใดตามที่คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ประกาศกำหนด”<sup>68</sup>

Cryptocurrency เกิดขึ้นจากความต้องการสร้างเครื่องมือเพื่อใช้ในการชำระหนี้ โดยไม่ใช้ตัวกลางซึ่งทำได้โดยใช้เทคโนโลยีบล็อกเชน (Blockchain) หรือ Distributed Ledger Technology (DLT) ที่มีลักษณะของการกระจายศูนย์ในการเก็บข้อมูล และการร่วมกันทำงานระหว่างผู้ใช้งานในเครือข่ายเพื่อช่วยรับรองความถูกต้องของข้อมูลที่ถูกบันทึกลงในเครือข่ายได้อย่างโปร่งใส ตลอดจนใช้วิธีการเข้ารหัส (Cryptography) เพื่อเพิ่มความปลอดภัยในการทำธุรกรรม ป้องกันไม่ให้เกิดการปลอมแปลงหรือแก้ไขข้อมูลธุรกรรมที่ได้มีการทำธุรกรรมหรือบันทึกไปก่อนหน้านี้ ซึ่งเทคโนโลยีนี้ช่วยให้ผู้ใช้คริปโทเคอร์เรนซีสามารถทำธุรกรรมระหว่างกันโดยตรง ไม่ต้องผ่านตัวกลางอย่างธนาคารกลางหรือธนาคารพาณิชย์<sup>69</sup>

นอกจากนี้ธนาคารแห่งประเทศไทยยังได้ให้ความหมายของคำว่าบิตคอยน์ซึ่งเป็นหนึ่งในสกุลเงินดิจิทัล (Cryptocurrency) ไว้ในข่าวของธนาคารแห่งประเทศไทยฉบับที่ ธปท. 8/2557 เรื่อง ข้อมูลเกี่ยวกับบิตคอยน์และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่น ๆ ที่มีลักษณะใกล้เคียงกัน ซึ่งธนาคารแห่งประเทศไทยเห็นว่า บิตคอยน์คือหน่วยข้อมูลอิเล็กทรอนิกส์ที่เกิดจากกลไกทาง

---

Retrieved September 22, 2019 from <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>

<sup>67</sup> Financial Action Task Force, **Virtual Currencies: Key Definitions and Potential AML/CFT Risks** (Paris, France: FATF, 2014), Retrieved September 22, 2019 from <http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>

<sup>68</sup> มาตรา 3 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

<sup>69</sup> ธรรมรักษ์ หมื่นจักร, รัชพร วงศาโรจน์, กษิติศ ต้นสงวน และเกวลี สันตโยดม, “FAQ Cryptocurrencies and Friends: นวัตกรรม พัฒนาการ ความเสี่ยงและการกำกับดูแล,” **Digital Currency Series 2** (7 มีนาคม 2563): 1.

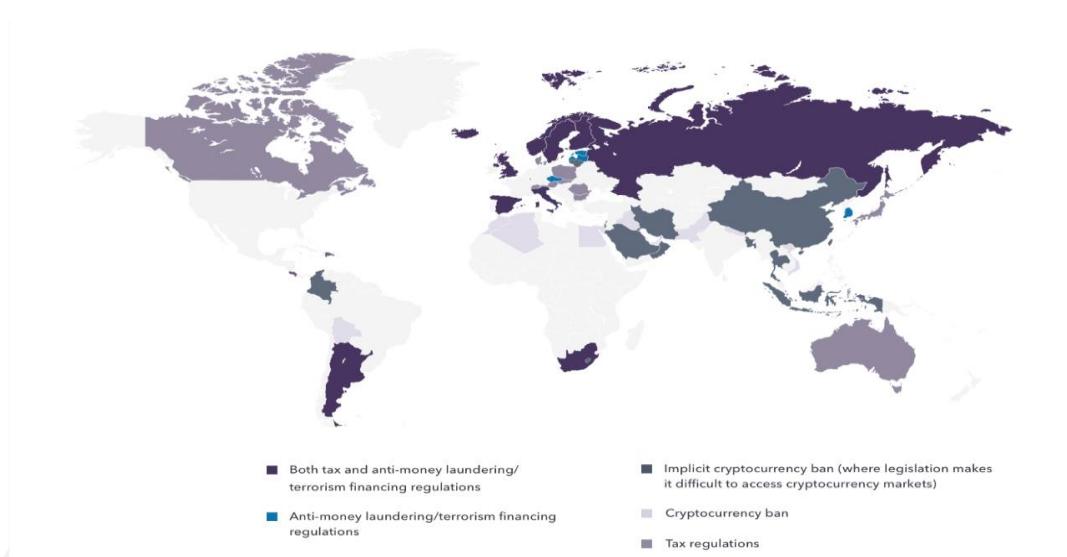
คอมพิวเตอร์ที่ถูกกำหนดไว้โดยคนกลุ่มหนึ่ง ซึ่งมุ่งหวังจะใช้บิตคอยน์เป็นสื่อกลางการแลกเปลี่ยนบิตคอยน์นั้นจะถูกจัดเก็บไว้ที่เครื่องคอมพิวเตอร์ แลปท็อปหรือสมาร์ตโฟนของผู้ใช้ซึ่งสามารถโอนให้กันได้ กระทั่งต่อมาเริ่มมีการนำบิตคอยน์มาใช้ชำระราคาสินค้าในลักษณะที่อาจทำให้เข้าใจว่าบุคคลใด ๆ สามารถใช้บิตคอยน์ซื้อขายสินค้าและนำมาแลกเปลี่ยนกับเงินตราสกุลต่าง ๆ ได้ โดยกำหนดอัตราแลกเปลี่ยนตามความพอใจกันเองในกลุ่มผู้ใช้ที่มีความเชื่อมั่นในระบบการเงินของบิตคอยน์ อย่างไรก็ตามธนาคารแห่งประเทศไทยยังไม่ได้ประกาศยอมรับให้บิตคอยน์มีสถานะเป็นเงินตราที่สามารถชำระหนี้ได้ตามกฎหมาย อีกทั้งยังไม่มีมูลค่าในตัวเอง มูลค่าของหน่วยข้อมูลนั้นจะแปรผันไปตามความต้องการของกลุ่มคนที่ซื้อขาย จึงเปลี่ยนแปลงได้อย่างรวดเร็วและกลายเป็นสิ่งที่ไม่มีความหมายเมื่อไม่มีผู้ใดต้องการแล้ว<sup>70</sup>

จากที่กล่าวถึงความหมายของสกุลเงินดิจิทัล จึงสรุปได้ว่าสกุลเงินดิจิทัลหมายถึงสิ่งที่ใช้เป็นตัวกลางในการแลกเปลี่ยนสินค้า บริการ มีมูลค่าทางการเงินและทำหน้าที่เสมือนเป็นเงินตราที่อยู่ในรูปแบบดิจิทัลซึ่งไม่ใช่เหรียญหรือธนบัตรในสกุลเงินบาทของประเทศไทยหรือของประเทศอื่น ปัจจุบันสกุลเงินดิจิทัลจึงยังไม่มีสถานะเป็นเงินตราตามกฎหมายไทย และยังไม่มีการควบคุมมิให้มีการนำไปใช้ในทางที่มิชอบ ดังนั้นหากเกิดความเสียหายก็อาจส่งผลกระทบต่อระบบเศรษฐกิจของประเทศได้

### 2.2.1.3 การยอมรับและสถานะของสกุลเงินดิจิทัล

ปัจจุบันสกุลเงินดิจิทัลเป็นที่รู้จักและถูกใช้อย่างแพร่หลายทั่วโลก เนื่องจากเป็นการทำธุรกรรมสามารถเชื่อมต่อกันได้ในโลกออนไลน์ แต่อย่างไรก็ตามการยอมรับและการกำหนดสถานะของสกุลเงินดิจิทัลของแต่ละประเทศยังมีความแตกต่างกันอยู่ตามบริบทของแต่ละประเทศ ซึ่งการยอมรับที่มากหรือน้อยนั้นรวมถึงบางประเทศอาจไม่ยอมรับสกุลเงินดิจิทัล ได้นำมาซึ่งการกำหนดกฎระเบียบที่เกี่ยวข้องกับสกุลเงินดิจิทัลที่แตกต่างกันออกไปด้วย

<sup>70</sup> ธนาคารแห่งประเทศไทย, “ข้อมูลเกี่ยวกับบิตคอยน์และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่น ๆ ที่มีลักษณะใกล้เคียงกัน,” ข่าวของธนาคารแห่งประเทศไทย 8 (2557).



ภาพที่ 2.1 World Map Showing Differences in Cryptocurrency Regulation<sup>71</sup>

ปัจจุบันแต่ละประเทศมีมาตรการภายในที่เกี่ยวข้องกับ Cryptocurrency แตกต่างกันไป ตั้งแต่ยอมรับสถานภาพทางกฎหมาย การกำหนดกฎเกณฑ์เงื่อนไขต่าง ๆ ในการควบคุม ตลอดจนบางประเทศได้กำหนดให้เป็นสิ่งต้องห้ามหรือเป็นสิ่งผิดกฎหมาย ทั้งนี้แนวทางการออกมาตรการกำกับดูแลบริหารจัดการ Cryptocurrency เป็นไปตามบริบทของแต่ละประเทศซึ่งมีนโยบายในการควบคุม 5 แนวทาง ดังนี้

<sup>71</sup> The Law Library of Congress, **Regulation of Cryptocurrency Around the World**, Retrieved November 26, 2021 from <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>

ตารางที่ 2.1 การควบคุมสกุลเงินดิจิทัลของแต่ละประเทศ

Absolute Cryptocurrency Ban	Implicit Cryptocurrency Ban*	Tax Regulations	Anti-money Laundering/ Terrorism Financing Regulations	Both tax and Anti-money Laundering/ Terrorism Financing Regulations
ประเทศที่ออก กฎหมายห้ามทำ ธุรกรรมเกี่ยวกับ สกุลเงินดิจิทัล	ประเทศที่ออก กฎหมายที่มีการ ตรวจสอบธุรกรรม การเข้าถึงสกุลเงิน ดิจิทัล	ประเทศที่ ออกกฎหมาย เกี่ยวกับสกุล เงินดิจิทัลเพื่อ ประโยชน์ ในทางภาษี	ประเทศที่ออก กฎหมายว่าด้วย การป้องกันและ ปราบปรามการ ฟอกเงิน/การ สนับสนุนทาง การเงินกับการก่อ การร้าย	ประเทศที่ออก กฎหมายเพื่อ ประโยชน์ในทาง ภาษีและกฎหมาย ว่าด้วยการป้องกัน และปราบปราม การฟอกเงิน/การ สนับสนุนทาง การเงินกับการก่อ การร้าย
Algeria	Bahrain	Argentina	Cayman Islands	Australia
Bolivia	Bangladesh	Austria	Costa Rica	Australia
Egypt	China	Bulgaria	Czech Republic	Denmark
Iraq	Colombia	Finland	Estonia	Japan
Morocco	Dominican Republic	Iceland	Gibraltar	Switzerland
Nepal	Indonesia	Israel	Hong Kong	
Pakistan	Iran	Italy	Isle of Man	
United Emirates	Arab Kuwait	Norway	Jersey	
	Lesotho	Poland	Latvia	

Absolute Cryptocurrency Ban	Implicit Cryptocurrency Ban*	Tax Regulations	Anti-money Laundering/ Terrorism Financing Regulations	Both tax and Anti-money Laundering/ Terrorism Financing Regulations
ประเทศที่ออก กฎหมายห้ามทำ ธุรกรรมเกี่ยวกับ สกุลเงินดิจิทัล	ประเทศที่ออก กฎหมายที่มีการ ตรวจสอบธุรกรรม การเข้าถึงสกุลเงิน ดิจิทัล	ประเทศที่ ออกกฎหมาย เกี่ยวกับสกุล เงินดิจิทัลเพื่อ ประโยชน์ ในทางภาษี	ประเทศที่ออก กฎหมายว่าด้วย การป้องกันและ ปราบปรามการ ฟอกเงิน/การ สนับสนุนทาง การเงินกับการก่อ การร้าย	ประเทศที่ออก กฎหมายเพื่อ ประโยชน์ในทาง ภาษีและกฎหมาย ว่าด้วยการป้องกัน และปราบปราม การฟอกเงิน/การ สนับสนุนทาง การเงินกับการก่อ การร้าย
	Lithuania Macau Oman Qatar Saudi Arabia Taiwan	Romania Russia Slovakia South Africa Spain Sweden United Kingdom	Liechtenstein Luxembourg Singapore	

จากภาพและตารางข้างบนสามารถแบ่งการยอมรับสกุลเงินดิจิทัลออกเป็น 2 กลุ่มใหญ่ด้วยกันคือ กลุ่มที่หนึ่งคือกลุ่มประเทศที่รัฐไม่มีนโยบายในการสนับสนุนให้ประกอบธุรกรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัลรวมถึงประเทศที่รัฐไม่ได้มีการห้ามประกอบธุรกรรมเกี่ยวข้องกับสกุลเงินดิจิทัลโดยตรงแต่ได้ออกกฎหมายเพื่อไม่ให้เกิดการทำธุรกรรมเกิดความคล่องตัว ได้แก่ กลุ่มประเทศที่ปรากฏตามตาราง Absolute Cryptocurrency Ban และ Implicit Cryptocurrency Ban ส่วนกลุ่มที่สองคือ ประเทศที่มี

การยอมรับสกุลเงินดิจิทัลโดยออกกฎหมายควบคุมการทำธุรกรรมตามลักษณะการใช้หรือการถือครองที่อาจก่อให้เกิดความเสียหายต่อรัฐหรือประชาชนได้ ได้แก่กลุ่มประเทศที่ปรากฏตามตาราง Tax Regulations Anti-money Laundering/Terrorism Financing Regulations และ Both Tax and Anti-money Laundering/Terrorism Financing Regulations จากการศึกษาพบว่าแม้ประเทศในกลุ่มที่สองนี้จะมีกฎหมายออกมาควบคุมสกุลเงินดิจิทัลบ้างแล้วก็ตาม ปัจจุบันมีเพียงประเทศเอลซัลวาดอร์ประเทศเดียวในโลกที่ยอมรับให้บิตคอยน์ซึ่งเป็นหนึ่งในสกุลเงินดิจิทัลสามารถชำระหนี้ได้ตามกฎหมาย (Legal Tender)<sup>72</sup> ส่วนประเทศญี่ปุ่นยังไม่มีกรยอมรับให้คริปโทเคอร์เรนซีเป็นเงินที่ใช้ชำระหนี้ได้ตามกฎหมาย เพียงแต่มีการรับรองให้ใช้เป็นช่องทางในการชำระเงินเท่านั้น (Means of Payment, Not a Legal Currency)<sup>73</sup>

สำหรับประเทศไทยอาจจัดอยู่ในประเทศกลุ่มที่สองเนื่องจากประเทศไทยยังไม่ได้มีการยอมรับให้สกุลเงินดิจิทัลมีสถานะเป็นเงินตราแต่ก็ได้มีการประกาศห้ามมิให้ใช้สกุลเงินดิจิทัล ดังนั้นสกุลเงินดิจิทัลจึงไม่มีสิ่งผิดกฎหมายโดยสภาพ แต่ได้มีออกกฎหมายเพื่อควบคุมการประกอบธุรกิจที่เกี่ยวข้องกับสกุลเงินดิจิทัลไว้ คือ พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 มีวัตถุประสงค์ในการกำกับและควบคุมการดำเนินกิจกรรมและการประกอบธุรกิจเกี่ยวกับสินทรัพย์ดิจิทัล พระราชบัญญัติป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542 ที่กำหนดให้สถาบันการเงินมีหน้าที่ต้องรายงานธุรกรรม<sup>74</sup> และพระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19) พ.ศ. 2561 ที่กำหนดให้มีการจัดเก็บภาษีเงินได้จากกำไรการซื้อขายคริปโทเคอร์เรนซี<sup>75</sup>

ดังนั้นจะเห็นได้ว่าประเทศไทยไม่ได้มีนโยบายที่จะห้ามมิให้ใช้สกุลเงินดิจิทัล แต่ได้มีการกำหนดเงื่อนไขบางประการตามแต่ละวัตถุประสงค์ที่ต้องการควบคุมให้อยู่ในความดูแลของรัฐ

#### 2.2.1.4 แนวคิดเกี่ยวกับบล็อกเชน

บล็อกเชน คือเทคโนโลยีที่ถูกคิดค้นขึ้นมาครั้งแรกเพื่อใช้ในการจัดเก็บข้อมูล การบันทึก การแก้ไข ตลอดจนการตรวจสอบข้อมูลในการทำธุรกรรมทางการเงินอย่างเป็นระบบโดยไม่ผ่านองค์กรกลางหรือธนาคารใด ๆ จึงมีความปลอดภัยสูง ระบบนี้จึงมีความแตกต่างจากการทำ

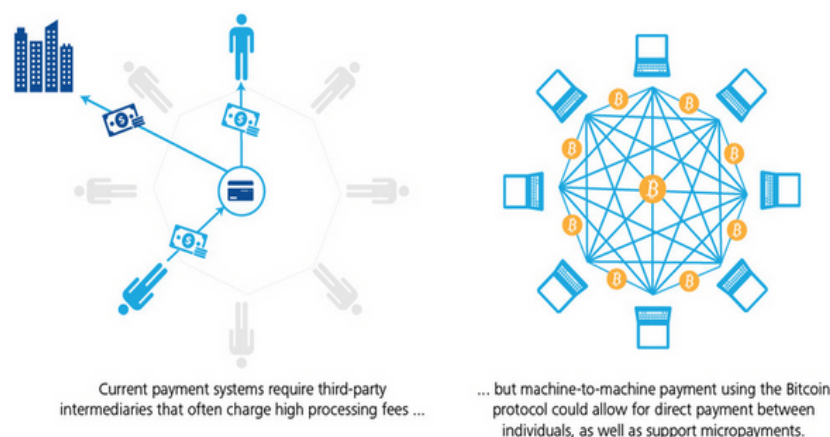
<sup>72</sup> CNBC, *El Salvador Looks to Become the World's First Country to Adopt Bitcoin as Legal Tender*, Retrieved June 7, 2021 from <https://www.cnbc.com/2021/06/05/el-salvador-becomes-the-first-country-to-adopt-bitcoin-as-legal-tender.html>

<sup>73</sup> Article 2-5 of Japan's Payment Services Act (PSA) 25 May 2016

<sup>74</sup> มาตรา 13 แห่งพระราชบัญญัติการป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542

<sup>75</sup> มาตรา 3 (ณ) แห่งพระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19) พ.ศ. 2561

ธุรกรรมแบบเดิมที่ให้ธนาคารเป็นศูนย์กลางในการจัดเก็บข้อมูลและเป็นสถานที่เชื่อมต่อธุรกรรมระหว่างบุคคล ส่งผลให้ต้องใช้เวลาในการทำธุรกรรมกับธนาคารหรือตัวกลางอื่น ๆ ในแต่ละครั้งและมีค่าธรรมเนียมในการให้บริการ



ภาพที่ 2.2 การเก็บข้อมูลแบบรวมศูนย์โดยมีตัวกลางและแบบกระจายข้อมูลโดยที่ไม่มีตัวกลาง<sup>76</sup>

จากภาพข้างต้นการเก็บข้อมูลแบบรวมศูนย์โดยมีตัวกลางและแบบกระจายข้อมูลโดยที่ไม่มีตัวกลางทำให้การทำธุรกรรมการเงินเป็นได้อย่างสะดวกสบาย โดยใช้ช่องทางออนไลน์ ในขณะที่บล็อกเชนนั้น สามารถลดขั้นตอนที่เกี่ยวกับธนาคารหรือองค์กรกลางในการจัดเก็บข้อมูลได้อย่างมาก โดยบล็อกเชนจะทำการเก็บข้อมูลต่าง ๆ ไว้ในแต่บล็อก ซึ่งข้อมูลในแต่ละบล็อกนั้นสามารถแชร์ต่อไปยังบุคคลที่เกี่ยวข้องคล้องต่อเป็นห่วงโซ่ หรือ เชน (Chain) โดยที่ทุกคนสามารถทราบได้ว่าใครเป็นเจ้าของข้อมูล เนื่องจากข้อมูลที่บรรจุอยู่ภายในแต่ละบล็อกนั้นจะมีการบันทึกไว้ หากมีข้อมูลเพิ่มขึ้นบล็อกก็จะมีจำนวนเพิ่มขึ้น โดยแต่ละบล็อกจะมีการรักษาความปลอดภัยด้วยวิธีการใช้รหัส (Cryptography) ผู้ที่ต้องการเข้าถึงข้อมูลจะต้องทราบรหัส ในแต่ละบล็อกจะประกอบด้วยส่วนหลัก ๆ คือแฮชรหัสลับ (Cryptographic Hash) ของบล็อกก่อนหน้า ข้อมูลการประทับเวลา

<sup>76</sup> Tiffany Wan and Max Hoblitzell, **Bitcoin Fact. Fiction. Future**, Retrieved July 25, 2021 from <https://www2.deloitte.com/us/en/insights/topics/emerging-technologies/bitcoin-fact-fiction-future.html>

(Timestamp) และข้อมูลการทำธุรกรรม (Transaction Data) ดังนั้นเมื่อรายละเอียดของข้อมูลการทำธุรกรรมถูกบันทึกไว้ในบล็อกเชนแล้ว รหัสจะฝังติดอยู่กับบล็อกนั้นมีสภาพถาวร แก้ไขได้ยาก แต่หากต้องการเปลี่ยนแปลงแก้ไขข้อมูลในบล็อกจะต้องมีการใส่รหัสเพื่อเปลี่ยนแปลงข้อมูลของบล็อกถัดไปที่ผูกเชื่อมต่อกับบล็อกที่ต้องการเปลี่ยนแปลง ซึ่งจะต้องได้รับความยินยอมเป็นฉันทามติหรือเสียงส่วนใหญ่ของเครือข่ายบล็อกเชนนั้นเสียก่อน<sup>77</sup>

นอกจากนี้สิ่งที่สำคัญที่สุดของกระบวนการบล็อกเชนที่เกิดขึ้นทั้งหมด คือ ไม่มีผู้ควบคุม แต่ดำเนินการได้ด้วยตัวของมันเอง รายการของธุรกรรมทั้งหมดจะถูกบันทึกอยู่ในบล็อกเชนทุกบล็อกด้วยตัวของมันเอง และสามารถทำการยืนยัน รับรองธุรกรรมนั้นโดยอัตโนมัติ ด้วยเหตุนี้บล็อกเชนจึงเป็นเทคโนโลยีที่เรียกว่า Distributed Ledger Technology ซึ่งหมายความว่า เป็นระบบบัญชีแยกประเภท (Ledger) เป็นบล็อกแบบกระจายตัว (Distributed) และไม่มีกรรมกรรวมศูนย์กลาง (Decentralized) ดังนั้นหากธุรกรรมมีการเคลื่อนไหว จะถูกบันทึกไว้ทั้งหมดทุกบล็อกโดยไม่ต้องมีนายทะเบียนหรือผู้ใดมาควบคุมอีก

ปัจจุบันบล็อกเชนไม่เพียงแต่ถูกนำมาใช้กับวงการการเงินดิจิทัลเท่านั้น แต่บล็อกเชนยังเป็นเทคโนโลยีที่มีบทบาทสำคัญในการจัดเก็บข้อมูลที่สามารถนำไปประยุกต์ใช้และยังมีการพัฒนาการใช้บล็อกเชน ในการโอนเงินระหว่างประเทศ จากเดิมที่ใช้เวลาหลายวันและมีขั้นตอนยุ่งยาก แต่ขณะนี้ใช้เวลาเพียงไม่กี่นาที นอกจากนี้ยังมีการนำไปประยุกต์ใช้กับวงการอื่น ๆ เช่น ธุรกิจเกี่ยวกับสุขภาพในการเก็บประวัติการรักษาโรคต่าง ๆ ยาที่ใช้ในการรักษา จะถูกเก็บไว้ในบล็อกเชนทั้งหมด รวมถึงหากมีการเปลี่ยนโรงพยาบาล ข้อมูลดังกล่าวของคนไข้ก็จะถูกส่งต่อไปยังโรงพยาบาลใหม่ เพื่อให้แพทย์วินิจฉัยโรคจากประวัติเดิมได้ หรือในวงการธุรกิจอสังหาริมทรัพย์สามารถใช้บล็อกเชน ในการเก็บเอกสาร หลักฐานต่าง ๆ เกี่ยวกับที่ดิน เพื่อพิสูจน์ความเป็นเจ้าของ โดยไม่ต้องมีนายทะเบียนที่ดิน<sup>78</sup> ทำให้ลดขั้นตอนในการติดต่อราชการ ประหยัดเวลา และช่วยลดปริมาณกระดาษเพื่อรักษาสิ่งแวดล้อมให้กับโลกได้อีกทาง

อย่างไรก็ตามแม้บล็อกเชนจะเป็นเทคโนโลยีมีต่อประโยชน์และนำไปประยุกต์ใช้ได้หลากหลายวงการก็ตาม แต่บล็อกเชนก็อาจมีข้อจำกัดในการใช้บางประการ กล่าวคือ ความซับซ้อนของระบบบล็อกเชนเป็นระบบเก็บรักษาข้อมูล ที่คิดค้นขึ้นเพื่อให้มีลักษณะที่ยากต่อการแก้ไข

<sup>77</sup> พรชัย บุญบรรรฉัตรกุล, การศึกษารูปแบบและการควบคุมการใช้เครือข่ายระบบเงินดิจิทัลเพื่อป้องกันการฟอกเงิน (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2561), หน้า 6-7.

<sup>78</sup> ทพพล น้อยปัญญา, กฎหมายเรื่อง Bitcoin Blockchain ICO and etc. (กรุงเทพมหานคร: วิญญูชน, 2561), หน้า 45-46.

โดยข้อมูลที่ถูกลบทิ้งไปแล้วจะไม่สามารถกลับไปแก้ไขข้อมูลชุดก่อนหน้าได้ ดังนั้นข้อมูลที่จะนำเข้าระบบบล็อกเชนต้องมีความถูกต้องตั้งแต่แรก แต่เมื่อผู้ที่ระบุข้อมูลนั้นเป็นมนุษย์ จึงอาจเกิดข้อผิดพลาดในการระบุข้อมูลขึ้นได้ เมื่อต้องการแก้ไขข้อมูลในระบบที่ถูกออกแบบมาเพื่อให้อายุต่อการแก้ไข จึงเป็นเรื่องที่ทำได้ค่อนข้างยาก ต้องอาศัยผู้ที่มีความรู้ ความเข้าใจในระบบดังกล่าว อีกทั้งในช่วงระหว่างการแก้ไขข้อมูลอาจทำให้ข้อมูลที่ผิดพลาดยังคงค้างอยู่ในระบบบล็อกเชน จำเป็นต้องมีผู้ที่มีความรู้ความเชี่ยวชาญในการวางระบบรวมถึงสามารถแก้ไขปัญหาที่อาจเกิดความผิดพลาดขึ้นได้

นอกจากนี้ระบบบล็อกเชนเป็นระบบที่พึ่งพาการยืนยัน ตรวจสอบโดยการยอมรับข้อมูลจากผู้ใช้ในระบบโดยใช้คะแนนเสียงเกินกึ่งหนึ่ง ดังนั้นเพื่อให้ระบบบล็อกเชนปลอดภัย จึงจำเป็นที่จะต้องมีการใช้คนจำนวนมากให้ระบบมีขนาดที่ใหญ่พอที่จะทำให้ระบบบล็อกเชนไม่เกิดการรวมศูนย์อยู่กับคนใดคนหนึ่ง หรือกลุ่มใดกลุ่มหนึ่งได้ ระบบจึงจะมีประสิทธิภาพและมีความน่าเชื่อถือ

#### 2.2.1.5 สกุลเงินดิจิทัลในปัจจุบัน

ปัจจุบันสกุลเงินดิจิทัลมีมากกว่า 20,000 สกุล (ข้อมูลตั้งแต่ปี 2013-กรกฎาคม 2022)<sup>79</sup> ซึ่งแต่ละสกุลเงินที่ถูกสร้างขึ้นนั้นมีระดับความนิยมและความน่าเชื่อถือแตกต่างกันไป อย่างไรก็ตามแม้ในตลาดการเงินจะมีสกุลเงินดิจิทัลต่าง ๆ ที่เกิดขึ้นใหม่มากมาย แต่สำหรับประเทศไทยสำนักงานคณะกรรมการตลาดหลักทรัพย์ได้มีการกำหนดสกุลเงินดิจิทัลที่สามารถซื้อ-ขาย แลกเปลี่ยน ในฐานะที่เป็นสินทรัพย์ดิจิทัลตามกฎหมายไทย ภายใต้พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ได้กำหนดไว้เพียง 7 สกุล ดังต่อไปนี้<sup>80</sup>

1) บิตคอยน์ (Bitcoin) สกุลเงินสมมติที่ถูกสร้างขึ้นในรูปแบบดิจิทัลเป็นคริปโทเคอร์เรนซีสกุลแรกที่เป็นที่รู้จักของโลก ถูกสร้างขึ้นในปี ค.ศ. 2009 โดยบุคคลหรือกลุ่มบุคคลที่ใช้นามแฝงว่า “ซาโตชิ นากาโมโตะ” (Satoshi Nakamoto) โดยมีแนวคิดเริ่มแรกมาจากการสร้างสกุลเงินใหม่เพื่อใช้เป็นตัวกลางในการแลกเปลี่ยนสินค้าและบริการในโลกออนไลน์ที่สามารถทำธุรกรรมกันได้โดยที่ไม่ผ่านองค์กรกลางหรือธนาคารกลางในการดูแลตรวจสอบ

บิตคอยน์ได้ออกแบบให้บล็อกเชนเข้ามาเป็นส่วนประกอบที่สำคัญของบิตคอยน์ในการทำหน้าที่เป็นเซิร์ฟเวอร์มีบัญชีแยกประเภทสาธารณะสำหรับการดำเนินการธุรกรรมทั้งหมด และยังมีกลไกในแก้ปัญหาการชำระเงินซ้ำซ้อนโดยไม่ต้องพึ่งหน่วยงานที่เชื่อถือได้ในการตรวจสอบการชำระเงินดังกล่าว นอกจากนี้ยังได้มีการกำหนดปริมาณเงินบิตคอยน์ไว้ในระบบ 21 ล้านหน่วย เมื่อถึงจำนวนดังกล่าวแล้วจะหยุดการออกโดยอัตโนมัติ ซึ่งอุปทานของบิตคอยน์ที่มีจำกัด

<sup>79</sup> Cryptocurrency Prices, Charts and Market Capitalizations, Retrieved December 31, 2022 from <https://coinmarketcap.com/>

<sup>80</sup> สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์

ส่งผลให้ราคาของบิตคอยน์ปรับสูงขึ้นอย่างรวดเร็วเมื่อมีความนิยมเพิ่มมากขึ้น อย่างไรก็ตาม การออกแบบของบิตคอยน์ที่ให้ผู้ร่วมเครือข่ายทุกคนมาร่วมกันรับรองธุรกรรมทำให้ต้องใช้เวลาในการรับรองธุรกรรมค่อนข้างนาน โดยอยู่ที่ประมาณ 10 นาที เมื่อมีจำนวนธุรกรรมหนาแน่นก็อาจทำให้ต้องใช้เวลามากกว่าหนึ่งชั่วโมง ส่งผลให้การนำบิตคอยน์ไปใช้ในการทำธุรกรรมชำระค่าสินค้าและบริการในชีวิตประจำวันทำได้ไม่สะดวก ขณะที่ราคาของบิตคอยน์ค่อนข้างผันผวน จึงส่งผลให้ปัจจุบันผู้ใช้ส่วนใหญ่มักจะนำบิตคอยน์ไปใช้ในการลงทุนเพื่อการเก็งกำไรในตลาดคริปโทเคอร์เรนซี หรือเป็นตัวกลางในการไปซื้อคริปโทเคอร์เรนซีอื่นมากกว่าที่จะมาใช้เพื่อชำระค่าสินค้าและบริการจริง<sup>81</sup>

การได้มาซึ่งบิตคอยน์หรือการครอบครองบิตคอยน์นั้น สามารถทำได้ 3 วิธี ดังนี้

(1) การได้มาโดยการซื้อขาย

การซื้อขายหรือแลกเปลี่ยนบิตคอยน์ การแลกเปลี่ยนบิตคอยน์ แตกต่างจากการแลกเปลี่ยนด้วยประการอย่างอื่นเนื่องจากราคาของบิตคอยน์ มีการเปลี่ยนแปลงได้ง่ายจากเครดิตที่ใช้แลกเปลี่ยนภายในสมาคมซึ่งจะมีราคาคงที่ปัจเจกบุคคลสามารถแลกเปลี่ยนเงินตราจริงกับบิตคอยน์ได้เพราะบิตคอยน์สามารถใช้ในการซื้อสินค้าหรือบริการได้เหมือนกันปกติทั่วไป<sup>82</sup>

(2) การได้รับชำระค่าสินค้าหรือบริการ

ปัจจุบันบิตคอยน์ เป็นทางเลือกหนึ่งในการชำระเงินค่าสินค้าหรือบริการ ที่บริษัทหรือร้านค้าออนไลน์หลายร้านให้การยอมรับเพื่ออำนวยความสะดวกให้แก่ลูกค้า อีกทั้งบางเว็บไซต์ยังเปิดให้บริการในการเป็นพื้นที่ดูแลสำหรับ การรับและจ่ายเงินทางออนไลน์ด้วย บิตคอยน์ โดยเปิดให้ผู้ประกอบการมาลงทะเบียนกับทางเว็บไซต์เพื่อเข้าใช้บริการ โดยสามารถชำระสินค้าด้วยการเปิดบริการทางออนไลน์ ลูกค้าจ่ายเงินออนไลน์ด้วยบิตคอยน์ได้ทันทีโดยไม่ต้องมีบัตรเครดิตหรือบัญชีธนาคารใด จึงไม่มีความเสี่ยงจากอัตราแลกเปลี่ยนของเงิน ไม่มีค่าธรรมเนียมในการโอน ร้านค้ามีความมั่นใจในการได้รับชำระหนี้เพราะทุกการชำระเงินผ่านบิตคอยน์ลูกค้าไม่สามารถเรียกเก็บเงินคืนได้<sup>83</sup>

<sup>81</sup> ธรรมรักษ์ หมิ่นจักร์ และคนอื่น ๆ, *เรื่องเดิม*, หน้า 2.

<sup>82</sup> Patrick McLeod, "Taxing and Regulation Bitcoin: The Government's Game of Catch Up," *Common Law Conspectus* 22 (2014): 389.

<sup>83</sup> *Ibid.*, p. 390.

### (3) การขุด (Mining)

การขุดบิตคอยน์หรือการทำเหมืองบิตคอยน์ คือ การใช้คอมพิวเตอร์ในการถอดรหัสเพื่อยืนยันการทำธุรกรรมของผู้ที่ถือสกุลเงินดิจิทัล นักขุดเป็นเสมือนผู้ตรวจสอบบัญชีที่ยืนยันว่าการทำธุรกรรมนั้นมีความถูกต้องหรือไม่ การตรวจสอบนี้จะมีค่าตอบแทนเป็นสกุลเงินดิจิทัลสกุลนั้นกลับมา ในอดีตจะใช้ฮาร์ดแวร์ในการขุดบิตคอยน์ (Bitcoin Mining Hardware) โดยปกติแล้วจะใช้การ์ดจอในการขุด ซึ่งการขุดลักษณะนี้ต้องใช้เงินทุนสูง ค่าเสื่อมและค่าซ่อมบำรุงจากการใช้อุปกรณ์ของตนเองจึงอาจไม่คุ้มค่าหากบริหารจัดการไม่ดี แต่มีข้อดีคือได้บิตคอยน์โดยไม่ต้องมีการแบ่งปันกับผู้อื่น และสามารถควบคุมการขุดได้ตลอดเวลาด้วยคอมพิวเตอร์ที่บ้านแต่มีข้อจำกัดคือการขุดบิตคอยน์ โดยใช้ฮาร์ดแวร์มีต้นทุนค่าไฟที่สูง ต่อมาได้มีการพัฒนาการขุดบิตคอยน์โดยใช้ Asic Miner คือการใช้ฮาร์ดแวร์ของคอมพิวเตอร์ (Bitcoin Mining Hardware) ที่ประกอบขึ้นเพื่อขุดบิตคอยน์โดยเฉพาะ ซึ่งมีหลายบริษัทที่ผลิตเครื่องเหล่านี้มาจำหน่าย ข้อดีคือประหยัดไฟมากกว่าการใช้ฮาร์ดแวร์ของเครื่องคอมพิวเตอร์ แต่ข้อเสียคือเครื่องคอมพิวเตอร์ที่ประกอบขึ้นมาเพื่อการขุดบิตคอยน์นั้นไม่สามารถทำประโยชน์อย่างอื่นได้เลย ประกอบกับบิตคอยน์มีจำนวนจำกัดการขุด ในระยะหลังจึงยากขึ้นเรื่อย ๆ ทำให้ต้องมีการพัฒนาเครื่อง Asic Miner รุ่นใหม่ออกมาเรื่อย ๆ ขณะเดียวกันทำให้เครื่องรุ่นเก่ามีราคาถูกลงไปโดยปริยาย ด้วยข้อจำกัดดังกล่าวจึงเกิดการพัฒนาการขุดบิตคอยน์ขึ้นในรูปแบบการลงทุนในสัญญาขุดร่วมกัน (Cloud Mining หรือ Cloud Hashing) คือการที่ผู้ต้องการขุดสามารถซื้อกำลังในการขุดของฮาร์ดแวร์จากผู้ประกอบการซึ่งได้วางข้อเสนอไว้ในเว็บไซต์ต่าง ๆ การขุดรูปแบบนี้ทำให้การขุดบิตคอยน์เป็นเรื่องง่าย เนื่องจากผู้ให้บริการจะทำการลงทุนในเรื่องนี้ทั้งหมดและเปิดให้ผู้ลงทุนเข้าไปเช่ากำลังขุดแทน การทำ Cloud Mining มีข้อดีคือ เป็นการเพิ่มความสะดวกในการเข้าไปลงทุนในกิจกรรมการขุดบิตคอยน์ ผู้ลงทุนไม่ต้องแบกรับภาระค่าไฟฟ้า ไม่ต้องจัดซื้อเครื่องมืออุปกรณ์ในการขุดและไม่มีต้นทุนในการซ่อมบำรุงเครื่อง แต่มีข้อจำกัดคือมีความเสี่ยงต่อการหลอกและการถูกโกงจากเว็บไซต์ที่ไม่น่าเชื่อถือ นอกจากนี้การขุดบิตคอยน์ลักษณะนี้บางครั้งไม่โปร่งใส เจ้าของ Cloud มีต้นทุนค่าอุปกรณ์ค่อนข้างสูง และหากประสบภาวะขาดทุนอันเนื่องมาจากความผันผวนของราคาบิตคอยน์หรือปัจจัยอื่น ๆ อาจทำให้ต้องปิดตัวลง<sup>84</sup>

---

<sup>84</sup> Bitcoin Mining, **Best Bitcoin Cloud Mining Contract Reviews and Comparisons**, Retrieved April 16, 2020 from <https://www.bitcoinmining.com/best-bitcoin-cloud-mining-contract-reviews/>

## 2) บิตคอยน์แคช (Bitcoin Cash) (BCH)<sup>85</sup>

บิตคอยน์แคชเป็นสกุลเงินที่มีการพัฒนาแยกตัวออกมาจากบิตคอยน์เมื่อเดือนสิงหาคม 2017 เนื่องจากมูลค่าตลาดของบิตคอยน์เพิ่มสูงขึ้น มีคนจำนวนมากขาดเหรียญและเริ่มลงทุนในเวลาเดียวกัน จึงทำให้เกิดความล่าช้าในการทำธุรกรรมที่คนขาดสกุลเงินไม่สามารถเพิ่มบล็อกได้มากทันเวลา บิตคอยน์แคชจึงได้แยกออกจากสกุลเงินเดิมเพื่อแก้ปัญหาดังกล่าว โดยทำงานในลักษณะเดียวกับบิตคอยน์ แต่ได้เพิ่มบล็อกขึ้นจาก 1MB เป็น 2MB เพื่อช่วยเพิ่มความเร็วในการทำธุรกรรมและรักษาอัตราให้ต่ำ สกุลเงินดิจิทัลนี้จึงที่มีค่าโอนที่ถูกลงและโอนได้รวดเร็วยิ่งขึ้น ด้วยเหตุนี้บิตคอยน์แคชจึงใช้เวลาเพียงไม่นานก็ได้รับการยอมรับและประสบความสำเร็จอย่างมาก จนกลายเป็นเงินดิจิทัลมาแรงที่มีมูลค่าตลาดสูงติดอันดับต้น ๆ ในเดือนมิถุนายน 2561 บิตคอยน์แคชมีมูลค่าตลาดอยู่ที่ 14,000 ล้านดอลลาร์สหรัฐ หรือราว 4.5 แสนล้านบาท แต่ในเดือนธันวาคม 2565 มีมูลค่าตลาดลดลงอยู่ที่ 1,861 ล้านดอลลาร์สหรัฐ หรือประมาณ 64,980 ล้านบาท<sup>86</sup> (ข้อมูล ณ วันที่ 30 ธันวาคม 2565)

## 3) อีเทอร์เรียม (Ethereum) (ETH)<sup>87</sup>

Ethereum เป็นหนึ่งในสกุลเงินดิจิทัลที่ใช้เทคโนโลยี Blockchain ทำงานอยู่เบื้องหลัง เช่นเดียวกับอีกหลาย ๆ สกุลเงิน ซึ่งถูกพัฒนาขึ้นโดย Vitalik Buterin ชาวรัสเซีย ที่เคยอยู่ในทีมพัฒนาของ Bitcoin ก่อนจะแยกตัวออกมาสร้าง Ethereum ในปี 2556 โดยทีมพัฒนาต้องการให้ Ethereum สามารถใช้งานได้ไม่ต่างกับ Bitcoin แต่ได้ปรับปรุงข้อบกพร่องต่าง ๆ และเพิ่มความสามารถของเหรียญให้หลากหลายขึ้น โดยบล็อกเชนและโทเคนของ Bitcoin ต้องนำไปใช้ในการแลกเปลี่ยนสินค้าและบริการเท่านั้น ในขณะที่อีเทอร์เรียมได้พัฒนาเทคโนโลยีบล็อกเชนของบริษัททำให้สามารถใช้ได้ทั้งกับตัวเงินและไม่ใช้ตัวเงินได้ และธนาคารยังสามารถใช้บล็อกเชนของ Ethereum เพื่อปรับปรุงการตรวจสอบและการชำระเงินของธุรกรรมได้อย่างง่ายดายเช่นเดียวกับการที่ผู้ค้าปลีกสามารถใช้บล็อกเชนของ Ethereum ในการติดตามสินค้าที่เคลื่อนผ่านห่วงโซ่อุปทานแบบ

<sup>85</sup> Satoshi Nakamoto, **Bitcoin: A Peer-to-Peer Electronic Cash System**, Retrieved October 18, 2020 from [https://www.uscc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging\\_Tech\\_Bitcoin\\_Crypto.pdf](https://www.uscc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf)

<sup>86</sup> Cryptocurrency Prices, *op. cit.*

<sup>87</sup> Josh Stark and Evan Van Ness, “**The Year in Ethereum 2019**” in **Ethereum Guides & Resources**, Retrieved March 6, 2020 from <https://ethereum.org/what-is-ethereum/>

เรียลไทม์ จุดเด่นอีกประการของอีเทอร์เรียม คือ การก่อตั้ง Smart Contracts โดยออกแบบให้ผู้ใช้งานสามารถเขียนโปรแกรมลงไป ข้อมูลของเหรียญได้ โดยจะเป็นการสร้างเงื่อนไขขึ้นมาตามที่เรากำหนด เมื่อมีใครทำตามเงื่อนไขนั้นสำเร็จ ก็จะได้รางวัลที่เรากำหนดไว้เป็นการตอบแทน ทำให้นักพัฒนาจำนวนมากหันมาสนใจ Ethereum และนำระบบ Smart Contract ไปประยุกต์ใช้ในหลากหลายธุรกิจทั่วโลก ตัวอย่างของการนำระบบ Smart Contract ไปใช้งาน เช่น การชำระค่าเช่าหอพัก โดยเป็นการทำสัญญาในระบบไว้ว่า ให้ผู้เช่าโอนเงินจ่ายค่าเช่าภายในวันที่ 30 ของแต่ละเดือน ซึ่งหากมีการโอนเงินเข้ามา Blockchain จะบันทึกข้อมูลไว้ ผู้เช่าก็สามารถอาศัยในหอพักได้ตามปกติ แต่หากไม่มีการโอนเงินเข้ามาหรือโอนมาไม่ครบ ระบบก็จะทำการล็อกประตูอัตโนมัติ ไม่ให้ผู้เช่าเข้ามาใช้งานหอพักต่อได้ วิธีการเดียวกันนี้ยังนำไปใช้ในธุรกิจเช่ารถ ซึ่งอาจมีการออกแบบให้รถยนต์เชื่อมต่อกับระบบ Blockchain ไว้ และจอดทิ้งโดยไม่ต้องมีคนมาคอยเฝ้าก็ได้ เมื่อมีลูกค้าเห็นรถและสนใจจะเช่า สามารถโอนเงินเข้ามาในบัญชีที่ระบุไว้ ระบบ Smart Contract จะตรวจสอบข้อมูลและเปิดประตูให้ลูกค้าสามารถเข้ามาขับรถออกไปได้เลย นอกจากนี้ Smart Contract ยังนำไปประยุกต์ใช้ได้อีกหลายรูปแบบ ไม่ว่าจะเป็นการซื้อขายสินค้าออนไลน์, โอนเงินข้ามประเทศ, การขอใบอนุญาตต่าง ๆ หรือแม้แต่การขอสินเชื่อจากสถาบันการเงิน เป็นต้น

#### 4) Ethereum Classic (ETC)<sup>88</sup>

Ethereum Classic เป็นอีกหนึ่งสกุลเงินที่แยกตัวออกมาจาก Ethereum เพราะทีมพัฒนาบางกลุ่ม ไม่เห็นด้วยกับเรื่องการแก้ปัญหาของ Ethereum ที่ถูกแฮ็กระบบ จึงออกมาพัฒนา Ethereum Classic ซึ่งในเดือนธันวาคมมีมูลค่ารวมอยู่ที่ 2,167 ล้านเหรียญสหรัฐ หรือราว 74,293 ล้านบาท<sup>89</sup> (ข้อมูล ณ วันที่ 30 ธันวาคม 2565)

#### 5) Litecoin<sup>90</sup>

เงินสกุลนี้ได้ถูกพัฒนามาตั้งแต่ปี 2554 โดย Charlie Lee อดีตรักบี้ของ Google เป็นสกุลเงินดิจิทัลที่มีจุดเด่นในเรื่องของความเร็วในการประมวลผลทำธุรกรรมต่าง ๆ ซึ่งเมื่อ

<sup>88</sup> Pyskell, "Ethereum and Ethereum Classic: What's the Difference?," **Ethereum Classic NEWS**, Retrieved May 2, 2020 from <https://medium.com/@pyskell/ethereum-and-classic-e0102dead543>

<sup>89</sup> Cryptocurrency Prices, *op. cit.*

<sup>90</sup> Bernard Marr, "Bitcoin and Litecoin - What's The Difference?," **Forbes** (21 March 2018), Retrieved December 23, 2020 from <https://www.forbes.com/sites/bernardmarr/2018/03/21/bitcoin-and-litecoin-whats-the-difference/#758bd0d05664>

เปรียบเทียบกับ Bitcoin แล้ว Litecoin จะใช้เวลาในการประมวลผลของบล็อกเร็วกว่าถึง 4 เท่า (เฉลี่ยเพียงประมาณ 2 นาที 30 วินาที) Litecoin มีวัตถุประสงค์เพื่อเป็นพันธมิตรกับผู้ค้าให้มากที่สุดเท่าที่จะเป็นไปได้ และทำผลงานได้ดีโดยเฉพาะในแง่ของการทำธุรกรรมรายวัน และได้มีการกำหนดเพดานการสร้างเหรียญดิจิทัลสูงสุดของระบบไว้ที่ 84 ล้านเหรียญ ซึ่งสูงกว่าบิตคอยน์กำหนดเพดานสูงสุดไว้ที่ 21 ล้านเหรียญ<sup>91</sup>

#### 6) Ripple (XRP)<sup>92</sup>

สกุลเงินนี้เริ่มต้นเปิดตัวในปี พ. ศ. 2555 เป็นสกุลเงินดิจิทัล ที่แตกต่างจากสกุลเงินอื่น ๆ เนื่องจากมีออกแบบภายใต้ระบบ Private Blockchain โดยมีบริษัท Ripple เป็นผู้ดูแลปริมาณเงินในระบบทั้งหมด และมีจุดเด่นคือมีความเชื่อมโยงกับสถานการณ์เงินต่าง ๆ ในการทำธุรกรรม โดยเฉพาะอย่างยิ่งการโอนเงินระหว่างประเทศที่ต้องอาศัยความเสถียรของค่าเงินที่ค่อนข้างสูง จึงได้มีการออกแบบให้เงินสกุลนี้ดังกล่าวไม่สามารถขุดได้เหมือนเช่นสกุลเงินดิจิทัลอื่น ๆ ที่กล่าวมา ด้วยเหตุผลนี้จึงทำให้ Ripple เป็นที่ยอมรับในวงกว้างของสถาบันการเงินและบริษัทชั้นนำทั่วโลก ทั้ง Google, SBI Group, Standard Chartered และ Seagate รวมถึงสถาบันการเงินของไทยก็ได้มีการเข้าไปลงทุนกับ Ripple ในการศึกษาการใช้เทคโนโลยีทางการเงิน (Fintech) เพื่อพัฒนาการโอนเงินข้ามประเทศผ่านระบบออนไลน์ให้สะดวก รวดเร็ว และลดค่าใช้จ่ายให้มากยิ่งขึ้น

#### 7) Stellar (XLM)<sup>93</sup>

Stellar เป็นสกุลเงินที่ถูกพัฒนาต่อยอดมาจาก Ripple ที่มีจุดประสงค์เพื่อเป็นเงินดิจิทัลสำหรับถ่ายโอนแลกเปลี่ยนกับสกุลเงินหลัก แต่จุดที่ Stellar แตกต่างออกไปคือการออกแบบมาเพื่อรองรับการใช้งานของคนทั่วไป ที่ถ่ายโอนเงินจำนวนไม่มาก ซึ่งต่างจาก Ripple ที่จะเน้นกลุ่มองค์กรและสถาบันการเงินเป็นหลัก นอกจากนี้ Stellar ยังได้นำจุดเด่นของสกุลเงินดิจิทัล

<sup>91</sup> Chris Burniske and Jack Tatar, *op cit*.

<sup>92</sup> Billy Bambrough, “Exclusive: Leak Reveals Surprising Reason Major Bitcoin Exchange Luno Is Adding Ripple’s XRP,” **Forbes** (28 March 2020), Retrieved January 15, 2021 from <https://www.forbes.com/sites/billybambrough/2020/02/28/exclusive-leak-reveals-surprising-reason-major-bitcoin-exchange-luno-is-adding-ripples-xrp/#434f2e8f4de4>

<sup>93</sup> Ben Jessel “What Stellar’s Investment in Abra Means for the ‘Robinhood of Cryptocurrency,’” **Forbes** (6 May 2020), Retrieved May 23, 2021 from <https://www.forbes.com/sites/benjessel/2020/05/06/what-stellars-investment-in-abra-means-for-the-robinhood-of-cryptocurrency/#50159a0fd155>

Ethereum มาประยุกต์ใช้ เช่นการนำ Smart Contract มาใช้ซึ่งทำให้บริษัทสามารถกำหนดสัญญาที่มีผลผูกพันตามกฎหมายเพื่อตอบสนองความต้องการทางธุรกิจอีกช่องทางหนึ่ง

#### 2.2.1.6 แนวโน้มการใช้สกุลเงินดิจิทัล

ความนิยมในการใช้สกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีมีเพิ่มมากขึ้นอันเนื่องมาจากหลายสาเหตุ สาเหตุที่สำคัญประการหนึ่งคือ การขาดเสถียรภาพในการบริหารการเงินในระบบสกุลเงินธรรมดา (Fiat Currency) ของประเทศซึ่งอิงกับนโยบายเศรษฐกิจ และการเมืองที่มีความผันผวนสูง จึงมักจะทำให้เกิดปรากฏการณ์เงินเฟ้อได้ง่าย นำมาซึ่งความล้มเหลวของระบบการเงินครั้งใหญ่ ทำให้มีเงินในตลาดมากและเกิดภาวะเงินเฟ้อในที่สุด ปัจจุบันอัตราหนี้ทั่วโลกที่พุ่งสูงขึ้น สะท้อนภาพความไม่มั่นคงของเศรษฐกิจโลกที่เพิ่มมากขึ้น เช่น กรณีที่รัฐบาลพิมพ์เงินออกมาได้ตามใจชอบ เพราะสกุลเงินของรัฐบาลนั้นไม่จำเป็นต้องได้รับการหนุนโดยทองคำจริง ๆ ดังที่เกิดขึ้นในประเทศเวเนซุเอลาที่ประสบวิกฤตเศรษฐกิจ เติบโตกับเงินเฟ้อสูงมากเกือบ 1 ล้านเปอร์เซ็นต์ในปี 2561 ทำให้เงินโบลิเวีย (Bolívar) ซึ่งเป็นสกุลเงินท้องถิ่นแทบไม่มีค่า คนจึงหนีภาวะเงินเฟ้อในสกุลเงินโบลิเวีย และขาดความเชื่อมั่นในการบริหารของรัฐไปถือคริปโทเคอร์เรนซี แม้รัฐบาลจะออกสกุลเงินดิจิทัลแห่งชาติชื่อ “Petro Coin” ที่หนุนหลังด้วยมูลค่าบ่อน้ำมันของรัฐ แต่ก็ไม่ประสบความสำเร็จที่จะทำให้คนกลับมาเชื่อถือในเงินของรัฐได้<sup>94</sup>

กรณีดังกล่าวจึงเป็นสาเหตุหนึ่งในการพยายามแก้ไขปัญหารัฐบาลหรือองค์กรกลางทางการเงินบริหารระบบสกุลเงินของประเทศผิดพลาด ด้วยการออกสกุลเงินดิจิทัลขึ้นโดยไม่ให้อยู่ภายใต้การควบคุมหรือแทรกแซงจากรัฐบาลเหมือนเช่นในอดีต จึงเป็นที่มาในการออกสกุลเงินดิจิทัลต่าง ๆ มากมายทั่วโลก สกุลเงินดิจิทัลที่มากมายเช่นนี้ย่อมแสดงให้เห็นว่าวิวัฒนาการทางการเงินได้เปลี่ยนจากระบบเงินปกติเป็นระบบสกุลเงินดิจิทัลที่มีความน่าเชื่อถือและได้รับการยอมรับมากขึ้น จะเห็นได้จากบริษัทข้ามชาติชั้นนำขนาดใหญ่หลายแห่งในสหรัฐอเมริกา เช่น เดลคอมพิวเตอร์ (Dell Computer) ไมโครซอฟท์ (Microsoft) เอ็กซ์พีเดีย (Expedia) ซับเวย์แซนด์วิช (Subway Sandwich) และซูเปอร์มาร์เก็ตโฮลฟู้ดส์ (Whole Foods) ได้เปิดโอกาสให้ประชาชนใช้บิตคอยน์เพื่อเพิ่มทางเลือกในการใช้จ่ายมากขึ้น

จนกระทั่งในปัจจุบันพบว่านอกจากการนำสกุลเงินดิจิทัลไปใช้ในการซื้อขายแลกเปลี่ยนสินค้าและบริการได้แล้ว ยังมีแนวโน้มในการนำสกุลเงินดิจิทัลมาลงทุนหรือเก็งกำไรอย่างมาก ซึ่งเป็นผลจากราคาของคริปโทเคอร์เรนซีที่ปรับเพิ่มขึ้นอย่างรวดเร็ว ทำให้มีจำนวนผู้ใช้ในตลาดคริปโทเคอร์เรนซีเพิ่มมากขึ้น ประกอบกับยังไม่มีหน่วยงานใดที่สามารถจำกัดหรือควบคุมการเกิดขึ้นของคริปโทเคอร์เรนซีตัวใหม่ ๆ ได้อย่างชัดเจน ทำให้มีการออกคริปโทเคอร์เรนซีในรูปแบบใหม่ ๆ มา

<sup>94</sup> ฐิติมา ชูเชิด, *เรื่องเดิม*.

อย่างต่อเนื่อง โดยเฉพาะอย่างยิ่งการทำธุรกรรมการโอนเงินระหว่างประเทศ มีความสะดวกรวดเร็ว และมีค่าธรรมเนียมต่ำกว่าเมื่อเปรียบเทียบกับการทำธุรกรรมผ่านสถาบันการเงิน

นอกจากนี้ยังมีการใช้คริปโทเคอร์เรนซีในรูปแบบเหรียญโทเคนเพื่อระดมทุนทำธุรกิจประเภท ICO ยังเป็นช่องทางการเข้าถึงทุนที่สะดวก รวดเร็ว ทั้งในประเทศและต่างประเทศ เพื่อสนับสนุนการสร้างนวัตกรรมต่าง ๆ ทำให้ได้รับความนิยมมากจากกลุ่ม Tech Startups สิ่งสำคัญอีกประการที่ทำให้คริปโทเคอร์เรนซีมีแนวโน้มที่ผู้คนต้องการใช้ ถือครอง หรือลงทุนมากขึ้น เนื่องจากความมั่นใจในประสิทธิภาพของเทคโนโลยีบล็อกเชน ซึ่งเป็นเทคโนโลยีที่มีความปลอดภัยสูง ไม่สามารถแก้ไขเปลี่ยนแปลงธุรกรรม และยังสามารถตรวจสอบประวัติธุรกรรมได้ตั้งแต่เริ่มแรก นับวันยังมีการพัฒนาเทคโนโลยีบล็อกเชนให้มีเสถียรภาพ สามารถตอบสนองผู้ใช้งานมากขึ้น รวมถึงการพัฒนาบล็อกเชนเพื่อเป็นแบบอย่างให้กับวงการอื่น ๆ นอกเหนือจากวงการการเงิน<sup>95</sup>

ทั้งนี้แนวโน้มของสถานการณ์การใช้สกุลเงินดิจิทัลของประเทศไทยและต่างประเทศ ไม่ว่าจะเป็นภาครัฐหรือภาคเอกชนได้ให้ความสนใจในการพัฒนาดำเนินการต่าง ๆ ให้สกุลเงินดิจิทัลนั้นนำมาใช้ให้เกิดประโยชน์ได้หลากหลาย โดยมีการส่งเสริมการเผยแพร่ทั้งความรู้พื้นฐานเกี่ยวกับเงินสกุลดิจิทัลและการพัฒนาเทคโนโลยีควบคู่กันไป รวมถึงบุคคลากรที่เกี่ยวข้อง เพื่อให้เกิดการใช้ประโยชน์และลดโอกาสที่จะก่อให้เกิดผลเสียต่อระบบเศรษฐกิจต่อไป<sup>96</sup>

#### 2.2.1.7 ประโยชน์และข้อจำกัดของสกุลเงินดิจิทัล

สกุลเงินดิจิทัล เป็นการสร้างมุมมองใหม่ให้แก่ธุรกิจทางการเงินในยุคดิจิทัลโดยมีการนำเทคโนโลยีมาใช้ในการอำนวยความสะดวกต่าง ๆ ให้แก่ผู้ทำธุรกรรมและสามารถตอบสนองความต้องการของคนในยุคปัจจุบันได้เป็นอย่างดี ซึ่งการใช้สกุลเงินดิจิทัลมีประโยชน์ ดังนี้

- 1) การนำระบบบล็อกเชนและ DLT (Distributed Ledger Technology) มาใช้ในการทำธุรกรรมของสกุลเงินดิจิทัล สามารถลดค่าธรรมเนียมในการทำธุรกรรม เนื่องจากเป็นระบบที่ทำธุรกรรมโดยไม่ผ่านตัวกลาง (ธนาคาร) จึงลดต้นทุนในการทำธุรกิจได้ โดยข้อมูลที่เกี่ยวข้องกับธุรกรรมต่าง ๆ ที่เกิดขึ้นนั้นจะปรากฏอยู่ในเครือข่ายระหว่างผู้ใช้กันเอง (Peer to Peer) โดยตรง นอกจากนี้ระบบนี้ยังสามารถป้องกันการจ่ายเงินผิดพลาดหรือป้องกันการจ่ายเงินซ้ำซ้อนได้ Double Spending เนื่องจากรายการธุรกรรมทางการเงิน มีลักษณะเปิดเผย และมีการยืนยันธุรกรรมก่อนตัดสินใจ

<sup>95</sup> ธรรมรักษ์ หมิ่นจักร์ และคนอื่น ๆ, *เรื่องเดิม*, หน้า 3.

<sup>96</sup> สำนักงานส่งเสริมเศรษฐกิจดิจิทัล, *เทคโนโลยีที่สำคัญในยุคดิจิทัล: รู้จักกับเงินสกุล*

*ดิจิทัล Getting to Know Cryptocurrency*, ค้นวันที่ 25 เมษายน 2563 จาก

<https://www.depa.or.th/th/article-view/article-getting-know-cryptocurrency>

นวัตกรรมเทคโนโลยีบล็อกเชนและ DLT เป็นจุดเริ่มต้นในที่ภาคธุรกิจต่าง ๆ จะนำระบบนี้ไปพัฒนาต่อยอดเพื่อเพิ่มประสิทธิภาพในการทำงาน เนื่องจากเป็นการกระจายฐานข้อมูลที่มีข้อมูลชุดเดียวกันในระหว่างผู้ใช้ด้วยกัน ซึ่งจะช่วยให้ผู้ใช้เหล่านั้นเห็นข้อมูลต่าง ๆ พร้อมกันและสามารถทำธุรกรรมได้รวดเร็วขึ้น ลดต้นทุนในการตรวจสอบข้อมูลระหว่างกัน ตลอดจนลดความเสี่ยงด้านเทคโนโลยี เนื่องจากข้อมูลจะกระจายอยู่ในหลายผู้ใช้ ซึ่ง DLT สามารถนำมาพัฒนาเพิ่มเติมได้ เช่น การเพิ่มความสามารถของการใช้ Smart Contract การใช้ Consensus Mechanism ที่ไม่จำเป็นต้องให้ผู้ใช้ทุกรายมารับรองการทำธุรกรรม จะช่วยเพิ่มประสิทธิภาพและความเร็ว ตลอดจนลดต้นทุนของการทำธุรกรรมได้และเพิ่มประสิทธิภาพในการแข่งขันกับธุรกิจรายอื่นได้<sup>97</sup>

2) การทำธุรกรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัลนั้นต้องทำผ่านระบบอินเทอร์เน็ตของผู้ใช้ ซึ่งสามารถทำธุรกรรมการเงินผ่านโทรศัพท์มือถือได้ทุกที่ทุกเวลา จึงสะดวกในการเข้าทำธุรกรรม อีกทั้งการเข้าใช้หรือทำธุรกรรมแต่ละครั้ง จะต้องมีการตรวจสอบมาตรฐานสากลระบบนี้จึงมีความปลอดภัยและความเป็นส่วนตัวสูง

3) การเปิดบัญชีเพื่อขอเข้าทำธุรกรรม ไม่ยุ่งยาก เนื่องจากไม่มีการตรวจสอบตัวตนของผู้ขอใช้ และไม่ต้องการทำความรู้จักกับผู้ใช้ตามหลัก KTC (Know Your Customer) เหมือนเช่นระบบที่ทำผ่านธนาคาร จึงทำให้ผู้ใช้หนึ่งคนสามารถเปิดบัญชีได้หลายบัญชี จึงอำนวยความสะดวกต่อผู้ใช้ในการทำธุรกรรม

4) การถือครองของสกุลเงินดิจิทัลมีมูลค่าสูง โดยเฉพาะอย่างยิ่งสกุลเงินดิจิทัลบางสกุลที่อาจได้มาจากการขุด เช่น Bitcoin Ethereum การขุดหาเหรียญเสมือนกับการขุดหาทองคำหรือเพชรพลอยหรือโลหะที่มีค่า เนื่องจากการขุดต้องใช้โปรแกรมที่ซับซ้อน และมีลักษณะขั้นตอนทางเทคนิคโดยเฉพาะ ผู้ใช้ต้องมีการลงทุนกับอุปกรณ์คอมพิวเตอร์ อุปกรณ์ดังกล่าวต้องมีคุณสมบัติในการใช้งานเฉพาะทางในการถอดรหัส จึงได้รับผลตอบแทนสูง

5) สกุลเงินดิจิทัลบางประเภทเช่น Bitcoin ได้มีการกำหนดจำนวนการผลิตไว้ตั้งแต่ต้นว่าจะผลิตเพียง 21 ล้าน BTC การกำหนดอุปสงค์ไว้เช่นนี้ ทำให้สามารถป้องกันภาวะการเกิดเงินเฟ้อและทำให้เงินมีมูลค่าสูงอยู่เสมอหากมีผู้ใช้ในระบบมากขึ้น

6) การมีอยู่ของสกุลเงินดิจิทัลในระบบการเงินนั้นอาศัยการยอมรับและความน่าเชื่อถือ จากผู้ใช้ในกลุ่ม โดยไม่ได้อิงกับระบบเศรษฐกิจหรือนโยบายของรัฐและไม่ผันแปรไปตามค่าเงินสกุลอื่น จึงทำให้ผู้ใช้ไม่ต้องกังวลกับสถานการณ์ความไม่แน่นอนจากปัจจัยภายนอก

<sup>97</sup> ธรรมรักษ์ หมื่นจักร์ และคนอื่น ๆ, *เรื่องเดิม*, หน้า 8-9.

อย่างไรก็ตามแม้การใช้สกุลเงินดิจิทัลจะมีความนิยมในเพิ่มขึ้นมากทั้งภาครัฐและภาคเอกชนเนื่องจากสกุลเงินดิจิทัลได้มีการนำระบบบล็อกเชนและ DLT ซึ่งเป็นนวัตกรรมใหม่ของวงการการเงิน การใช้สกุลเงินดิจิทัลจึงมีประโยชน์และตอบสนองความต้องการของคนในยุคปัจจุบันอย่างมาก ทั้งในด้านความสะดวกรวดเร็ว ความเป็นส่วนตัว และผลประโยชน์ตอบแทนที่สูง สกุลเงินดิจิทัลเปรียบเสมือนเหรียญที่มีสองด้าน แม้จะมีประโยชน์และข้อดีต่าง ๆ ตามที่กล่าวมาแต่ก็อาจมีความเสี่ยงในการใช้เนื่องจากประโยชน์ต่าง ๆ อาจเป็นสิ่งจูงใจให้มีฉ้อโกงใช้ช่องทางนี้ก่ออาชญากรรมได้เช่นเดียวกัน ทั้งนี้จึงควรพิจารณาข้อจำกัดของสกุลเงินดิจิทัลควบคู่กันไป<sup>98</sup> ซึ่งแบ่งข้อจำกัดออกเป็น 2 กรณี คือข้อจำกัดทั่วไปและข้อจำกัดเฉพาะด้าน ดังนี้

#### 1) ข้อจำกัดทั่วไป

(1) สถานะของสกุลเงินดิจิทัล (Cryptocurrency) แม้จะมีคำว่า “เงิน” หรือคำว่า “Currency” เข้ามาเกี่ยวข้อง แต่สถานะทางกฎหมายของสกุลเงินดิจิทัลนั้นไม่ถือว่าเป็นเงินตราตามกฎหมายไทย เนื่องจากพระราชบัญญัติเงินตรา พ.ศ. 2501 กำหนดว่าเงินตราที่สามารถชำระหนี้ได้ตามกฎหมายนั้นจะต้องมีลักษณะเป็นเหรียญกษาปณ์หรือธนบัตรเท่านั้น<sup>99</sup>

(2) ปัญหาการค้นหาหลักฐานเพื่อต่อสู้คดีจะเป็นเรื่องค่อนข้างยากหากมีการฟ้องร้องคดี เนื่องจากผู้ทำธุรกรรมนั้น ไม่มีการแสดงตัวที่แท้จริงหรือข้อมูลที่เชื่อมโยงกับตัวตนจริงได้ ดังนั้นหากมีการหลอกลวง ฉ้อโกงหรือเกิดกรณีที่เกิดปัญหาในการใช้งาน เช่นการโอนไปยังผู้รับผิดชอบหรือผิดจำนวนหรือโอนไปยังร้านค้าแล้วไม่ได้รับสินค้า การติดตามข้อมูลการโอนหรือการค้นหาพยานหลักฐานเพื่อพิสูจน์ความผิดจึงทำได้ยาก แม้ปัจจุบันอาจมีบางกรณีกระทำได้โดยผู้เชี่ยวชาญก็ตาม

(3) มูลค่าของสกุลเงินดิจิทัลที่ผันผวนอย่างรวดเร็ว เนื่องจากมูลค่าของหน่วยข้อมูลอิเล็กทรอนิกส์เกิดจากความต้องการแลกเปลี่ยนในกลุ่มของผู้ใช้ด้วยกัน ดังนั้นมูลค่าจึงมีความผันผวนสูงและไม่สัมพันธ์กับสภาพเศรษฐกิจจริงผู้ถือครองหน่วยข้อมูลจึงมีความเสี่ยงที่จะสูญเสียเงินจากการที่มูลค่าของหน่วยข้อมูลลดต่ำลงอย่างรวดเร็ว<sup>100</sup>

<sup>98</sup> สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, **สถานการณ์ Cryptocurrency ของประเทศไทย**, ค้นวันที่ 25 พฤศจิกายน 2565 จาก <https://www.etda.or.th/th/Useful-Resource/knowledge-sharing/articles/index-article-other-p1/สถานการณ์-Cryptocurrency-ของประเทศไทย.aspx>

<sup>99</sup> มาตรา 6 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>100</sup> “รพท.เตือนประชาชนห้ามใช้เงินบิตคอยน์,” **กรุงเทพธุรกิจออนไลน์** (18 มีนาคม 2557), อ้างถึงใน ภัทรพร สหกิจวิจารณ์, **ปัญหาการจัดเก็บภาษีเงินได้บุคคลธรรมดาจากบิตคอยน์:**

(4) ความเสี่ยงจากการถูกขโมยข้อมูลเนื่องจากข้อมูลทางอิเล็กทรอนิกส์ดังกล่าวจะต้องจัดเก็บไว้ในคอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์เท่านั้นจึงมีความเสี่ยงที่ผู้ถือครองอาจสูญเสียข้อมูลดังกล่าวได้จากการถูกลักลอบหรือโจรกรรมข้อมูล

ตัวอย่างเช่น ในปี พ.ศ. 2557 บริษัท Mt.Gox ศูนย์ให้บริการรับแลกเปลี่ยนบิตคอยน์ที่ใหญ่ที่สุดในโลกขณะนั้น ได้ปิดตัวลงโดยอ้างสาเหตุจากการถูกลักลอบโจรกรรมหน่วยข้อมูล ทำให้บริษัทต้องยื่นล้มละลายในที่สุด และมูลค่าหรือราคาของบิตคอยน์ได้ลดลงอย่างมากภายในระยะเวลาอันรวดเร็ว ส่งผลให้ประชาชนที่ทำธุรกรรมแลกเปลี่ยนกับบริษัทดังกล่าวและผู้ถือครอง Bitcoin ต้องสูญเสียเงินเป็นจำนวนมาก ยิ่งไปกว่านั้น ยังพบว่าธุรกิจเงินสกุลดิจิทัลนี้ยังปรากฏนักหลอกลวงต้มตุ๋นเกิดขึ้นมากมาย เช่น การเปิดเงินสกุลดิจิทัลขึ้นใหม่และมาหลอกระดมทุนในลักษณะคล้ายแชร์ลูกโซ่

ในปี พ.ศ. 2560 กรณี ยูบิท เว็บไซต์ตลาดแลกเปลี่ยนสกุลเงินดิจิทัลซึ่งเป็นสกุลเงินดิจิทัลแห่งหนึ่งของเกาหลีใต้ ปิดตัวและยื่นขอพิทักษ์ทรัพย์ในฐานะล้มละลาย สาเหตุเพราะถูกเจาะระบบขโมยสกุลเงินดิจิทัลเป็นครั้งที่สองของปี ทำให้ทรัพย์สินเสียหาย ส่งผลต่อสกุลเงินดิจิทัลของลูกค้ำลดลง 75% ด้วยเหตุนี้ธนาคารกลางในหลายประเทศได้เริ่มมีการแจ้งเตือนประชาชนเกี่ยวกับความเสี่ยงในการใช้หน่วยข้อมูลทางอิเล็กทรอนิกส์เหล่านี้

วันที่ 7 ตุลาคม 2565 Binance ศูนย์ซื้อขายสินทรัพย์ดิจิทัล รายใหญ่ที่สุดในโลกถูกขโมยเหรียญ Binance Coin มูลค่าประมาณ 100 ล้านเหรียญ (ราว 3,740 ล้านบาท) จาก BNB Chain ซึ่งเป็นบล็อกเชนของ Binance แม้นายชางเผิง เจา (Changpeng Zhao) หรือ CZ CEO ของ Binance จะได้ให้ความมั่นใจว่า Binance สามารถควบคุมสถานการณ์ดังกล่าวได้แล้ว แต่การถูกแฮ็กส่งผลให้ราคาเหรียญของ Binance Coin (BNB) ในช่วงเช้าของวันดังกล่าวที่ตลาดโตเกียวตกลงกว่า 3.3%<sup>101</sup>

ในช่วงเดือนพฤศจิกายน พ.ศ. 2565 FTX ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Exchange) ที่มีมูลค่าการซื้อขายเป็นอันดับ 2 ของโลก ถูกเจาะระบบโดยพบว่ามีเงินกว่า 600 ล้านเหรียญสหรัฐไปยัง DEX (Decentralized Exchange) โดยไม่ทราบที่มา ซึ่งสอดคล้องกับผู้ใช้งานจำนวนมากของ FTX พบว่าเงินใน wallet ของตนเองเหลือ '0' ซึ่งทาง FTX Official ได้

---

**การรับรู้เงินได้** (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณະนิตศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2559), หน้า 19.

<sup>101</sup> A \$568 Million Hack of Binance Coin Roils Crypto Sector Anew, Retrieved December 31, 2022 from <https://www.bloomberg.com/news/articles/2022-10-06/bnb-chain-says-bsc-temporarily-paused-on-irregular-activity>

ออกมาเตือนผู้ใช้งานว่าขณะนี้ FTX เป็นมัลแวร์ ให้ผู้ใช้งานลบแอปพลิเคชัน FTXทันทีและอย่าใช้งานบนเว็บไซต์ของ FTX เนื่องจากอาจติดโทรจัน (Trojans) ในเครื่องได้<sup>102</sup>

ปัจจุบันการเยียวยาความเสียหายจากการถูกโจรกรรมยังมีทางเลือกค่อนข้างจำกัด แตกต่างจากการที่บัตรเครดิตถูกขโมย หรือกรณีที่บัญชีเงินฝากถูกแฮ็กลูกค้าของธนาคารมีโอกาสได้รับเงินคืนโดยธนาคารเป็นผู้ชดเชย แต่การใช้สกุลเงินดิจิทัลเมื่อถูกโจรกรรมแล้วยากที่จะติดตามทวงคืน เนื่องจากการโจรกรรมเกิดขึ้นจากการเจาะระบบที่เชื่อมต่อกับอินเทอร์เน็ต<sup>103</sup> ตลอดเวลาจึงทำให้ผู้ใช้อาจไม่ทราบถึงความเสียหายได้ทันเวลาที่

## 2) ข้อจำกัดเฉพาะด้าน<sup>104</sup>

ปัจจุบันได้มีการตั้งคณะทำงานเพื่อศึกษาและเสนอแนะเชิงนโยบายเกี่ยวกับเรื่องดังกล่าว ประกอบด้วย กระทรวงการคลัง ธนาคารแห่งประเทศไทย สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ และสำนักงานป้องกันและปราบปรามการฟอกเงิน ได้ประเมินถึงข้อจำกัดของการใช้สกุลเงินดิจิทัล ซึ่งอาจก่อให้เกิดความเสี่ยง 7 ด้าน ดังนี้

(1) การฟอกเงินและการสนับสนุนทางการเงินแก่การก่อการร้าย (Money Laundering and Terrorism Finance) การใช้สกุลเงินดิจิทัลส่วนใหญ่สามารถทำได้โดยมีการปกปิดตัวตนในการโอนชำระระหว่างกันทำให้มีความยากต่อหน่วยงานภาครัฐในการติดตามเส้นทางการส่ง ดังนั้น สกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีจึงถูกใช้เป็นช่องทางในการสนับสนุนการก่อการร้ายและทำธุรกรรมที่ผิดกฎหมายได้โดยง่าย

(2) การเก็งกำไรในสกุลเงินดิจิทัลและความเสี่ยงของนักลงทุน (Investor Protection) สกุลเงินดิจิทัลมีความผันผวนทางราคาสูง และไม่สามารถหามูลค่าที่แท้จริงได้ต่างจากหุ้นหรือพันธบัตร ดังนั้น นักลงทุนที่เข้าไปเก็งกำไรในคริปโทเคอร์เรนซีจำเป็นต้องเข้าใจถึงความเสี่ยงก่อนการตัดสินใจลงทุน นอกจากนี้ ในต่างประเทศยังพบว่าการเข้าไปเก็งกำไรผ่านศูนย์ซื้อขายแลกเปลี่ยนที่มีได้มีการกำกับดูแล และไม่มีมาตรฐานการรักษาความปลอดภัยทางไซเบอร์อย่างเพียงพอ อาจถูกฉ้อโกงโดยศูนย์ซื้อขายแลกเปลี่ยนนั้น และมีโอกาสที่จะถูกโจรกรรมจากกระเป๋าเงินอิเล็กทรอนิกส์ที่ศูนย์ซื้อขายแลกเปลี่ยนนั้นได้โดยง่าย

<sup>102</sup> **FTX Has Been Hacked': Crypto Disaster Worsens as Exchange Sees Mysterious Outflows Exceeding \$600M**, Retrieved December 30, 2022 from <https://www.coindesk.com/business/2022/11/12/ftx-crypto-wallets-see-mysterious-late-night-outflows-totalling-more-than-380m/>

<sup>103</sup> ภัทรพร สหกิจพิจารณา, *เรื่องเดิม*, หน้า 60.

<sup>104</sup> ธรรมรักษ์ หมื่นจักร์ และคนอื่น ๆ, *เรื่องเดิม*, หน้า 10-11.

(3) การถูกนำไปใช้แอบอ้างในแชร์ลูกโซ่และการฉ้อโกงประชาชน (Ponzi Scheme) ราคาของสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีที่ปรับตัวสูงขึ้นอย่างรวดเร็วได้ส่งผลให้มีการโฆษณาหลอกลวงระดมเงินจากประชาชนเพื่อนำไปลงทุนในคริปโทเคอร์เรนซีในลักษณะแชร์ลูกโซ่บ่อยครั้งขึ้นนอกจากนี้ในหลายประเทศยังพบว่าการออก ICO ที่ทำได้ง่ายโดยไม่มีการกำกับดูแลได้ส่งผลให้มีฉ้อโกงในการทำ ICO เพื่อระดมเงินจากประชาชน โดยที่ผู้ออกมิได้มีความสามารถด้านเทคโนโลยีหรือโมเดลธุรกิจที่เหมาะสมแต่อย่างใด

(4) การหลีกเลี่ยงกฎเกณฑ์ควบคุมกำไรแลกเปลี่ยนเงิน (Exchange Control) กฎเกณฑ์ควบคุมการแลกเปลี่ยนเงินมีไว้เพื่อช่วยในการดูแลเสถียรภาพเศรษฐกิจการเงินของประเทศ โดยผู้ที่ต้องการนำเงินเข้าหรือออกนอกประเทศ จะต้องปฏิบัติตามกฎเกณฑ์การกำกับการดูแลของทางการ เช่น การรายงานปริมาณและวัตถุประสงค์ในการทำธุรกรรมโอน ขำระธุรกรรมระหว่างประเทศให้ทางการ การใช้คริปโทเคอร์เรนซีเพื่อการโอน ขำระธุรกรรมระหว่างประเทศ จึงอาจถูกใช้เป็นช่องทางในการหลีกเลี่ยงกฎเกณฑ์การควบคุมต่าง ๆ ของหน่วยงานภาครัฐ และยากที่จะติดตาม

(5) การหลีกเลี่ยงภาษี (Taxation) การโอนสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีระหว่างกระเป๋าเงินอิเล็กทรอนิกส์ของบุคคลทั่วไป ทำให้หน่วยงานภาครัฐติดตามธุรกรรมได้ยาก จึงอาจเป็นช่องทางในการหลีกเลี่ยงภาษีได้ ทั้งนี้เนื่องจากปัจจุบันกฎหมายกำหนดให้มีการเก็บภาษีจากผลตอบแทนการซื้อขายสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีเช่นเดียวกับการถือครองสินทรัพย์หรือหลักทรัพย์ประเภทอื่น ๆ เช่น หุ้น หรือพันธบัตร

(6) ผลต่อเสถียรภาพระบบการเงินจากการให้บริการที่เกี่ยวข้องกับสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีโดยสถาบันการเงิน (Financial Stability) เนื่องจากราคาของสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีมีความผันผวนสูง การโจรกรรมคริปโทเคอร์เรนซีที่ก่อให้เกิดความสูญเสียเป็นมูลค่าสูงมากเกิดขึ้นบ่อยครั้ง และมีความเสี่ยงจากการที่คริปโทเคอร์เรนซีจะถูกใช้การฟอกเงินหรือซื้อขายสิ่งผิดกฎหมาย สถาบันการเงินจึงไม่ควรเข้าไปลงทุนหรือเก็งกำไรในคริปโทเคอร์เรนซีโดยตรง และใช้ความระมัดระวังในการให้บริการที่เกี่ยวข้องกับคริปโทเคอร์เรนซี เนื่องจากปัญหาที่เกิดขึ้นจะส่งผลกระทบต่อความน่าเชื่อถือของสถาบันการเงินและระบบการเงินโดยรวม

(7) การใช้สกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีในการชำระเงินอย่างแพร่หลาย (Means of Payment) หากในอนาคตการใช้คริปโทเคอร์เรนซีเป็นสื่อกลางในการชำระค่าสินค้าและบริการแพร่หลายมากขึ้น หน่วยงานภาครัฐจำเป็นต้องเข้ามาดูแลความเสี่ยงที่เกี่ยวข้องนี้ เช่นเดียวกับการใช้ระบบการชำระเงินอิเล็กทรอนิกส์ เช่น e-Money ในประเทศไทยซึ่งมีกฎหมายกำกับดูแลเพื่อคุ้มครองผู้ใช้บริการอย่างชัดเจนแล้ว

## 2.2.2 แนวคิดในการควบคุมสกุลเงินดิจิทัล

### 2.2.2.1 หน่วยงานที่เกี่ยวข้องกับการควบคุมสกุลเงินดิจิทัล

สำนักงานคณะกรรมการกำกับตลาดหลักทรัพย์ (ก.ล.ต.)

เป็นหน่วยงานของรัฐที่จัดตั้งขึ้นตามพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 มีอำนาจหน้าที่ในการส่งเสริมและพัฒนาตลาดจูงกำกับดูแลตลาดทุน อาทิ การระดมทุน สินค้าและบริการ ผู้ประกอบธุรกิจที่เกี่ยวข้อง การกระทำอันไม่เป็นธรรมในตลาดทุน นอกจากนี้พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 หมวด 2 ยังได้มีการกำหนดให้สำนักงานคณะกรรมการตลาดหลักทรัพย์มีหน้าที่กำกับดูแลสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีในภาคธุรกิจ โดยการวางนโยบายออกกระเปียบ ข้อบังคับ ประกาศ คำสั่ง หรือข้อกำหนดเกี่ยวกับการออกและเสนอขายโทเคนดิจิทัลและการประกอบธุรกิจสินทรัพย์ดิจิทัล<sup>105</sup> กำหนดแนวทางการกำกับดูแลเพื่อป้องกันปัญหาและผลกระทบอันเกิดจากความเสี่ยงที่เกี่ยวข้องกับเงินดิจิทัลและการระดมทุนแบบ ICO ซึ่งได้กำหนดให้การประกอบธุรกิจสินทรัพย์ดิจิทัลจะต้องได้รับใบอนุญาตประกอบสินทรัพย์ดิจิทัล<sup>106</sup> รวมถึงการกำหนดค่าธรรมเนียมสำหรับคำขออนุญาต การอนุญาต คำขอความเห็นชอบ การให้ความเห็นชอบ การยื่นแบบแสดงรายการข้อมูลการเสนอขายโทเคนดิจิทัล การยื่นแบบแสดงรายการ ข้อมูลประจำปี การยื่นคำขอต่าง ๆ หรือการประกอบกิจการ<sup>107</sup> ทั้งนี้การดำเนินการต่าง ๆ ต้องเป็นไปตามวัตถุประสงค์ของพระราชกำหนดดังกล่าว

การกำกับดูแลสกุลเงินดิจิทัลภายใต้คณะกรรมการกำกับตลาดหลักทรัพย์ จึงได้มีวัตถุประสงค์ในการควบคุมผู้ประกอบธุรกิจซื้อขายสินทรัพย์ดิจิทัล ซึ่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล ได้ให้นิยามคำว่า “ผู้ประกอบธุรกิจซื้อขายสินทรัพย์ดิจิทัล” หมายถึง “ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่ได้รับใบอนุญาตประกอบธุรกิจสินทรัพย์ดิจิทัล แต่ทั้งนี้มิให้หมายความรวมถึงผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลที่เป็นธนาคารพาณิชย์ตามกฎหมายว่าด้วยธุรกิจ

<sup>105</sup> มาตรา 10 (1) แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

<sup>106</sup> สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, **ผู้ประกอบธุรกิจที่ได้รับใบอนุญาตศูนย์ซื้อขายสินทรัพย์ดิจิทัล**, ค้นวันที่ 25 พฤษภาคม 2564 จาก <https://www.sec.or.th/digitalasset#EBD>

<sup>107</sup> มาตรา 10 (2) แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

สถาบันการเงิน บริษัทประกันชีวิตตามกฎหมายว่าด้วยการประกันชีวิต บริษัทหลักทรัพย์ตามกฎหมายว่าด้วยหลักทรัพย์และตลาดหลักทรัพย์” ซึ่งมีดังต่อไปนี้<sup>108</sup>

1) ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Digital Asset Exchange) หมายถึง ศูนย์กลางหรือเครือข่ายใด ๆ ที่จัดให้มีขึ้นเพื่อการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัล โดยการจับคู่หรือหาคู่สัญญาให้ หรือการจัดระบบหรืออำนวยความสะดวกให้ผู้ซึ่งประสงค์จะซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัลสามารถทำความตกลงหรือจับคู่กันได้ โดยกระทำเป็นทางคำปกติ แต่ทั้งนี้ ไม่รวมศูนย์กลางหรือเครือข่ายในลักษณะที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด

2) นายหน้าซื้อขายสินทรัพย์ดิจิทัล (Digital Asset Broker) หมายถึง บุคคลซึ่งให้บริการหรือแสดงต่อบุคคลทั่วไปว่าพร้อมจะให้บริการเป็นนายหน้าหรือตัวแทน เพื่อซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัลให้แก่บุคคลอื่นโดยกระทำเป็นทางคำปกติและได้รับค่าธรรมเนียมหรือค่าตอบแทนอื่น แต่ไม่รวมถึงการเป็นนายหน้าหรือตัวแทนในลักษณะที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด

3) ผู้ค้าสินทรัพย์ดิจิทัล (Digital Asset Dealer) หมายถึง บุคคลซึ่งให้บริการหรือแสดงต่อบุคคลทั่วไปว่าพร้อมจะให้บริการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัลในนามของตนเองเป็นทางคำปกติ โดยกระทำนอกศูนย์ซื้อขายสินทรัพย์ดิจิทัล แต่ไม่รวมถึงการให้บริการในลักษณะตามที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด

4) ที่ปรึกษาสินทรัพย์ดิจิทัล (Digital Asset Advisory Service) หมายถึง บุคคลซึ่งให้คำแนะนำแก่ประชาชนไม่ว่าโดยทางตรงหรือทางอ้อมเกี่ยวกับคุณค่าของสินทรัพย์ดิจิทัล หรือความเหมาะสมในการลงทุนที่เกี่ยวกับสินทรัพย์ดิจิทัลนั้น หรือที่เกี่ยวกับการซื้อ ขาย หรือแลกเปลี่ยนสินทรัพย์ดิจิทัลใด ๆ เป็นทางคำปกติ ทั้งนี้ โดยได้รับค่าธรรมเนียมหรือค่าตอบแทนอื่น แต่ไม่รวมถึงการให้คำแนะนำอันเป็นส่วนหนึ่งหรือเกี่ยวเนื่องกับการประกอบกิจการของศูนย์ซื้อขายสินทรัพย์ดิจิทัล นายหน้าซื้อขายสินทรัพย์ดิจิทัล ผู้ค้าสินทรัพย์ดิจิทัล หรือผู้จัดการเงินทุนสินทรัพย์ดิจิทัล หรือการให้คำแนะนำแก่ประชาชนในลักษณะที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด

5) ผู้จัดการเงินทุนสินทรัพย์ดิจิทัล (Digital Asset Fund Manager) หมายถึง บุคคลซึ่งเข้าจัดการเงินทุน หรือแสดงต่อบุคคลทั่วไปว่าพร้อมจะรับจัดการเงินทุนให้แก่บุคคลอื่น เพื่อแสวงหาประโยชน์จากสินทรัพย์ดิจิทัล โดยกระทำเป็นทางคำปกติ แต่ไม่รวมถึงการจัดการเงินทุนสินทรัพย์ดิจิทัลในลักษณะที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด

<sup>108</sup> สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, **ผู้ประกอบการธุรกิจ**

ภายหลังจากได้รับอนุญาตให้ประกอบธุรกิจสินทรัพย์ดิจิทัลแล้ว ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลมีหน้าที่ต้องปฏิบัติตามหลักเกณฑ์ วิธีการ และเงื่อนไขที่กำหนดไว้ภายใต้ พระราชกำหนด สินทรัพย์ดิจิทัลฯ และกฎเกณฑ์อื่น ๆ ที่คณะกรรมการ ก.ล.ต. หรือสำนักงาน ก.ล.ต. ประกาศกำหนดโดยอาศัยอำนาจตาม พ.ร.ก. สินทรัพย์ เช่น เช่น การมีโครงสร้างการบริหารจัดการระบบงาน และบุคลากร ที่เหมาะสมและเพียงพอต่อการประกอบธุรกิจ การมีแหล่งเงินทุนที่เพียงพอรองรับการประกอบการและความเสี่ยงในด้านต่าง ๆ การดูแลรักษาความปลอดภัยของระบบเทคโนโลยีสารสนเทศ การติดต่อและให้บริการลูกค้า การมีระบบบัญชีที่เหมาะสม การทำ KYC/CDD เป็นต้น<sup>109</sup> โดยหลักเกณฑ์ในรายละเอียดจะแตกต่างกันไปตามลักษณะการประกอบธุรกิจของผู้ประกอบธุรกิจฯ แต่ละประเภท

#### 2.2.2.2 กฎหมายที่เกี่ยวข้องกับสกุลเงินดิจิทัล

##### 1) พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

ปัจจุบันได้มีการนำสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีมาเป็นสื่อกลางในการแลกเปลี่ยนรวมถึง นำซื้อขายหรือแลกเปลี่ยนในศูนย์ซื้อขายคริปโทเคอร์เรนซี พระราชกำหนดนี้จึงมีขึ้นเพื่อกำกับและควบคุมการประกอบธุรกิจและการดำเนินกิจกรรมเกี่ยวกับสินทรัพย์ดิจิทัล และเพื่อรองรับการนำเทคโนโลยีมาทำให้เกิดการพัฒนาทางเศรษฐกิจและสังคมอย่างยั่งยืน และสนับสนุนอำนวยความสะดวกให้ผู้ประกอบธุรกิจที่มีศักยภาพมีเครื่องมือในการระดมทุนที่หลากหลาย รวมทั้งประชาชนผู้ที่เกี่ยวข้องมีข้อมูลที่ชัดเจนเพียงพอเพื่อให้ใช้ในการตัดสินใจเกิดความโปร่งใสในการดำเนินการและป้องกันมิให้มีการนำสินทรัพย์ดิจิทัลที่ไม่มีแหล่งที่มาที่ชัดเจนไปใช้ประโยชน์หรือกระทำการใดในลักษณะที่เป็นการหลอกลวงประชาชน<sup>110</sup>

กฎหมายฉบับนี้ได้ให้ความหมายคำว่าสินทรัพย์ดิจิทัลไว้ดังนี้<sup>111</sup>

(1) “คริปโทเคอร์เรนซี” คือ หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้ เป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และหมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นที่คณะกรรมการ ก.ล.ต. ประกาศกำหนดเพิ่มเติม

<sup>109</sup> มาตรา 30 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

<sup>110</sup> สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, **สรุปสาระสำคัญของพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล** (กรุงเทพมหานคร: สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, 2561), หน้า 1-8, ค้นวันที่ 4 สิงหาคม 2562 จาก [https://www.sec.or.th/TH/Documents/DigitalAsset/digitalasset\\_summary.pdf](https://www.sec.or.th/TH/Documents/DigitalAsset/digitalasset_summary.pdf)

<sup>111</sup> มาตรา 3 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

(2) “โทเคนดิจิทัล” คือ หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีวัตถุประสงค์เพื่อกำหนดสิทธิของบุคคลในการเข้าร่วมลงทุนในโครงการหรือกิจการใด ๆ หรือกำหนดสิทธิในการได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใดที่เฉพาะเจาะจง ทั้งนี้ ตามที่กำหนดในข้อตกลงระหว่างผู้ออกและผู้ถือ และหมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นที่คณะกรรมการ ก.ล.ต. ประกาศกำหนดเพิ่มเติม ซึ่งคณะกรรมการ ก.ล.ต. ได้ออกประกาศกำหนดให้คริปโทเคอร์เรนซีที่ผู้ออกมีวัตถุประสงค์ในการระดมทุนจากประชาชนและมีการกำหนดสิทธิของบุคคลในการเข้าร่วมลงทุนในโครงการหรือกิจการใด ๆ หรือมีการกำหนดสิทธิในการได้มาซึ่งสินค้าหรือบริการหรือสิทธิอื่นใด ๆ ถือเป็นโทเคนดิจิทัลด้วย

อย่างไรก็ตามในส่วนของหลักทรัพย์นั้นพระราชกำหนดสินทรัพย์ดิจิทัลฯ ได้กำหนดว่า “หลักทรัพย์” ตามพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 แม้จะอยู่ในรูปของหน่วยข้อมูลอิเล็กทรอนิกส์ แต่ไม่ถือเป็นสินทรัพย์ดิจิทัลในประเภทคริปโทเคอร์เรนซีและโทเคนดิจิทัลภายใต้พระราชกำหนดนี้ ทั้งนี้เพื่อให้เกิดความชัดเจนและป้องกันความซ้ำซ้อนของกฎหมาย<sup>112</sup> และยังสามารถกำกับดูแลกิจกรรมอื่นที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล ได้แก่ (1) การระดมทุนด้วยการเสนอขายโทเคนดิจิทัลต่อประชาชน หมวด 3 ซึ่งมีได้กำกับดูแลการเสนอขายคริปโทเคอร์เรนซี เว้นแต่คริปโทเคอร์เรนซีนั้นได้ถูกประกาศกำหนดให้ถือเป็นโทเคนดิจิทัล (2) การให้บริการเป็นตัวกลางในการซื้อขายแลกเปลี่ยนสินทรัพย์ดิจิทัล หมวด 4 ธุรกิจสินทรัพย์ดิจิทัล กล่าวคือเป็นการควบคุมผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัลจะต้องได้รับอนุญาตจากรัฐมนตรีตามข้อเสนอแนะของคณะกรรมการ ก.ล.ต.

นอกจากนี้พระราชบัญญัติดังกล่าวยังมีบทบัญญัติในการควบคุมการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายสินทรัพย์ดิจิทัล ซึ่งเป็นการควบคุมผู้ประกอบการธุรกิจซื้อขายสินทรัพย์ดิจิทัลโดยได้กำหนดลักษณะของการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายหรือแลกเปลี่ยนสินทรัพย์ดิจิทัล ไว้ดังต่อไปนี้

(1) False Dissemination: การห้ามบอกกล่าว เผยแพร่ หรือให้คำรับรองข้อความอันเป็นเท็จหรือข้อความอันอาจก่อให้เกิดความสำคัญผิดในสาระสำคัญที่เกี่ยวข้องกับผู้เสนอขายโทเคนดิจิทัล โทเคนดิจิทัล หรือราคาซื้อขายสินทรัพย์ดิจิทัล ซึ่งน่าจะทำให้มีผลกระทบต่อราคาหรือต่อการตัดสินใจลงทุนในสินทรัพย์ดิจิทัล<sup>113</sup> รวมถึงการวิเคราะห์หรือคาดการณ์โดยนำข้อมูลที่รู้ว่าเป็นเท็จหรือไม่ครบถ้วนอันอาจก่อให้เกิดความสำคัญผิดในสาระสำคัญมาใช้ หรือละเลยที่จะพิจารณาความถูกต้องของข้อมูล หรือบิดเบือนข้อมูลที่ใช้ในการวิเคราะห์หรือคาดการณ์ และได้

<sup>112</sup> มาตรา 5 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

<sup>113</sup> มาตรา 40 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

เปิดเผยความเห็นเกี่ยวกับการวิเคราะห์หรือคาดการณ์นั้นต่อประชาชนในประการที่น่าจะทำให้มีผลกระทบต่อราคาหรือต่อการตัดสินใจลงทุนในสินทรัพย์ดิจิทัล<sup>114</sup>

(2) Insider Trading: การห้ามมิให้บุคคลซึ่งรู้หรือครอบครองข้อมูลภายในที่เกี่ยวข้องกับผู้เสนอขายโทเคนดิจิทัล หรือโทเคนดิจิทัล ซื้อขายหรือเข้าผูกพันตามสัญญาซื้อขายล่วงหน้าที่เกี่ยวข้องกับโทเคนดิจิทัลไม่ว่าเพื่อตนเองหรือบุคคลอื่น และห้ามเปิดเผยข้อมูลภายในแก่บุคคลอื่น โดยรู้หรือควรรู้ว่าผู้รับข้อมูลอาจนำไปใช้ประโยชน์ในการซื้อขาย เว้นแต่จะเข้าข้อยกเว้นตามที่กำหนดไว้<sup>115</sup> รวมทั้งได้กำหนดบทสันนิษฐานบุคคลซึ่งรู้หรือครอบครองข้อมูลภายในไว้อีกด้วย<sup>116</sup>

(3) Front Running: การห้ามผู้ประกอบการธุรกิจฯ ประเภทย่อยหน้าซื้อขายสินทรัพย์ดิจิทัล รวมทั้งพนักงาน หรือลูกจ้าง ซึ่งรู้หรือครอบครองข้อมูลเกี่ยวกับการสั่งซื้อขายสินทรัพย์ดิจิทัล หรือสัญญาซื้อขายล่วงหน้าที่เกี่ยวข้องกับสินทรัพย์ดิจิทัลของลูกค้า กระทำการซื้อขายตัดหน้าลูกค้าหรือเปิดเผยข้อมูลเกี่ยวกับคำสั่งของลูกค้าให้แก่บุคคลอื่น โดยรู้หรือควรรู้ว่าบุคคลนั้นจะอาศัยข้อมูลดังกล่าวเพื่อซื้อขายตัดหน้าลูกค้าทั้งนี้ไม่ว่าจะเป็นการซื้อขายเพื่อตนเองหรือบุคคลอื่นในประการที่น่าจะทำให้ลูกค้ารายดังกล่าวเสียประโยชน์<sup>117</sup>

(4) Market Manipulation: การห้ามมิให้ส่งคำสั่งซื้อขาย หรือซื้อขายสินทรัพย์ดิจิทัลอันทำให้บุคคลทั่วไปเข้าใจผิดเกี่ยวกับราคาหรือปริมาณการซื้อขายสินทรัพย์ดิจิทัล รวมถึงการส่งคำสั่งซื้อขาย หรือซื้อขายในลักษณะที่ต่อเนื่องกัน โดยมีมุ่งหมายให้ราคา หรือปริมาณการซื้อขายสินทรัพย์ดิจิทัลผิดไปจากสภาพปกติของตลาด<sup>118</sup>

ตัวอย่างการดำเนินคดีที่เกี่ยวข้องกับสกุลเงินดิจิทัลภายใต้พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ตรวจสอบเหตุสงสัยว่าอาจมีการสร้างปริมาณเทียมในศูนย์ซื้อขาย B โดยพบการกระทำเข้าข่ายเป็นความผิดของบุคคล 3 ราย ได้แก่ (1) บริษัท บ (2) นาย อ ร่วมกันในการส่งคำสั่งซื้อหรือขายสินทรัพย์ดิจิทัล หรือซื้อหรือขายสินทรัพย์ดิจิทัล จำนวน 18 สกุลเงินดิจิทัล เป็นความผิดกรณีทำให้บุคคลทั่วไป

<sup>114</sup> มาตรา 41 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

<sup>115</sup> มาตรา 42 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

<sup>116</sup> มาตรา 43 และมาตรา 44 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

<sup>117</sup> มาตรา 45 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

<sup>118</sup> มาตรา 46 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

เข้าใจผิดเกี่ยวกับปริมาณการซื้อขายหลักทรัพย์ดิจิทัลในศูนย์ซื้อขาย B และ (3) นาย ส ซึ่งในขณะกระทำความผิดดำรงตำแหน่งเป็นประธานเจ้าหน้าที่บริหารและกรรมการผู้มีอำนาจจัดการของบริษัท บ ได้สั่งการหรือกระทำการหรือไม่สั่งการหรือไม่กระทำการอันเป็นหน้าที่ที่ต้องกระทำ เป็นเหตุให้บริษัท บ กระทำความผิดดังกล่าว ดังนี้

บริษัท บ โดยนาย ส ได้ทำสัญญากับนาย อ ให้นาย อ ทำหน้าที่ดูแลสภาพคล่อง (Market Maker) ในศูนย์ซื้อขาย B และให้นาย อ ยืมเงินเพื่อใช้ในการทำหน้าที่ดังกล่าว โดยนาย อ ได้จับคู่ซื้อขายกันเองในบัญชีซื้อขายเหรียญคริปโทเคอร์เรนซีของตนเองในศูนย์ซื้อขาย B จำนวน 18 สกุลเงินดิจิทัล มีสัดส่วนตั้งแต่ร้อยละ 74-99 ของปริมาณการซื้อขายรวมทั้งตลาด ทั้งนี้บริษัท บ และนาย ส รับทราบถึงการจับคู่ซื้อขายกันเองในบัญชีซื้อขายของนาย อ แต่ไม่ได้มีการทักท้วงการส่งคำสั่งซื้อขายเหรียญคริปโทเคอร์เรนซีแต่อย่างใด

การกระทำของบริษัท บ และนาย อ จึงเป็นความผิดฐานส่งคำสั่งซื้อหรือขายหลักทรัพย์ดิจิทัล หรือซื้อหรือขายหลักทรัพย์ดิจิทัล อันเป็นการทำให้บุคคลทั่วไปเข้าใจผิดเกี่ยวกับปริมาณการซื้อขายหลักทรัพย์ดิจิทัลตามมาตรา 46 (1) ประกอบมาตรา 48 (2) (3) แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ประกอบมาตรา 83 แห่งประมวลกฎหมายอาญา ซึ่งมีบทกำหนดโทษตามมาตรา 70 แห่งพระราชกำหนดฉบับเดียวกัน เป็นความผิด 18 กระทง (นับตามจำนวนเหรียญ) ส่วนการกระทำของนาย ส เป็นความผิดในฐานะเป็นบุคคลที่รับผิดชอบในการดำเนินงานของบริษัท บ สั่งการ หรือกระทำการ หรือไม่สั่งการ หรือไม่กระทำการอันเป็นหน้าที่ที่ต้องกระทำ เป็นเหตุให้บริษัท บ กระทำความผิดในกรณีข้างต้น ซึ่งต้องรับโทษเดียวกันตามมาตรา 94 ประกอบมาตรา 46 (1) ประกอบมาตรา 48 (2) (3) แห่ง พ.ร.ก. สินทรัพย์ดิจิทัลฯ ซึ่งต้องระวางโทษตามมาตรา 70 แห่งพระราชกำหนดฉบับเดียวกัน เป็นความผิด 18 กระทง (นับตามจำนวนเหรียญ)<sup>119</sup>

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ได้ดำเนินคดีโดยใช้มาตรการลงโทษทางแพ่งกับผู้กระทำความผิด 4 ราย ได้แก่ (1) บริษัท ส (2) บริษัท L ร่วมกันในการส่งคำสั่งซื้อหรือขายหลักทรัพย์ดิจิทัล หรือซื้อหรือขายหลักทรัพย์ดิจิทัล จำนวน 3 สกุลเงินดิจิทัล อันเป็นการทำให้บุคคลทั่วไปเข้าใจผิดเกี่ยวกับปริมาณการซื้อขายหลักทรัพย์ดิจิทัลในศูนย์ซื้อขาย S (3) นาย ป ขณะกระทำความผิดดำรงตำแหน่งเป็นประธานเจ้าหน้าที่บริหารและกรรมการผู้

<sup>119</sup> สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, ก.ล.ต. ใช้มาตรการลงโทษทางแพ่งกับผู้กระทำความผิด 3 ราย กรณีสร้างปริมาณเทียมสินทรัพย์ดิจิทัลจำนวน 18 เหรียญ ในศูนย์ซื้อขายสินทรัพย์ดิจิทัลของบริษัท บิทคับ ออนไลน์ จำกัด, ค้นวันที่ 30 ธันวาคม 2565 จาก [https://www.sec.or.th/TH/Pages/News\\_Detail.aspx?SECID=9793&NewsNo=9793&NewsYear=9793&Lang=9793](https://www.sec.or.th/TH/Pages/News_Detail.aspx?SECID=9793&NewsNo=9793&NewsYear=9793&Lang=9793)

มีอำนาจจัดการของบริษัท ส และ (4) นาย M เจ้าของและกรรมการผู้จัดการบริษัท L ในความผิดกรณีสั่งการ หรือกระทำการ หรือไม่สั่งการ หรือไม่กระทำการอันเป็นหน้าที่ที่ต้องกระทำ เป็นเหตุให้บริษัท ส และบริษัท L (ตามลำดับ) กระทำความผิดดังกล่าว

คณะกรรมการพิจารณามาตรการลงโทษทางแพ่ง (ค.ม.พ.) ได้มีมติให้ดำเนินมาตรการลงโทษทางแพ่ง โดยให้นาย ป ร่วมรับผิดชอบในมาตรการลงโทษทางแพ่งที่ดำเนินการกับบริษัท ส อย่างลูกหนี้ร่วมตามมาตรา 99 แห่งพระราชกำหนดสินทรัพย์ดิจิทัล ประกอบมาตรา 317/11 วรรคสอง แห่งพระราชบัญญัติหลักทรัพย์และตลาดหลักทรัพย์ พ.ศ. 2535 ที่แก้ไขเพิ่มเติมฉบับที่ 5 พ.ศ. 2559 และให้นาย M ร่วมรับผิดชอบในมาตรการลงโทษทางแพ่งที่ดำเนินการกับบริษัท L อย่างลูกหนี้ร่วมตามมาตรา 99 แห่ง พ.ร.ก. สินทรัพย์ดิจิทัลฯ ประกอบมาตรา 317/11 วรรคสอง แห่ง พ.ร.บ. หลักทรัพย์ฯ ที่แก้ไขเพิ่มเติมฉบับที่ 5 ทั้งนี้ เงินค่าปรับทางแพ่งที่ได้รับจากการกระทำความผิดเป็นรายได้แผ่นดินที่นำส่งกระทรวงการคลัง<sup>120</sup>

อย่างไรก็ตามพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 มีวัตถุประสงค์ในการกำกับและควบคุมการประกอบธุรกิจที่เกี่ยวกับสินทรัพย์ดิจิทัลในการซื้อขาย แลกเปลี่ยน และเก็งกำไรในภาคธุรกิจเป็นสำคัญอันเป็นการเพิ่มศักยภาพในการลงทุนและสร้างความเชื่อมั่นให้แก่ผู้ใช้ในฐานะผู้ลงทุน อย่างไรก็ตามในการใช้หรือการถือครองสกุลเงินดิจิทัลได้มีการจำกัดแค่เพียงผู้ประกอบธุรกิจหรือธุรกรรมทางแพ่งเท่านั้น แต่ในส่วนของภาคประชาชนที่ได้มีเข้าถึงและใช้สกุลเงินดิจิทัลหากมีการกระทำความผิดอันเกิดจากการใช้หรือถือครองสกุลเงินดิจิทัล เช่นการขโมยสกุลเงินดิจิทัล การกระทำความผิดดังกล่าวจะไม่อยู่ในบังคับของกฎหมายฉบับนี้

## 2) พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2545

ปัจจุบันการติดต่อสื่อสารระหว่างบุคคลอาศัยการพัฒนาเทคโนโลยีทางอิเล็กทรอนิกส์ซึ่งมีความสะดวก รวดเร็วและมีประสิทธิภาพ แต่เนื่องจากการทำธุรกรรมทางอิเล็กทรอนิกส์ดังกล่าวมีความแตกต่างจากวิธีการทำธุรกรรมซึ่งมีกฎหมายรองรับอยู่ในปัจจุบันเป็นอย่างมาก อันส่งผลให้ต้องมีการรองรับสถานะทางกฎหมายของข้อมูลทางอิเล็กทรอนิกส์ให้เท่าเทียมกับการทำเป็นหนังสือ หรือหลักฐานเป็นหนังสือ การรับรองวิธีการส่งและรับข้อมูลอิเล็กทรอนิกส์ การใช้ลายมือชื่ออิเล็กทรอนิกส์ ตลอดจนการรับฟังพยานหลักฐานที่เป็นข้อมูลอิเล็กทรอนิกส์ เพื่อเป็น

<sup>120</sup> สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, ก.ล.ต. ใช้มาตรการลงโทษทางแพ่งกับผู้กระทำความผิด 4 ราย กรณีสร้างปริมาณเทียมสินทรัพย์ดิจิทัลจำนวน 3 เหรียญ ในศูนย์ซื้อขายสินทรัพย์ดิจิทัลของบริษัท สตาดาร์ คอร์ปอเรชั่น จำกัด, ค้นวันที่ 30 ธันวาคม 2565 จาก [https://www.sec.or.th/TH/Pages/News\\_Detail.aspx?SECID=9794&NewsNo=9794&NewsYear=9794&Lang=9794](https://www.sec.or.th/TH/Pages/News_Detail.aspx?SECID=9794&NewsNo=9794&NewsYear=9794&Lang=9794)

สร้างความน่าเชื่อถือให้กับการทำธุรกรรมทางอิเล็กทรอนิกส์ และมีผลในทางกฎหมายเช่นเดียวกับการทำธุรกรรมโดยวิธีการทั่วไปที่เคยปฏิบัติอยู่เดิม ดังนั้นจึงควรส่งเสริมการพัฒนาการทางเทคโนโลยี เพื่อให้ศักยภาพและมาตรฐานที่น่าเชื่อถือ สอดคล้องกับมาตรฐานที่นานาประเทศยอมรับ<sup>121</sup>

หลักการที่สำคัญของพระราชบัญญัติฉบับนี้คือ หลักความเท่าเทียมกันในการทำหน้าที่ (Functional-Equivalent Approach) นั้นเป็นหลักการที่ใช้รองรับสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ กล่าวคือ เมื่อการใดกระทำลงโดยใช้วิธีการติดต่อสื่อสารแบบดั้งเดิม (โดยใช้เอกสาร) แล้วสามารถทำหน้าที่ได้และมีผลสมบูรณ์ตามกฎหมาย หากการนั้นได้กระทำลงโดยใช้ข้อมูลอิเล็กทรอนิกส์แทนเอกสารปดัตถกรรมดา การนั้นก็ต้องทำหน้าที่ได้อย่างเดียวกันกับการที่กระทำลงโดยวิธีการดั้งเดิมและมีผลทางกฎหมายอย่างเดียวกัน เช่น ในกรณีที่กฎหมายกำหนดว่าการใดต้องทำเป็นหนังสือหรือมีหลักฐานเป็นหนังสือ ก็ให้ถือว่าการทำเป็นหนังสือหรือมีหลักฐานเป็นหนังสือที่ทำโดยวิธีการทางอิเล็กทรอนิกส์มีผลทางกฎหมายเช่นเดียวกัน หรือกล่าวอีกหนึ่งคือ ห้ามมิให้ปฏิเสธความมีผลทางกฎหมายของวิธีการทางอิเล็กทรอนิกส์<sup>122</sup>

พระราชบัญญัติฉบับดังกล่าวมีผลบังคับแก่ธุรกรรมทางอิเล็กทรอนิกส์ ในทางแพ่งและพาณิชย์ที่ดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์<sup>123</sup> และได้นิยามคำว่า ข้อมูลอิเล็กทรอนิกส์ หมายถึง ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือ โทรสาร และคำว่า อิเล็กทรอนิกส์ หมายความว่า การประยุกต์ใช้วิธีการทางอิเล็กทรอนิกส์ ฟ้า คลื่นแม่เหล็กไฟฟ้า หรือวิธีการอื่นใดในลักษณะคล้ายกัน และให้หมายความรวมถึง การประยุกต์ใช้วิธีการทางแสง วิธีการทางแม่เหล็ก หรืออุปกรณ์ที่เกี่ยวข้องกับการประยุกต์ใช้วิธีต่าง ๆ

จากนิยามดังกล่าว ข้อมูลอิเล็กทรอนิกส์ มีความเชื่อมโยงกับสกุลเงินดิจิทัล เนื่องจากสกุลเงินดิจิทัลถูกสร้างและประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ อีกทั้งยังดำเนินการโดยใช้ข้อมูลอิเล็กทรอนิกส์ สกุลเงินดิจิทัลจึงมีลักษณะเป็นข้อมูลอิเล็กทรอนิกส์อย่างหนึ่ง ซึ่งจำกัดเฉพาะข้อมูลที่จัดเก็บ หรือรับส่งระหว่างกันด้วยคอมพิวเตอร์ สมาร์ทโฟน อาจเรียกได้ว่าเป็นข้อมูลคอมพิวเตอร์ ซึ่งถือเป็นส่วนหนึ่งของข้อมูลอิเล็กทรอนิกส์

<sup>121</sup> หมายเหตุท้าย แห่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544

<sup>122</sup> พินัย ฌ นคร, **กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ในยุคดิจิทัล** (กรุงเทพมหานคร: วิญญูชน, 2561), หน้า 143.

<sup>123</sup> *เรื่องเดียวกัน*, หน้า 138.

3) พระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร ฉบับที่ 19 พ.ศ. 2561 พระราชกำหนดฉบับนี้เกี่ยวข้องกับการถือครองสกุลเงินดิจิทัลโดยตรง กล่าวคือ สกุลเงินดิจิทัลเป็นที่ยอมรับว่ามีมูลค่า สามารถซื้อขายแลกเปลี่ยน เก่งกำไรได้จริง และนำมาซึ่งรายได้ ดังนั้นรัฐจึงมองว่ารายได้ดังกล่าวนี้ถือเป็นเงินได้พึงประเมินที่ต้องนำมารวมคำนวณเพื่อเสียภาษี

กฎหมายในส่วนนี้มีแก้ไขใหม่ซึ่งเกี่ยวข้องกับการใช้ การถือครองสกุลเงินดิจิทัล 2 ประการ คือ คือ

(1) กำหนดให้เงินส่วนแบ่งของกำไรหรือผลประโยชน์อื่นใดในลักษณะเดียวกันที่ได้จากการถือหรือครอบครองโทเคนดิจิทัลและผลประโยชน์ที่ได้รับจากการโอนคริปโทเคอร์เรนซีหรือโทเคนดิจิทัลเฉพาะซึ่งตีราคาเป็นเงินได้เกินกว่าที่ลงทุน ถือเป็นเงินได้พึงประเมินตามมาตรา 40 (4) แห่งประมวลรัษฎากร ประเภทผลตอบแทนทางการเงินโดยอยู่ใน (ซ) และ (ณ) ของมาตรา 40 (4) ดังกล่าว ซึ่งจะต้องนำเงินที่ได้จากแหล่งดังกล่าวนำมารวมคำนวณเป็นรายได้ประจำปี<sup>124</sup>

(2) กำหนดให้เงินได้ประเภทที่เป็นเงินส่วนแบ่งของกำไรหรือผลประโยชน์อื่นใดในลักษณะเดียวกันที่ได้จากการถือหรือครอบครองโทเคนดิจิทัลและผลประโยชน์ที่ได้รับจากการโอนคริปโทเคอร์เรนซีหรือโทเคนดิจิทัลเฉพาะซึ่งตีราคาเป็นเงินได้เกินกว่าที่ลงทุนตามมาตราที่ 40 (4) (ซ) และ (ณ) ต้องเสียภาษี โดยหัก ณ ที่จ่าย ในอัตราร้อยละ 15 ของเงินได้บุคคลธรรมดาที่มีเงินได้พึงประเมินตามมาตราดังกล่าว<sup>125</sup>

อย่างไรก็ตามพระราชกำหนดดังกล่าวเป็นการควบคุมรายได้ที่เกิดจากการทำธุรกรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัล แต่ไม่ได้มีวัตถุประสงค์ในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลไว้เป็นการเฉพาะ

2.2.2.3 ประเด็นปัญหาสถานะทางกฎหมายอาญาของสกุลเงินดิจิทัลในประเทศไทย สำหรับประเทศไทยแม้จะมีการออกกฎหมายที่เกี่ยวข้องกับสกุลเงินดิจิทัลมาหลายฉบับ ได้แก่ พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 พระราชบัญญัติธุรกรรมทางอิเล็กทรอนิกส์ พระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร แต่กฎหมายดังกล่าวมีวัตถุประสงค์ในการควบคุมที่แตกต่างกันไป อีกทั้งไม่ได้มีขึ้นเพื่อใช้ในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลไว้โดยตรง และไม่ได้มีการกำหนดสถานะของสกุลเงินดิจิทัลไว้แต่อย่างใด

<sup>124</sup> มาตรา 3 แห่งพระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร ฉบับที่ 19 พ.ศ. 2561

<sup>125</sup> มาตรา 4 แห่งพระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร ฉบับที่ 19 พ.ศ. 2561

ทั้งนี้สถานะของสกุลเงินดิจิทัลสามารถแยกพิจารณาได้ ดังนี้



ภาพที่ 2.3 สถานะทางกฎหมายที่เกี่ยวข้องกับสกุลเงินดิจิทัล

1) สกุลเงินดิจิทัลเป็นทรัพย์สิน เนื่องจากคำว่าทรัพย์สิน หมายถึง “วัตถุที่ไม่มีรูปร่าง ซึ่งอาจมีราคาและอาจถือเอาได้”<sup>126</sup> ดังนั้นเมื่อสกุลเงินดิจิทัลเป็นวัตถุที่ไม่มีรูปร่างจึงอาจเป็นทรัพย์สินได้ แต่หากมีการกระทำความผิดทางอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลเกิดขึ้น จึงต้องนำประมวลกฎหมายอาญาลักษณะ 12 ซึ่งได้กำหนดลักษณะความผิดเกี่ยวกับทรัพย์สินมาพิจารณา โดยความผิดในลักษณะดังกล่าวได้มีการกำหนดวัตถุแห่งการกระทำอันเป็นองค์ประกอบความผิดที่มีทั้งทรัพย์สินและทรัพย์สินแตกต่างกันไปตามแต่ละฐานความผิด ดังนั้นจึงมีปัญหาว่หากกำหนดให้สกุลเงินดิจิทัลมีสถานะเป็นทรัพย์สินแล้ว ฐานความผิดที่กำหนดให้วัตถุแห่งการกระทำเป็นทรัพย์สินจึงไม่อาจนำมาปรับใช้กับความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัลได้ เนื่องจากกฎหมายอาญาจะต้องตีความโดยเคร่งครัดตามหลักความรับผิดทางอาญา ซึ่งบุคคลจะรับผิดทางอาญาก็ต่อเมื่อมีกฎหมายกำหนดว่าการกระทำนั้นเป็นความผิดและกำหนดโทษไว้<sup>127</sup>

<sup>126</sup> มาตรา 138 แห่งประมวลกฎหมายแพ่งและพาณิชย์

<sup>127</sup> มาตรา 2 แห่งประมวลกฎหมายอาญา

2) สกุลเงินดิจิทัลเป็นเงินตรา แม้ประเทศไทยยังไม่ได้มีการยอมรับให้สกุลเงินดิจิทัลเป็นเงินตราที่สามารถชำระหนี้ได้ตามกฎหมายก็ตาม แต่เมื่อพิจารณาถึงลักษณะการใช้สกุลเงินดิจิทัลซึ่งสามารถทำหน้าที่ได้ไม่ต่างจากเงินตรา กล่าวคือ สามารถใช้สกุลเงินดิจิทัลเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการ สามารถแบ่งเป็นหน่วยย่อยได้โดยที่ยังรักษามูลค่าของสินค้าและบริการได้รวมถึงใช้เป็นมาตรฐานในการชำระหนี้ในภาคหน้าได้ อย่างไรก็ตามการกำหนดให้สกุลเงินดิจิทัลมีสถานะเป็นเงินตรายังมีปัญหาว่า “เงินตรา” ตามพระราชบัญญัติเงินตรา พ.ศ. 2501 กำหนดว่าเงินตรา หมายถึง เหรียญกษาปณ์และธนบัตร<sup>128</sup> ซึ่งทั้งเหรียญกษาปณ์และธนบัตรเป็นเงินที่ชำระหนี้ได้ตามกฎหมายโดยไม่จำกัดจำนวน<sup>129</sup> และมีข้อห้ามไม่ให้ผู้ใดทำ จำหน่าย ใช้ หรือนำออกใช้ซึ่งวัตถุหรือเครื่องหมายใด ๆ แทนเงินตรา เว้นแต่จะได้รับอนุญาตจากรัฐมนตรี<sup>130</sup> ดังนั้นเมื่อสกุลเงินดิจิทัลไม่ได้มีลักษณะภายนอกเป็นเงินตราที่สามารถจับต้องได้อย่างเช่นเหรียญกษาปณ์หรือธนบัตรและไม่ได้มีการอนุญาตให้ทำหรือนำออกใช้โดยรัฐบาล สกุลเงินดิจิทัลจึงไม่เป็นเงินตราได้ตามความหมายนี้ จึงมีปัญหาว่าจะนำความผิดเกี่ยวกับเงินตราและองค์การที่ควบคุมเงินตรามาบังคับใช้กับความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลหรือไม่

3) สกุลเงินดิจิทัลเป็นข้อมูลคอมพิวเตอร์ จากพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ที่ได้ให้ความหมายคำว่า คริปโทเคอร์เรนซี หมายถึง หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือ เครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และให้หมายความรวมถึงหน่วยข้อมูล อิเล็กทรอนิกส์อื่นใดตามที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด<sup>131</sup> การกำหนดความหมายเช่นนี้อาจนำไปปรับใช้ได้กับความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ที่มีองค์ประกอบความผิดเป็นข้อมูลคอมพิวเตอร์เท่านั้น แต่การกระทำความผิดต่อสกุลเงินดิจิทัลนั้นมิได้มีแค่ความผิดตามที่บัญญัติไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์เท่านั้น ดังนั้นความผิดที่เกี่ยวข้องกับข้อมูลคอมพิวเตอร์ตามพระราชบัญญัตินี้ จึงมีอำนาจมาปรับใช้กับความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัลได้อย่างครอบคลุม

4) สกุลเงินดิจิทัลอาจเป็นเอกสาร จากคำพิพากษาฎีกาที่ 4311/2557 ที่วินิจฉัยรับรองให้ข้อมูลคอมพิวเตอร์มีสถานะเช่นเดียวกับเอกสารจึงมีผลทำให้นำความผิดเกี่ยวกับ

<sup>128</sup> มาตรา 6 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>129</sup> มาตรา 11 และมาตรา 15 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>130</sup> มาตรา 9 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>131</sup> มาตรา 3 แห่งพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561

เอกสารมาใช้กับข้อมูลคอมพิวเตอร์ได้ จึงมีประเด็นที่ต้องพิจารณาว่าหากสกุลเงินดิจิทัลมีความเป็นข้อมูลคอมพิวเตอร์แล้ว และข้อมูลคอมพิวเตอร์ถือเป็นเอกสาร ดังนั้นสกุลเงินดิจิทัลจะมีสถานะเป็นเอกสารด้วยหรือไม่ นอกจากนี้ หากพิจารณาถึงกฎหมายที่กำหนดให้เอกสารเป็นองค์ประกอบความผิด จะเห็นว่าเป็นลักษณะความผิดที่ไม่อาจเกิดขึ้นกับสกุลเงินดิจิทัลได้ จึงยังมีข้อจำกัดในการนำมาปรับใช้กับสกุลเงินดิจิทัลเช่นเดียวกับสถานะอื่น ๆ

จากที่ได้กล่าวมาข้างต้นจะเห็นได้ถึงปัญหาการกำหนดสถานะของสกุลเงินสกุลดิจิทัลโดยเทียบเคียงจากสถานะที่มีอยู่เดิม ซึ่งสกุลเงินดิจิทัลมีทั้งความเป็นทรัพย์สิน เงินตรา ข้อมูลคอมพิวเตอร์ อยู่ในตัวเอง กล่าวคือ เป็นวัตถุที่ไม่มีรูปร่างเหมือนทรัพย์สิน มีคุณสมบัติการใช้งานเหมือนเงินตรา และมีวิธีการใช้งานที่ต้องอยู่ในระบบอิเล็กทรอนิกส์เหมือนข้อมูลคอมพิวเตอร์ รวมถึงอาจมีสถานะเป็นเอกสารได้จากการตีความของศาล ทั้งนี้เมื่อพิจารณาจากลักษณะของสกุลเงินดิจิทัลและบทบัญญัติของกฎหมายที่ควบคุมการกระทำความผิดเกี่ยวกับทรัพย์สิน เงินตรา ข้อมูลคอมพิวเตอร์ และเอกสาร เมื่อนำมาปรับใช้กับสกุลเงินดิจิทัลยังมีข้อจำกัดบางประการอยู่ ดังนั้นจึงควรกำหนดสถานะที่เหมาะสมกับสกุลเงินดิจิทัลเป็นการเฉพาะเพื่อให้มีกฎหมายในการควบคุมสอดคล้องกับการกระทำความผิดที่เกี่ยวกับสกุลเงินดิจิทัล

### 2.3 แนวคิดในการควบคุมการกระทำความผิดทางอาญาเกี่ยวกับสกุลเงินดิจิทัล

มุมมองทางกฎหมายที่มีต่อสกุลเงินดิจิทัลในประเทศไทยนั้นแม้ว่าจะไม่ได้ยอมรับให้มีสถานะเป็นเงินตราแต่ก็ไม่ได้มีการห้ามมิให้ใช้หรือกำหนดให้สกุลเงินดิจิทัลเป็นสิ่งที่ผิดกฎหมายแต่อย่างใด ปัจจุบันอัตราการขยายตัวของสกุลเงินดิจิทัลเพิ่มขึ้นอย่างรวดเร็วมีการนำสกุลเงินดิจิทัลไปใช้ในการชำระสินค้าและบริการรวมถึงการลงทุนหรือเก็งกำไร<sup>132</sup> แม้ประเทศไทยนี้ได้มีกฎหมายออกมาควบคุมการทำธุรกรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัลก็ตาม แต่การใช้สกุลเงินดิจิทัลไม่ได้ถูกจำกัดอยู่ในภาคธุรกิจเท่านั้น ในภาคประชาชนทั่วไปสามารถเข้าถึง มีไว้ใช้หรือมีไว้ในครอบครองได้เช่นกัน และด้วยสกุลเงินดิจิทัลเป็นสิ่งที่มูลค่าที่ผู้ใช้ไม่ต้องเปิดเผยตัวตน มีฉาบฉวยจึงใช้ช่องทางดังกล่าวกระทำเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล ซึ่งยากต่อการติดตามหาร่องรอยผู้กระทำความผิด การกระทำดังกล่าวจึงเป็นภัยต่อสังคมและส่งผลกระทบต่อความน่าเชื่อถือและระบบเศรษฐกิจเป็นวงกว้าง

<sup>132</sup> Parma Bains, Arif Ismail, Fabiana Melo, and Nobuyasu Sugimoto, **Regulating the Crypto Ecosystem the Case of Unbacked Crypto Assets** (Washington: International Monetary Fund, 2022), p. 13.

ดังนั้นกฎหมายอาญาในฐานะเป็นกฎหมายที่มีภารกิจในการจัดระเบียบสังคม จึงควรมีบทบาทในการควบคุมการกระทำเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัลในทางที่มิชอบ เพื่อให้สังคมปลอดภัยจากการกระทำที่ไม่พึงปรารถนา ทั้งนี้จึงมีความจำเป็นต้องศึกษาความหมาย วัตถุประสงค์ และหลักเกณฑ์ในการบัญญัติความผิดทางอาญาที่จะนำมาใช้ในการควบคุมการกระทำความผิดเพื่อวิเคราะห์แนวทางในการกำหนดความผิดอาญาที่กระทำเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัลโดยมิชอบให้ชัดเจนยิ่งขึ้น

### 2.3.1 ความหมายและวัตถุประสงค์ของกฎหมายอาญา

#### 2.3.1.1 ความหมายของกฎหมายอาญา

แม้จะไม่ปรากฏความหมายของกฎหมายอาญาในประมวลกฎหมายอาญา หรือบทบัญญัติกฎหมายลายลักษณ์อักษรอื่น แต่ในทางตำราวิชาการก็ได้มีการให้ความหมายของกฎหมายอาญาไว้ดังต่อไปนี้คือ

ศาสตราจารย์ จิตติ ดิงศภัทย์ อธิบายว่า “กฎหมายอาญา เป็นกฎหมายมหาชนว่าด้วยความผิดและโทษอาญา”<sup>133</sup>

ศาสตราจารย์ ดร.หยุด แสงอุทัย อธิบายว่า “กฎหมายอาญา หมายถึงกฎหมายที่ว่าด้วยความผิดและโทษ”<sup>134</sup>

ศาสตราจารย์ ดร.คณิต ฒ นคร อธิบายว่า “กฎหมายอาญา คือ บรรดากฎหมายทั้งหลายที่ระบุงถึงความผิดอาญา โทษ วิธีการเพื่อความปลอดภัยและมาตรการบังคับทางอาญาอื่นและเป็นกฎหมายที่กำหนดให้ความผิดอาญาเป็นเงื่อนไขของการใช้โทษ วิธีการเพื่อความปลอดภัยและมาตรการบังคับทางอาญาอื่นนั้น”<sup>135</sup>

<sup>133</sup> จิตติ ดิงศภัทย์, คำอธิบายประมวลกฎหมายอาญา ภาค 1, พิมพ์ครั้งที่ 10 (กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2546), หน้า 2.

<sup>134</sup> หยุด แสงอุทัย, กฎหมายอาญา ภาค 1, พิมพ์ครั้งที่ 21 (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2556), หน้า 13.

<sup>135</sup> คณิต ฒ นคร, กฎหมายอาญาภาคทั่วไป, พิมพ์ครั้งที่ 4 (กรุงเทพมหานคร: วิญญูชน, 2554), หน้า 45.

ศาสตราจารย์พิเศษ ดร.เกียรติขจร วัจนะสวัสดิ์ อธิบายว่า “กฎหมายอาญา คือ กฎหมายที่บัญญัติว่า การกระทำหรือการไม่กระทำการอย่างใดเป็นความผิด และกำหนดโทษที่จะลงแก่ผู้กระทำความผิดไว้ด้วย”<sup>136</sup>

ศาสตราจารย์ ดร.ทวีเกียรติ มีนะกนิษฐ อธิบายว่า “กฎหมายอาญา หมายถึง กฎหมายที่บัญญัติถึงความผิดและโทษ”<sup>137</sup>

จากการให้ความหมายทางวิชาการสรุปได้ว่ากฎหมายอาญาเป็นกฎหมายที่กำหนดว่าการกระทำใด หรืองดเว้นไม่กระทำการใดบ้างเป็นความผิดทางอาญา และกำหนดโทษที่ผู้กระทำความผิดต้องได้รับเนื่องจากการฝ่าฝืนกฎหมายนั้น ซึ่งเมื่อพิจารณาความหมายของกฎหมายอาญานี้ จะเห็นได้ว่ากฎหมายอาญามี 2 ส่วนได้แก่ส่วนองค์ประกอบ คือ ความผิดทางอาญาและส่วนผลทางกฎหมาย คือ มาตรการบังคับทางอาญา<sup>138</sup>

### 2.3.1.2 วัตถุประสงค์ของกฎหมายอาญา

วัตถุประสงค์ของกฎหมายอาญาได้มีการกล่าวถึงไว้ ดังนี้

รายงานของคณะกรรมการวุล์ฟเฟินเดน (Wolfenden Committee) เกี่ยวกับความผิดฐานรักร่วมเพศ และการค้าประเวณี กล่าวว่า กฎหมายอาญานั้นมีวัตถุประสงค์เพื่อรักษาความถูกต้องชอบธรรมและความสงบเรียบร้อยของสังคม เพื่อปกป้องสาธารณชนจากการกระทำที่เป็นอันตราย และปกป้องคุ้มครองบุคคลจากการทุจริตหรือแสวงหาประโยชน์อันมิชอบด้วยกฎหมาย ซึ่งตามปกติแล้วกฎหมายไม่อาจแทรกแซงการดำเนินชีวิตส่วนตัวของประชาชนได้ เว้นแต่จะเป็นไปเพื่อให้บรรลุวัตถุประสงค์ข้างต้นนี้<sup>139</sup>

ประมวลกฎหมายอาญาต้นแบบของสหรัฐอเมริกา (The US Model Penal Code) กล่าวถึงวัตถุประสงค์ของกฎหมายอาญาว่า มี 5 ประการ ดังนี้<sup>140</sup>

<sup>136</sup> เกียรติขจร วัจนะสวัสดิ์, **คำอธิบายกฎหมายอาญา ภาค 1**, พิมพ์ครั้งที่ 10 (กรุงเทพมหานคร: พลสยามพริ้นติ้ง, 2551), หน้า 1.

<sup>137</sup> ทวีเกียรติ มีนะกนิษฐ, **คำอธิบายกฎหมายอาญาภาคทั่วไป**, พิมพ์ครั้งที่ 9 (กรุงเทพมหานคร: วิญญูชน, 2551), หน้า 14.

<sup>138</sup> คณิต ณ นคร, **กฎหมายอาญาภาคทั่วไป**, หน้า 44.

<sup>139</sup> Michael Jefferson, **Criminal Law**, 8<sup>th</sup> ed. (London: Pearson Education, 2007), p. 9.

<sup>140</sup> David Ormerod, **Criminal Law**, 13<sup>th</sup> ed. (New York: Oxford University Press, 2011), p. 4.

- 1) เพื่อห้ามและป้องกันการกระทำที่ก่อให้เกิดหรืออาจก่อให้เกิดความเสียหายต่อสาธารณประโยชน์ โดยการกระทำนั้นเป็นการกระทำที่ไม่ชอบด้วยกฎหมายและไม่อาจยกโทษให้ได้
- 2) เพื่อให้รัฐควบคุมบุคคลที่มีพฤติกรรมหรือแนวโน้มที่จะประกอบอาชญากรรม
- 3) เพื่อเป็นหลักประกันว่าการกระทำที่ไม่มีความผิดจะไม่ถูกลงโทษทางอาญา
- 4) เพื่อประกาศเตือนให้ทราบว่า การกระทำใดถือเป็นความผิดอาญา
- 5) เพื่อแยกแยะความแตกต่างระหว่างความผิดร้ายแรงกับความผิดเล็กน้อยโดยอยู่บนพื้นฐานของการใช้เหตุผล

นอกจากนี้วัตถุประสงค์ของกฎหมายอาญายังอาจกล่าวได้ว่ามีขึ้นเพื่อคุ้มครองบุคคลและสัตว์จากการกระทำที่มีลักษณะโหดร้าย ซึ่งเป็นการกระทำโดยเจตนา และคุ้มครองบุคคลจากภัยอันตรายบางประการที่เกิดจากการกระทำโดยไม่เจตนา รวมไปถึงคุ้มครองสภาวะจิตใจของบุคคลในสังคมจากการกระทำที่มีลักษณะผิดธรรมชาติเพื่อไม่ให้บุคคลและสาธารณชนได้รับความกระทบกระเทือนทางจิตใจจากการดูหมิ่น ผรุสวาท หมิ่นประมาท หรือการอนาจาร ตลอดจนป้องกันมิให้มีพฤติกรรมที่อาจก่อให้เกิดความไม่สงบสุขต่อส่วนรวม กฎหมายอาญาจึงคำนึงถึงความผาสุกในการอยู่ร่วมกันเป็นสำคัญ และจำเป็นต้องมีการบังคับใช้วิธีต่าง ๆ อันเป็นการลงโทษเพื่อให้บรรลุวัตถุประสงค์<sup>141</sup> จากวัตถุประสงค์ที่กล่าวมาสะท้อนให้เห็นถึงภารกิจที่สำคัญของกฎหมายอาญามี 3 ประการ คือ

- 1) ภารกิจในการคุ้มครองสังคม คือ เมื่อมนุษย์อยู่ร่วมกันเป็นสังคม ความแตกต่างทางทัศนคติ ความเชื่อ ความคิดของปัจเจกชน ย่อมก่อให้เกิดข้อพิพาทหรือความขัดแย้งขึ้นได้ เพื่อแก้ไขข้อขัดแย้งและเพื่อให้บุคคลสามารถอยู่ร่วมกันได้อย่างปกติสุข จึงจำเป็นต้องมีระเบียบ หรือข้อบังคับใช้ควบคุมความประพฤติของบุคคล ซึ่งในสังคมนั้นมีสิ่งที่เรียกว่า “ระเบียบสังคม” เป็นเครื่องมือควบคุมความประพฤติของบุคคลอยู่แล้ว แต่มีข้อจำกัดคือ การปฏิบัติตามระเบียบสังคมนั้นเป็นเรื่องของความสมัครใจและปราศจากสภาพบังคับภายนอก ด้วยเหตุนี้จึงต้องใช้กฎหมายควบคุมความประพฤติของบุคคล โดยเฉพาะอย่างยิ่งกฎหมายอาญาที่มีสภาพบังคับรุนแรง เพื่อให้สังคมมีความสงบสุขและเป็นระเบียบเรียบร้อย ดังนั้นหากมีการใช้กฎหมายอาญาบังคับ หรือควบคุมการกระทำทุกอย่างของบุคคลโดยไม่คำนึงถึงความเหมาะสมแล้ว ก็ย่อมกระทบต่อสิทธิ เสรีภาพของ

<sup>141</sup> อภิรัตน์ เพ็ชรศิริ, **ทฤษฎีอาญา**, พิมพ์ครั้งที่ 3 (กรุงเทพมหานคร: วิญญูชน, 2556), หน้า 49-50.

ประชาชนอย่างร้ายแรงดังนั้น “กฎหมายอาญาจึงไม่เพียงแต่มุ่งจะจำกัดสิทธิและเสรีภาพของบุคคลเท่านั้น แต่กฎหมายอาญาจะต้องเป็นหลักประกันสิทธิและเสรีภาพของบุคคลด้วย”<sup>142</sup>

2) การกึ่งในการปราบปรามและป้องกันการกระทำความผิด เป็นภารกิจสองประการที่มีความเชื่อมโยงกัน กล่าวคือเมื่อมีการกำหนดว่าการกระทำใดเป็นความผิดแล้ว ต้องมีการบังคับใช้กฎหมายอาญาเพื่อนำตัวผู้กระทำความผิดมาลงโทษและแสดงให้เห็นว่าสังคมไม่ยอมรับพฤติกรรมเช่นนั้น จึงเป็นการปราบปรามการกระทำความผิด ในขณะที่เดียวกันก็เป็นการป้องกันมิให้บุคคลทั่วไปประพฤติดนในลักษณะเช่นนั้นด้วย เพราะหากมีการกระทำความผิดเหมือนกันเกิดขึ้นอีกก็ย่อมจะต้องถูกลงโทษดุจเดียวกัน รวมถึงการใช้ “วิธีการเพื่อความปลอดภัย” ซึ่งเป็นมาตรการบังคับทางอาญาซึ่งมีโทษสำหรับผู้กระทำความผิด เพื่อให้บรรลุวัตถุประสงค์ในการป้องกันและปราบปรามการกระทำความผิด

3) การกึ่งในการคุ้มครองคุณธรรมทางกฎหมายและคุ้มครองคุณภาพการกระทำ “คุณธรรมทางกฎหมาย” (Rechtsgut) หมายถึง “ประโยชน์หรือคุณค่าของการอยู่ร่วมกันที่กฎหมายคุ้มครอง” หรือ “ประโยชน์ที่กฎหมายคุ้มครอง”<sup>143</sup> แบ่งออกเป็น “คุณธรรมทางกฎหมายที่เป็นส่วนบุคคล” เช่น ชีวิต ความปลอดภัยทางร่างกาย เสรีภาพ และความเป็นเจ้าของ กับ “คุณธรรมทางกฎหมายที่เป็นส่วนรวม” เช่น ความมั่นคงเชื่อถือและการชำระหนี้ได้ของเงินตรา และความบริสุทธิ์สะอาดแห่งอำนาจรัฐหรือความบริสุทธิ์สะอาดแห่งตำแหน่ง กฎหมายอาญาถูกบัญญัติขึ้นเพื่อคุ้มครองคุณธรรมทางกฎหมายเหล่านี้ มิให้ถูกคุกคามจากอันตรายต่าง ๆ ไม่ว่าผู้บัญญัติกฎหมายจะได้คำนึงถึงเรื่องคุณธรรมทางกฎหมายโดยตรงหรือไม่ก็ตาม

### 2.3.2 หลักเกณฑ์การบัญญัติความผิดทางอาญา

รัฐมีอำนาจรักษาความสงบเรียบร้อยของสังคม (Police Power) ซึ่งเป็นอำนาจหน้าที่ของฝ่ายบริหารที่ต้องดูแลให้ประชาชนของตนมีความปลอดภัยในชีวิต ร่างกาย และทรัพย์สินให้สังคมปราศจากอาชญากรรม และมีความสงบเรียบร้อย ภายใต้เงื่อนไขที่ฝ่ายนิติบัญญัติได้ใช้กฎหมายอาญาเป็นเครื่องมือในการทำหน้าที่กำหนดว่าการกระทำเป็นความผิด และมีบทลงโทษอย่างชัดเจน<sup>144</sup> อย่างไรก็ตามแม้ว่ารัฐมีอำนาจรักษาความสงบเรียบร้อยและมีอำนาจในการบัญญัติกฎหมายอาญาแต่ไม่ได้หมายความว่ารัฐจะบัญญัติกฎหมายอาญาได้อย่างไร้ขอบเขต เนื่องจากกฎหมายอาญามีสภาพ

<sup>142</sup> เรื่องเดียวกัน, หน้า 58.

<sup>143</sup> เรื่องเดียวกัน, หน้า 149.

<sup>144</sup> อมราวดี อังคสุวรรณ, “กฎหมายอาญาและอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคม,” วารสารกฎหมาย 2, 12 (ตุลาคม 2531): 112.

บังคับรุนแรง จำกัดสิทธิ เสรีภาพของบุคคล ฉะนั้นการบัญญัติกฎหมายจึงต้องสอดคล้องกับความต้องการของประชาชน และคำนึงถึงสิทธิ เสรีภาพของประชาชนภายใต้รัฐธรรมนูญด้วยเสมอ<sup>145</sup>

ดังนั้นในการกำหนดว่าการกระทำใดสมควรถูกบัญญัติว่าเป็นการกระทำเป็นความผิดอาญา จำเป็นจะต้องมีหลักเกณฑ์ในการบัญญัติความผิด ทั้งนี้ได้มีนักวิชาการเสนอหลักเกณฑ์การบัญญัติความผิดทางอาญาไว้ ดังนี้

### 2.3.2.1 หลักเกณฑ์ตามนโยบายในการบัญญัติกฎหมายอาญาของรัฐ

นโยบายการบัญญัติกฎหมายอาญาของรัฐขึ้นอยู่กับระบอบการปกครองของรัฐว่ารัฐนั้นเป็นประเทศเสรีนิยม หรือเป็นประเทศสังคมนิยม ทั้งนี้ประเทศที่มีนโยบายเสรีนิยมนั้น จะบัญญัติความผิดอาญาด้วยความระมัดระวังและกำหนดหน้าที่แก่ประชาชนให้น้อยที่สุดเท่าที่จะเป็นไปได้ เนื่องจากการกำหนดความผิดอาญาเป็นการกำหนดหน้าที่ให้แก่ประชาชน นอกจากการกำหนดหน้าที่พอสมควรแล้ว รัฐยังหวังให้ผู้กระทำความผิดแก้ไขปรับปรุงตนเป็นคนดีอีกด้วย จึงกำหนดระวางโทษให้ผ่อนเบา ดังนั้นการบัญญัติกฎหมายอาญาตามนโยบายเสรีนิยมจึงบัญญัติเท่าที่มีความจำเป็นในการรักษาความสงบเรียบร้อยของสังคมเท่านั้น เพื่อมิให้เป็นการสร้างภาระหน้าที่และกระทบกระเทือนต่อสิทธิเสรีภาพของประชาชนเกินสมควร ส่วนประเทศสังคมนิยมที่มีนโยบายแบบเผด็จการจะบัญญัติความผิดอาญาโดยให้ความสำคัญกับการรักษาประโยชน์ของรัฐมากกว่าปัจเจกบุคคล ทำให้ในประเทศสังคมนิยมมีอัตราโทษของความผิดอาญาเกี่ยวกับประโยชน์ของรัฐสูงกว่าอัตราโทษของความผิดเกี่ยวกับประโยชน์ของปัจเจกชนมาก<sup>146</sup>

ดังนั้นประเทศที่ปกครองด้วยระบอบที่แตกต่างกันจึงมีที่มาของแนวคิดในการบัญญัติกฎหมายอาญาและอัตราโทษที่แตกต่างกัน

### 2.3.2.2 หลักเกณฑ์การคุ้มครองนิติสมบัติในวิถีทางสุดท้าย

การพิจารณาว่าการกระทำใดควรเป็นความผิดอาญาหรือไม่นั้นเป็นเรื่องคุณสมบัติในทางเนื้อหา ซึ่ง Prof. Dr. H.C. Mult. Claus Roxin เสนอว่าการกำหนดให้การกระทำเป็นความผิดอาญาและจะนำมาตราการทางอาญามาบังคับใช้ได้ก็ต่อเมื่อไม่สามารถใช้วิธีการอื่น เช่น วิธีการทาง

<sup>145</sup> ปาริชาติ มั่นสกุล, การกำหนดมาตรการทางอาญาเกี่ยวกับการโจมตีค่าเงินบาท (วิทยานิพนธ์ปริญญาโทมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546), หน้า 11.

<sup>146</sup> คณิต ฦ นคร, “ปรัชญาและแนวความคิดของการกำหนดความผิดอันยอมความได้,” วารสารกฎหมายธุรกิจบัณฑิตย์ 1, 4 (มกราคม-มิถุนายน 2547): 1-2.

แพ่ง วิธีการทางปกครอง ซึ่งเป็นวิธีการที่รุนแรงน้อยกว่าได้แล้ว จึงจะนำกฎหมายอาญาที่เป็น มาตรการรุนแรงและกระทบต่อสิทธิ เสรีภาพของประชาชนมาใช้บังคับ<sup>147</sup>

จากแนวคิดดังกล่าวก่อให้เกิดผล 2 ประการคือ 1) “การกระทำที่เป็นแต่เพียงการขัด ต่อศีลธรรมอันดี จะยังไม่เป็นความผิดอาญา” กล่าวคือตามแนวความคิดฝ่ายเสรีนิยม กฎหมายอาญา และมาตรการทางอาญามีขึ้นเพื่อคุ้มครองนิติสมบัติ การกระทำใดที่เกิดขึ้นด้วยความยินยอมของ บุคคลทั้งสองฝ่ายที่บรรลุนิติภาวะแล้ว และไม่สร้างความเดือดร้อนให้แก่ผู้อื่น แม้การกระทำนั้นจะขัด ต่อศีลธรรมอันดี แต่หากมิได้ทำให้นิติสมบัติหรือสิ่งที่กฎหมายมุ่งคุ้มครองนั้นเสียหาย ก็ย่อมไม่เป็น ความผิดทางอาญา แนวความคิดนี้นำไปสู่การยกเลิกความผิดฐานรักร่วมเพศ ความผิดฐานมี เพศสัมพันธ์กับสัตว์ และการเผยแพร่ภาพลามกอนาจาร 2) “การกระทำที่เป็นเพียงการละเมิดต่อ ระเบียบไม่เป็นความผิดอาญา” กฎหมายอาญามีขึ้นเพื่อคุ้มครองนิติสมบัติและสิทธิของบุคคลที่มีอยู่ ก่อนการเกิดขึ้นของรัฐ ดังนั้นหากกฎหมายต่าง ๆ ที่รัฐกำหนดขึ้นเพื่อให้การบริหารงานเป็นไปด้วย ความสะดวกเรียบร้อย แต่มิได้กำหนดไว้เพื่อคุ้มครองนิติสมบัติ เช่น การกำหนดจุดจอดรถ หรือการ กำหนดให้แจ้งย้ายเมื่อมีการย้ายที่อยู่ เป็นสิ่งที่เกิดขึ้นโดยรัฐไม่ได้มีอยู่ก่อนการเกิดขึ้นของรัฐ จึงไม่ใช่ นิติสมบัติ ดังนั้นการฝ่าฝืนละเมิดกฎระเบียบดังกล่าวจึงไม่ควรถูกลงโทษทางอาญา แนวความคิดนี้ นำไปสู่การยกเลิกความผิดละเมิดโทษในประมวลกฎหมายอาญาเยอรมัน และบัญญัติเป็นกฎหมาย เกี่ยวกับการละเมิดต่อระเบียบแทน

นอกจากนี้การกำหนดว่าการกระทำใดควรบัญญัติเป็นกฎหมายอาญา จะต้องเป็นสิ่งที่ สามารถดำเนินได้ตัวผู้กระทำผิดได้แล้ว (Culpable Wrongdoing) ยังต้องมีความร้ายแรงเพียงพอที่จะเป็นความผิดอาญาด้วย เนื่องจากกฎหมายอาญามีการลงโทษที่มีลักษณะเป็นตราบาปติดตัว อาชญากร<sup>148</sup> ดังนั้นหากไม่เป็นการกระทำที่ไม่สมควรถูกดำเนินและไม่ได้มีความร้ายแรงแล้ว ก็ไม่ สมควรจะนำการกระทำนั้นมาบัญญัติเป็นความผิดในกฎหมายอาญา

### 2.3.2.3 หลักเกณฑ์การบัญญัติความผิดอาญาของ Nigel Walker

ขอบเขตการบัญญัติกฎหมายอาญาตามแนวความคิดของ Nigel Walker อธิบายได้ ดังต่อไปนี้<sup>149</sup>

<sup>147</sup> สุรสิทธิ์ แสงวิโรจน์พัฒน์, “การกำหนดความผิดอาญาตามกฎหมายเยอรมัน,” **ข่าวเนติ บัณฑิตยสภา** 16, 192 (กรกฎาคม 2548): 11-12.

<sup>148</sup> *เรื่องเดียวกัน*, หน้า 11-12.

<sup>149</sup> Nigel Walker, **Punishment, Danger and Stigma: The Morality of Criminal Justice** (New York: Basic Books, 1980), pp. 4-23, อ้างถึงใน ฌักทรี สร้อซท์, **ความเหมาะสม**

1) รัฐไม่ควรบัญญัติข้อห้ามตามกฎหมายอาญาไว้เพียงเพื่อเป็นหลักประกันว่าเมื่อเกิดการฝ่าฝืนกฎหมายจะถูกแก้แค้นตอบแทนด้วยการลงโทษแต่เพียงอย่างเดียว และข้อห้ามนั้นเป็นข้อห้ามที่ปราศจากอรรถประโยชน์ที่เป็นแก่นสาร<sup>150</sup>

หลักการข้อนี้มีแนวคิดมาจากหลักอรรถประโยชน์นิยม (Utilitarianism) นำโดยซีซาร์ เบคคาเรีย (Cesare Beccaria) มุ่งพิจารณาว่าการลงโทษว่าทำอย่างไรจึงจะได้ประโยชน์จากการลงโทษนั้น เบคคาเรียเสนอว่า “การป้องกันอาชญากรรมย่อมดีกว่าการปราบปรามอาชญากรรม ซึ่งเป็นเป้าหมายสูงสุดแห่งกฎหมายนิติบัญญัติที่ดี” ซึ่งข้อเสนอของเบคคาเรียได้รับการยอมรับและยึดถือตามจากนักอรรถประโยชน์ในยุคหลัง

2) รัฐไม่ควรใช้กฎหมายอาญาลงโทษความประพฤติที่ไม่ก่อให้เกิดอันตรายหรือปราศจากพิษภัย เป็นหลักที่เจอเรมี เบนธัม (Jeremy Bentham) ได้เสนอเพิ่มเติมจากหลักการของเบคคาเรียข้างต้น กล่าวคือ หากการกระทำใดไม่มีความชั่วร้ายก็ไม่มีควมจำเป็นต้องใช้กฎหมายอาญาลงโทษการกระทำนั้น เช่น ไม่ควรลงโทษบุคคลที่มีมารยาทเลว หรือสิ่งที่บุคคลเห็นว่าเป็นความเลว<sup>151</sup> อย่างไรก็ตามหลักการของเบนธัมนี้ยังมีข้อบกพร่องและอาจโต้แย้งได้ว่าการกระทำใดเรียกว่าชั่วร้ายหรือการกระทำนั้นเป็นอันตรายมีพิษภัยแล้วหรือไม่

3) รัฐไม่ควรใช้กฎหมายอาญาเพื่อให้บรรลุวัตถุประสงค์ที่สามารถใช้วิธีอื่นที่บรรลุผลได้อย่างมีประสิทธิภาพเช่นเดียวกัน โดยเฉพาะอย่างยิ่งวิธีการอื่นนั้นก่อให้เกิดความทุกข์ทรมานน้อยกว่า รัฐควรใช้มาตรการนั้น เช่น การใช้โทษปรับแทนการกักขัง หรือการตัดเดือนแทนการลงโทษ<sup>152</sup> แต่หลักการนี้ยังมีปัญหาถกเถียงอยู่ว่าการลงโทษจะมีผลเป็นการยับยั้งการกระทำความผิดได้หรือไม่

4) รัฐไม่ควรใช้กฎหมายอาญาที่จะก่อให้เกิดผลร้ายจากการลงโทษมากกว่าผลร้ายที่เกิดจากการกระทำความผิด หลักการนี้เป็นการชั่งน้ำหนักระหว่างประโยชน์ที่จะได้รับและผลเสียที่จะเกิดขึ้นจากการลงโทษ โดยเห็นว่าหากมีผลเสียมากกว่าประโยชน์ก็ไม่ควรลงโทษทางอาญากับบุคคล แต่ข้อเสนอนี้ก็มีข้อโต้แย้งอีกเช่นเดียวกันคือ ไม่อาจวัดได้ว่าผลร้ายที่เกิดจากการกระทำความผิดกับผลร้ายที่เกิดจากการลงโทษนั้นสิ่งใดจะมากกว่ากัน เนื่องจากยังมีความ

---

**ในการกำหนดความผิดและโทษทางอาญา: ศึกษากรณีกฎหมายการแข่งขันทางการค้า** (สารนิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 16-17.

<sup>150</sup> อภิรัตน์ เพ็ชรศิริ, *เรื่องเดิม*, หน้า 52.

<sup>151</sup> ประธาน วัฒนวานิชย์, “การปฏิรูประบบการลงโทษ แนวทางสหวิทยาการโดยเน้นทางด้านอาชญาวิทยา,” *บทบัญญัติ* 54, 4 (ธันวาคม 2541): 12.

<sup>152</sup> อภิรัตน์ เพ็ชรศิริ, *เรื่องเดิม*, หน้า 53.

แตกต่างด้านบุคลิกภาพของบุคคล อีกทั้งวิธีการลงโทษที่ยังคงมีข้อโต้เถียงว่าระหว่างการประหารชีวิตกับจำคุกตลอดชีวิตนั้นวิธีการใดจะก่อให้เกิดประโยชน์แก่สังคมมากกว่ากัน<sup>153</sup> ด้วยเหตุนี้วอลท์เกอร์จึงได้ปรับปรุงหลักการดังกล่าวเป็น “กฎหมายอาญาไม่ควรบัญญัติห้ามการกระทำ ซึ่งจะก่อให้เกิดผลพลอยได้ (By Product) อันเป็นผลร้ายมากกว่าการกระทำที่รัฐไม่ส่งเสริม” ตัวอย่างของหลักการนี้คือ การที่กฎหมายห้ามมิให้ขายและเสพกัญชาย่อมทำให้เกิดตลาดมืด หรือขบวนการค้ายาเสพติด ผู้ที่ต้องการเสพกัญชาจำต้องซื้อกัญชาจากพ่อค้าในตลาดมืดและเกิดการคบค้าสมาคมกับบรรดาอาชญากร ทำให้ผู้นั้นอาจติดยาเสพติดชนิดอื่นที่รุนแรงกว่ากัญชา และมีแนวโน้มในการประกอบอาชญากรรมร้ายแรงเพิ่มขึ้นด้วย กรณีนี้จึงกล่าวได้ว่าผลร้ายหรือผลพลอยได้ที่เกิดจากการห้ามขายและเสพกัญชาร้ายแรงมากกว่าผลร้ายของการเสพกัญชา<sup>154</sup>

5) รัฐไม่ควรใช้กฎหมายอาญาโดยมีวัตถุประสงค์ในการบังคับให้บุคคลกระทำเพื่อประโยชน์สูงสุดของตนเองเท่านั้น หลักการนี้พัฒนาขึ้นโดยจอห์น สจิวต มิลล์ (John Stuart Mill) ซึ่งยึดหลักอิสรภาพและเสรีภาพของบุคคลเป็นสำคัญ หลักการดังกล่าวได้ปรากฏอยู่ในบทความว่าด้วยเสรีภาพความว่า “...ในสังคมที่เจริญแล้วนั้น การใช้กำลังอำนาจเหนือสมาชิกในสังคมของตน จะถือเป็นการถูกต้องก็ต่อเมื่อมีจุดประสงค์ที่จะป้องกันภัยอันตรายอันจะเกิดแต่บุคคลอื่นในสังคมนั้น ภัยอันตรายที่จะเกิดแก่ตนเองโดยมิได้มีบุคคลอื่นเป็นผู้ก่อให้เกิดไม่ว่าจะเป็นทางกายภาพหรือทางจริยธรรมแล้ว ย่อมไม่อาจถือเป็นข้ออ้างที่เพียงพอสำหรับการจำกัดเสรีภาพการกระทำของมนุษย์”<sup>155</sup> ดังนั้นการที่รัฐจะเข้าไปควบคุมการกระทำของบุคคลได้นั้น จะต้องปรากฏว่าการกระทำดังกล่าวมีการใช้ความรุนแรงและก่อให้เกิดความเดือดร้อนแก่สังคม หรือเป็นอันตรายต่อผู้อื่น อย่างไรก็ตามหลักการนี้มีข้อยกเว้นอยู่บางประการ เช่น กรณีบิดามารดาปกครองบุตร หรือการบังคับให้เด็กเข้ารับการศึกษาขั้นพื้นฐานตามเกณฑ์อายุ<sup>156</sup>

6) รัฐไม่ควรใช้กฎหมายอาญาห้ามการกระทำซึ่งไม่ได้รับการสนับสนุนจากสาธารณชน หลักการนี้เสนอโดยฟิสเจมส์ สตีเฟน ซึ่งเป็นผู้พิพากษาและมีความเห็นว่าการกำหนดขอบเขตของกฎหมายอาญานั้นควรจะให้หนักปฏิบัติที่เป็นผู้บังคับใช้กฎหมายเป็นฝ่ายกำหนด ไม่ใช่ให้ฝ่ายนักวิชาการหรือนักปรัชญามาเป็นผู้กำหนด เพราะการใช้กฎหมายในทางปฏิบัตินี้มีข้อจำกัด

<sup>153</sup> ประธาน วัฒนาวณิชย์, *เรื่องเดิม*, หน้า 12-13.

<sup>154</sup> อภิรัตน์ เพ็ชรศิริ, *เรื่องเดิม*, หน้า 54.

<sup>155</sup> *เรื่องเดียวกัน*, หน้า 56.

<sup>156</sup> ประธาน วัฒนาวณิชย์, *เรื่องเดิม*, หน้า 14.

ซึ่งนักวิชาการอาจมองข้ามไป<sup>157</sup> แต่หลักการดังกล่าวยังมีข้อโต้แย้งในประเด็นการสำรวจความเห็นหรือประชามติของบุคคลในสังคมนั้นกระทำได้อย่างไร

7) รัฐไม่ควรบัญญัติความผิดที่บังคับใช้ไม่ได้ไว้ในกฎหมายอาญา เรื่องของความผิดที่บังคับใช้ไม่ได้ หมายถึงการไม่สมควรบัญญัติการกระทำบางอย่างให้เป็นความผิด หากว่ามีผู้ฝ่าฝืนบทบัญญัติแล้วถูกดำเนินคดีและถูกลงโทษเป็นจำนวนเพียงเล็กน้อยเท่านั้น เหตุผลของหลักการนี้คือ ความผิดนั้นใช้บังคับไม่ได้ เนื่องจากจับกุมผู้กระทำความผิดได้น้อยจะทำให้ประชาชนไม่สนใจและจะส่งผลให้ผู้คนในสังคมไม่เคารพกฎหมายและกฎหมายจะขาดความศักดิ์สิทธิ์ไปในที่สุด หลักการนี้มีปัญหาในเรื่องการวัดจำนวน คือจำนวนเท่าใดจึงจะถือว่าน้อย เมื่อคิดเป็นอัตราส่วนหรือร้อยละ

8) รัฐไม่ควรบัญญัติกฎหมายอาญาที่รวมข้อห้ามบางประการไว้ ซึ่งเมื่อมีการละเมิดข้อห้ามแล้ว ไม่สามารถพิสูจน์ได้ว่าการกระทำความผิดเกิดขึ้นจริง บทบัญญัติของกฎหมายอาญาช่วยวางรากฐานความประพฤติอันดีของบุคคลในสังคมได้ แม้ในทางปฏิบัติบทกฎหมายบางข้อจะไม่มี การบังคับใช้หรือไม่มีผู้ใดถูกลงโทษจากบทบัญญัตินั้นก็ตาม อีกทั้งการที่บทกฎหมายบางมาตราไม่มีการบังคับใช้ก็ไม่ได้ทำให้บทบัญญัติอื่นในประมวลกฎหมายเสื่อมความศักดิ์สิทธิ์ไปแต่อย่างใด ประชาชนยังคงให้ความเคารพต่อกฎหมายอื่นอยู่ ดังนั้นหลักการข้อนี้จึงไม่ควรใช้เป็นหลักเกณฑ์การบัญญัติกฎหมายอาญา หรือเป็นข้ออ้างในการไม่กำหนดความผิดอาญาบางประการ แต่อาจใช้เป็นหลักหรือข้อควรระวังในการฟ้องคดีเกี่ยวกับกฎหมายที่ไม่สามารถบังคับใช้หรือใช้บังคับไม่ได้<sup>158</sup>

#### 2.3.2.4 หลักเกณฑ์การบัญญัติความผิดอาญาของ Herbert L. Packer

Herbert L. Packer เป็นนักทฤษฎีกฎหมายที่เห็นว่ามาตรการทางอาญาควรใช้ลงโทษผู้กระทำความผิดอย่างชั่วร้ายและเพื่อป้องกันอาชญากรรม เนื่องจากกฎหมายอาญามีข้อจำกัดในการบังคับใช้ทั้งในด้านต้นทุนที่มีความสิ้นเปลืองสูงและในด้านโทษที่มีความรุนแรง จึงควรใช้มาตรการทางอาญากับความผิดที่ร้ายแรงเท่านั้น<sup>159</sup>

นอกจากนี้ Packer ยังเห็นว่าในการปกครองแบบเสรีนิยม รัฐสามารถควบคุมหรือมีอำนาจบังคับประชาชนเพียงเท่าที่เขากระทำเท่านั้น ไม่ใช่บังคับให้เป็นไปตามที่รัฐต้องการ และเมื่อมี

<sup>157</sup> เรื่องเดียวกัน, หน้า 59.

<sup>158</sup> เรื่องเดียวกัน, หน้า 61-62.

<sup>159</sup> สกล นิสารัตน์, *กฎหมายอาญาและการลงโทษที่เหมาะสม: แนวความคิดทางด้านปรัชญาและความยุติธรรมทางสังคม* (วิทยานิพนธ์ปริญญาโทมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2545), หน้า 34.

การกระทำแล้วก็ไม่จำเป็นต้องรับโทษเสมอไป เพราะการลงโทษนั้นต้องคำนึงถึงสภาพจิตใจของผู้กระทำด้วย กล่าวคือรัฐไม่พึงลงโทษบุคคลผู้มีจิตบกพร่องหรือไม่รู้ผิดชอบ เนื่องจากการลงโทษบุคคลเหล่านี้ไม่ใช่การลงโทษในสิ่งที่เขาได้กระทำหรือเชื่อว่าได้กระทำ ซึ่งการลงโทษพิจารณาจากสภาพจิตใจของผู้กระทำนั้นเป็นการป้องกันมิให้ใช้กฎหมายอาญาในเชิงอรรถประโยชน์อย่างไม่มีขีดจำกัด นอกจากนี้รัฐไม่ควรลงโทษบุคคลด้วยเหตุผลทางศีลธรรมเท่านั้น เพราะเป็นเรื่องที่มีความคลุมเครือ ยากลำบากในการกำหนดว่าสิ่งใดผิดศีลธรรม อีกทั้งไม่สามารถใช้กฎหมายอาญาลงโทษการกระทำทุกอย่างที่ผิดศีลธรรมได้ และไม่อาจพิสูจน์ได้ว่ากฎหมายอาญาจะทำให้ผู้คนมีศีลธรรมที่ดีขึ้นหรือไม่ ซึ่งหากรัฐมุ่งใช้กฎหมายอาญากับพฤติกรรมที่เป็นเพียงเรื่องศีลธรรม แต่ไม่ได้คำนึงถึงความเสียหายของส่วนรวม ย่อมก่อให้เกิดผลกระทบตามมาคือ ฝ่ายผู้บังคับใช้กฎหมายประสบความลำบากในการควบคุมพฤติกรรมและรู้สึกไม่ต้องการบังคับใช้กฎหมาย ประกอบกับเมื่อประชาชนพบว่ากฎหมายไม่อาจบังคับได้จริงในทางปฏิบัติและรัฐไม่อาจแสดงให้เห็นถึงผลร้ายอื่นนอกเหนือจากผลทางศีลธรรมได้ ย่อมส่งผลให้ประชาชนขาดความเคารพในกฎหมายมากขึ้น<sup>160</sup>

จากแนวคิดดังกล่าว Herbert L. Packer จึงได้เสนอหลักเกณฑ์การบัญญัติความผิดอาญาไว้ ดังต่อไปนี้<sup>161</sup>

- 1) การกระทำนั้นเป็นสิ่งที่เห็นได้ชัดเจนในหมู่ประชาชนว่าเป็นการกระทำที่กระทบกระเทือนต่อสังคมมีลักษณะที่น่าหวาดหวั่นและประชาชนส่วนมากมิได้ให้อภัยการกระทำนั้น
- 2) การกระทำที่เป็นความผิดอาญาจะต้องไม่ขัดแย้งกับวัตถุประสงค์ของการลงโทษ
- 3) การกระทำนั้นถูกกำหนดเป็นความผิดอาญาจะไม่มีผลเป็นการลดการกระทำที่สังคมเห็นว่าถูกต้องให้น้อยลงไป
- 4) เมื่อเป็นความผิดอาญาแล้วจะมีการบังคับใช้กฎหมายอย่างเสมอภาคและเท่าเทียมกัน ไม่มีการเลือกปฏิบัติ
- 5) การใช้กระบวนการยุติธรรมทางอาญากับการกระทำดังกล่าวจะไม่มีผลทำให้เกิดการใช้กระบวนการนั้นอย่างเกินขีดความสามารถทั้งทางด้านคุณภาพและปริมาณ
- 6) กฎหมายอาญาในการจัดการกับปัญหาก็ต่อเมื่อไม่มีมาตรการควบคุมอื่นที่สมเหตุผลแล้ว

<sup>160</sup> เรื่องเดียวกัน, หน้า 34-36.

<sup>161</sup> Herbert L. Packer, **The Limits of the Criminal Sanction** (California: Stanford University Press, 1968), p. 296.

### 2.3.2.5 หลักเกณฑ์การบัญญัติความผิดอาญาของ Lon Fuller

Lon Fuller เป็นนักคิดที่มีความเห็นตรงกันข้ามกับ H.L.A Hart และฝ่ายสำนักกฎหมายบ้านเมือง คือในขณะที่สำนักกฎหมายบ้านเมืองเห็นว่ากฎหมายกับศีลธรรมแยกต่างหากจากกันอย่างชัดเจน แต่ Fuller เห็นว่ากฎหมายกับศีลธรรมนั้นมีความสัมพันธ์กันผ่านทางเหตุผลของการบังคับใช้กฎหมาย<sup>162</sup> โดย Fuller ได้เสนอหลักเกณฑ์การบัญญัติความผิดอาญาไว้ดังนี้<sup>163</sup>

- 1) ต้องมีการวางกฎเกณฑ์ในการบังคับอย่างแจ่มชัดว่ากฎหมายประสงคจะควบคุมการกระทำใดบ้าง
- 2) เกณฑ์ดังกล่าวต้องใช้สำหรับเหตุการณ์ในอนาคต ไม่มีผลย้อนหลังไปใช้กับเหตุการณ์ในอดีตที่เกิดขึ้นแล้ว การใช้กฎหมายย้อนหลังเท่ากับเป็นการลงโทษการกระทำที่ไม่เป็นความผิดในอดีต
- 3) กฎเกณฑ์นั้นจะต้องมีการประกาศเผยแพร่ให้ทราบโดยทั่วกัน เพื่อให้ประชาชนได้ทราบว่า การกระทำใดต้องห้ามหรือถูกควบคุม และการกระทำใดสามารถกระทำได้
- 4) กฎเกณฑ์นั้นต้องมีลักษณะที่รัดกุม ชัดแจ้ง เหมาะสม
- 5) เกณฑ์การควบคุมต้องไม่ขัดแย้งกับกฎเกณฑ์อื่น ๆ เพื่อมิให้ประชาชนเกิดความสับสนว่าจะยึดถือปฏิบัติตามหลักเกณฑ์ใด
- 6) การปฏิบัติตามกฎเกณฑ์นั้นสามารถปฏิบัติได้จริง เนื่องจากกฎที่ไม่สามารถปฏิบัติตามได้ย่อมไม่เกิดประโยชน์ใด ๆ จึงไม่ควรบัญญัติกฎเกณฑ์เช่นนั้นขึ้นมา
- 7) กฎเกณฑ์ต้องมีความแน่นอน ไม่เปลี่ยนแปลงบ่อย หากต้องการให้ผู้คนปฏิบัติตามกฎเกณฑ์เพื่อบรรลุวัตถุประสงค์ในการควบคุมการกระทำของบุคคลกฎเกณฑ์นั้นก็ต้องมีความแน่นอน
- 8) กฎเกณฑ์ที่ประกาศเผยแพร่ให้สาธารณชนรับทราบต้องสอดคล้องกับแนวทางการปฏิบัติของเจ้าหน้าที่ผู้รับผิดชอบการบังคับใช้กฎหมาย เพื่อให้ประชาชนคาดเห็นได้ว่าตนจะได้รับผลกระทบเช่นใดหากฝ่าฝืนกฎเกณฑ์นั้น

### 2.3.2.6 หลักเกณฑ์การบัญญัติความผิดอาญาของ Douglas Husak

Douglas Husak ได้เสนอหลักเกณฑ์การบัญญัติความผิดอาญาเอาไว้หลายประการดังต่อไปนี้

<sup>162</sup> Austin M. Chinhengo, *Essential Jurisprudence* (London: Cavendish Publishing Limited, 1995), p. 68.

<sup>163</sup> *Ibid.*, pp. 69-70.

- 1) ไม่ควรบัญญัติกฎหมายอาญาขึ้นเพื่อห้ามการกระทำที่ไม่มีอันตรายหรือไม่มีความชั่วร้าย<sup>164</sup>
- 2) กฎหมายอาญาควรใช้ลงโทษการประพฤตินิยมชอบหรือการกระทำที่ผิดกฎหมาย<sup>165</sup>
- 3) การลงโทษทางอาญาจะมีความชอบธรรมต่อเมื่อเป็นการลงโทษที่เหมาะสม<sup>166</sup>
- 4) ผู้เสนอให้มีการบัญญัติความผิดอาญามีภาระต้องพิสูจน์ถึงความจำเป็นที่จะต้องใช้กฎหมายอาญาลงโทษการกระทำนั้น ๆ<sup>167</sup>
- 5) การบัญญัติกฎหมายอาญาต้องเป็นไปเพื่อปกป้องผลประโยชน์ที่สำคัญของรัฐ<sup>168</sup>
- 6) การบัญญัติความผิดอาญาจะต้องไม่เกินกว่าที่จำเป็นในการบรรลุวัตถุประสงค์ของกฎหมายอาญา<sup>169</sup>

จากที่ได้กล่าวถึงหลักเกณฑ์การบัญญัติความผิดอาญาที่นักกฎหมายและนักวิชาการได้เสนอนั้นเป็นสาระสำคัญที่ควรคำนึงเมื่อมีการบัญญัติให้การกระทำใดเป็นความผิดอาญานอกจากนั้นแล้วยังควรคำนึงถึงมิติทางสังคมซึ่งเป็นปัจจัยสำคัญในการกำหนดความเหมาะสมของการบัญญัติความผิดอาญาคือ ควรเป็นการกระทำที่มีความรุนแรงหรือความก้าวร้าว ความเสียหายหรือผลกระทบจากการกระทำนั้นเป็นอันตรายต่อสังคม ซึ่งจะเห็นได้ปฏิกิริยาตอบสนองหรือความหวาดกลัวของคนส่วนใหญ่ในสังคม<sup>170</sup> :ซึ่งนำมาเป็นข้อสรุปหลักเกณฑ์บัญญัติความผิดทางอาญาได้ 4 ประการ ดังนี้

- 1) การกระทำนั้นต้องเป็นการกระทำที่น่าตำหนิ และขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนการกระทำใดบ้างเป็นการกระทำที่น่าตำหนิ โดยพิจารณาว่าเป็นการกระทำที่ฝ่าฝืนคุณธรรมทางกฎหมายที่สำคัญหรือไม่ ประกอบกับในขณะที่กระทำการนั้น

<sup>164</sup> Douglas Husak, *Overcriminalization: The Limits of the Criminal Law* (Oxford: Oxford University Press, 2008), p. 66.

<sup>165</sup> *Ibid.*, p. 73.

<sup>166</sup> *Ibid.*, p. 82.

<sup>167</sup> *Ibid.*, p. 100.

<sup>168</sup> *Ibid.*, p. 121.

<sup>169</sup> *Ibid.*, p. 154.

<sup>170</sup> สกล นิสารัตน์, *เรื่องเดิม*, หน้า 50.

ผู้กระทำได้รู้ถึงสิ่งที่กฎหมายมุ่งคุ้มครองและยังมีเจตจำนงประสงค์จะทำสิ่งนั้นหรือไม่ ส่วนการกระทำที่ขัดต่อความสงบเรียบร้อยนั้น พิจารณาว่าเป็นการกระทำที่ไม่เกี่ยวกับเอกชนคนใดคนหนึ่งโดยเฉพาะ แต่เกี่ยวข้องและกระทบต่อส่วนรวม หรือเป็นกรณีที่เป็นเรื่องของเอกชนแต่อาจส่งผลกระทบต่อบุคคลอื่นได้ด้วย<sup>171</sup>

2) การกระทำนั้นต้องเป็นการกระทำที่ก่อให้เกิดอันตรายต่อประโยชน์หรือความสงบสุขของบุคคล หรือก่อให้เกิดอันตรายแก่ประโยชน์ของสังคมหรือประโยชน์ของรัฐ

3) การกำหนดให้การกระทำนั้นเป็นความผิดอาญาจะไม่ก่อให้เกิดผลร้ายกับสังคมมากกว่าการกระทำที่เป็นความผิด

4) การกำหนดให้การกระทำใดเป็นความผิดอาญาจะต้องเป็นทางเลือกสุดท้าย เมื่อไม่มีทางอื่นที่จะแก้ไขการกระทำดังกล่าวได้แล้ว<sup>172</sup>

## 2.4 รูปแบบการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล

### 2.4.1 การเจาะข้อมูล/การโจรกรรม (Hack/Theft)

คริปโทเคอร์เรนซีหรือสกุลเงินดิจิทัลเป็นระบบที่ออกแบบมาโดยมีบล็อกเชนเป็นฐานในการบันทึกและจัดเก็บข้อมูลแบบกระจาย (Distributed) ทุกคนที่อยู่ในเครือข่ายสามารถเข้าถึงบล็อกเชนเพื่อตรวจสอบดูข้อมูลทางธุรกรรมได้โดยการเข้ารหัส (Cryptographic) เมื่อข้อมูลถูกบันทึกแล้วจะไม่สามารถถูกลบออกได้ (Immutable) และข้อมูลที่ถูกบันทึกไว้ในแต่ละบล็อกจะได้รับการตรวจสอบความถูกต้อง (Proof of Work) ว่าข้อมูลสามารถเชื่อมโยงกับบล็อกทุกบล็อกเข้าด้วยกันได้ ดังนั้นระบบดังกล่าวจึงเป็นที่ยอมรับว่ามีความปลอดภัยสูง ยากต่อการขโมยหรือถูกแฮ็กได้ เนื่องจากการโอนสกุลเงินดิจิทัลเจ้าของบัญชีผู้โอนออกไปยังบัญชีอื่นจำเป็นต้องใส่รหัสกุญแจสาธารณะ (Public Key) และรหัสรหัสกุญแจส่วนตัว (Private Key) ของตน เพื่อยืนยันตัวตนเจ้าของบัญชีก่อนทำธุรกรรมการโอนสกุลเงินออกไป ทั้งนี้รหัสกุญแจส่วนตัวนั้นจะเป็นความลับที่รู้เฉพาะเจ้าของบัญชีเท่านั้น จึงยากที่คนทั่วไปและอาชญากรจะเข้าถึงหรือแฮ็กรหัสเพื่อนำสกุลเงินดิจิทัลออกมาได้

ทั้งนี้รูปแบบการกระทำความผิดนี้เป็นลักษณะเฉพาะที่เกี่ยวกับสกุลเงินดิจิทัล เนื่องจากหากเป็นการเจาะระบบเพื่อเข้าถึงข้อมูลคอมพิวเตอร์ทั่วไปนั้นอาจเป็นเพียงการสำเนาข้อมูลออกมาอีกชุด

<sup>171</sup> เรื่องเดียวกัน, หน้า 25.

<sup>172</sup> ฌักพร สรอัทม์, ความเหมาะสมในการกำหนดความผิดและโทษทางอาญา: ศึกษา

กรณีกฎหมายการแข่งขันทางการค้า (สารนิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์

มหาวิทยาลัยธรรมศาสตร์, 2548), หน้า 20-21.

(ต้นฉบับจึงยังอยู่ที่เจ้าของเดิม) ในขณะที่หากเป็นการกระทำต่อสกุลเงินดิจิทัลนั้น ไม่สามารถทำสำเนาออกมาได้เหมือนเช่นข้อมูลทั่วไป แต่ต้องเป็นการนำออกมาจากบัญชีต้นทางหรือได้มีการเอาไปซึ่งสกุลเงินดิจิทัลด้วย (ไม่มีสกุลเงินดิจิทัลอยู่ที่บัญชีต้นทาง) การกระทำดังกล่าวนี้จึงเป็นรูปแบบของการเจาะระบบหรือเจาะข้อมูลเพื่อขโมยสกุลเงินดิจิทัล

อย่างไรก็ตามหากเป็นการเจาะหรือแฮ็กข้อมูลเพื่อขโมยสกุลเงินดิจิทัลจากระบบบล็อกเชน เป็นเรื่องที่ทำได้ยากกว่าการเจาะหรือแฮ็กข้อมูลจากอุปกรณ์เชื่อมต่อ เช่น คอมพิวเตอร์ สมาร์ทโฟน เป็นต้น สกุลเงินดิจิทัล (Cryptocurrency Wallet) เนื่องจากอุปกรณ์เชื่อมต่อเหล่านี้จะมีระบบป้องกันที่น้อยกว่าระบบการเข้ารหัสกุญแจส่วนตัวจากบล็อกเชน การแฮ็กอุปกรณ์เหล่านี้จึงทำได้ง่ายกว่าแฮ็กระบบบล็อกเชน อาชญากรจึงมักเลือกใช้วิธีการเจาะระบบหรือเจาะข้อมูลคอมพิวเตอร์เพื่อเข้าไปยัง Wallet ที่เจ้าของบัญชีได้เชื่อมต่อกับระบบออนไลน์ไว้อยู่แล้ว (Hot Wallet) จากนั้น อาชญากรเพียงกรอกรหัสบัญชีปลายทางหรือที่เรียกว่ากุญแจสาธารณะที่ต้องการโอนออกไปเท่านั้น สกุลเงินดิจิทัลก็ถูกถ่ายโอนแล้ว

รูปแบบที่พบเห็นบ่อยและสร้างมูลค่าความเสียหายมหาศาลมักจะเป็นการแฮ็กเว็บไซต์ผู้ให้บริการรับซื้อแลกเปลี่ยนคริปโทเคอร์เรนซีซึ่งเป็นรูปแบบที่เกิดขึ้นในหลายประเทศทั่วโลก ดังจะเห็นได้จาก ตัวอย่างศูนย์บริการซื้อขายสกุลเงินดิจิทัลที่ประสบปัญหาการเจาะข้อมูล ได้แก่

1) COINCHECK ผู้ให้บริการซื้อขายสกุลเงินดิจิทัลในประเทศญี่ปุ่น โดย CipherTrace ระบุว่าในปี 2018 เว็บไซต์ Coincheck ได้รับผลกระทบจากแฮ็กเกอร์ขโมยเงิน NEM กว่า 500 ล้านเหรียญสหรัฐฯ คิดเป็นประมาณ 530 ล้านดอลลาร์

2) MT. GOX ในปี 2014 ผู้ให้บริการซื้อขายสกุลเงินดิจิทัลในประเทศญี่ปุ่นถูกโจรกรรมสกุลเงินดิจิทัลจากเว็บไซต์นี้ คิดเป็นเงินกว่า 460 ล้านดอลลาร์และนับเป็นจุดเริ่มต้นที่ทำให้ประเทศญี่ปุ่นและทั่วโลกได้มีการกำหนดระเบียบเกี่ยวกับการซื้อขายสกุลเงินดิจิทัลที่เข้มงวดมากขึ้น รวมถึงการสร้างระบบรักษาความปลอดภัยเพื่อป้องกันการโจรกรรมที่จะเกิดขึ้นในอนาคต

3) BITGRAIL ในปี 2018 ผู้ให้บริการซื้อขายสกุลเงินดิจิทัลในประเทศอิตาลี สูญเสียโทเค็นนาโน 17 ล้าน มูลค่าประมาณ 170 ล้านดอลลาร์จากการแฮ็กเว็บไซต์ ซึ่งปัจจุบันศาลก็สั่งให้เจ้าของเว็บไซต์คืนเงินให้กับลูกค้าแล้ว<sup>173</sup>

อย่างไรก็ตามผู้ให้บริการดังกล่าวล้วนแต่มีชื่อเสียงระดับโลกและได้มีลงทะเบียนการให้บริการอย่างถูกต้องตามกฎหมายของแต่ละประเทศแล้วก็ตาม แต่ความเสียหายที่เกิดขึ้นอาจส่งผลกระทบต่อ

<sup>173</sup> Admin Intrend, **ย้อนรอยประวัติศาสตร์ 5 อันดับการแฮ็คคริปโตที่ปริมาณมากที่สุดในโลก**, ค้นวันที่ 25 พฤศจิกายน 2565 จาก <https://cryptointrend.com/top-5-biggest-crypto-exchange-heists-in-history/>

บุคคลทั่วโลกได้ เนื่องจากการกระทำในระบบออนไลน์ความเสียหายจึงไม่ได้จำกัดอยู่ในประเทศใดประเทศหนึ่งเท่านั้น กรณีดังกล่าวจึงเป็นที่มาที่ทำให้ประเทศต่าง ๆ สร้างมาตรการในการควบคุมและป้องกันความเสียหายที่อาจเกิดขึ้นให้ได้มากที่สุด

สำหรับประเทศไทยมีทั้งกรณีที่มีผู้ใช้ถูกแฮ็กข้อมูลหรือระบบ กรณีที่ผู้ใช้อ้างว่าสกุลเงินดิจิทัลในบัญชีของตนถูกโจรกรรมไปจากศูนย์รับแลกเปลี่ยนคริปโทเคอร์เรนซีที่ตนได้ลงทะเบียนไว้ โดยแฮ็กเกอร์ได้ทำการเทขายเหรียญ XRP, XLM ที่ตนถือไว้ เพื่อซื้อ เหรียญ ETH ก่อนที่เหรียญจะโอนไปยังกระเป๋าของแฮ็กเกอร์ โดยที่ตนไม่ทราบเรื่องและไม่เคยได้รับอีเมลยืนยันการซื้อขายจากทางศูนย์ฯ<sup>174</sup> และยังมีกรณีที่ศูนย์ซื้อขายคริปโทเคอร์เรนซี BX ถูกดำเนินคดีโดยสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) กล่าวโทษกรรมการ ผู้จัดการ หรือบุคคลที่ได้รับมอบหมายให้เก็บรักษา Private Key ของ BX พร้อมแจ้งเบาะแสบุคคลที่อาจเป็นบุคคลที่บริษัทมอบหมายให้เก็บรักษา Private Key ซึ่งอยู่ในข่ายที่อาจเป็นผู้กระทำความผิด ภายหลังตรวจสอบพบการกระทำ ความผิดตามพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัลโดยผู้กระทำความผิดโอนสินทรัพย์ดิจิทัลของลูกค้ำที่อยู่ในความดูแลหรือครอบครองของบริษัทบิตคอยน์ จำกัด (BX) ออกไปยังกระเป๋าเงินดิจิทัล (Wallet) ที่ไม่ได้มีไว้เพื่อเก็บสินทรัพย์ดิจิทัลของลูกค้ำ ต่อกองบังคับการปราบปรามการกระทำความผิดเกี่ยวกับอาชญากรรมทางเศรษฐกิจ (ปอศ.) เพื่อพิจารณาสอบสวนดำเนินคดีต่อผู้กระทำความผิด และแจ้งการกล่าวโทษให้สำนักงานป้องกันและปราบปรามการฟอกเงินเพื่อพิจารณาดำเนินการตามที่เห็นสมควร เนื่องจากในวันที่ 3 เมษายน 2563 BX ได้แจ้งการหยุดกิจการของบริษัททั้งหมด โดยยุติการให้บริการติดต่อกับลูกค้ำที่ประสงค์จะขอรับทรัพย์สินคืนและปลดพนักงานทั้งหมดก.ล.ต. ตรวจสอบว่า หลังจากนั้นกลับปรากฏรายการโอนสินทรัพย์ดิจิทัลของลูกค้ำที่อยู่ภายใต้ความดูแลและความครอบครองของ BX ใน Wallet ที่ BX ใช้เก็บรักษาสินทรัพย์ดิจิทัลของลูกค้ำ ออกไปยัง Wallet ที่อยู่นอกเหนือการควบคุมดูแลของ BX โดยไม่ได้เกิดจากการขอรับทรัพย์สินคืนจากลูกค้ำ กรณีดังกล่าวได้ทำให้เกิดความเสียหายแก่ผู้อื่นหรือประชาชน<sup>175</sup>

<sup>174</sup> Jeerichuda, นักเทรด Bitcoin บนเว็บเทรดไทยแห่งหนึ่งเผยถูกแฮค ชุมชนคาดเป็นความผิดพลาดผู้ใช้งานมากกว่า, ค้นวันที่ 21 พฤศจิกายน 2564 จาก <https://siamblockchain.com/2020/04/22/user-on-bitkub-was-hacked-lost-8000-thb/>

<sup>175</sup> สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, ก.ล.ต.กล่าวโทษ กรรมการผู้จัดการ หรือบุคคลที่ได้รับมอบหมายให้เก็บรักษา Private Key ของ BX พร้อมแจ้งเบาะแสบุคคลที่อาจเข้าข่ายเป็นผู้กระทำความผิด กรณีโอนสินทรัพย์ดิจิทัลของลูกค้ำที่อยู่ในความดูแลหรือครอบครองของ BX ออกไปยัง Wallet ที่ไม่ได้มีไว้เพื่อเก็บสินทรัพย์ดิจิทัลของลูกค้ำ,

## 2.4.2 การใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล (Cryptojacking)

รูปแบบในการกระทำความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัลรูปแบบใหม่และมีเกิดขึ้นเฉพาะกับการกระทำที่เกี่ยวข้องกับสกุลเงินดิจิทัลเท่านั้น เป็นการนำพลังงานจากการประมวลผลคอมพิวเตอร์ของผู้อื่น เพื่อนำไปใช้ในการตรวจสอบความถูกต้องของธุรกรรมสกุลเงินดิจิทัล (การขุด) ซึ่งผู้ตรวจสอบจำเป็นต้องใช้ทรัพยากรคอมพิวเตอร์ในการประมวลผลมหาศาลในการถอดรหัสเพื่อยืนยันความถูกต้องของการทำธุรกรรมของผู้อื่นแต่ละครั้ง ผู้ตรวจสอบอาจต้องใช้จำนวนเครื่องคอมพิวเตอร์มากหรือใช้อุปกรณ์ที่สร้างขึ้นมาเพื่อการขุดโดยเฉพาะ หรืออาจใช้วิธีการ Pool Mining เพื่อให้ได้กำลังประมวลผลที่มากพอ ยังมีกำลังมากก็ยิ่งจะช่วยให้การประมวลผลทำได้เร็วยิ่งขึ้น ดังนั้นการเป็นผู้ตรวจสอบธุรกรรมหรือการขุดนี้จึงมีต้นทุนที่มีราคาแพง จึงทำให้มีอาชีพใช้วิธีการดังกล่าวลดต้นทุนโดยใช้วิธีการอันมิชอบด้วยแอปใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นในการช่วยผู้ใดสามารถถอดรหัสได้เร็วที่สุดจะได้รับสกุลเงินดิจิทัลเป็นรางวัลจากการขุด

วิธีการ มี 2 รูปแบบ คือ 1) การทำผ่านโค้ด JavaScript ที่ฝังอยู่บนเว็บไซต์ ด้วยการเข้ารหัสลับที่หน้าเว็บสามารถมีไฟล์ JavaScript โค้ดที่ทำงานในเบราว์เซอร์ของผู้อื่นและขณะที่ผู้ใช้นั้นเปิดหน้าเว็บนั้นโค้ด JavaScript มีงานอาชีพก็ได้ดูดพลังงานจากเครื่องนั้นไปใช้ในขุดจากเบราว์เซอร์ได้ หรืออาจใช้วิธีการหลอกล่อให้ผู้เสียหายติดตั้งมัลแวร์ที่มีงานอาชีพสามารถเรียกใช้สคริปต์การขุด วิธีการนี้สามารถใช้ได้กับทุกระบบปฏิบัติการไม่ว่าจะเป็น Windows PC, Mac หรือแม้แต่ในแอปบนอุปกรณ์เคลื่อนที่ เช่น Android เป็นต้น<sup>176</sup> 2) การฝังมัลแวร์ลงในเครื่องคล้ายกับการโจมตีของ Ransomware แต่ส่วนใหญ่แล้วแฮกเกอร์จะทำทั้ง 2 วิธีเพื่อให้มีโอกาสขโมยพลังงานของ CPU ได้มากที่สุด

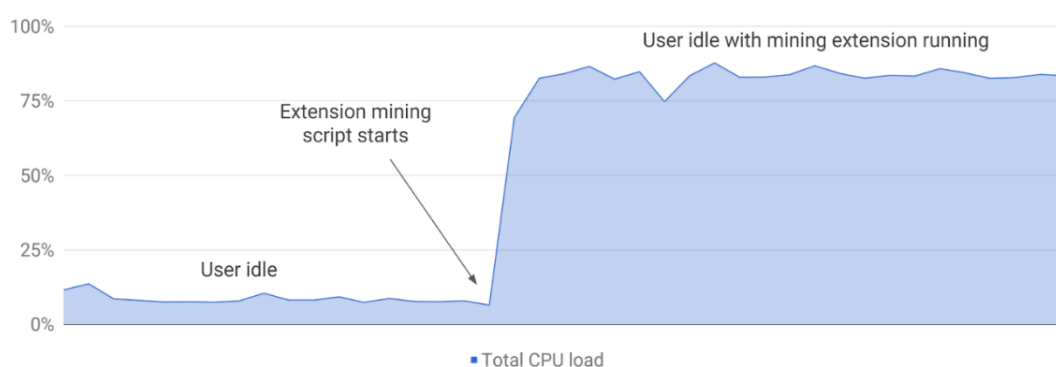
ผลจากการถูก Cryptojacking คือ ผู้ที่ถูกขโมยหรือแย่งใช้พลังงานคอมพิวเตอร์นี้ จะทำให้เนตเวิร์กภายในบ้านช้าลง แต่ค่าไฟกลับเพิ่มขึ้นมาก และยังทำให้คอมพิวเตอร์ในบ้านเสื่อมสภาพก่อนเวลาอันควร รวมทั้งยังเสี่ยงที่จะติดมัลแวร์ตัวอื่น ๆ รวมทั้งมีโอกาสที่คอมพิวเตอร์ภายในบ้านจะเป็นฐานกำลังในการถูกโจมตีอย่างอื่นในอนาคตได้อีกด้วย

---

ค้นวันที่ 14 มกราคม 2564 จาก [https://www.sec.or.th/TH/Pages/News\\_Detail.aspx?SECID=8695](https://www.sec.or.th/TH/Pages/News_Detail.aspx?SECID=8695)

<sup>176</sup> The Fast Code, **Cryptojacking คืออะไรและคุณจะป้องกันตัวเองได้อย่างไร?**, ค้นวันที่ 14 มกราคม 2564 จาก <https://www.thefastcode.com/th-thb/article/what-is-cryptojacking-and-how-can-you-protect-yourself>

Cryptojacking เป็นพื้นที่การเติบโตที่ใหญ่ที่สุดของอาชญากรรมในโลกไซเบอร์ในปี พ.ศ. 2560 โดยมีการตรวจจับแอนตี้ไวรัสเพิ่มขึ้น 8,500 เฟอร์เซ็นต์ ระหว่างเดือนกันยายนถึงธันวาคม 2017 ตัวเลขการตรวจจับมัลแวร์จากการขุดได้เปลี่ยนจากหลักหมื่นขึ้นเป็นล้านครั้ง ซึ่งกิจกรรมการขุดมีมากกว่า 8 ล้านครั้งในแต่ละบล็อก<sup>177</sup> เหตุผลสำคัญที่ทำให้ Cryptojacking เพิ่มขึ้นนั้นเพราะเรื่องของความคุ้มค่าและมีผลตอบแทนชัดเจน ต่างจาก Ransomware ที่ต้องเสี่ยงว่าผู้เสียหายจะจ่ายเงินหรือไม่ รวมทั้งการกระทำที่ผู้เสียหายอาจรู้ตัวและไม่ได้ออกกฎหมายชัดเจนในการคุ้มครอง เพราะไม่ได้ขโมยข้อมูลคอมพิวเตอร์แต่เป็นการขโมยพลังงานของ CPU



ภาพที่ 2.4 การใช้พลังงาน CPU ในการขุดสกุลเงินดิจิทัล<sup>178</sup>

ตัวอย่างของการ Cryptojacking ซึ่งเป็นการใช้พลังงานจากคอมพิวเตอร์ของผู้อื่นเพื่อนำไปใช้ในการตรวจสอบธุรกรรมสกุลเงินดิจิทัล (การขุดสกุลเงินดิจิทัล)

1) หลังจากที่ Kobe Bryant อดีตนักบาสเกตบอลที่มีชื่อเสียงเสียชีวิตลงจากอุบัติเหตุ มีกลุ่มคนส่วนหนึ่งสร้างภาพพื้นหลังบนเครื่องคอมพิวเตอร์ (Wallpaper) เป็นรูป Kobe Bryant และมีการแชร์ต่อให้บุคคลอื่นใช้เพื่อรำลึกถึง Kobe Bryant อย่างแพร่หลาย แต่กลับมีอาชญากรไซเบอร์อาศัยประโยชน์จากเหตุการณ์นี้สร้างภาพพื้นหลังบนเครื่องคอมพิวเตอร์ (Wallpaper) เป็น

<sup>177</sup> Mark J. Krone, Emily M. Lukes, Chris McKibbin, “Tales from the Crypt: Cryptocurrency is here--how will Crime Insurers Respond?,” **Fidelity Law Journal** 24 (November 2018): 52.

<sup>178</sup> Chromium Blog, **Protecting Users from Extension Cryptojacking**, Retrieved June 7, 2021 from <https://blog.chromium.org/2018/04/protecting-users-from-extension-cryptojacking.html>

รูป Kobe Bryant เช่นเดียวกัน แต่แอบใช้วิธี Steganography เพื่อซ่อนโค้ดที่ทำให้เครื่องคอมพิวเตอร์ของผู้ใช้ภาพพื้นหลังบนเครื่องคอมพิวเตอร์ (Wallpaper) ดังกล่าวเข้าไปยังเว็บไซต์ที่ทำให้เครื่องคอมพิวเตอร์ทำการประมวลผลเพื่อขุด Monero (สกุลเงินดิจิทัลสกุลหนึ่ง) ให้แก่อาชญากรไซเบอร์

อย่างไรก็ตามหากผู้ใช้เครื่องคอมพิวเตอร์ที่ใช้ระบบปฏิบัติการ Window 10 จะมีโปรแกรม Windows Defender SmartScreen ซึ่งสร้างขึ้นมาเพื่อป้องกันไม่ให้เครื่องคอมพิวเตอร์เข้าไปในเว็บไซต์ที่ไม่ปลอดภัย เป็นการป้องกันการถูกโจมตีจากอาชญากรไซเบอร์ได้ส่วนหนึ่ง<sup>179</sup>

2) ในปี 2019 Symantec พบว่าแอปพลิเคชัน 8 ตัว บน Microsoft Store ที่ใช้พลังงาน CPU ของผู้อื่นในการนำไปใช้ในการตรวจสอบธุรกรรมสกุลเงินดิจิทัล เมื่อมีการดาวน์โหลดและเปิดแอปใดแอปหนึ่ง Google Tag Manager ในบริการโดเมนจะดึงโค้ด JavaScript ที่เข้ารหัสลับบางส่วน นักขุดจะเปิดใช้งานและเริ่มขุดหา Monero โดยใช้ทรัพยากรหรือพลังงานจากคอมพิวเตอร์เครื่องนั้นเป็นจำนวนมาก และยังทำให้การประมวลผลของเครื่องที่ดาวน์โหลดแอปนั้นไปทำงานช้าลงอย่างมาก<sup>180</sup>

ในบทนี้จึงเป็นการรวบรวมความเป็นมา ลักษณะทั่วไปของสกุลเงินดิจิทัล แนวคิดในการควบคุมความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลตามหลักเกณฑ์ของกฎหมายอาญา และยังได้นำเสนอรูปแบบการกระทำความผิดอีกสองกรณี คือ การขโมยสกุลเงินดิจิทัล และการใช้พลังงานคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล ซึ่งเป็นการกระทำที่มีลักษณะเฉพาะและอาจยังไม่มีกฎหมายใดควบคุมการกระทำความผิดดังกล่าวไว้อย่างชัดเจน ผู้เขียนจึงได้นำทั้งสองกรณีนี้มาเป็นรูปแบบในการศึกษาหลักกฎหมายที่ใช้ในการควบคุมการกระทำความผิดที่เกี่ยวข้องกับกรณีดังกล่าวทั้งของไทยและต่างประเทศ ซึ่งจะกล่าวต่อไปในบทที่ 3

<sup>179</sup> Josh Lake, **What is Cryptojacking (With Examples) and How do you Stop it?**, Retrieved May 16, 2021 from [https://www.comparitech.com/blog/informationsecurity/cryptojacking/#Other\\_examples\\_of\\_cryptojacking](https://www.comparitech.com/blog/informationsecurity/cryptojacking/#Other_examples_of_cryptojacking)

<sup>180</sup> Yuanjing Guo and Tommy Dong, **Several Cryptojacking Apps Found on Microsoft Store**, Retrieved May 19, 2021 from <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cryptojacking-apps-microsoft-store>

### บทที่ 3

## หลักกฎหมายต่างประเทศและหลักกฎหมายประเทศไทยเกี่ยวกับการกระทำ ความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล

การกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล ได้ศึกษาถึงแนวคิด ความเป็นมา ลักษณะ และรูปแบบการกระทำความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัลมาแล้ว ในบทนี้จะทำการศึกษาถึงสถานะทางกฎหมาย ความผิดอาญาที่เป็นรูปแบบเฉพาะของสกุลเงินดิจิทัลซึ่งยังเป็นช่องว่างทางกฎหมาย หลักเกณฑ์ทางกฎหมายในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลของประเทศไทยและต่างประเทศ รวมถึงความร่วมมือทางอาญาระหว่างประเทศ เพื่อเป็นแนวทางในการกำหนดความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลในการนำมาวิเคราะห์เพื่อแสวงหามาตรการที่เหมาะสมในการควบคุมการกระทำความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัล

ในหัวข้อนี้ผู้เขียนได้เลือกทำการศึกษากฎหมายของสหรัฐอเมริกา เนื่องจากเป็นประเทศที่มีนโยบายในการกำกับดูแลสกุลเงินดิจิทัลหลากหลายมุมมอง ดังจะเห็นได้จากการมีองค์กรต่าง ๆ เข้ามาควบคุมการใช้งานของสกุลเงินดิจิทัลตามแต่ละอำนาจหน้าที่ขององค์กรนั้น ๆ และสหรัฐยังเป็นประเทศที่มีความเจริญก้าวหน้าทางเทคโนโลยีมากเป็นอันดับต้นของโลกและอีกประเทศหนึ่ง que เลือกทำการศึกษา คือ สหราชอาณาจักร (อังกฤษ) ด้วยเหตุที่มีการรวบรวมและเผยแพร่แนวปฏิบัติการกำกับดูแลสกุลเงินดิจิทัล (Guidance on Cryptoassets)<sup>181</sup> โดยหน่วยงานที่ทำหน้าที่กำกับนโยบายทางการเงินไว้ จึงทำให้เห็นโครงสร้างและกฎหมายที่เกี่ยวข้องในการกำกับดูแลสกุลเงินดิจิทัลได้อย่างชัดเจน และประเทศอังกฤษแม้จะอยู่ในระบบคอมมอนลอว์ แต่กฎหมายอาญาความผิดเกี่ยวกับทรัพย์สินมีการให้ความหมายอธิบายองค์ประกอบความผิดคล้ายกับกฎหมายของประเทศไทย จึงเป็นเหตุผลที่เลือกสองประเทศนี้มาทำการศึกษา

---

<sup>181</sup> Financial Conduct Authority, **Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3**, Retrieved July 18, 2022 from <https://www.fca.org.uk/publication/policy/ps19-22.pdf>

### 3.1 หลักกฎหมายในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลของสหรัฐอเมริกา

#### 3.1.1 สถานะของสกุลเงินดิจิทัล

การกำหนดสถานะของสกุลเงินดิจิทัลในสหรัฐอเมริกานั้นไม่ได้มีการกำหนดให้เป็นสถานะใดสถานะหนึ่ง แต่เป็นการกำหนดสถานะตามแต่ละองค์กรที่มีหน้าที่ในการควบคุม<sup>182</sup> ดังนั้นจึงไม่มีสถานะที่ชัดเจน ทั้งนี้องค์กรที่ทำหน้าที่ในการควบคุมความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัลมี ดังนี้

##### 3.1.1.1 คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (Security and Exchange Commission)

คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (Security and Exchange Commission) หรือ SEC เป็นหน่วยงานกำกับดูแลตลาดหุ้นที่มีอำนาจในการตีความและบังคับใช้กฎหมายว่าด้วยหลักทรัพย์ของรัฐบาลกลาง Salesperson กำหนดและแก้ไขกฎระเบียบต่าง ๆ นอกจากนี้ยังมีอำนาจโดยตรงในการกำกับดูแลตรวจสอบผู้ที่เกี่ยวข้องกับการซื้อขายผลิตภัณฑ์ที่เป็นหลักทรัพย์เช่นบริษัทหลักทรัพย์โบรกเกอร์ Dealer และที่ปรึกษาการลงทุนเพื่อให้การดำเนินการในตลาดทุนเป็นไปอย่างมีประสิทธิภาพมีความยุติธรรมและเป็นการคุ้มครองผู้ลงทุน<sup>183</sup>

ในมุมมองของ SEC ยังไม่ได้มีการกำหนดอย่างชัดเจนว่า สกุลเงินดิจิทัลมีสถานะเป็นหลักทรัพย์หรือมีสถานะใด แต่ได้มีความเห็นว่าการออกคริปโตเคอร์เรนซีซึ่งมีวัตถุประสงค์เป็นสื่อกลางในการแลกเปลี่ยนที่มีลักษณะเป็นข้อมูลทางอิเล็กทรอนิกส์ที่เรียกว่าโทเค็นที่มีการกำหนดให้มีสิทธิพิเศษในการถือครองโทเค็นนั้น ๆ เพื่อเสนอขายแก่นักลงทุนเพื่อระดมทุนไปใช้ในกิจการต่าง ๆ หรือที่เรียกว่า Initial Coin Offering ICO ในปี 2017 SEC ได้เสนอรายการสอบสวนว่าการเสนอขายโทเค็นที่ชื่อ DAO โทเค็น เป็นการเสนอขายหลักทรัพย์ซึ่งต้องตกอยู่ภายใต้ข้อกำหนดใน Section 21 (a) ของ The Securities Exchange Act of 1934 เนื่องจากลักษณะและเงื่อนไขของการเสนอขาย

<sup>182</sup> Ralph E. McKinney, Jr., Casey W. Baker, Lawrence P. Shao, and Jeff Y. L., Cryptocurrency: Utility Determines Conceptual Classification Despite Regulatory Uncertainty, *USF Intellectual Property and Technology Law Journal* 25, 1 (Fall 2020): 1-18.

<sup>183</sup> นันทน์ภัส พูลเพิ่ม, ผลกระทบจากการทำธุรกรรมเกี่ยวกับคริปโตเคอร์เรนซี: กรณีศึกษาธุรกรรมซื้อขาย (วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2560), หน้า 47.

ซึ่งระบุว่ากฎหมายหลักทรัพย์ของรัฐบาลกลางมีผลบังคับใช้ไม่ว่าผู้ออกโทเคนจะเป็นบริษัทธรรมดาหรือองค์กรอิสระแบบไม่ศูนย์กลางในการควบคุมก็ตาม ไม่ว่าจะระบบจะจัดทำขึ้นบนเทคโนโลยีนอกเหนือกฎหมายหลักทรัพย์และไม่ว่าสินทรัพย์ประเภทนี้จะถูกซื้อด้วยเงินดอลลาร์หรือสกุลเงินดิจิทัลก็ตาม ดังนั้นหากมีการใช้เพื่อวัตถุประสงค์ในการลงทุนหรือระดมทุนที่เกี่ยวข้องกับสกุลเงินดิจิทัลจะอยู่ภายใต้กฎหมายนี้<sup>184</sup>

อย่างไรก็ตามสำหรับสถานะของสกุลเงินดิจิทัลยังไม่มีศาลใดที่ตัดสินว่าสกุลเงินดิจิทัลมีสถานะเป็นหลักทรัพย์<sup>185</sup>

### 3.1.1.2 สำนักงานคณะกรรมการกำกับการซื้อขายสินค้าโภคภัณฑ์ (Commodity Futures Trading Commission)

สำนักงานคณะกรรมการกำกับการซื้อขายสินค้าโภคภัณฑ์ (Commodity Futures Trading Commission) หรือ CFTC คือ หน่วยงานอิสระจากรัฐบาลกลางสหรัฐ มีหน้าที่ในการกำกับดูแลตลาดทุนในส่วนสินค้าโภคภัณฑ์ และควบคุมสัญญาซื้อขายล่วงหน้าสินค้าโภคภัณฑ์ที่อิงจากสินค้าโภคภัณฑ์พื้นฐาน โดยมีวัตถุประสงค์ต่อต้านการฉ้อโกงและการปั่นราคาตลาด

ในการควบคุมการกระทำความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัลนั้น CFTC มองว่าสกุลเงินดิจิทัลบางสกุล เช่น บิตคอยน์ อีเทอร์เรียม เป็นสินค้าโภคภัณฑ์ จึงถูกกำหนดให้เป็นสินค้าภายใต้สินค้าโภคภัณฑ์ตามกฎหมาย the Commodity Exchange Act (CEA)<sup>186</sup> แต่สำหรับ ริฟเฟิล (Ripple) ซึ่งใช้ชื่อว่า XRP แม้จะเป็นสกุลเงินดิจิทัลเช่นเดียวกับบิตคอยน์ และอีเทอร์เรียมแต่ CFTC ยอมรับว่ายังไม่มีความชัดเจนถึงการกำหนดสถานะของ XRP ความไม่ชัดเจนนี้ทำให้ยังไม่สามารถเข้าใจได้ว่าจะควบคุมสิ่งนี้อย่างไร อย่างไรก็ตามการกำหนดสถานะและการกำกับดูแลของ XRP นี้

<sup>184</sup> **Securities and Exchange Commission Securities Exchange Act of 1934**, Retrieved July 17, 2021 from <https://www.sec.gov/litigation/investreport/34-81207.pdf>

<sup>185</sup> Regulation of the unregulated: How bitcoin and cryptocurrencies show that the government can regulate anything

<sup>186</sup> **Customer Advisory: Understand the Risks of Virtual Currency Trading**, Retrieved July 17, 2021 from [https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory\\_urvct121517.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_urvct121517.pdf)

CFTC จะทำงานร่วมกับสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ของสหรัฐอเมริกา (SEC) เพื่อพิจารณาว่า XRP จะอยู่ภายใต้การกำกับดูแลในสถานะและองค์กรใด<sup>187</sup>

### 3.1.1.3 เครือข่ายการบังคับใช้กฎหมายอาชญากรรมทางการเงิน (Financial Crime Enforcement Network)

เครือข่ายการบังคับใช้กฎหมายอาชญากรรมทางการเงิน (Financial Crime Enforcement Network) หรือ FinCEN เป็นหน่วยงานที่ก่อตั้งมาในปี ค.ศ. 1990 เพื่อเป็นศูนย์กลางในการทำหน้าที่ป้องกันระบบการเงินจากการกระทำที่ผิดกฎหมายตรวจสอบสืบสวนวิเคราะห์ข้อมูลอาชญากรรมตามนโยบายต่อต้านการฟอกเงินในประเทศซึ่งมีกลไกในการกำกับดูแลธุรกรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัล เนื่องจากเป็นธุรกรรมที่มีความเสี่ยงต่อการนำไปใช้ในการกระทำความผิดโดยใช้อำนาจตาม Bank Secrecy Act กำหนดให้ผู้ให้บริการธุรกิจบริการเงิน (Money Services Business) รวมถึงผู้ส่งเงิน (Money Transmitter)<sup>188</sup> ที่เกี่ยวกับสกุลเงินดิจิทัล จะต้องขึ้นทะเบียนการประกอบธุรกิจกับ FinCEN และมีหน้าที่ต้องรายงานข้อมูลการทำธุรกรรมต่อ FinCEN<sup>189</sup>

ทั้งนี้แม้ FinCEN จะไม่ได้มีการกำหนดสถานะของสกุลเงินดิจิทัลไว้อย่างชัดเจน แต่ได้มีการเพิ่มความหมายคำว่า Money Transmitter ไว้ว่านอกจากจะหมายถึง “สกุลเงินที่ใช้ชำระหนี้ได้ตามกฎหมาย” แล้ว (Currency)<sup>190</sup> ยังให้หมายความรวมถึง “มูลค่าอื่นที่แทนเงิน” (Other Value that Substitutes for Currency)<sup>191</sup> จากการเพิ่มความหมายนี้จึงทำให้ธุรกรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัลหน้าที่ต้องมีการขึ้นทะเบียนและรายงานข้อมูลการทำธุรกรรมต่อ FinCEN เช่นเดียวกับธุรกรรมการเงินทั่วไป

### 3.1.1.4 กรมสรรพากร (The Internal Revenue Service)

กรมสรรพากร (The Internal Revenue Service) หรือ IRS มองว่าสกุลเงินดิจิทัลหรือเงินเสมือนอาจนำไปใช้ชำระค่าสินค้าหรือบริการหรือถือครองไว้เพื่อลงทุนสกุลเงินดิจิทัลมีมูลค่าที่ถูกนำเสนอทางดิจิทัลทำหน้าที่เป็นสื่อกลางในการแลกเปลี่ยนหน่วยของบัญชีเงินฝากและเป็นที่ยอมรับมูลค่าและในบางสถานการณ์สกุลเงินดิจิทัลมีการใช้งานเหมือนกับสกุลเงินจริง ตัวอย่างเช่น เหรียญ

<sup>187</sup> Helen Partz, **Bitcoin and ETH Are Commodities, While XRP's Status Is Unclear, CFTC Says**, Retrieved July 17, 2021 from <https://cointelegraph.com/news/bitcoin-and-eth-are-commodities-while-xrps-status-is-unclear-cftc-says>

<sup>188</sup> 31 C.F.R. § 1010.100 (ff).

<sup>189</sup> 31 C.F.R. § 1022.380 (a) (1).

<sup>190</sup> 31 CFR § 1010.100

<sup>191</sup> 31 C.F.R. § 1010.100 (ff) (5) (i) (A)

หรือธนบัตรของสหรัฐอเมริกาหรือประเทศอื่นใดซึ่งได้ออกตามกฎหมายหมุนเวียนนำออกใช้ตามปกติ และได้รับการยอมรับในฐานะเป็นสื่อกลางในการแลกเปลี่ยนในประเทศผู้ออกเพียงแต่สกุลเงินดิจิทัล ไม่มีสถานะตามกฎหมายของประเทศใด ดังนั้นกรมสรรพากรของสหรัฐอเมริกาจึงออก Notice 2014-21<sup>192</sup> ว่าสกุลเงินดิจิทัลนั้นได้ถูกจัดเก็บภาษีในฐานะที่เป็นทรัพย์สินและนำเอาหลักการทางภาษีทั่วไปของธุรกรรมที่เกี่ยวข้องกับทรัพย์สินมาปรับใช้เท่าที่จะเป็นไปได้กับธุรกรรมสกุลเงินดิจิทัลได้

ดังนั้นการควบคุมความผิดเกี่ยวกับสกุลเงินดิจิทัลของสหรัฐอเมริกายังไม่มีโครงสร้างหรือแบบแผนที่ชัดเจนและเป็นทางการหนึ่งเดียว เห็นได้จากการที่หน่วยงานกลางในระดับรัฐบาลกลาง (Federal Government) ยังคงไม่มีการกำหนดนิยามของสกุลเงินดิจิทัลที่ชัดเจนร่วมกัน การกำกับดูแลที่เกิดขึ้นในปัจจุบันจึงค่อนข้างจะกระจัดกระจายไปตามการตีความและการกำหนดนิยามเหรียญเงินดิจิทัลของหน่วยงานกลางแต่ละหน่วยงาน ซึ่งล้วนมีความพยายามที่จะกำหนดนิยามให้สอดคล้องไปตามขอบเขตกฎหมายที่อยู่ในความรับผิดชอบของตน สกุลเงินดิจิทัลในสหรัฐอเมริกาจึงมีหลากหลายบทบาท เป็นได้ทั้งสกุลเงิน สินทรัพย์ หลักทรัพย์ และสินค้าโภคภัณฑ์ แตกต่างกันไปตามมุมมองของแต่ละองค์กรที่ทำหน้าที่กำกับดูแล

### 3.1.2 ความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล

สกุลเงินดิจิทัลเป็นสิ่งที่มูลค่า แม้จะไม่มีรูปร่างแต่สามารถนำมาใช้ซื้อขายแลกเปลี่ยนได้จริง ซึ่งทำหน้าที่เป็นสื่อกลางคล้ายกับเงินตราได้ ดังนั้นสกุลเงินดิจิทัลจึงเป็นสิ่งมีค่าและเป็นที่ต้องการได้ จึงสามารถถูกขโมยหรือกระทำการเพื่อให้ได้มาโดยมิชอบได้เหมือนสิ่งของที่มีค่าทั่วไป แต่วิธีการได้ไปนั้นมีความแตกต่างเนื่องจากต้องการกระทำในระบบออนไลน์ไม่ว่าจะผ่านอุปกรณ์เชื่อมต่อใดก็ตาม เช่น คอมพิวเตอร์ มือถือ เป็นต้น จึงมีโอกาสที่อาชญากรจะเจาะระบบหรือแฮ็ก (Hack) จากอุปกรณ์เชื่อมต่อเหล่านี้ เพื่อขโมยสกุลเงินดิจิทัลโดยการโอนไปยัง Wallet ของผู้กระทำความผิดหรือของผู้อื่น

ดังนั้นจุดประสงค์ของการ Hack ไม่ใช่เพียงเพื่อเข้าถึงหรือเพื่อล้วงรู้ถึงข้อมูลคอมพิวเตอร์ แต่เป็นการขโมยโดยการนำเอาสกุลเงินดิจิทัลออกมาจากเจ้าของบัญชี Wallet นั้น โดยไม่ได้รับอนุญาต

นอกจากนี้ความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัลยังมีรูปแบบของการขโมยพลังงานจาก CPU หรือ GPU (Cryptojacking) ซึ่งแฝงมากับมัลแวร์ หรือซอฟต์แวร์ที่ใช้อยู่ตามปกติ เพื่อนำพลังงานที่ได้ไปใช้ในการตรวจสอบความถูกต้องของธุรกรรมสกุลเงินดิจิทัล (การขุด) ผู้กระทำจะได้เหรียญของสกุลเงินดิจิทัลนั้นเป็นค่าตอบแทนในการตรวจสอบธุรกรรม

<sup>192</sup> Notice 2014-21, Retrieved July 17, 2021 from <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>

### 3.1.3 กฎหมายเกี่ยวกับการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล

Wire Fraud 18 U.S.C.1343 การควบคุมการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลนั้นมีกฎหมายหลายฉบับเข้ามาเกี่ยวกับตามแต่มุมมองที่กฎหมายฉบับนั้นมีวัตถุประสงค์ในการควบคุม แต่สำหรับการโจรกรรมสกุลเงินดิจิทัลอันเป็นความผิดอาญานั้น Wire Fraud 18 U.S.C.1343 เป็นทางเลือกที่ดีที่สุดวิธีหนึ่งสำหรับการดำเนินคดีอาญาของรัฐบาลกลาง<sup>193</sup> สอดคล้องกับความผิดรูปแบบใหม่ซึ่งมีความซับซ้อนจากระบบบล็อกเชน<sup>194</sup>

กฎหมายการฉ้อโกงผ่านสายอิเล็กทรอนิกส์ (Wire Fraud §1343) เป็นกฎหมายที่สภาองเกรสประกาศใช้วัตถุประสงค์เบื้องต้นเพื่อป้องกันการกระทำความผิดอันเป็นการฉ้อโกงหรือเพื่อให้ได้มาซึ่งเงินตราหรือทรัพย์สินโดยแสดงข้อความอันเป็นเท็จหรือสัญญา โดยการส่งข้อมูลหรือก่อให้เกิดการส่งข้อมูลผ่านระบบสายอิเล็กทรอนิกส์ทางคอมพิวเตอร์ รวมถึงใช้กับการดำเนินคดีกับการฉ้อโกงรูปแบบใหม่<sup>195</sup> และการพยายามที่จะฉ้อโกงเพื่อให้ได้ข้อมูลทางการเงินส่วนบุคคลของบุคคลเพื่อจุดประสงค์ในการโจรกรรม<sup>196</sup> หรือการโจรกรรมข้อมูลประจำตัว<sup>197</sup> กฎหมายฉบับนี้มีองค์ประกอบดังนี้<sup>198</sup>

#### องค์ประกอบความผิด

- 1) ผู้กระทำความผิดต้องมีเจตนาที่จะหลอกลวงผู้อื่น

<sup>193</sup> “Prosecuting Cryptocurrency Theft with the Defend Trade Secrets Act of 2016,” **University of Pennsylvania Law Review** 167 (2018): 245.

<sup>194</sup> Henry S. Zaytoun, “Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft,” **North Carolina Law Review** 97, 2 (2019): 427.

<sup>195</sup> William M. Sloan, “Mail and Wire Fraud,” **American Criminal Law Review** 48, 2 (Spring 2011): 905.

<sup>196</sup> Corporate Finance Institute, **Wire Fraud**, Retrieved January 12, 2021 from <https://corporatefinanceinstitute.com/resources/knowledge/other/wire-fraud/>

<sup>197</sup> The United States Department of Justice, **Russian Project Lakhta Member Charged with Wire Fraud Conspiracy**, Retrieved April 18, 2021 from <https://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy>

<sup>198</sup> Matthew J. Galluzzo, **Federal Wire Fraud Charges (18 USC 1343 and 1349)**, Retrieved January 12, 2021 from <https://www.gjllp.com/news/federal-wire-fraud-charges-18-usc-1343-and-1349/>

2) มีการใช้การสื่อสารที่การกระทำเชื่อมโยงกันระหว่างรัฐ กล่าวคือ ความผิดในฐานนี้ มีลักษณะแตกต่างจากความผิดในฐานอาญาของประเทศไทย เนื่องจากในสหรัฐนั้น มี 50 มลรัฐ แต่ละรัฐมีอำนาจในการออกกฎหมายอาญาและควบคุมการกระทำทางอาญาภายในเขตมลรัฐของตนเอง แต่ความผิดระหว่างมลรัฐ หากมีความผิดอาญาที่เกิดขึ้นและข้ามดินแดนแต่ละมลรัฐแล้ว หากรัฐบาลกลางของสหรัฐฯ ไม่มีมาตรการควบคุมแล้ว ก็จะทำให้เกิดภาวะสุญญากาศในทางกฎหมายได้ หรือ การป้องกันอาชญากรรมอาจจะไม่มีประสิทธิภาพได้ รัฐบาลสหรัฐฯ จึงออกกฎหมายที่ควบคุมการกระทำที่มีลักษณะข้ามมลรัฐ ข้ามเขตอำนาจศาลของแต่ละมลรัฐ เช่น การป้องกันการฉ้อโกงที่กระทำลงในลักษณะข้ามมลรัฐ ซึ่งผู้กระทำผิดอาจจะใช้วิธีการส่งจดหมาย หรือ การหลอกลวงให้โอนเงินเข้าบัญชีผ่านระบบ Wire<sup>199</sup> ด้วยเหตุที่ความผิดที่เกี่ยวกับสกุลเงินดิจิทัลเป็นการกระทำผ่านระบบออนไลน์ซึ่งสามารถกระทำความผิดเชื่อมโยงถึงกันได้ทุกรัฐ จึงนำกฎหมาย Wire Fraud มาปรับใช้กับการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลได้

3) เกิดความเสียหายที่เป็นตัวเงิน ทรัพย์สิน หรือการไม่ได้รับบริการ<sup>200</sup>

บทลงโทษ

ความผิดตามกฎหมายนี้มีทั้งโทษจำคุกและปรับ คือ จำคุกสูงสุด 20 ปี และหากเป็นการฉ้อโกงที่ส่งผลกระทบต่อสถาบันการเงินหรือเกี่ยวข้องกับภัยพิบัติหรือเหตุฉุกเฉิน จะต้องรับโทษหนักขึ้นเป็นจำคุกสูงสุด 30 ปีและปรับไม่เกิน \$1,000,000 ดอลลาร์

รูปแบบอาชญากรรมที่ใช้กับ Wire Fraud 18 U.S.C.1343

รูปแบบอาชญากรรมตามกฎหมายนี้ได้แก่ การฉ้อโกงโดยส่งผ่านจดหมายอิเล็กทรอนิกส์การส่งหรือรับเงินผ่านธนาคารโดยระบบสายอิเล็กทรอนิกส์ การฉ้อโกงหุ้น การฉ้อโกงที่ดิน การฉ้อโกงธนาคาร การฉ้อโกงประกันภัย และการฉ้อโกงสินค้าโภคภัณฑ์ รวมถึง การเรียกค่าไถ่ การปลอมแปลง การฉ้อโกงการเลือกตั้ง และการติดสินบน และยังใช้ดำเนินคดีกับการฟอกเงินและกฎหมายเกี่ยวกับการป้องกันและปราบปรามอาชญากรรมในรูปแบบขององค์กรอาชญากรรม (Racketeer Influenced and Corrupt Organizations Act (RICO))<sup>201</sup>

<sup>199</sup> ศิริพล กุศลศิลป์วุฒิ, กฎหมายอาชญากรรมทางเศรษฐกิจของประเทศสหรัฐอเมริกา, คำนวนที่ 24 มีนาคม 2564 จาก <https://siriphonku.wordpress.com/2008/08/27/กฎหมายอาชญากรรมทางเศรษฐกิจ/>

<sup>200</sup> William M. Sloan, *op. cit.*, p. 907.

<sup>201</sup> *Ibid.*, p. 907.

คดีตัวอย่างความผิดที่เกี่ยวกับการ Hack/Theft ที่ใช้ Wire Fraud 18 U.S.C.1343

1) นาย Blake Kantor ดำเนินการบริษัทไบนารีออปชันที่รู้จักกันในชื่อ Blue Bit Banc และ Blue Bit Analytics (“BBB”) หลอกวงนักลงทุนมาลงทุนกับ BBB ในธุรกิจเกี่ยวกับสกุลเงินดิจิทัลที่เรียกว่า “ATM Coin” และยังได้ขโมยจากนายทุนไป นาย Kantor สารภาพและถูกตัดสินให้มีความผิดตามกฎหมาย Wire Fraud ซึ่งมีโทษจำคุก ถึง 86 เดือน แต่ศาลอนุญาตให้ปล่อยตัวโดยมีเงื่อนไขภายใต้การดูแลเป็นเวลา 3 ปี และศาลได้สั่งให้ชดใช้ค่าเสียหายเป็นจำนวน 806,405 ดอลลาร์สหรัฐฯ แก่ผู้เสียหาย และริบเงินจำนวน 1.5 ล้านดอลลาร์ จากที่ขโมยมาได้ประมาณ 153,000<sup>202</sup>

2) Meiggs ชายชาวแมสซาชูเซตส์ยอมรับต่อศาลรัฐบาลกลางว่าได้เจาะระบบเข้าไปยังโทรศัพท์ของเหยื่อและบัญชีโซเชียลมีเดีย และใช้ข้อมูลส่วนบุคคลเพื่อขโมยเงินหลายพันดอลลาร์ในสกุลเงินดิจิทัล ตั้งแต่เดือนพฤศจิกายน 2017 ถึงพฤศจิกายน 2019 Meiggs และพวกได้เจาะระบบเข้าไปในโทรศัพท์มือถือของเหยื่อและเข้ายึดถือโซเชียลมีเดีย อีเมล และบัญชีสกุลเงินดิจิทัลของผู้เสียหายด้วยวิธีการที่เรียกว่า “การเปลี่ยนซิม” โดยผู้กระทำผิดได้เปลี่ยนซิมของผู้เสียหายจากผู้ให้บริการโทรศัพท์มือถือ และเปลี่ยนรหัสผ่านในบัญชี Gmail ของผู้เสียหาย ในคดีนี้มีผู้เสียหายกว่า 10 ราย กระทรวงยุติธรรมสหรัฐได้แถลงว่า Meiggs และพวกได้พยายามที่จะขโมยเงินมากกว่า 530,000 ดอลลาร์ในสกุลเงินดิจิทัล จึงมีความผิดตามกฎหมาย CFAA, Wire Fraud 1343, และ 18 U.S.C.A. §§ 371 (Conspiracy to Commit Offense or to Defraud United States)<sup>203</sup>

3) Joseph Kim อายุ 24 ปีทำงานเป็นผู้ช่วยในการซื้อขายสกุลเงินดิจิทัลให้กับบริษัท Consolidated Trading LLC ในชิคาโก ได้กระทำความผิดขโมย Bitcoin และ Litecoin Cryptocurrency ของบริษัทอย่างน้อย 2 ล้านดอลลาร์ เพื่อผลประโยชน์ส่วนตัวของเขาเอง และได้

---

<sup>202</sup> The United States Attorney’s Office Eastern District of New York, **Defendant Sentenced to 86 Months in Prison for Defrauding Investors in Binary Options and Cryptocurrency Scheme**, Retrieved March 8, 2021 from <https://www.justice.gov/usao-edny/pr/defendant-sentenced-86-months-prison-defrauding-investors-binary-options-and>

<sup>203</sup> The United States Department of Justice, **Massachusetts Man Pleads Guilty to Operating Nationwide Scheme to Steal Social Media Accounts and Cryptocurrency**, Retrieved April 21, 2021 from <https://www.justice.gov/opa/pr/massachusetts-man-pleads-guilty-operating-nationwide-scheme-steal-social-media-accounts-and> 9

ให้การเท็จและเป็นตัวแทนของฝ่ายบริหารของบริษัทเพื่อปกปิดการโจรกรรม ถูกดำเนินคดีตามกฎหมาย Wire Fraud ซึ่งมีโทษจำคุกสูงสุด 20 ปี<sup>204</sup>

สำหรับความผิด Cryptojacking ซึ่งเป็นการขโมยพลังงานคอมพิวเตอร์ของผู้อื่นไปใช้ในการตรวจสอบความถูกต้องในการทำธุรกรรมสกุลเงินดิจิทัล หรือ “การขุด” นั้น ในสหรัฐอเมริกา มีหน่วยงาน Federal Trade Commission (FTC) ได้มีการประกาศแจ้งเตือนประชาชนถึงอันตราย และวิธีการป้องกันจากการถูก Cryptojacking ที่อาจมาจากมิดจาชิปที่ฝังโค้ดที่เป็นอันตรายไว้ในเว็บไซต์หรือโฆษณาเพื่อทำให้อุปกรณ์คอมพิวเตอร์ติดไวรัสโดยไม่รู้ตัว และเมื่อใดที่มีการเข้าเว็บไซต์นั้น โค้ดหรือไวรัสจะทำงานโดยการนำพลังงานจากเครื่องคอมพิวเตอร์ไปใช้ในการขุดแก้มิดจาชิป หรืออาจเป็นวิธีการหลอกให้คลิกลิงก์ในอีเมลหรือมีการสร้างที่อยู่เว็บไซต์ที่คล้ายกับเว็บไซต์จริงเพื่อให้ผู้ใช้พิมพ์ผิด สิ่งเหล่านี้อาจนำไปสู่การถูก Cryptojacking ได้ทั้งสิ้น

ข้อปฏิบัติเบื้องต้นที่สามารถทำได้เอง เช่น การหลีกเลี่ยงมัลแวร์ การใช้ซอฟต์แวร์ป้องกันไวรัส การตั้งค่าซอฟต์แวร์และแอปให้อัพเดทโดยอัตโนมัติ และไม่ควรติดตั้งซอฟต์แวร์หรือแอปพลิเคชันที่น่าเชื่อถือ<sup>205</sup>

อย่างไรก็ตามกฎหมาย Wire Fraud มิได้มีขึ้นเพื่อป้องกันการกระทำความผิดเกี่ยวกับการขโมยสกุลเงินดิจิทัลโดยตรง แต่เป็นการปรับใช้กรณีที่เกี่ยวข้องกับความผิดที่ได้กระทำต่อสกุลเงินดิจิทัล รวมทั้งการกระทำอันมิชอบซึ่งเป็นการหลอกลวงเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัลด้วย ประการสำคัญที่ทำให้กฎหมายนี้สามารถปรับใช้กับสกุลเงินดิจิทัลได้ คือ กฎหมายแต่ละรัฐในสหรัฐมีความแตกต่างกัน แต่กฎหมายฉบับนี้เป็นกฎหมายกลางในการป้องกันและปราบปรามการกระทำความผิดที่เกี่ยวข้องกับการติดต่อสื่อสารระหว่างรัฐที่เหมือนกันทุกรัฐ ทั้งนี้เนื่องจากการทำธุรกรรมสกุลเงินดิจิทัลได้ทำในระบบออนไลน์ซึ่งถือเป็นการติดต่อสื่อสารระหว่างรัฐด้วยวิธีการออนไลน์ การใช้จ่ายข้ามรัฐทำได้ง่ายดาย กฎหมายดังกล่าวจึงถูกนำมาปรับใช้กับความผิดฐานนี้ อย่างไรก็ตามความผิดลักษณะนี้อาจเทียบเคียงได้กับประมวลกฎหมายอาญาของไทยซึ่งกำหนดลักษณะความผิดที่เป็นการลักทรัพย์อันมีวัตถุแห่งการกระทำเป็นทรัพย์ (วัตถุที่มีรูปร่าง) ในขณะที่การลักสกุลเงินดิจิทัลเป็นการกระทำต่อวัตถุที่ไม่มีรูปร่าง

<sup>204</sup> The United States Attorney’s Office, Northern District of Illinois, **Chicago Trader Facing Federal Fraud Charge for Allegedly Misappropriating \$2 Million in Cryptocurrencies**, Retrieved April 21, 2021 <https://www.justice.gov/usao-ndil/pr/chicago-trader-facing-federal-fraud-charge-allegedly-misappropriating-2-million>

<sup>205</sup> Jason Adler, **Protecting your Devices from Cryptojacking**, Retrieved April 11, 2021 from <https://www.consumer.ftc.gov/blog/2018/06/protecting-your-devices-cryptojacking>

จึงเกิดปัญหาว่าการขโมยสกุลเงินดิจิทัลจะปรับใช้กับฐานความผิดลักทรัพย์ได้หรือไม่ อย่างไรก็ตาม หากมองว่าสกุลเงินดิจิทัลเป็นทรัพย์สินเหมือน Wire Fraud การนำมาปรับใช้กับองค์ประกอบความผิดตามประมวลกฎหมายอาญาอาจยังมีปัญหาอยู่

ตัวอย่างคดีความผิดที่เกี่ยวกับ Cryptojacking ที่ใช้ Wire Fraud 18 U.S.C.1343

1) Thompson อดีตวิศวกรซอฟต์แวร์ของบริษัท Ormer Seattle ได้สร้างซอฟต์แวร์ที่ทำให้ลูกค้าของบริษัท Cloud Computing กำหนดค่าไฟร์วอลล์ซึ่งมีผลทำให้คำสั่งภายนอกสามารถเจาะและเข้าถึงเซิร์ฟเวอร์ของลูกค้าได้ Thompson ไม่ได้ใช้วิธีการเข้าถึงนี้เพื่อขโมยข้อมูลเท่านั้น แต่ยังใช้พลังคอมพิวเตอร์ที่ได้ขโมยมาเพื่อ “ขุด” Cryptocurrency เพื่อประโยชน์ของตัวเองอีกด้วย ซึ่งเรียกว่า “Cryptojacking” ผู้เสียหายจากการกระทำดังกล่าวมีมากกว่า 30 หน่วยงาน ได้แก่ หน่วยงานของรัฐนอร์ธเวสต์ กลุ่มบริษัทโทรคมนาคมนอกสหรัฐอเมริกา และ มหาวิทยาลัยวิจัยสาธารณสุขนอร์ธเวสต์ เมื่อวันที่ 28 สิงหาคม 2019 Thomsan จึงถูกตั้งข้อหาโดยรัฐบาลกลางในข้อหา Wire Fraud และการโจรกรรมข้อมูลคอมพิวเตอร์<sup>206</sup>

2) Danial Jeloudar และ Saeed Safaei ชาวอิหร่านซึ่งอาศัยอยู่ต่างประเทศถูกตัดสินว่ามีความผิดตามกฎหมาย Wire Fraud จากการ Cryptojacking โดยทั้งสองได้เข้าถึงอุปกรณ์ของเหยื่อด้วยวิธีการอันมิชอบเพื่อใช้พลังการประมวลผลในการ “ขุด” cryptocurrency และจำเลยทั้งสองได้สมคบกันหลอกเหยื่อซึ่งเป็นบริษัทเทคโนโลยีในเซนต์ชาร์ลส์ รัฐมิสซูรีเพื่อใช้บัญชีของบริษัทรับบริการคลาวด์ จำเลยได้หลอกหลวงให้ผู้ให้บริการคลาวด์สร้างและติดตั้งเซิร์ฟเวอร์คอมพิวเตอร์ใหม่อย่างน้อยห้าเครื่องในระบบคลาวด์ผ่านบัญชีของบริษัทเหยื่อ จุดประสงค์ของจำเลยในการติดตั้งเซิร์ฟเวอร์ใหม่มีขึ้นเพื่อใช้งานโปรแกรมซอฟต์แวร์ในการขุดหรือใช้พลังงานคอมพิวเตอร์อย่างมหาศาลเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล มูลค่าความเสียหายของเหยื่อในคดีนี้มากกว่า 760,000 ดอลลาร์ จากค่าบริการคลาวด์ในการใช้เซิร์ฟเวอร์ดังกล่าว<sup>207</sup>

<sup>206</sup> The United States Attorney’s Office, Western District of Washington, **Former Seattle Tech Worker Indicted on Federal Charges for Wire Fraud and Computer Data Theft**, Retrieved June 21, 2021 <https://www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-indicted-federal-charges-wire-fraud-and-computer-data-theft>

<sup>207</sup> The United States Attorney’s Office, Eastern District of Missouri, **Two Iranian Nationals Indicted in Local Cryptojacking Case** Retrieved December 2, 2022 <https://www.justice.gov/usao-edmo/pr/two-iranian-nationals-indicted-local-cryptojacking-case>

ทั้งนี้ความผิด Cryptojacking สหรัฐได้นำกฎหมาย Wire Fraud มาปรับใช้เช่นเดียวกับความผิดฐานขโมยสกุลเงินดิจิทัลที่กล่าวไว้แล้วข้างต้นด้วยเหตุผลเดียวกัน คือ เป็นความผิดที่เป็นการขโมยพลังงานซึ่งมีลักษณะการกระทำใกล้เคียงกับการขโมยสกุลเงินดิจิทัลและด้วยเหตุที่กฎหมายกำหนดองค์ประกอบความผิดโดยใช้คำว่าได้ไปซึ่งเงินตราหรือทรัพย์สิน จึงสามารถครอบคลุมสกุลเงินดิจิทัลซึ่งเป็นวัตถุที่ไม่มีรูปร่างได้

## 3.2 หลักกฎหมายในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลของสหราชอาณาจักร (อังกฤษ)

### 3.2.1 สถานะของสกุลเงินดิจิทัล

กระทรวงการคลัง องค์กรอิสระที่ทำหน้าที่กำกับนโยบายทางการเงินและธนาคารแห่งประเทศไทยได้ร่วมกันจัดทำรายงานฉบับสมบูรณ์ (Cryptoassets Taskforce report 2018)<sup>208</sup> โดยกำหนดสถานะให้กับสกุลเงินดิจิทัลในการใช้ประกอบการทำธุรกรรมต่าง ๆ ในรายงานฉบับนี้กำหนดให้เงินเสมือนมีสถานะที่มีตัวตนอยู่จริงแต่อยู่ในโลกดิจิทัลซึ่งมีค่าเป็น “สินทรัพย์” ที่เรียกว่า “Cryptoasset” หรือ “สินทรัพย์ดิจิทัล” หรือกล่าวอีกนัยหนึ่งคือสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีเป็นส่วนหนึ่งของ Cryptoasset (สินทรัพย์ดิจิทัล) ความแตกต่างระหว่างคริปโทเคอร์เรนซี กับ Cryptoasset คือ “Cryptoasset” มีความหมายกว้างกว่าคริปโทเคอร์เรนซี เนื่องจากคริปโทเคอร์เรนซีเป็นสกุลเงินดิจิทัลที่สามารถนำมาใช้จ่ายซื้อสินค้าหรือบริการได้ แต่ในขณะที่ Cryptoasset นอกจากจะสามารถโอนได้จากบัญชีหนึ่งไปสู่บัญชีหนึ่งแล้ว Cryptoasset ยังสามารถเก็บไว้เพื่อประโยชน์จากมูลค่าเพิ่มที่อาจเกิดขึ้นได้ในอนาคต ดังนั้น ในประเทศอังกฤษจึงจัด Cryptoasset ให้อยู่ในรูปแบบของสินทรัพย์ที่มีราคาและถือเอาได้เพียงแต่อยู่ในโลกออนไลน์เท่านั้น

สกุลเงินดิจิทัลในสหราชอาณาจักร (อังกฤษ) นั้นไม่สามารถตีความเป็นเงินตราได้ แม้จะมีความคล้ายคลึงกันก็ตาม เช่น สามารถนับเป็นจำนวนหน่วย มีแหล่งเก็บข้อมูล และสามารถโอนให้กันได้ แต่ก็ยังมีความแตกต่างจากเงินตราอยู่หลายประการ และในตอนแรกยังไม่ได้มีการตีความให้อยู่ภายใต้คำนิยามของคำว่า “ทรัพย์สิน” (Property) หรือ ในลักษณะที่เป็นทรัพย์สินส่วนบุคคล

<sup>208</sup> The Open Government Licence, **Cryptoassets Taskforce: Final Report**, Retrieved March 3, 2021 from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/752070/cryptoassets\\_taskforce\\_final\\_report\\_final\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf)

(Personal Property) ตามกฎหมายอังกฤษ โดยมองว่าเป็นสิ่งที่ไม่สามารถครอบครองได้ (Choses in Possession) เนื่องจากเป็นสิ่งที่จับต้องไม่ได้จึงไม่มีตัวตนที่ก่อให้เกิดการก่อตั้งสิทธิในการครอบครองได้

แต่อย่างไรก็ตาม ภายหลังได้เกิดปัญหาในการตีความอยู่หลายครั้ง จนกระทั่งวันที่ 18 พฤศจิกายน ค.ศ. 2019 หน่วยงาน The UK Taskforce's Legal Statement ได้มีการตีความว่า Cryptoasset เป็นทรัพย์สิน (Property) ชนิดหนึ่งตามหลักการของกฎหมายได้ โดยไม่ได้พิจารณาจากลักษณะภายนอกของทรัพย์สินแต่เป็นการพิจารณาถึงความสัมพันธ์ทางกฎหมายในลักษณะกรรมสิทธิ์ที่มีขึ้นระหว่างบุคคลกับทรัพย์สิน ซึ่งหมายถึงสิทธิในการครอบครองตามกฎหมายแพ่งที่อาจได้รับการเยียวยา (Civil Remedy) หากถูกละเมิด และสามารถถูกประทุษร้ายเป็นคดีความทางอาญาได้เหมือนกับการถูกขโมยและถูกฉ้อโกงได้<sup>209</sup>

คดีตัวอย่างที่เกี่ยวกับการฉ้อโกง Cryptoasset ที่ศาลประเทศอังกฤษได้ตีความว่าเป็นทรัพย์สินคือคดี AA v Persons Unknown & Ors, Re Bitcoin คดีนี้เกี่ยวข้องกับบริษัทประกันภัยแคนาดา ได้ถูกเข้าระบบโดยมิชอบและถูกติดตั้งโปรแกรมมัลแวร์เข้ามาในระบบ (System Hacked and Malware Installed) โดยบริษัทได้รับคำเสนอจากมิจฉาชีพให้ชำระค่าไถ่ด้วยบิตคอยน์เพื่อแลกกับการถอดรหัส (Decryption Tool) บริษัทประกันภัยแคนาดาผู้เสียหายได้ติดต่อบริษัทประกันของตนเอง (Insurer) ที่ทำหน้าที่เป็นตัวแทนในการเจรจาต่อรองค่าไถ่กับผู้กระทำความผิด ตัวแทนเจรจาต่อรองค่าไถ่โดยขอให้ลดจำนวนลง จากนั้นจึงโอนบิตคอยน์จำนวนหนึ่งไปยังผู้กระทำความผิดเพื่อแลกกับเครื่องมือถอดรหัส

ภายหลังเมื่อระบบของบริษัทประกันแคนาดาได้รับการกู้คืนมาเป็นปกติแล้ว บริษัทประกันได้พยายามกู้คืนบิตคอยน์ที่จ่ายไปสำหรับเครื่องมือถอดรหัสลับนั้น นอกจากนี้บริษัทประกันได้สั่งให้ผู้ตรวจสอบบล็อกเชนที่เชี่ยวชาญในการติดตาม Cryptoasset นั้นกลับคืนมา โดยระบุว่าบิตคอยน์บางส่วนถูกเก็บไว้ในบัญชีกับการแลกเปลี่ยน Bitfinex แล้ว และบิตคอยน์บางส่วนได้ถูกโอนไปเป็นเงินตราแล้ว (Fiat Currency)<sup>210</sup>

<sup>209</sup> UK Jurisdiction Taskforce, **Legal Statement on Cryptoassets and Smart Contracts** (London: The LawTech Delivery Panel, 2009), Retrieved March 3, 2021 from [https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056\\_JO\\_Cryptocurrencies\\_Statement\\_FINAL\\_WEB\\_111119-1.pdf](https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf)

<sup>210</sup> AA v Persons Unknown & Ors, Re Bitcoin, [2019] EWHC 3556 (Comm).

อย่างไรก็ดี บริษัทประกันได้ยื่นคำร้องต่อศาลสูงอังกฤษเพื่อทำการติดตามบิตคอยน์ บางส่วนที่ยังคงค้างอยู่ในระบบ และในคดีนี้เอง UK Taskforce จึงต้องพิจารณาให้ความเห็นในการตีความอธิบายเกี่ยวกับสถานะการถือครองกรรมสิทธิ์ของ Cryptocurrencies ด้วยเหตุนี้จึงสรุปว่าบิตคอยน์ในกรณีนี้เป็นทรัพย์สินรูปแบบหนึ่งที่สามารถจดทะเบียนกรรมสิทธิ์ได้ และศาลสูงอังกฤษก็ยอมรับในการตีความนี้เช่นกัน

### 3.2.2 ความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล

สกุลเงินดิจิทัลเป็นสิ่งที่มีการยอมรับว่ามีมูลค่าสามารถนำมาเป็นสื่อกลางในการแลกเปลี่ยนสินค้าหรือบริการได้ สามารถเปลี่ยนมือและโอนได้จากบัญชีหนึ่งไปสู่อีกรายหนึ่งได้อย่างสะดวก รวดเร็วภายใต้ระบบออนไลน์ โดยที่ไม่ต้องระบุตัวตน สกุลเงินดิจิทัลจึงเป็นที่ต้องการของอาชญากรด้วยวิธีการหลากหลายรูปแบบทั้งการขโมยไปจากบัญชี การฉ้อโกง การสับเปลี่ยน SIM<sup>211</sup> เป็นต้น

สำหรับกรณีการขโมยสกุลเงินดิจิทัลนี้การจำลองสถานการณ์ที่อาจเกิดขึ้นได้ โดยที่การขโมยสกุลเงินดิจิทัลนั้นมิใช่เป็นการกระทำที่อยู่ในรูปแบบที่เกิดขึ้นในระบบออนไลน์ทั้งหมดแต่อาจเกิดกรณีมีการข่มขู่หรือใช้กำลังประทุษร้ายทำให้เหยื่อหรือผู้เสียหายเป็นผู้กระทำการโอนสกุลเงินดิจิทัลออกไปเสียเอง ซึ่งมี 3 รูปแบบดังนี้<sup>212</sup>

- 1) D ผู้โจมตี เล็งปืนไปที่ V ผู้เป็นเหยื่อ และเรียกร้องให้ V โอนสกุลเงินดิจิทัลไปยังกระเป๋าเงินของ D โดยให้ V เป็นผู้ทำธุรกรรมและใช้คีย์ส่วนตัวของ V เอง
- 2) D เล็งปืนไปที่ V และเรียกร้องให้ V เปิดเผยกุญแจส่วนตัวของ V โดยที่ D เป็นผู้ทำธุรกรรมการโอนสกุลเงินดิจิทัลของ V ไปยังกระเป๋าของตนเอง (กระเป๋าของ D)
- 3) D เล็งปืนไปที่ V ซึ่งมีบัญชีในตลาดแลกเปลี่ยนสกุลเงินดิจิทัล และบังคับให้ V ส่งคำร้องผ่านแพลตฟอร์มแลกเปลี่ยนสกุลเงินดิจิทัลเพื่อขอโอนสกุลเงินดิจิทัลในบัญชีของ V ไปยังบัญชีที่ D ต้องการ

กรณีที่ 1 และ 2 นั้น เป็นกรณีที่ D ผู้กระทำ ได้กระทำต่อ V ผู้เสียหาย ซึ่งเป็นผู้ที่สามารถทำธุรกรรมการโอนได้เอง ในกรณีที่ 1 นั้น D ให้ V เป็นผู้โอนสกุลเงินดิจิทัลออกจากบัญชีของ V ด้วย

<sup>211</sup> Ben Winck, **One Cryptocurrency Investor Reportedly Lost \$24 Million Worth of Bitcoin in a SIM Swap Attack**, Retrieved March 12, 2021 from <https://markets.businessinsider.com/currencies/news/bitcoin-investor-loses-24-million-of-crypto-sim-swaphackers-2019-11-1028677818>

<sup>212</sup> Alex Taylor and Micheal O' Flynn, "Bitcoin Burglaries and the Theft Act 1968," **Criminal Law Review** 3 (2021): 169.

ตัวเอง ส่วนในกรณีที่ 2 D เป็นผู้กระทำการโอนสกุลเงินดิจิทัลออกไปจากบัญชีของ V โดยที่ให้ V บอกรู้อย่างแจ่มชัดของ V เพื่อให้เข้าถึงบัญชีของ V ได้ และกรณีสุดท้ายต่างจากทั้งสองกรณีที่กล่าวมา คือ V ผู้เสียหายไม่สามารถกระทำการธุรกรรมการโอนได้เองทันที เนื่องจากเปิดบัญชีไว้กับผู้ประกอบธุรกิจ แลกเปลี่ยน ดังนั้นหาก V ต้องการทำการธุรกรรม V ต้องแจ้งความต้องการไปยัง Exchange เพื่อให้ Exchange ทำธุรกรรมการโอนให้ ดังนั้นสิ่งที่ D ได้กระทำต่อ V คือการบังคับให้ V กระทำการแจ้งความต้องการที่จะทำการธุรกรรมการโอนไปยัง Exchange เนื่องจากทั้งสามรูปแบบที่กล่าวมามีการใช้เงินไปให้ผู้เสียหายซึ่งเป็นเจ้าของบัญชีสกุลเงินดิจิทัล จึงเป็นการลักทรัพย์โดยใช้ประทุษร้ายหรือขู่เข็ญว่าในทันใดนั้นจะใช้กำลังประทุษร้าย ซึ่งอาจเทียบเคียงกับความผิดฐานชิงทรัพย์ตามประมวลกฎหมายอาญาของไทยได้

อย่างไรก็ตามทั้งสามกรณีนี้เป็นกรณีก่อการที่ผู้กระทำได้มีการ “เอาไป” ซึ่งสกุลเงินดิจิทัล อันเป็นการโจรกรรมสกุลเงินดิจิทัลโดยที่มิได้มีการแย่งชิงความเป็นส่วนตัวของผู้เสียหายแต่อย่างใด เนื่องจากให้ V ผู้เสียหายเป็นผู้เข้าระบบเอง กรณีดังกล่าวเป็นรูปแบบการโจรกรรมที่อาจเกิดขึ้นได้ โดยผู้กระทำอาจไม่มีความผิดเกี่ยวกับคอมพิวเตอร์ได้

นอกจากนี้ในประเทศอังกฤษยังมีการขโมยพลังงานคอมพิวเตอร์ของผู้อื่นเพื่อไปใช้ในการตรวจสอบความถูกต้องของธุรกรรมสกุลเงินดิจิทัล (Cryptojacking) เป็นถืออาชญากรรมไซเบอร์ที่สร้างรายได้อย่างมากและจูงใจให้มีการกระทำความผิดมากขึ้น เนื่องจากการขโมยพลังงานแต่ละครั้งทำให้มีผู้ตกเป็นเหยื่อได้จำนวนมาก วิธีการไม่ซับซ้อน ไม่มีต้นทุนในการกระทำความผิด และมีความเสี่ยงที่จะถูกดำเนินคดีต่ำ<sup>213</sup> ในช่วงครึ่งแรกของปี 2022 พบว่าอาชญากรรมดังกล่าวมีจำนวนเพิ่มขึ้น 30% เมื่อเทียบกับครึ่งปีแรกของปี 2021<sup>214</sup> กลุ่มเป้าหมายมีหลากหลายทั้งภาคธุรกิจ ประชาชนทั่วไป ยังพบว่าเว็บไซต์ของทางราชการและอีกกว่า 4,000 เว็บไซต์ก็เคยถูกขโมยพลังงานในลักษณะดังกล่าวเช่นกัน<sup>215</sup>

<sup>213</sup> McAfee, **McAfee Labs Threats Report’2018**, Retrieved July 5, 2021 from <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun2018.pdf>

<sup>214</sup> SonicWall, **Cryptojacking Reaches Record High**, Retrieved December 31, 2022 from <https://www.sonicwall.com/2022-cyber-threat-report/>

<sup>215</sup> Wired, **UK Government Websites Were Caught Cryptomining. But it could have been a Lot Worse**, Retrieved December 31, 2022 from <https://www.wired.co.uk/article/browsealoud-ico-texthelp-cryptomining-how-cryptomining-work>

### 3.2.3 กฎหมายเกี่ยวกับการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล

#### 3.2.3.1 Theft Act 1968

ภายหลังปี ค.ศ. 2019 ที่ The UK Taskforce’s Legal Statement ที่ได้ตีความว่า Cryptoasset เป็นทรัพย์สิน ประกอบกับการวางหลักของศาลสูงแห่งประเทศอังกฤษ ส่งผลให้มีการตีความโดยนำ Theft Act 1968 มาใช้กับกรณีการขโมยสกุลเงินดิจิทัล ภายใต้ มาตรา 4 (1) ซึ่งครอบคลุมถึงเงินและทรัพย์สินอื่น ๆ ทั้งหมด รวมถึงสิ่งต่าง ๆ ที่สามารถทำธุรกรรมได้ หรือทรัพย์สินอื่นที่จับต้องไม่ได้อื่น ๆ ซึ่งเป็นการตีความเพิ่มเติมในปี ค.ศ. 2019 ให้การขโมยหรือโจรกรรมสกุลเงินดิจิทัลเป็นความผิดที่มีโทษทางอาญาอย่างชัดเจนภายใต้กฎหมายอังกฤษ<sup>216</sup>

นอกจากนี้ เมื่อมีการตีความให้สกุลเงินดิจิทัลอยู่ภายในคำจำกัดความของทรัพย์สิน ตามกฎหมายฉบับข้างต้นแล้ว ต่อมาจึงมีการพิจารณาข้อเท็จจริงในบางกรณี ให้การฉ้อโกงเกี่ยวกับสกุลเงินดิจิทัลสามารถเป็นความผิดทางอาญาได้เช่นเดียวกัน ทั้งนี้มีการขยายขอบเขตความรับผิดชอบจนถึงผู้สมรู้ร่วมคิด (Conspiracy) ในกฎหมายอื่น ๆ ที่เกี่ยวกับการฉ้อโกง หรือ กฎหมายว่าด้วยการฉ้อโกง 2006 (เป็นการฉ้อโกงโดยการเป็นตัวแทน)<sup>217</sup>

ทั้งนี้ Theft Act 1968 เป็นกฎหมายในระบบคอมมอนลอว์ซึ่งต้องพิจารณาจากโครงสร้าง ดังนี้

1) องค์ประกอบภายนอก (Actus Reus) กล่าวคือ มีการเอาไปซึ่งทรัพย์สินของผู้อื่น โดยผู้อื่นมิได้ยินยอมและเป็นการเอาไปจากการครอบครองทรัพย์สินของผู้อื่น นอกจากนี้วัตถุแห่งการกระทำความผิดตาม กฎหมายนี้ หมายถึง “ทรัพย์สิน” ซึ่งหมายความรวมถึงเงิน ทรัพย์สินอื่น ๆ ที่เป็นสังหาริมทรัพย์ สิทธิเรียกร้องซึ่งเป็นวัตถุที่ไม่มีรูปร่างทั้งหลาย<sup>218</sup> แต่ไม่รวมถึงอสังหาริมทรัพย์ หรือสิ่งประกอบเป็นอสังหาริมทรัพย์<sup>219</sup>

<sup>216</sup> Laura Douglas, **The Virtual Currency Regulation Review: United Kingdom**, Retrieved November 27, 2021 from <https://thelawreviews.co.uk/title/the-virtual-currency-regulation-review/united-kingdom>

<sup>217</sup> *Ibid.*

<sup>218</sup> Theft Act section 4 (1) “Property” includes money and all other property, real or personal, including things in action and other intangible property.

<sup>219</sup> Theft Act section 4 (2) “A person cannot steal land, or things forming part of land and severed from it by him or by his directions, except in the following cases, that is to say—”

2) องค์ประกอบภายใน (Mens Rea) กล่าวคือ ผู้กระทำมีเจตนาที่จะพรากทรัพย์สินไปจากผู้อื่นอันมีลักษณะเป็นการตัดกรรมสิทธิ์จากเจ้าของเดิมเป็นการถาวร<sup>220</sup> และแม้แต่กรณีที่บุคคลที่เอาทรัพย์สินของผู้อื่นไปโดยไม่มีเจตนาทำให้ผู้อื่นต้องสูญเสียทรัพย์สินนั้นอย่างถาวร แต่หากผู้กระทำมีเจตนาปฏิบัติต่อทรัพย์สินเสมือนเป็นของตนเอง โดยไม่คำนึงถึงสิทธิของผู้อื่น เช่น การยืมหรือการให้ยืมในช่วงเวลาหนึ่งที่มีลักษณะเช่นเดียวกับการเอาไป หรือการจำหน่ายจ่ายโอนโดยเปิดเผย<sup>221</sup> ก็ถือว่ามีเจตนาพรากทรัพย์สินนั้นไปจากผู้อื่นได้เช่นกัน นอกจากนี้ในกรณีที่มีการครอบครองหรือควบคุมทรัพย์สินไม่ว่าจะโดยชอบด้วยกฎหมายหรือไม่ก็ตามซึ่งทรัพย์สินของบุคคลอื่น ภายได้เงื่อนไขที่ต้องนำกลับมาคืน แต่ไม่อาจจะทำได้ และการกระทำนั้นได้เป็นไปเพื่อประโยชน์ของตนเอง และไม่มีอำนาจกระทำ การกระทำดังกล่าวก็ถือเป็นการปฏิบัติต่อทรัพย์สินนั้นเสมือนเป็นของตนเอง โดยไม่คำนึงถึงสิทธิของผู้อื่นเช่นกัน<sup>222</sup>

นอกจากนี้ “เจตนา” อันเป็นองค์ประกอบภายในยังต้องประกอบด้วย มูลเหตุจูงใจพิเศษ คือเจตนาโดยทุจริต ซึ่งไม่ใช่กรณีดังต่อไปนี้<sup>223</sup>

<sup>220</sup> Theft Act section 6 “With the intention of permanently depriving the other of it”.

<sup>221</sup> Theft Act section 6 (1) A person appropriating property belonging to another without meaning the other permanently to lose the thing itself is nevertheless to be regarded as having the intention of permanently depriving the other of it if his intention is to treat the thing as his own to dispose of regardless of the other’s rights; and a borrowing or lending of it may amount to so treating it if, but only if, the borrowing or lending is for a period and in circumstances making it equivalent to an outright taking or disposal.

<sup>222</sup> Theft Act section 6 (2) Without prejudice to the generality of subsection (1) above, where a person, having possession or control (lawfully or not) of property belonging to another, parts with the property under a condition as to its return which he may not be able to perform, this (if done for purposes of his own and without the other’s authority) amounts to treating the property as his own to dispose of regardless of the other’s rights.

<sup>223</sup> Theft Act section 2 (1) A person’s appropriation of property belonging to another is not to be regarded as dishonest—

- 1) ถ้าเอาทรัพย์สินไปเพื่อตนเองหรือผู้อื่น โดยเชื่อว่าตนมีสิทธิตามกฎหมาย
- 2) ถ้าผู้เอาทรัพย์สินไปเชื่อว่าเจ้าของได้ยินยอม ถ้าเจ้าของได้รู้ถึงการเอาไป
- 3) ถ้าผู้เอาทรัพย์สินไปเชื่อว่าทรัพย์สินนั้นไม่อาจหาพบ หรือไม่สามารถติดตามได้แล้ว เว้นแต่เป็นกรณีที่ทรัพย์สินนั้นได้มาอยู่กับผู้กระทำความผิดในฐานะของผู้ดูแลทรัพย์สินของบุคคลอื่นหรือเป็นตัวแทน

กฎหมายฉบับนี้ได้นิยามความหมายของคำว่า เป็นความผิดที่ผู้กระทำความผิดโดยทุจริตในการเอาไปซึ่งทรัพย์สินของผู้อื่น ในลักษณะที่เป็นการเอาไปอย่างถาวร ไม่ว่าจะเป็นการเอาไปเพื่อตนเองหรือเอาไปให้ผู้อื่นก็ตาม<sup>224</sup> ทั้งนี้คำว่า “ทรัพย์สิน” ซึ่งเป็นวัตถุอันเป็นองค์ประกอบ

(a) if he appropriates the property in the belief that he has in law the right to deprive the other of it, on behalf of himself or of a third person; or

(b) if he appropriates the property in the belief that he would have the other's consent if the other knew of the appropriation and the circumstances of it; or

(c) (except where the property came to him as trustee or personal representative) if he appropriates the property in the belief that the person to whom the property belongs cannot be discovered by taking reasonable steps.

(2) A person's appropriation of property belonging to another may be dishonest notwithstanding that he is willing to pay for the property.

<sup>224</sup> Theft Act 1968 Section 1 Basic definition of theft.

(1) A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and “thief” and “steal” shall be construed accordingly.

(2) It is immaterial whether the appropriation is made with a view to gain, or is made for the thief's own benefit.

ความผิดนี้ หมายถึง เงิน วัตถุที่สามารถจับต้องได้ สิทธิเรียกร้อง รวมถึงวัตถุที่ไม่มีรูปร่าง<sup>225</sup> จึงนำไปปรับใช้กับสกุลเงินดิจิทัล ซึ่งเป็นวัตถุที่ไม่มีรูปร่างแต่มีมูลค่า และถูกพรางหรือขโมยไปได้<sup>226</sup>

ตัวอย่างคดีความผิดที่เกี่ยวกับการ Hack/Theft สกุลเงินดิจิทัลที่ใช้ Theft Act 1968

1) ในปี ค.ศ. 2017 มีคดีความของชายคนหนึ่งทำการโจรกรรม Bitcoin จากบัญชีของผู้เสียหายด้วยวิธีการเจาะระบบ (Hacker) หลายบัญชีเป็นจำนวนประมาณ 9,000 ปอนด์ ต่อมาศาลได้มีการพิพากษาลงโทษชายผู้นั้นให้จำคุกและสั่งให้ยึดเงินเสมือนไว้ทั้งหมดเกือบหนึ่งล้านปอนด์เพื่อคืนให้กับผู้เสียหายเป็นไปตามกฎหมาย The Proceeds of Crime Act 2002 (POCA)<sup>227</sup>

2) เมื่อวันที่ 22 มกราคม พ.ศ. 2561 ผู้บุกรุกสวมหน้ากากได้ตะประตู่บ้านของแดนนี่ แอสตันและเอมี เจย์ ซึ่งเป็นกรรมการในบริษัท Aston Digital Currencies Ltd. โดยเข้าไปขโมยสองสามสิบล้านปอนด์ด้วยอาวุธปืน และทำร้ายร่างกายนายแอสตันด้วยการตีที่ศีรษะและบังคับให้ส่งบิตคอยน์<sup>228</sup>

3) คดีนี้กล่าวถึงการโจรกรรมสกุลเงินดิจิทัลที่ชื่อ Ethereum Classic (ETC) ได้ถูกโจมตีถึง 3 ครั้ง ในเดือนสิงหาคม 2020 คิดเป็น หรือ 51% ในเครือข่ายบล็อกเชนของ ETC โดยพบว่าผู้กระทำความผิดได้โอนแลกเปลี่ยน ETC มากกว่า 807,000 ยังบัญชีผู้รับหลายบัญชี โดยไม่สามารถระบุว่าเป็นการโอนมาจาก Exchange ใด<sup>229</sup>

<sup>225</sup> Theft Act 1968 Section 4 (1) “Property”.

(1) “Property” includes money and all other property, real or personal, including things in action and other intangible property.

<sup>226</sup> Alex Taylor and Micheal O’ Flynn, *op. cit.*, p. 163.

<sup>227</sup> The Guardian, **Bitcoin Worth £900,000 Seized from Hacker to Compensate Victims**, Retrieved March 4, 2021 from <https://www.theguardian.com/technology/2019/aug/23/bitcoin-seized-hacker-grant-west-uk-compensate-victims>

<sup>228</sup> Andrew Ffrench, **Gang Targeting Bitcoin Traders Fled Empty-handed**, Retrieved March 12, 2021 from <https://www.oxfordmail.co.uk/news/15907000.gangtargeting-bitcoin-traders-fled-empty-handed/>

<sup>229</sup> Rahman Ravelli, **Cryptocurrency: Theft and Asset Recovery**, Retrieved April 5, 2021 from <https://www.lexology.com/library/detail.aspx?g=db7e8959-b309-4495-8b3e-200124dd07fb>

3) บริษัทประกันภัยถูกเจาะระบบข้อมูลในซอฟต์แวร์ แฮ็กเกอร์ได้เรียกค่าไถ่เป็น Bitcoin จำนวน 950,000 ดอลลาร์ เพื่อแลกกับรักษาข้อมูลของบริษัทไว้ จากการตรวจสอบพบว่า Bitcoin ที่บริษัทยอมจ่ายตามแฮ็กเกอร์เรียกร้อยนั้น ถูกโอนไปยังอีกหลายบัญชีโดยผ่านศูนย์ซื้อขาย Bitfinex คดีดังกล่าวศาลได้ออกคำสั่งอายัด Bitcoin ไว้โดยศาลตีความว่าสกุลเงินดิจิทัลเป็นทรัพย์สินประเภทหนึ่ง<sup>230</sup> ซึ่งสอดคล้องกับแนวทางของ The UK Taskforce’s Legal Statement ที่มองว่า Cryptoasset เป็นทรัพย์สินได้เช่นเดียวกัน

ดังนั้นความผิดที่เป็นการขโมยสกุลเงินดิจิทัลในประเทศอังกฤษได้ปรับใช้กับ The Theft Act 1968 ได้ เนื่องจากวัตถุอันเป็นองค์ประกอบความผิดฐานขโมยในมาตรา 4 (1) ได้กำหนดไว้ว่าเป็น Property หมายถึงทรัพย์สินและหมายความรวมถึงสกุลเงินดิจิทัลด้วย อย่างไรก็ตามสำหรับประเทศไทยการตีความให้สกุลเงินดิจิทัลเป็นทรัพย์สินเช่นเดียวกับกฎหมายของประเทศอังกฤษจะต้องพิจารณาองค์ประกอบความผิดฐานลักทรัพย์ตามกฎหมายไทยนั้นสามารถนำมาใช้กับทรัพย์สินได้หรือไม่ ไม่อาจปรับความผิดฐานนี้ได้กับประมวลกฎหมายอาญา เนื่องจากประมวลกฎหมายอาญาได้กำหนดไว้อย่างชัดเจนว่าวัตถุอันเป็นองค์ประกอบความผิดฐานลักทรัพย์และความผิดฐานอื่นที่มีลักทรัพย์เป็นพื้นฐานนั้นต้องว่าเป็น “ทรัพย์” ซึ่งกฎหมายไทยได้ให้นิยามไว้ว่าเป็น วัตถุที่มีรูปร่าง ดังนั้นความเป็นทรัพย์สินตาม the Theft Act 1968 จึงไม่สามารถนำมาปรับใช้กับองค์ประกอบความผิดฐานลักสกุลเงินดิจิทัลตามประมวลกฎหมายอาญาได้

### 3.2.3.2 The Computer Misuse Act 1990

สำหรับความผิดกรณี Cryptojacking ในประเทศอังกฤษอาจปรับใช้ได้กับ The Computer Misuse Act 1990<sup>231</sup> เนื่องจากเป็นความผิดที่เกี่ยวข้องกับคอมพิวเตอร์ The Computer Misuse Act 1990 ซึ่งได้กำหนดความผิดไว้ 3 กรณี ดังนี้

1) ความผิดกรณีการเข้าสู่ระบบคอมพิวเตอร์โดยปราศจากอำนาจ (Unauthorized Access to Computer Material)<sup>232</sup> กล่าวคือ บุคคลมีความผิดเมื่อเข้าถึงระบบ

<sup>230</sup> In the High Court of Justice Business & Property Courts of England and Wales Commercial Court (QBD), Retrieved January 1, 2023 from <https://www.judiciary.uk/wp-content/uploads/2020/02/AA-v-Persons-Unknown-summary-case-note-SB-amended.pdf>

<sup>231</sup> Domhnall Carlin, Jonah Burgess, Philip OKane, and Sakir Sezer, “You could be Mine(d): The Rise of Cryptojacking,” *IEEE Security & Privacy Magazine* 99 (2019): 1.

<sup>232</sup> The Computer Misuse Act 1990 section 1

คอมพิวเตอร์หรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์ที่มีระบบป้องกันความปลอดภัยโดยปราศจากอำนาจ ซึ่งขณะกระทำนั้นผู้นั้นรู้อยู่แล้วว่าได้กระทำโดยไม่มีอำนาจ การกระทำดังกล่าวเป็นความผิดตาม มาตรานี้โดยไม่จำเป็นที่ผู้กระทำต้องมีจุดมุ่งหมายว่าจะเข้าไปยังโปรแกรม ข้อมูล หรือโปรแกรมหรือ ข้อมูลที่เก็บไว้ในคอมพิวเตอร์เครื่องใดเครื่องหนึ่งโดยเฉพาะ

2) ความผิดกรณีการเข้าถึงโดยไม่ได้รับอนุญาตโดยมีเจตนาที่จะกระทำ หรืออำนวยความสะดวกในการกระทำความผิดเพิ่มเติม (Unauthorised Access with Intent to Commit or Facilitate Commission of Further Offences)<sup>233</sup>

(1) A person is guilty of an offence if—

(a) he causes a computer to perform any function with intent to secure access to any program or data held in any computer, or to enable any such access to be secured;

(b) the access he intends to secure [F2, or to enable to be secured,] is unauthorised; and

(c) he knows at the time when he causes the computer to perform the function that that is the case.

(2) The intent a person has to have to commit an offence under this section need not be directed at—

(a) any particular program or data;

(b) a program or data of any particular kind; or

(c) a program or data held in any particular computer.

(3) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding two years or to a fine or to both.

<sup>233</sup> Computer Misuse Act 1990 section 2

บุคคลจะมีความผิดตามมาตรา<sup>๑๑</sup>หากได้กระทำความผิดตามข้อ 1 ที่กล่าวมาข้างต้น โดยมีเจตนากระทำความผิดหรือผู้กระทำได้ให้ความสะดวกในการกระทำความผิดไม่ว่าจะเป็นการกระทำความผิดของตนหรือของผู้อื่นและความผิดที่จะกล่าวต่อไปนี้ ให้ถือว่าผู้กระทำความผิด

---

(1) A person is guilty of an offence under this section if he commits an offence under section 1 above (“the unauthorised access offence”) with intent—

- (a) to commit an offence to which this section applies; or
- (b) to facilitate the commission of such an offence (whether by himself or by any other person);

and the offence he intends to commit or facilitate is referred to below in this section as the further offence.

(2) This section applies to offences—

- (a) for which the sentence is fixed by law; or
- (b) for which a person who has attained the age of twenty-one years (eighteen in relation to England and Wales) and has no previous convictions may be sentenced to imprisonment for a term of five years (or, in England and Wales, might be so sentenced but for the restrictions imposed by section 33 of the Magistrates’ Courts Act 1980).

(3) It is immaterial for the purposes of this section whether the further offence is to be committed on the same occasion as the unauthorised access offence or on any future occasion.

(4) A person may be guilty of an offence under this section even though the facts are such that the commission of the further offence is impossible.

(5) A person guilty of an offence under this section shall be liable—

- (a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

- (b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

- (c) on conviction on indictment, to imprisonment for a term not exceeding five years or to a fine or to both.

เช่นเดียวกับผู้ที่กระทำความผิดที่ตนช่วยเหลือ มาตรานี้ใช้กับผู้กระทำความผิด ที่มีอายุซึ่งบุคคลซึ่งมีอายุครบ 21 ปี (18 ปี สำหรับอังกฤษและเวลส์) และหากไม่มีการกระทำความผิดใด ๆ มาก่อนอาจถูกพิพากษาให้จำคุกเป็นเวลา 5 ปี ผู้กระทำความผิดตามมาตรานี้ต้องรับโทษในอังกฤษและเวลส์ จำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินกฎหมายสูงสุด หรือทั้งจำทั้งปรับ แต่หากได้กระทำความผิดในสก๊อตแลนด์ จะต้องรับโทษจำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินกฎหมายสูงสุดหรือทั้งจำทั้งปรับ หรืออาจได้รับโทษจำคุกไม่เกิน 5 ปี หรือปรับ หรือทั้งจำทั้งปรับ

3) ความผิดกรณีไม่ได้รับอนุญาตโดยมีเจตนาทำให้เสียหาย หรือโดยประมาทเลินเล่อในความบกพร่อง การทำงานของคอมพิวเตอร์ (Unauthorised Acts with Intent to Impair, or with Recklessness as to Impairing, Operation of Computer)<sup>234</sup>

<sup>234</sup> Computer Misuse Act 1990 section 3

(1) A person is guilty of an offence if—

- (a) he does any unauthorised act in relation to a computer;
- (b) at the time when he does the act he knows that it is unauthorised;

and

(c) either subsection (2) or subsection (3) below applies.

(2) This subsection applies if the person intends by doing the act—

- (a) to impair the operation of any computer;
- (b) to prevent or hinder access to any program or data held in any computer; or
- (c) to impair the operation of any such program or the reliability of any such data; or
- (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.

(3) This subsection applies if the person is reckless as to whether the act will do any of the things mentioned in paragraphs (a) to (d) of subsection (2) above.

(4) The intention referred to in subsection (2) above, or the recklessness referred to in subsection (3) above, need not relate to—

- (a) any particular computer;
- (b) any particular program or data; or

ผู้กระทำความผิดตามมาตรานี้หากไม่ได้รับอนุญาตให้กระทำการเกี่ยวกับคอมพิวเตอร์ในกรณีต่อไปนี้ไม่ว่าจะกระทำโดยเจตนาหรือประมาทก็ตาม ในกรณีดังต่อไปนี้

- (1) เพื่อให้การทำงานของคอมพิวเตอร์เสียหาย
- (2) เพื่อป้องกันหรือขัดขวางการเข้าถึงโปรแกรมหรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์เครื่องใดก็ได้
- (3) เพื่อให้การทำงานของโปรแกรมดังกล่าวเสียหายหรือความน่าเชื่อถือของข้อมูลดังกล่าว
- (4) เพื่อเปิดใช้งานในข้อ (1) – (3) ที่กล่าวมาข้างต้น

ทั้งนี้ความผิดดังกล่าวเป็นความผิดโดยผู้กระทำไม่จำเป็นต้องมีจุดมุ่งหมายว่าจะเข้าไปยังโปรแกรม ข้อมูล หรือโปรแกรมหรือข้อมูลที่เก็บไว้ในคอมพิวเตอร์เครื่องใดเครื่องหนึ่งโดยเฉพาะ และเป็นความผิดแม้กระทำโดยชั่วคราวก็ตาม

ผู้กระทำความผิดตามมาตรานี้จะได้รับโทษที่กระทำในอังกฤษและเวลส์ จำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินกฎหมายสูงสุด หรือทั้งจำทั้งปรับ หากกระทำความผิดในสกอตแลนด์ จำคุกไม่เกิน 12 เดือน หรือปรับไม่เกินสูงสุดตามกฎหมายหรือทั้งจำทั้งปรับ หรือรับโทษจำคุกไม่เกิน 10 ปี หรือปรับ หรือทั้งจำทั้งปรับ

(c) a program or data of any particular kind.

(5) In this section—

(a) a reference to doing an act includes a reference to causing an act to be done;

(b) “act” includes a series of acts;

(c) a reference to impairing, preventing or hindering something includes a reference to doing so temporarily.

(6) A person guilty of an offence under this section shall be liable—

(a) on summary conviction in England and Wales, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(b) on summary conviction in Scotland, to imprisonment for a term not exceeding 12 months or to a fine not exceeding the statutory maximum or to both;

(c) on conviction on indictment, to imprisonment for a term not exceeding ten years or to a fine or to both.

จากความผิดทั้ง 3 กรณีที่ได้กล่าวมาข้างต้นจะเห็นได้ว่าประเทศอังกฤษมองว่า ความผิดรูปแบบ Cryptojacking นั้น สามารถนำมาปรับใช้กับ The Computer Misuse Act 1990 ได้ เนื่องจากมีการกระทำโดยปราศจากอำนาจในการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นและการเข้าถึง นั้นเป็นการกระทำโดยเจตนา จึงความผิดตามที่กำหนดไว้ใน The Computer Misuse Act 1990

### 3.3 หลักกฎหมายในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลของประเทศไทย

#### 3.3.1 สถานะทางกฎหมายของสกุลเงินดิจิทัล

กฎหมายอาญาไม่ได้มีกำหนดสถานะของสกุลเงินดิจิทัลไว้ แต่เมื่อพิจารณาจากลักษณะทางกายภาพและลักษณะการใช้งานของสกุลเงินดิจิทัล จะเห็นได้ว่าสกุลเงินดิจิทัลมีสถานะคือเป็นทั้งทรัพย์สิน เงินตรา และข้อมูลคอมพิวเตอร์ รวมอยู่ในตัวกล่าวคือ เป็นทรัพย์สินเนื่องจาก ลักษณะทางกายภาพเป็นสิ่งที่ไม่มีรูปร่าง ตามความหมายของคำว่า “ทรัพย์สิน” ในประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 138 “หมายความรวมถึงทรัพย์สินและวัตถุไม่มีรูปร่าง ซึ่งอาจมีราคาและอาจถือเอาได้” เป็นเงินตราหรืออาจเรียกได้ว่าเป็นเงินเสมือน เนื่องจากทำหน้าที่เป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการได้ และจากลักษณะการใช้งานสกุลเงินดิจิทัลเป็นข้อมูลคอมพิวเตอร์เนื่องจากจะต้องใช้ผ่านอุปกรณ์อิเล็กทรอนิกส์มีการประมวลผลข้อความที่ปรากฏในระบบคอมพิวเตอร์ นอกจากนี้ยังมีคำพิพากษาศาลฎีกาที่ 4311/2557 ที่วินิจฉัยว่าการพิมพ์ข้อมูลลงในเครื่องคอมพิวเตอร์ถือได้ว่าเป็นการพิมพ์ข้อมูลลง “เอกสาร”<sup>235</sup> โดยอธิบายว่าเครื่องคอมพิวเตอร์ถือเป็นวัตถุอื่นที่ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น จากคำพิพากษาศาลฎีกานี้ มีผลทำให้สิ่งที่เป็ข้อมูลคอมพิวเตอร์มีค่าเทียบเท่ากับเอกสาร ดังนั้นหากสกุลเงินดิจิทัลมีความเป็นข้อมูลคอมพิวเตอร์อยู่ในตัว ก็อาจแปลความได้ว่าสกุลเงินดิจิทัลมีความเป็นเอกสารได้เช่นกัน ดังนั้นเอกสารจึงเป็นอีกสถานะที่ต้องนำมาพิจารณา

ทั้งนี้การกำหนดสถานะสกุลเงินดิจิทัล มีความจำเป็นอย่างยิ่งเนื่องจากสถานะจะเป็นสิ่งที่กำหนดว่านำกฎหมายใดมาปรับใช้และกฎหมายที่เหมาะสมกับสถานะของสกุลเงินดิจิทัลควรเป็นอย่างไร (จะกล่าวต่อไปในบทวิเคราะห์) ดังนั้นจึงควรกำหนดสถานะที่ชัดเจนเพื่อกำหนดแนวทางการควบคุมการกระทำความผิดสกุลเงินดิจิทัลให้ได้อย่างเหมาะสม

<sup>235</sup> มาตรา 1 (7) แห่งประมวลกฎหมายอาญา

### 3.3.2 ความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล

การกระทำความผิดอาญาที่กระทำต่อสกุลเงินดิจิทัลนั้นมีลักษณะเฉพาะที่ต่างจากการกระทำความผิดอาญาที่ได้กระทำต่อวัตถุอื่นทั่วไป เนื่องจากการกระทำความผิดต่อสกุลเงินดิจิทัลนี้ เป็นวัตถุที่ไม่มีรูปร่าง และอยู่ในระบบออนไลน์เท่านั้น จึงจำเป็นต้องเกี่ยวข้องกับเทคโนโลยีและอุปกรณ์ต่าง ๆ ที่ใช้เชื่อมโยงในการเข้าสู่ระบบออนไลน์ จึงหลีกเลี่ยงไม่ได้ที่จะมีความผิดเกี่ยวกับคอมพิวเตอร์ ไม่ว่าจะเป็นกรณีการเจาะระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ การเข้าถึงข้อมูลคอมพิวเตอร์ ไม่ว่าจะเข้าถึงด้วยตนเองหรือผ่านการเชื่อมต่อระยะไกล โดยปราศจากอำนาจและการเข้าถึงข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันของผู้อื่นโดยมิชอบ เช่น การลวงรู้ Password ของผู้อื่นโดยที่เจ้าของไม่ยินยอม แล้วนำมากรอกเพื่อเข้าถึงข้อมูลคอมพิวเตอร์นั้น รวมถึงความผิดฐานทำให้เสียหาย เปลี่ยนแปลงข้อมูลคอมพิวเตอร์โดยมิชอบ เช่น การปล่อยไวรัสทำให้ข้อมูลนั้นไม่สามารถใช้งานได้ และความผิดฐานกระทำให้การทำงานของระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติ คือการชะลอ รบกวน หรือขัดขวางการทำงานของระบบคอมพิวเตอร์<sup>236</sup> โดยระบบคอมพิวเตอร์ถูกควบคุมจากบุคคลอื่น ซึ่งอาจมีสาเหตุจาก เจ้าของระบบไม่ติดตั้งโปรแกรมหรือระบบป้องกันความปลอดภัย ระบบจึงมีช่องโหว่ให้ถูกบุกรุก หรือมีการดาวน์โหลดโปรแกรมที่มี Malware ประเภทที่มีคุณสมบัติในการควบคุมคอมพิวเตอร์เครื่องอื่น เช่น Trojan Horse เป็นต้น

นอกจากนี้ด้วยลักษณะที่สำคัญประการหนึ่งของสกุลเงินดิจิทัลคือ เป็นสิ่งที่มีมูลค่า แม้ว่าจะถูกกำหนดโดยกลุ่มคนที่ใช้ก็ตาม แต่สกุลเงินดิจิทัลก็เป็นที่ยอมรับและถูกนำมาใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้า บริการ หรือแก่งกำไรได้จริง จึงทำให้สกุลเงินดิจิทัลเป็นที่ต้องการหรือถูกขโมยไปได้ ซึ่งการขโมยนี้อาจเป็นความผิดตามประมวลกฎหมายอาญาในฐานความผิดลักทรัพย์ ฐานฉ้อโกงทรัพย์ ฐานชิงทรัพย์ ฐานปล้นทรัพย์ ทั้งนี้ความผิดที่กล่าวมาเป็นความผิดที่มีองค์ประกอบความผิดเดียวกัน คือ การเอาไปซึ่งทรัพย์ของผู้อื่นหรือผู้อื่นเป็นเจ้าของรวมอยู่ด้วย แต่ความผิดลักษณะนี้ต่างจากการเข้าถึงข้อมูลคอมพิวเตอร์ กล่าวคือ การเข้าถึงข้อมูลคอมพิวเตอร์ผู้กระทำอาจกระทำโดยไม่กระทบต่อข้อมูลหรือไม่ได้นำข้อมูลออกไป เช่น การทำสำเนา การจดจำข้อมูล การถ่ายภาพข้อมูลจากหน้าจอ เป็นต้น ในขณะที่การขโมยสกุลเงินดิจิทัลผู้กระทำไม่สามารถทำได้โดยการสำเนาหรือถ่ายภาพ เช่นเดียวกับการกระทำต่อข้อมูลคอมพิวเตอร์ แต่ต้องเป็นการเอาสกุลเงินดิจิทัลออกมาจากบัญชีของผู้เสียหาย ซึ่งการเอาไปนั้นเป็นองค์ประกอบความผิดเกี่ยวกับทรัพย์ตามประมวลกฎหมายอาญา และเป็นการกระทำที่กระทบต่อสกุลเงินดิจิทัลของผู้ถือครองโดยตรง และยังรวมถึงความผิดฐานยกยอก

<sup>236</sup> สาวตรี สุขศรี, **กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์** (กรุงเทพมหานคร: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563), หน้า 134.

ทรัพย์อาจเกิดขึ้นกับศูนย์ซื้อขายสินทรัพย์ดิจิทัลที่ยกยอกสกุลเงินดิจิทัลได้เช่นกัน เช่นกรณีที่มีการซื้อขายสกุลเงินดิจิทัลโดยผ่านผู้ประกอบธุรกิจศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Exchange) ซึ่งได้เก็บรักษา Private Key ของลูกค้าได้ทำการโอนสกุลเงินดิจิทัลของลูกค้าออกไปยังกระเป๋าเงินดิจิทัลอื่นที่ไม่ได้มีไว้เพื่อเก็บสกุลเงินดิจิทัลของลูกค้า

นอกจากนี้ยังมีความผิดที่เกี่ยวกับสกุลเงินดิจิทัลที่ได้บัญญัติขึ้นเพื่อเป็นการป้องกันการกระทำอันไม่เป็นธรรมเกี่ยวกับการซื้อขายสินทรัพย์ดิจิทัลตามพระราชกำหนดการประกอบสินทรัพย์ดิจิทัล ไว้อีกส่วนหนึ่ง ซึ่งความผิดตามพระราชกำหนดนี้แม้จะมีขึ้นเพื่อการควบคุมการประกอบธุรกิจซื้อขายสกุลเงินดิจิทัลให้เป็นไปอย่างโปร่งใส ซึ่งมีลักษณะทางกฎหมายแพ่ง แต่หากมีการฝ่าฝืนบทบัญญัติดังกล่าวจะมีการกำหนดโทษทางอาญาไว้เช่นกัน เช่น ความผิดในการบอกกล่าว เผยแพร่ หรือให้คำรับรองข้อความอันเป็นเท็จหรือข้อความที่ก่อให้เกิดความสำคัญผิดอันผลกระทบต่อราคา หรือต่อการตัดสินใจลงทุนในสินทรัพย์ดิจิทัล ความผิดในการปั่นราคาสินทรัพย์ดิจิทัล เป็นต้น

### 3.3.3 กฎหมายเกี่ยวกับการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล

#### 3.3.3.1 พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์

พ.ศ. 2550

ปัจจุบันระบบคอมพิวเตอร์ได้เป็นส่วนสำคัญของการประกอบกิจการและการดำรงชีวิตของมนุษย์ หากมีผู้กระทำความผิดด้วยประการใด ๆ ให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามคำสั่งที่กำหนดไว้หรือทำให้การทำงานผิดพลาดไปจากคำสั่งที่กำหนดไว้ หรือใช้วิธีการใด ๆ เข้าล่วงรู้ข้อมูล แก่ใจ หรือทำลายข้อมูลของบุคคลอื่นโดยมิชอบ หรือใช้ระบบคอมพิวเตอร์เพื่อเผยแพร่ข้อมูลคอมพิวเตอร์อันเป็นเท็จหรือมีลักษณะอันลามกอนาจาร การกระทำความผิดดังกล่าวย่อมก่อให้เกิดความเสียหายต่อเศรษฐกิจ สังคม และความมั่นคงของรัฐ รวมถึงความสงบสุขเรียบร้อยและศีลธรรมอันดีของประชาชน จึงสมควรกำหนดมาตรการเพื่อป้องกันและปราบปรามการกระทำความผิด<sup>237</sup> แต่หลังจากมีการบังคับใช้พระราชบัญญัติดังกล่าวมาประมาณ 10 ปี พบว่า มีบทบัญญัติบางประการที่ไม่เหมาะสมต่อการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ในปัจจุบัน จึงได้มีการแก้ไขปรับปรุงฉบับที่ 2 พ.ศ. 2560 โดยมีการกำหนดบทบัญญัติให้เหมาะสมยิ่งขึ้นและมีการบูรณาการการป้องกันและปราบปรามการกระทำความผิด ตลอดจนให้อำนาจคณะกรรมการเปรียบเทียบความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

<sup>237</sup> เหตุผลในการประกาศใช้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

และแก้ไขเพิ่มเติมอำนาจหน้าที่ของพนักงานเจ้าหน้าที่ให้เหมาะสมยิ่งขึ้น เพื่อเป็นการส่งเสริมพัฒนา เศรษฐกิจดิจิทัลของประเทศและสร้างความเชื่อมั่นในด้านมาตรฐานและมาตรการในการรักษาความ มั่นคงปลอดภัยของระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์<sup>238</sup> จึงเป็นพระราชบัญญัติว่าการกระทำ ผิดเกี่ยวกับคอมพิวเตอร์ฉบับที่บังคับใช้อยู่จนถึงปัจจุบัน

พระราชบัญญัติดังกล่าวว่าด้วยเรื่องที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับการใช้ คอมพิวเตอร์ซึ่งการทำธุรกรรมสกุลเงินดิจิทัลจำเป็นต้องใช้คอมพิวเตอร์หรืออุปกรณ์อิเล็กทรอนิกส์ อื่น ๆ ในการเชื่อมต่อกับอินเทอร์เน็ต ดังนั้นจึงจะต้องพิจารณาว่าพระราชบัญญัตินี้มีบทบัญญัติใดที่ เกี่ยวข้องกับการกระทำความผิดทางอาญาที่เกี่ยวกับสกุลเงินดิจิทัล และจะนำไปปรับกับความผิดที่ เกิดขึ้นได้มากน้อยเพียงใด ทั้งนี้จะขอจำแนกตามรูปแบบการกระทำความผิดที่ได้กล่าวไว้ในบทที่ 2 ดังนี้

1) กรณีการขโมยสกุลเงินดิจิทัล แม้สกุลเงินดิจิทัลจะเป็นวัตถุไม่มีรูปร่าง ซึ่งอยู่ในรูปแบบของอิเล็กทรอนิกส์ แต่สกุลเงินดิจิทัลก็อาจถูกขโมยได้เช่นเดียวกับวัตถุอื่นทั่วไป ซึ่งวิธีการขโมยจะแตกต่างจากการเอาไปซึ่งวัตถุที่มีรูปร่างและแม้จะเป็นการขโมยวัตถุที่ไม่มีรูปร่าง เช่นเดียวกันการขโมยสกุลเงินดิจิทัลก็ยังคงมีความแตกต่างและมีวิธีการเฉพาะเนื่องจากจะต้องกระทำ ผ่านอุปกรณ์อิเล็กทรอนิกส์ เช่น คอมพิวเตอร์ Smartphone Tablet ผู้กระทำความผิดต้องใช้วิธีการทาง อิเล็กทรอนิกส์ในการเข้าถึงระบบหรือข้อมูลเกี่ยวกับสกุลเงินดิจิทัลของผู้เสียหาย แล้วโอนสกุลเงิน ดิจิทัลของผู้เสียหายไปเป็นของตนเองหรือผู้อื่นโดยมิชอบ ซึ่งการกระทำความผิดดังกล่าวจะเป็น ความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 หรือไม่ จำเป็นต้องเข้าใจคำว่า “ระบบคอมพิวเตอร์” และ “ข้อมูลคอมพิวเตอร์” ซึ่งสองสิ่งนี้เป็นวัตถุแห่งการ กระทำอันเป็นองค์ประกอบความผิดตามพระราชบัญญัตินี้

ระบบคอมพิวเตอร์ (Computer System) หมายถึง อุปกรณ์หรือชุด อุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน และได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่น ใด กับแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ทั้งนี้การ กระทำความผิดที่เกี่ยวกับสกุลเงินดิจิทัลเป็นการทำธุรกรรมที่สามารถทำได้ในระบบออนไลน์โดยใช้ คอมพิวเตอร์เป็นอุปกรณ์เชื่อมต่อเพื่อเข้าถึงข้อมูลที่อยู่ในระบบได้ ดังนั้นจึงอาจมีกรณีการเจาะระบบ คอมพิวเตอร์หรือการแฮ็กเข้าระบบคอมพิวเตอร์เพื่อเข้าถึงบัญชีที่เก็บสกุลเงินดิจิทัลของผู้อื่นโดยมิ ชอบได้

<sup>238</sup> สภานิติบัญญัติแห่งชาติ, เอกสารประกอบการพิจารณา ร่างพระราชบัญญัติว่าด้วยการ กระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่..) พ.ศ.... (คณะรัฐมนตรีเป็นผู้เสนอ) อ.พ28/2559. (เอกสารไม่ตีพิมพ์เผยแพร่)

ข้อมูลคอมพิวเตอร์ (Computer Data) คือ ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด บรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย

นอกจากนี้คำว่าข้อมูลคอมพิวเตอร์ยังอาจรวมถึงสกุลเงินดิจิทัลได้ เนื่องจากพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 ได้ให้ความหมายของสกุลเงินดิจิทัลหรือคริปโทเคอร์เรนซีไว้ว่า หมายถึง “หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นตัวกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และให้หมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นใดตามที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด”

จากการให้ความหมายดังกล่าวสกุลเงินดิจิทัลจึงมีความเป็น “ข้อมูลคอมพิวเตอร์” อยู่ในตัว ดังนั้นทำให้การกระทำความผิดต่อข้อมูลคอมพิวเตอร์อาจเป็นการกระทำความผิดต่อสกุลเงินดิจิทัลซึ่งเป็นความผิดตามพระราชบัญญัตินี้ด้วย

(1) บทบัญญัติที่เกี่ยวข้องกับการการขโมยสกุลเงินดิจิทัล มีดังนี้

ก) มาตรา 5 ความผิดฐานเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ บัญญัติว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งระบบคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน ต้องระวางโทษ.....”

องค์ประกอบความผิด

(ก) การเข้าถึง หมายถึง การกระทำใด ๆ ที่เป็นการทำให้สามารถเข้าไปดำเนินการต่าง ๆ เกี่ยวกับระบบคอมพิวเตอร์นั้นได้ โดยมีได้ทั้ง (1) ในระดับกายภาพหรือทางไกล เช่น กรณีที่มีการกำหนดรหัสผ่าน (Password) เพื่อป้องกันมิให้บุคคลอื่นใช้เครื่องคอมพิวเตอร์และผู้กระทำความผิดดำเนินการด้วยวิธีใดวิธีหนึ่งเพื่อให้ได้รหัสผ่านนั้นมาและสามารถเข้าควบคุมหรือใช้อำนาจบังคับบัญชาคอมพิวเตอร์เครื่องนั้นได้เสมือนเป็นผู้ทรงสิทธิ หรือ (2) เข้าถึงระบบคอมพิวเตอร์ซึ่งอยู่ในระยะทางที่ไกลแต่สามารถที่จะควบคุมระบบคอมพิวเตอร์ได้<sup>239</sup> ก็คือการเจาะเข้าระบบคอมพิวเตอร์ที่เรียกกันว่า Hacking or Cracking<sup>240</sup> นอกจากนั้นยังหมายถึงการเข้าถึงระบบคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้ ดังนั้นจึงหมายถึง การเข้าถึงอุปกรณ์ต่าง ๆ ที่ประกอบ

<sup>239</sup> ธนากร อุษานิชย์, “การจารกรรมข้อมูลทางคอมพิวเตอร์กับความรับผิดทางอาญา,” **วารสารเทคโนโลยีสารสนเทศ** 6, 12 (กรกฎาคม-ธันวาคม 2553): 61.

<sup>240</sup> สราวุธ ปิตียาศักดิ์, **คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ (ฉบับที่ 2) พ.ศ. 2560**, พิมพ์ครั้งที่ 2 (กรุงเทพมหานคร: นิติธรรม, 2561), หน้า 59.

ขึ้นเป็นเครื่องคอมพิวเตอร์ที่สามารถจับต้องได้ เช่น จอภาพ คีย์บอร์ด รวมถึงส่วนประกอบต่าง ๆ ของคอมพิวเตอร์ ที่มีไว้เพื่อรับและบันทึกข้อมูลในระบบเพื่อส่งต่อหรือโอนให้บุคคลอื่น ในเรื่องวิธีการเข้าถึงนั้นให้รวมไปถึงการกระทำใด ๆ ไม่ว่าจะเป็นการเข้าถึงโดยผ่านทางเครือข่ายสาธารณะ เช่น อินเทอร์เน็ตที่เป็นการเชื่อมโยงระหว่างเครือข่ายหลาย ๆ เครือข่ายเข้าด้วยกันและยังรวมไปถึงการเข้าถึงโดยผ่านระบบเครือข่ายเดียวกันด้วยก็ได้ เช่น ระบบ LAN (Local Area Network) เป็นเครือข่ายที่เชื่อมต่อระหว่างคอมพิวเตอร์ที่อยู่ในพื้นที่ใกล้ ๆ กันและยังรวมถึงการเข้าถึงโดยการติดต่อสื่อสารแบบไร้สาย (Wireless Communication) ตลอดจน เครือข่ายส่วนบุคคล (Personal Area Network)<sup>241</sup>

(ข) ระบบคอมพิวเตอร์ หมายความว่า อุปกรณ์หรือชุดอุปกรณ์ของคอมพิวเตอร์ที่เชื่อมการทำงานเข้าด้วยกัน โดยได้มีการกำหนดคำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใด และแนวทางปฏิบัติงานให้อุปกรณ์หรือชุดอุปกรณ์ทำหน้าที่ประมวลผลข้อมูลโดยอัตโนมัติ ฉะนั้นระบบคอมพิวเตอร์จึงหมายถึง อุปกรณ์หรือชุดอุปกรณ์ในทางวิทยาศาสตร์ ได้แก่ ฮาร์ดแวร์ตัวเครื่อง และซอฟต์แวร์หรือโปรแกรมที่มีการทำงานประมวลผลข้อมูลโดยอัตโนมัติได้แล้ว ระบบคอมพิวเตอร์อาจเป็นเครื่องคอมพิวเตอร์เพียงเครื่องเดียวหรือหลายเครื่องเชื่อมกันผ่านระบบเครือข่ายโดยมีลักษณะการทำงานโดยอัตโนมัติตามซอฟต์แวร์หรือโปรแกรมที่กำหนดไว้<sup>242</sup>

(ค) มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมิได้มีไว้สำหรับตน หมายถึง ก่อนการเข้าใช้ระบบคอมพิวเตอร์เครื่องหรืออุปกรณ์ได้มีการกำหนดให้ผู้ใช้กรอกชื่อผู้ใช้งาน (Username) และรหัสผ่าน (Password) หรือมีการสแกนลายนิ้วมือหรือมีการติดตั้งไพรวัลล แต่หากเจ้าของเครื่องไม่ได้ตั้งมาตรการป้องกันใด ๆ ไว้ แล้วมีผู้อื่นหรือใครก็ตามสามารถเข้าใช้ระบบคอมพิวเตอร์เครื่องนั้นได้ทันที ผู้ที่เข้าถึงไม่มีความผิดตามมาตรานี้ การฝ่ามาตรการป้องกันการเข้าถึง อาจทำได้วิธีการเดารหัสผ่านได้ถูกต้อง หรือแอบจดจำรหัสผ่านของผู้อื่นมาใช้เพื่อการเข้าถึงก็ได้<sup>243</sup>

(ง) โดยมีขอบ หมายถึง การเข้าถึงระบบคอมพิวเตอร์โดยปราศจากสิทธิโดยชอบธรรม (Without Right) หรือไม่มีสิทธิกระทำได้ รวมถึงการอนุญาตให้เข้าได้บางเวลาหรือตามเวลาที่กำหนดแต่มีการเข้าถึงเกินจากที่ได้รับอนุญาต

<sup>241</sup> พรเพชร วิชิตชลชัย, คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 (กรุงเทพมหานคร: สำนักงานศาลยุติธรรม, 2550).

<sup>242</sup> เรื่องเดียวกัน.

<sup>243</sup> คณาธิป ทองรวีวงศ์, กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1 (กรุงเทพมหานคร: นิติธรรม, 2563), หน้า 120.

(จ) โดยเจตนา เป็นองค์ประกอบภายใน มีความหมาย เช่นเดียวกับเจตนาทางอาญาตามประมวลกฎหมายอาญา มาตรา 59 กล่าวคือ ผู้กระทำรู้สำนึกในการกระทำของตนว่าเป็นการเข้าถึงและรู้ข้อเท็จจริงอันเป็นองค์ประกอบความผิดว่า ระบบคอมพิวเตอร์นั้นมีมาตรการการเข้าถึงโดยเฉพาะและมาตรการนั้นมีได้มีไว้สำหรับตน เข้าองค์ประกอบได้ ไม่ว่าจะผู้กระทำจะมีวัตถุประสงค์อื่นหรือมีมูลเหตุจูงใจใดก็ตาม นอกจากนี้ความผิดฐานดังกล่าวไม่ได้มีการกำหนดองค์ประกอบความผิดเกี่ยวกับการกระทำอื่นหลังจากการเข้าถึงไว้<sup>244</sup> ดังนั้นเมื่อมีการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบ แม้ไม่ได้เข้าถึงเพื่อกระทำความผิดอื่นต่อ ก็เป็นความผิดสำเร็จทันทีตามมาตรานี้

ข) มาตรา 7 ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 บัญญัติว่า “ผู้ใดเข้าถึงโดยมิชอบซึ่งข้อมูลคอมพิวเตอร์ที่มีมาตรการป้องกันการเข้าถึงโดยเฉพาะและมาตรการนั้นมีได้มีไว้สำหรับตน ต้องระวางโทษ.....”

#### องค์ประกอบความผิด

ความผิดฐานนี้มีความหมายเช่นเดียวกับความผิดฐานเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ตามมาตรา 5 แต่แตกต่างกันตรงที่มาตรา 5 เป็นการเข้าถึงระบบคอมพิวเตอร์ ส่วนมาตรา 7 เป็นการเข้าถึงข้อมูลคอมพิวเตอร์ ในที่นี้จึงขออธิบายเฉพาะความหมายคำว่า ข้อมูลคอมพิวเตอร์ ซึ่งหมายความว่า ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึงข้อมูลอิเล็กทรอนิกส์ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ด้วย ซึ่งพระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544 มาตรา 4 ได้นิยามคำว่า “ข้อมูลอิเล็กทรอนิกส์” หมายความว่า ข้อความที่ได้สร้าง ส่ง รับ เก็บรักษา หรือประมวลผลด้วยวิธีการทางอิเล็กทรอนิกส์ เช่น วิธีการแลกเปลี่ยนข้อมูลทางอิเล็กทรอนิกส์ จดหมายอิเล็กทรอนิกส์ โทรเลข โทรพิมพ์ หรือโทรสาร

ดังนั้น “ข้อมูลอิเล็กทรอนิกส์” ย่อมอยู่ในความหมายของข้อมูลคอมพิวเตอร์ข้างต้น เพื่อให้ครอบคลุมถึงข้อมูลประเภทอื่น ๆ ที่อาจสร้างด้วยวิธีการทางอิเล็กทรอนิกส์อื่น ๆ ในอนาคตที่ไม่ใช่เทคโนโลยีคอมพิวเตอร์ก็ได้<sup>245</sup> และข้อมูลคอมพิวเตอร์ตามพระราชบัญญัตินี้ย่อมหมายถึงข้อมูลที่จัดเก็บอยู่ในระบบคอมพิวเตอร์เท่านั้น ไม่รวมถึงข้อมูลที่ถูกบันทึกไว้ในสื่อบันทึกข้อมูลอื่น เช่น แผ่นซีดี แฟลชไดรฟ์ แต่หากนำสื่อบันทึกข้อมูลดังกล่าวไป

<sup>244</sup> เรื่องเดียวกัน, หน้า 121.

<sup>245</sup> พรเพชร วิชิตชลชัย, เรื่องเดิม.

เชื่อมต่อกับคอมพิวเตอร์แล้ว ข้อมูลนั้นก็จะเป็นข้อมูลคอมพิวเตอร์ที่ได้รับการคุ้มครองตามมาตรา<sup>246</sup>

นอกจากนี้ ผู้กระทำความผิดฐานเข้าถึงระบบคอมพิวเตอร์หรือเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ตามมาตรา 5 หรือมาตรา 7 ยังอาจต้องรับโทษหนักขึ้น หากเข้าเงื่อนไขที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 12<sup>247</sup> ดังนี้

(ก) กรณี กระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ

(ข) กรณี กระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ เป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น

(ค) กรณี กระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ

<sup>246</sup> *เรื่องเดียวกัน.*

<sup>247</sup> มาตรา 12 “ถ้าการกระทำความผิดตามมาตรา 5 มาตรา 6 มาตรา 7 มาตรา 8 หรือมาตรา 11 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงเจ็ดปี และปรับตั้งแต่สองหมื่นบาทถึงหนึ่งแสนสี่หมื่นบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งเป็นเหตุให้เกิดความเสียหายต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ดังกล่าว ต้องระวางโทษจำคุกตั้งแต่หนึ่งปีถึงสิบปี และปรับตั้งแต่สองหมื่นบาทถึงสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 เป็นการกระทำต่อข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ตามวรรคหนึ่ง ต้องระวางโทษจำคุกตั้งแต่สามปีถึงสิบห้าปี และปรับตั้งแต่หกหมื่นบาทถึงสามแสนบาท

ถ้าการกระทำความผิดตามวรรคหนึ่งหรือวรรคสามโดยมิได้มีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย แม้มิได้เจตนาฆ่าก็ตาม

ค) วิเคราะห์กรณีการขโมยสกุลเงินดิจิทัลกับความผิดฐานเข้าถึงระบบคอมพิวเตอร์และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ ซึ่งแบ่งวิธีการขโมยออกเป็น 3 ขั้นตอน ดังนี้

ขั้นตอนที่ 1 คือ การเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นเพื่อเข้าไปขโมยสกุลเงินดิจิทัล การเข้าถึงระบบคอมพิวเตอร์นั้นไม่ว่าจะเป็นการเข้าถึงโดยทางกายภาพ โดยการกรอกชื่อผู้ใช้และรหัสผ่านได้ถูกต้องหรือเข้าถึงด้วยการเจาะระบบคอมพิวเตอร์ที่มีมาตรการป้องกันโดยผู้กระทำอาจใช้คอมพิวเตอร์อีกเครื่องหนึ่งแฮ็กเข้าไปยังระบบคอมพิวเตอร์ของผู้เสียหาย โดยไม่ได้รับอนุญาต การกระทำดังกล่าวเป็นการฝ่ามาตรการป้องกันการเข้าถึงโดยเฉพาะแล้ว ผู้กระทำมีความผิดฐานเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบตาม มาตรา 5 แม้ผู้กระทำจะไม่ได้กระทำการใด ๆ ต่อหลังจากการเข้าถึงระบบคอมพิวเตอร์แล้วก็ตาม

ดังนั้นขั้นตอนนี้จึงเป็นส่วนหนึ่งของการกระทำเพื่อขโมยสกุลเงินดิจิทัล แม้จะยังไม่ได้ไปซึ่งสกุลเงินดิจิทัลก็มีความผิดฐานเข้าถึงระบบคอมพิวเตอร์โดยมิชอบตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์แล้ว

ขั้นตอนที่ 2 คือ เป็นกรณีการเข้าถึงข้อมูลคอมพิวเตอร์ คือ สกุลเงินดิจิทัล ดังนั้นผู้กระทำจะต้องเข้าไปยังที่เก็บสกุลเงินดิจิทัล (Wallet) แต่ผู้กระทำจะยังไม่สามารถโอนสกุลเงินดิจิทัลออกมาได้ทันที เนื่องจากการเข้าถึงกระเป๋าเงินได้นั้นจะมีมาตรการป้องกันการเข้าถึงโดยเฉพาะอีกชั้นหนึ่ง โดยการกรอกชื่อผู้ใช้งานและรหัสผ่านก่อนจะเข้าสู่กระเป๋าสกุลเงินดิจิทัล ดังนั้นเมื่อผู้กระทำฝ่ามาตรการป้องกันขั้นที่ 2 นี้เพื่อปลดล็อกคีย์แจ็ไปยังกระเป๋าที่เก็บสกุลเงินดิจิทัลได้ ผู้กระทำจึงจะมีความผิดตามมาตรา 7 ทั้งนี้ไม่ว่าผู้กระทำจะเพียงแค่อ่านข้อมูลที่มิได้กระทำความผิดใดอีกก็ตาม (เช่นเดียวกับมาตรา 5) ทั้งนี้เนื่องจาก มาตรา 5 และมาตรา 7 มิได้มีองค์ประกอบเจตนาพิเศษหรือมูลเหตุจูงใจในการเข้าถึง เพื่อการกระทำความผิดใดต่อ ดังนั้น เพียงแค่เข้าถึง ก็เป็นความผิดทั้งสองมาตรานี้แล้ว

อย่างไรก็ตามเป็นความผิดตามมาตรา 7 ได้ด้วยเหตุผลที่ว่าสกุลเงินดิจิทัลมีสถานะเป็นข้อมูลคอมพิวเตอร์ เพราะการกระทำตามมาตรา 7 เป็นกรณีการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบ ดังนั้น หากสกุลเงินดิจิทัลมีสถานะอื่นที่ไม่ใช่ข้อมูลคอมพิวเตอร์แล้ว ก็ไม่อาจนำบทบัญญัติแห่งกฎหมายดังกล่าวมาใช้บังคับได้

ขั้นตอนที่ 3 ขั้นตอนสุดท้าย คือผู้กระทำได้ทำการโอนสกุลเงินดิจิทัลของผู้เสียหายออกไปยังบัญชีอื่น

การกระทำขั้นตอน 3 นี้เป็นขั้นตอน “การได้มา” ซึ่งสกุลเงินดิจิทัลนี้ไม่มีบทบัญญัติใดในพระราชบัญญัตินี้ที่ครอบคลุมการกระทำความผิดดังกล่าว ทั้งนี้เนื่องมาจากแนวคิดในการกำหนดความผิดฐานขโมยข้อมูลคอมพิวเตอร์ตามอนุสัญญาอาชญากรรมไซเบอร์ (Convention on Cybercrime) ได้กำหนดแนวทางต้นแบบให้แต่ละประเทศต้องมีมาตรการทางกฎหมายในกรณีการเข้าถึงระบบคอมพิวเตอร์โดยมิชอบไม่ว่าจะทั้งหมดหรือบางส่วนที่ได้กระทำโดยเจตนาเป็นความผิดตามกฎหมายอาญาภายในประเทศของตน โดยเปิดโอกาสให้ประเทศสมาชิกสามารถเลือกกำหนดให้การเข้าถึงข้อมูลคอมพิวเตอร์นั้นการกระทำดังกล่าวเป็นความผิดเฉพาะกรณีที่มีการฝ่าฝืนมาตรการป้องกันโดยเจตนาหรือจะกำหนดให้เป็นการเข้าเพื่อให้ได้มาซึ่งข้อมูลคอมพิวเตอร์โดยกำหนดเจตนาพิเศษเพิ่มเติมหรือกำหนดให้เป็นความผิดที่มีความสัมพันธ์กับการเข้าถึงระบบคอมพิวเตอร์ที่เชื่อมโยงกับระบบอื่นก็ได้<sup>248</sup>

เมื่อพิจารณาพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ความผิดฐานเข้าถึงระบบคอมพิวเตอร์ มาตรา 5 และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ มาตรา 7 จะเห็นได้ว่าทั้ง 2 มาตรา กำหนดองค์ประกอบภายในคือเจตนาที่จะเข้าถึงก็เป็นความผิดแล้ว โดยไม่ได้กำหนดให้ต้องมีเจตนาพิเศษว่าการเข้าถึงนั้นต้องเป็นการเข้าถึงเพื่อกระทำความผิดใดต่อ จากการกำหนดองค์ประกอบภายในดังกล่าวจึงเห็นได้ว่าประเทศไทยเลือกแนวทางกำหนดให้การเข้าถึงข้อมูลคอมพิวเตอร์ให้เป็นความผิดในกรณีที่มีการฝ่าฝืนมาตรการป้องกันที่กระทำโดยเจตนาเท่านั้น กล่าวคือแค่เพียงมีเจตนาฝ่าฝืนมาตรการป้องกันของระบบคอมพิวเตอร์หรือข้อมูลคอมพิวเตอร์ที่มีการตั้งรหัสผ่านเข้าไปโดยไม่ได้รับอนุญาตก็เป็นความผิดฐานเข้าถึงแล้ว ดังนั้นจึงต้องพิจารณาบทบัญญัติอื่นประกอบหลังจากการเข้าถึงว่าการกระทำนั้นเป็นความผิดฐานใดอีกหรือไม่ ซึ่งแยกต่างหากจากความผิดฐานเข้าถึงโดยมิชอบ

---

<sup>248</sup> Convention on Cybercrime Article 2-Illegal access-Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

ทั้งนี้เมื่อพิจารณาบทบัญญัติอื่นที่เป็นการกระทำต่อข้อมูลคอมพิวเตอร์ มีฐานความผิด ดังนี้ 1) ความผิดฐานดักจับข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่ง<sup>249</sup> 2) ความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงหรือเพิ่มเติมซึ่งข้อมูลคอมพิวเตอร์<sup>250</sup> 3) ความผิดฐานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์รบกวนการใช้ระบบคอมพิวเตอร์โดยปกติสุขหรือก่อให้เกิดความเดือดร้อนรำคาญ<sup>251</sup> พบว่าทั้ง 3 ฐานความผิดที่กล่าวมาไม่มีบทบัญญัติใดกำหนดให้การนำข้อมูลคอมพิวเตอร์ออกไปจากระบบคอมพิวเตอร์เป็นความผิดที่แยกไว้อีกฐานหนึ่งโดยเฉพาะ ดังนั้นกรณีการขโมยสกุลเงินดิจิทัลนี้พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ จึงครอบคลุมเพียงการเข้าถึงระบบคอมพิวเตอร์และข้อมูลคอมพิวเตอร์ชั้นตอนที่ 1 และ 2 เท่านั้น แต่ยังไม่ครอบคลุมชั้นตอนที่ 3 จึงมีผลทำให้เกิดช่องว่างในการบังคับใช้กฎหมายหากนำไปปรับใช้กับกรณีดังกล่าว

2) ความผิดกรณีการใช้ทรัพยากรคอมพิวเตอร์ผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล

เป็นอาชญากรรมรูปแบบใหม่ที่ผู้กระทำใช้วิธีฝังโค้ดในเว็บเบราว์เซอร์หรือฝังมัลแวร์เข้าไปในไฟล์ข้อมูล หรือในเว็บไซต์ เมื่อผู้ใช้กดเข้าไปชมเว็บไซต์ โค้ดนั้นจะทำหน้าที่สั่งการให้พลังงานของระบบคอมพิวเตอร์เครื่องนั้นถูกนำไปช่วยในการตรวจสอบยืนยันธุรกรรม หากพลังงานคอมพิวเตอร์ในการประมวลผลมากและรวดเร็วพอจนสามารถตรวจสอบยืนยันธุรกรรมได้สำเร็จ จะได้ค่าตอบแทนเป็นสกุลเงินดิจิทัล

(1) บทบัญญัติที่เกี่ยวข้องกับกรณีการใช้ทรัพยากรคอมพิวเตอร์ผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล ได้แก่ มาตรา 10 ความผิดฐานกระทำเพื่อให้งานของระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติ ตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 10 บัญญัติว่า “ผู้ใดกระทำความผิดโดยประการใดโดยมิชอบ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ขัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ต้องระวางโทษ.....”

<sup>249</sup> มาตรา 8 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

<sup>250</sup> มาตรา 9 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

<sup>251</sup> มาตรา 11 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

### องค์ประกอบความผิด

ก) กระทำด้วยประการใด หมายถึง การกระทำทุกประการไม่จำกัดวิธีการตามที่ถูกกระทำตัดสินใจและได้ลงมือกระทำ โดยไม่ว่าจะเป็นวิธีการทางกายภาพ เช่น การทำลาย การทำให้ระเบิด หรือการเผาอุปกรณ์คอมพิวเตอร์เพื่อให้การทำงานของระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติ นอกจากนี้ยังรวมถึงวิธีการทางอิเล็กทรอนิกส์ต่อระบบคอมพิวเตอร์ เช่น การส่งไวรัสเข้าไปทำลายระบบคอมพิวเตอร์ หรือการโจมตีระบบคอมพิวเตอร์โดยส่งคำสั่งจำนวนมากเพื่อให้ระบบไม่อาจให้บริการได้ ที่เรียกว่า การโจมตีจนระบบล่ม

ข) โดยมีชอบ หมายถึง การกระทำโดยปราศจากอำนาจ

ค) โดยเจตนา เป็นองค์ประกอบภายใน หมายถึง การกระทำโดยรู้ว่าตนเองไม่มีอำนาจกระทำการ ดังนั้น จึงไม่รวมถึงการกระทำที่แม้จะไม่ชอบด้วยกฎหมาย แต่ผู้กระทำเข้าใจผิดว่าตนเองมีอำนาจกระทำได้

ง) เจตนาพิเศษ เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้

เจตนาพิเศษหรือมูลเหตุจูงใจ คือ มูลเหตุที่ก่อให้เกิดการกระทำนั้น จะมีได้เฉพาะความผิดที่กระทำโดยเจตนาเท่านั้น ความผิดที่กระทำโดยประมาทมิอาจมีเจตนาพิเศษได้<sup>252</sup> โดยทั่วไปแล้วกฎหมายอาญาจะกำหนดให้การกระทำโดยเจตนาตามมาตรา 59 วรรค 1 และวรรค 2 เป็นองค์ประกอบความผิด ซึ่งหากกำหนดไว้เช่นนี้กฎหมายจะไม่นำมูลเหตุจูงใจมาพิจารณาความรับผิดแต่อย่างใด กล่าวคือมูลเหตุจูงใจอยู่นอกเหนือองค์ประกอบความผิดที่ต้องนำมาพิจารณา ดังนั้นแม้มูลเหตุจูงใจจะชั่วร้ายแต่การกระทำนั้นชอบด้วยกฎหมาย การกระทำความผิดดังกล่าวก็ไม่เป็นความผิด<sup>253</sup>

อย่างไรก็ตามหากกฎหมายนำเจตนาพิเศษมาเป็นองค์ประกอบ การวินิจฉัยความผิดจะต้องมีการบัญญัติไว้โดยเฉพาะซึ่งอาจพิจารณาจากถ้อยคำในตัวบท<sup>254</sup> ดังเช่นมาตรานี้ได้กำหนดให้การกระทำไม่ว่าจะทางกายภาพหรือทางอิเล็กทรอนิกส์ที่ได้กระทำโดยเจตนาแล้ว ยังต้องมีมูลเหตุจูงใจในการกระทำนั้นเพื่อให้ระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติอีก จึงจะเป็นความผิดตามมาตรา นี้ ทั้งนี้คำว่า “ระงับ” หมายถึง ยับยั้งไว้หรือทำให้สงบ เช่น ทำให้ระบบคอมพิวเตอร์หยุด

<sup>252</sup> จิตติ ดิงศภัทย์, คำอธิบายประมวลกฎหมายอาญา ภาค 1, หน้า 245.

<sup>253</sup> จิตติ ดิงศภัทย์, รวมผลงานทางวิชาการของศาสตราจารย์จิตติ ดิงศภัทย์ เล่มที่ 1 (กรุงเทพมหานคร: สำนักงานศาลยุติธรรม, 2562), หน้า 174.

<sup>254</sup> จิตติ ดิงศภัทย์, คำอธิบายประมวลกฎหมายอาญา ภาค 1, หน้า 250.

ทำงานหรือไม่สามารถเข้าถึงระบบคอมพิวเตอร์ได้ คำว่า “ชะลอ” หมายถึง ทำให้ช้าลง เช่น ทำให้ระบบคอมพิวเตอร์ทำงานช้าลง คำว่า “ขัดขวาง” หมายถึง ทำให้ไม่สะดวกหรือทำให้ติดขัด เช่น ทำให้ระบบคอมพิวเตอร์ไม่สามารถรันโปรแกรมหรือเปิดไฟล์ข้อมูลได้ และคำว่า “รบกวน” หมายถึง ทำให้รำคาญหรือทำให้เดือดร้อน เช่น ทำให้หน้าจอคอมพิวเตอร์เกิดภาพสั่นและกระตุก ซึ่งพฤติกรรมเหล่านี้มีผลทำให้ระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติได้ นั้นหมายถึงการทำให้ระบบคอมพิวเตอร์นั้นไม่สามารถทำงานได้โดยสมบูรณ์ ดังนั้นถึงแม้ว่าระบบคอมพิวเตอร์จะทำงานได้ แต่เป็นการทำงานที่ไม่สมบูรณ์หรือผิดปกติไป (Malfunctioning) ก็ย่อมอยู่ในความหมายของถ้อยคำอันเป็นองค์ประกอบความผิดนี้แล้ว<sup>255</sup>

นอกจากนี้ ความผิดฐานกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติ ตามมาตรา 10 ผู้กระทำความผิดอาจต้องรับโทษหนักขึ้น หากเข้าเงื่อนไขที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 12 และมาตรา 12/1<sup>256</sup> ดังนี้

ก) กรณีทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบอันเป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น

ข) กรณีทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบอันเป็นเหตุให้บุคคลอื่นถึงแก่ความตาย แม้มิได้มีเจตนาฆ่าก็ตาม

ค) กรณีทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติม ไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบนั้นต้อง

<sup>255</sup> พรเพชร วิชิตชลชัย, *เรื่องเดิม*.

<sup>256</sup> มาตรา 12/1 “ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 เป็นเหตุให้เกิดอันตรายแก่บุคคลอื่นหรือทรัพย์สินของผู้อื่น ต้องระวางโทษจำคุกไม่เกินสิบปี และปรับไม่เกินสองแสนบาท

ถ้าการกระทำความผิดตามมาตรา 9 หรือมาตรา 10 โดยมีเจตนาฆ่า แต่เป็นเหตุให้บุคคลอื่นถึงแก่ความตาย ต้องระวางโทษจำคุกตั้งแต่ห้าปีถึงยี่สิบปี และปรับตั้งแต่หนึ่งแสนบาทถึงสี่แสนบาท”

เป็นข้อมูลเกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ<sup>257</sup>

ง) กรณีการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบนั้น ต้องเป็นข้อมูลหรือระบบที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะ เป็นเหตุให้เกิดความเสียหายแก่ข้อมูลคอมพิวเตอร์หรือระบบคอมพิวเตอร์นั้น<sup>258</sup>

จ) กรณีการทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง หรือเพิ่มเติมไม่ว่าทั้งหมดหรือบางส่วน ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบนั้น ต้องเป็นข้อมูลหรือระบบที่เกี่ยวกับการรักษาความมั่นคงปลอดภัยของประเทศ ความปลอดภัยสาธารณะ ความมั่นคงในทางเศรษฐกิจของประเทศหรือโครงสร้างพื้นฐานอันเป็นประโยชน์สาธารณะเป็นเหตุให้บุคคลอื่นถึงแก่ความตาย แม้มิได้เจตนาฆ่าก็ตาม<sup>259</sup>

(2) วิเคราะห์กรณีการใช้ทรัพยากรคอมพิวเตอร์ผู้อื่นเพื่อให้ได้มาซึ่ง สกิลกับความผิดฐานกระทำเพื่อให้งานของระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติ

กรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นในการตรวจสอบยืนยันธุรกรรมสกุลเงินดิจิทัลนั้น เริ่มต้นด้วยการปล่อยมัลแวร์ในเว็บไซต์ โปรแกรมต่าง ๆ ในเพจ หรือแม้แต่ในอีเมล โดยใช้ช่องทางอิเล็กทรอนิกส์ต่าง ๆ ที่คนทั่วไปสามารถกดเปิดเข้าไปดูได้ การกดเปิดเข้าไปดูนี้เปรียบเสมือนเป็นการเปิดประตูยอมรับให้ระบบคอมพิวเตอร์ของผู้ใช้ทำงานให้ผู้กระทำ การกระทำดังกล่าวจึงเป็นการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นด้วยวิธีการทางอิเล็กทรอนิกส์ซึ่งอยู่ในความหมายของการกระทำตามมาตรานี้ และเป็นการกระทำโดยไม่ได้รับความยินยอมจากผู้อื่น และไม่มีกฎหมายใดให้อำนาจบุคคลในการใช้ทรัพยากรของผู้อื่นด้วยวิธีนี้ จึงเป็นกระทำโดยไม่มีอำนาจซึ่งผู้กระทำมีเจตนาเพราะการกระทำด้วยวิธีดังกล่าวนี้ต้องมีความรู้ทางด้านเทคนิคในการเขียนโค้ดและฝังมัลแวร์เข้าไปในช่องทางที่ทำให้คนทั่วไปสามารถพบเห็นได้ อีกทั้งต้องเป็นโค้ดที่มีลักษณะเฉพาะ เพราะโค้ดนั้นจะต้องถูกออกแบบมาให้เชื่อมต่อกับบัญชี (Cryptocurrency Wallet)

<sup>257</sup> มาตรา 12 วรรค 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

<sup>258</sup> มาตรา 12 วรรค 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

<sup>259</sup> มาตรา 12 วรรค 4 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550

ของผู้กระทำได้ ในกรณีที่หากตรวจสอบธุรกรรมได้สำเร็จค่าตอบแทนที่ได้มาจะถูกโอนเข้าไปยังบัญชีของผู้กระทำทันที

อย่างไรก็ตามเมื่อพิจารณาถึงเจตนาพิเศษ อันเป็นหนึ่งในองค์ประกอบของความผิดฐานกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติได้ กำหนดให้ การกระทำนั้นทำไป เพื่อให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ดังนั้นผู้กระทำจะต้องมีเจตนาประสงค์ต่อผลในการกระทำใด ๆ ก็ตาม เพื่อให้ระบบคอมพิวเตอร์ไม่สามารถใช้งานได้ตามปกติซึ่งเป็นเจตนาพิเศษต่อเนื่องมาจากการกระทำโดยเจตนา แต่สำหรับการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นนั้นผู้กระทำมีเจตนาเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล โดยอาจมีได้ค่านึงถึงประสิทธิภาพการประมวลผลคอมพิวเตอร์ของผู้เสียหาย (ผู้กระทำสนใจแต่เป้าหมาย คือ เพื่อให้ตนได้มาซึ่งสกุลเงินดิจิทัล โดยมีได้สนใจว่าจะทำให้ระบบคอมพิวเตอร์ของผู้เสียหายมีประสิทธิภาพลดลงเพียงใด) การกระทำดังกล่าวจึงขาดเจตนาพิเศษ อันเป็นองค์ประกอบความผิดของมาตรา 10

ทั้งนี้ ความมุ่งหมายของมาตรานี้มีขึ้นเพื่อคุ้มครองระบบคอมพิวเตอร์มิให้ถูกรบกวน ชัดขวาง จากการกระทำที่ไม่ปลอดภัยต่อระบบ<sup>260</sup> จึงได้กำหนดเจตนาพิเศษขึ้นมาสำหรับความผิดฐานนี้ เพื่อแสดงให้เห็นถึงความมุ่งหมายของกฎหมายที่ต้องการคุ้มครอง ดังนั้นจะเป็นความผิดตามมาตรานี้ผู้กระทำจะต้องมีการกระทำ มีเจตนา และเจตนาพิเศษอันเป็นองค์ประกอบความผิดฐานต้องเป็นการกระทำไปเพื่อให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถทำงานได้ตามปกติ แต่สำหรับกรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นนั้น ผู้กระทำมีเจตนาที่จะกระทำการใด ๆ ด้วยวิธีการทางอิเล็กทรอนิกส์ และมีเจตนาพิเศษเพื่อให้ได้ไปซึ่งสกุลเงินดิจิทัล มิใช่เพื่อระงับ ชัดขวางระบบคอมพิวเตอร์ของ ดังนั้นเมื่อเจตนาพิเศษแตกต่างไปจากที่กฎหมายกำหนด ความผิดฐานนี้จึงไม่อาจนำมาปรับใช้กับกรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นได้ มีผลทำให้เกิดช่องว่างทางกฎหมาย ทั้งที่การกระทำนั้นเป็นการได้มาซึ่งผลประโยชน์ของผู้อื่นด้วยวิธีการอันมิชอบ กรณีดังกล่าวควรมีกฎหมายควบคุมหรือกำหนดให้เป็นความผิดต่อไป

### 3.3.3.2 ประมวลกฎหมายอาญา

ประมวลกฎหมายอาญา ได้บัญญัติฐานความผิดเกี่ยวกับทรัพย์ทั้งนี้มีบทบัญญัติที่เกี่ยวข้องกับกรณีการขโมยสกุลเงินดิจิทัลและกรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่น ดังนี้

1) กรณีการขโมยสกุลเงินดิจิทัล ดังที่ได้กล่าวถึงขั้นตอนการขโมยสกุลเงินดิจิทัลไว้แล้วในหัวข้อวิเคราะห์กรณีการขโมยสกุลเงินดิจิทัลกับความผิดฐานเข้าถึงระบบคอมพิวเตอร์ และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ซึ่งครอบคลุมความผิดได้เฉพาะในขั้นตอนที่ 1 และ 2

<sup>260</sup> Article 5, Convention on Cybercrime

ดังนั้นในส่วนของประมวลกฎหมายอาญานี้จะขอล่าเฉพาะขั้นตอนที่ 3 ที่ได้มีการโอนสกุลเงินดิจิทัลของผู้เสียหายออกไปยังบัญชีอื่น

(1) บทบัญญัติที่เกี่ยวข้องกับกรณีการขโมยสกุลเงินดิจิทัล คือ

ก) มาตรา 334 ความผิดฐานลักทรัพย์ บัญญัติว่า “ผู้ใดเอาทรัพย์ของผู้อื่น หรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปโดยทุจริตผู้นั้นกระทำความผิดฐานลักทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกหมื่นบาท”

องค์ประกอบความผิด

เอาไป คือการแย่งการครอบครองและเข้ายึดถือเพื่อพาทรัพย์ของผู้อื่น “เคลื่อนที่” ไปจากการครอบครอง ซึ่งศาลฎีกาเห็นว่าต้องเป็นการพาทรัพย์เคลื่อนจากที่นั้นทุกๆ จุดในลักษณะที่จะพาเอาไปได้ และเมื่อเคลื่อนที่แล้วแม้จะได้เอาทรัพย์กลับมาไว้ที่เดิมก็ไม่ทำให้ความผิดที่สำเร็จแล้วเปลี่ยนแปลงไป แม้ยังไม่ได้การครอบครองอย่างเด็ดขาดก็ตาม แต่ความเห็นทางตำราเห็นว่า จะมีการเอาไปสำเร็จบริบูรณ์ก็ต่อเมื่อผู้กระทำได้ไปซึ่งการครอบครองหรือมีอำนาจอย่างแท้จริงเหนือทรัพย์นั้น ซึ่งจะต้องพิจารณาจากจาริตประเพณี ลักษณะของทรัพย์ ความสามารถที่จะเข้าขัดขวางมิให้ผู้อื่นเข้าเกี่ยวข้องกับทรัพย์ และระยะห่าง ระหว่างผู้ครอบครองเดิมกับทรัพย์ แม้จะมีได้แต่ต้องทรัพย์นั้นเลยก็เป็นการเอาไปได้เช่นกัน ทั้งนี้กฎหมายในปัจจุบันมิได้ยึดถือตามความเห็นใดความเห็นหนึ่งอย่างเคร่งครัด หากแยกพิจารณาการกระทำที่ถือว่าการเอาไปสำเร็จบริบูรณ์จากลักษณะของทรัพย์เป็นหลัก เช่น หากเป็นพืชล้มลุกหรือไม้ยืนต้น จะต้องทำการแยกทรัพย์ออกมาให้อยู่ในลักษณะที่จะพาเคลื่อนที่ไปได้โดยการขุด ตัด ถอน หรือ แยกออกจากที่ทรัพย์ติดอยู่และจะถือว่ามี การเอาไปสำเร็จก็ต่อเมื่อมีการเคลื่อนที่ทรัพย์อีกครั้งหนึ่ง เพื่อเอาไป แม้จะยังไม่พ้นจากบริเวณที่ทรัพย์เคยอยู่ก็เป็นความผิดสำเร็จแล้ว<sup>261</sup>

นอกจากนี้การเอาไปต้องมีลักษณะเป็นการตัดกรรมสิทธิ์จากเจ้าของเดิมเป็นการถาวร หากเอาไปโดยวิสาสะ (ไม่ได้ขออนุญาตเจ้าของก่อน) หรือการเอาทรัพย์ไปโดยเข้าใจว่าเจ้าของอนุญาตแล้ว แม้จะพาทรัพย์เคลื่อนที่ไป ก็ไม่เป็นความผิดฐานลักทรัพย์

(ก) ทรัพย์ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย คือต้องเป็นทรัพย์ที่ผู้อื่นเป็นเจ้าของและทรัพย์นั้นอยู่ในความครอบครองของผู้อื่นด้วย สำหรับกรณีที่เจ้าของรวมคนหนึ่งเอาทรัพย์ที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยนั้น จะมีความผิดฐานนี้ได้ต้องปรากฏว่าทรัพย์นั้นไม่ได้อยู่ในความครอบครองของตน หากครอบครองอยู่ที่ตนแล้วจะเป็นความผิดฐานลักยกออกไม่ใช่ลักทรัพย์ เพราะความผิดฐานลักทรัพย์คือการแย่งการครอบครอง ส่วนในกรณีการเอาทรัพย์ของ

<sup>261</sup> ทวีเกียรติ มีนะกนิษฐ, รายงานวิจัยเรื่องความผิดฐานลักทรัพย์ (กรุงเทพมหานคร: โครงการวิจัยเสริมหลักสูตร มหาวิทยาลัยธรรมศาสตร์, 2529).

ตนเองที่อยู่ในความครอบครองของผู้อื่นไป ก็ไม่เป็นความผิดฐานนี้ เนื่องจากทรัพย์ที่เป็นวัตถุแห่งการกระทำนั้นไม่ใช่ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย จึงขาดองค์ประกอบภายนอก เช่น เจ้าของนำแหวนไปจำหน่ายกับโรงรับจำนำแล้วไปเอาแหวนนั้นคืนมา ไม่เป็นความผิดฐานลักทรัพย์แต่ผิดฐานโกงเจ้าหนี้ มาตรา 349

(ข) โดยเจตนา เป็นองค์ประกอบภายใน หมายถึง กระทำโดยรู้ว่าทรัพย์ที่เอาไปเป็นทรัพย์ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย ดังนั้น หากผู้กระทำเข้าใจผิดคิดว่าทรัพย์ดังกล่าวเป็นของตนเอง หรือเข้าใจว่าเจ้าของทรัพย์อนุญาตให้เอาไปได้ แม้ผู้กระทำผิดเอาทรัพย์ของผู้อื่นไปก็ไม่เป็นความผิด

(ค) มีเจตนาพิเศษหรือเหตุจูงใจโดยทุจริต คือ การเอาทรัพย์ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ไปนั้น ผู้กระทำต้องมีเจตนาพิเศษเพื่อแสวงหาประโยชน์ที่มิควรได้โดยชอบด้วยกฎหมายสำหรับตนเองหรือผู้อื่น<sup>262</sup> ทั้งนี้ไม่จำเป็นต้องเป็นประโยชน์ในลักษณะที่เป็นทรัพย์สิน เพียงแต่ได้รับประโยชน์ที่ทำให้สะดวกสบายขึ้นหรือได้รับเสรีภาพก็เป็นการกระทำโดยทุจริตแล้ว เช่น การหลอกลวงให้บุคคลอื่นนำ นส.3 มาใช้เป็นหลักประกันต่อศาลเพื่อขอประกันตัวศาลได้ให้ประกันตัว กรณีดังกล่าวถือว่าผู้กระทำได้รับประโยชน์ตามความหมายของคำว่าโดยทุจริตแล้ว แต่การเอาทรัพย์ไปเพื่อทิ้งหรือทำลาย ไม่เป็นผิดฐานลักทรัพย์เนื่องจากไม่ได้รับประโยชน์<sup>263</sup>

ข) มาตรา 188 ความผิดฐาน เอาไป ทำให้เสียหายซึ่งพินัยกรรมหรือเอกสาร บัญญัติว่า “ผู้ใดทำให้เสียหาย ทำลาย ซ่อนเร้น เอาไปเสีย หรือทำให้สูญหายหรือไร้ประโยชน์ ซึ่งพินัยกรรมหรือเอกสารใดของผู้อื่น ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ต้องระวางโทษจำคุกไม่เกินห้าปี และปรับไม่เกินหนึ่งแสนบาท”

#### องค์ประกอบความผิด

(ก) ทำให้เสียหาย ทำลาย ซ่อนเร้น เอาไปเสีย หรือทำให้สูญหายหรือไร้ประโยชน์ คำว่า เอาไปเสีย มิได้หมายความว่าอย่างเดียวกับการเอาไปในความผิดฐานลักทรัพย์ มาตรา 334 ซึ่งเป็นการตัดกรรมสิทธิ์จากเจ้าของเดิม แต่การเอาไปเสียความผิดฐานนี้ หมายถึงเอาไปจากที่เอกสารนั้นเคยอยู่<sup>264</sup> ดังนั้น เอาไปเสียจึงมีความหมายกว้างการเอาไปในความผิดฐานลักทรัพย์

<sup>262</sup> มาตรา 1 (6) แห่งประมวลกฎหมายอาญา

<sup>263</sup> ทวีเกียรติ มีนะกนิษฐ, รายงานวิจัยเรื่องเสริมหลักสูตร เรื่องความผิดฐานลักทรัพย์, กรุงเทพมหานคร: มหาวิทยาลัยธรรมศาสตร์, 2533

<sup>264</sup> เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 1, พิมพ์ครั้งที่ 5 ฉบับแก้ไขเพิ่มเติม (กรุงเทพมหานคร: พลสยามพริ้นติ้ง, 2553), หน้า 312.

(ข) ซึ่งพินัยกรรมหรือเอกสารผู้อื่นเอกสาร หมายถึง กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น<sup>265</sup> ทั้งนี้รวมถึงเอกสาร สิทธิ<sup>266</sup> และเอกสารราชการ<sup>267</sup> ซึ่งต้องเป็นของผู้อื่น

(ค) ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือ ประชาชน เป็นองค์ประกอบภายนอกที่ไม่ใช่ข้อเท็จจริง หรือพฤติการณ์ประกอบกรกระทำ<sup>268</sup> ความเสียหายไม่จำเป็นต้องเกิดขึ้นจริงเพียงแต่มีพฤติการณ์ที่น่าจะเสียหายอย่างไร้เพียงพอแล้ว

(ง) เจตนา กระทำให้เสียหายโดยรู้ยู่ว่าเป็นพินัยกรรมหรือ เอกสารของผู้อื่น

(2) วิเคราะห์กรณีการขโมยสกุลเงินดิจิทัลกับความผิดฐานลักทรัพย์ มาตรา 334

ความผิดฐานลักทรัพย์บัญญัติขึ้นโดยมีวัตถุประสงค์ที่จะมุ่งคุ้มครอง กรรมสิทธิ์และการ ครอบครองทรัพย์ของบุคคล ซึ่งต้องมีการเอาไปจากการครอบครองในลักษณะที่ เป็นการตัดกรรมสิทธิ์จึงจะเป็นความผิดตามมาตรา นี้ ดังนั้นในการวิเคราะห์จึงขอแยกเป็น 2 ประเด็น คือ 1) การเอาไป และ 2) ทรัพย์อันเป็นวัตถุแห่งการกระทำ ดังนี้

ก) การเอาไป หรือการขโมยสกุลเงินดิจิทัลด้วยวิธีการโอนออก จากบัญชีเจ้าของเดิมไปอยู่ที่บัญชีอื่น การกระทำดังกล่าวมีจึงลักษณะเป็นตัดกรรมสิทธิ์จากเจ้า ของเดิม ทำให้เจ้าของเดิมขาดจากการใช้ประโยชน์แห่งทรัพย์โดยสิ้นเชิง จึงมีลักษณะของการเอาไป ตามความหมายของความผิดฐานลักทรัพย์ ซึ่งหากมองถึงลักษณะการกระทำที่กระทำต่อสกุลเงิน ดิจิทัลเช่น สกุลเงินดิจิทัลจึงมีลักษณะเป็นทรัพย์สินอย่างหนึ่งที่ไม่อาจเอาไปได้ด้วยการทำสำเนา ต่างจากกรณีที่เป็นข้อมูลคอมพิวเตอร์เพราะข้อมูลคอมพิวเตอร์โดยทั่วไปสามารถนำออกจากระบบได้ ด้วยวิธีการคัดลอกโดยไม่กระทบถึงความมีอยู่หรือเนื้อหาของข้อมูลต้นฉบับแต่อย่างใด ประการสำคัญ คือกรรมสิทธิ์และการครอบครองยังอยู่ที่เจ้าของเดิม ในขณะที่การขโมยสกุลเงินดิจิทัลนั้นไม่สามารถ ทำสำเนาหรือการคัดลอกข้อมูลซ้ำได้เหมือนเช่นการกระทำกับข้อมูลคอมพิวเตอร์ได้ ดังนั้นการเอาไป ซึ่งสกุลเงินดิจิทัลจึงการเอาไปที่มีลักษณะเช่นเดียวกับลักตามมาตรา 334 แต่จะเป็นทรัพย์อันเป็นวัตถุ แห่งการกระทำในความผิดฐานลักทรัพย์ได้หรือไม่ ต้องพิจารณาในประเด็นต่อไป

<sup>265</sup> มาตรา 7 แห่งประมวลกฎหมายอาญา

<sup>266</sup> มาตรา 9 แห่งประมวลกฎหมายอาญา

<sup>267</sup> มาตรา 8 แห่งประมวลกฎหมายอาญา

<sup>268</sup> เกียรติขจร วัจนะสวัสดิ์, กฎหมายอาญาภาคความผิด เล่ม 1, หน้า 308.

ข) ทรัพย์อันเป็นวัตถุแห่งการกระทำ ประเด็นนี้เป็นที่ถกเถียงทางวิชาการกันมานาน และน่าจะมีที่มาจากคำพิพากษาฎีกา 877/2501 ซึ่งได้วางบรรทัดฐานว่า ผู้ใดลักกระแสรไฟฟ้าต้องมีความผิดฐานลักทรัพย์ตามมาตรา 334 โดยมีได้มีการให้เหตุผลในคำพิพากษาที่ชี้ให้เห็นว่ากระแสรไฟฟ้าเป็นทรัพย์หรือไม่ เพียงแต่ได้มีการลงมติโดยเสียงส่วนใหญ่ว่าการลักกระแสรไฟฟ้าเป็นความผิดฐานลักทรัพย์เท่านั้น ดังนั้นในส่วนของคำว่า “ทรัพย์” ที่ไม่ได้มีนิยามไว้ในประมวลกฎหมายอาญา จึงมีความเห็นทางวิชาการเกี่ยวกับความหมายคำว่า “ทรัพย์” ซึ่งเป็นวัตถุแห่งการกระทำ ความผิดอาญาฐานลักทรัพย์ ไว้ 4 ความเห็น โดยความเห็นที่ 1-3 เห็นว่าควรนำความหมายคำว่าทรัพย์ในประมวลกฎหมายแพ่งและพาณิชย์มาใช้ ส่วนความเห็นที่ 4 เห็นว่าไม่ควรนำประมวลกฎหมายแพ่งและพาณิชย์มาใช้ ซึ่งมีรายละเอียด ดังนี้

ความเห็นที่ 1 ประมวลกฎหมายอาญามีได้นิยามความหมายของคำว่า “ทรัพย์” ไว้ดังเช่นประมวลกฎหมายแพ่งและพาณิชย์ ดังนั้นจึงต้องนำนิยามในประมวลกฎหมายแพ่งและพาณิชย์มาใช้ตามหลักกฎหมายย่อมเกี่ยวข้องซึ่งกันและกันอยู่ เว้นแต่ตามบทบัญญัตินั้นจะแสดงว่าจะไม่ประสงค์ให้ความหมายดังที่ปรากฏตามกฎหมายอื่นซึ่งได้นิยามไว้ว่า “วัตถุที่มีรูปร่าง” และเห็นว่าไฟฟ้าไม่ใช่วัตถุที่มีรูปร่างอันเป็นองค์ประกอบความผิดตามมาตรา 334 แต่เป็นเพียงพลังงานหรือแรงธรรมชาติเท่านั้น<sup>269</sup>

ความเห็นที่ 2 มีความเห็นว่าต้องนำบทบัญญัติ คำว่าทรัพย์ในประมวลกฎหมายแพ่งและพาณิชย์มาใช้เหมือนความเห็นที่ 1 แต่มีความเห็นต่างกันตรงที่มองว่ากระแสรไฟฟ้าเป็นสิ่งที่รูปร่าง “วัตถุที่มีรูปร่าง” โดยเข้าใจว่าความหมายถึงวัตถุที่ประกอบด้วยรูปและร่างในตัวเอง โดยลำพัง มีตัวตนส่วนกว้างยาว สูงต่ำ ฤๅส่วนกลมซึ่งกินที่ โดยทั้งนี้แม้จะเป็นปริมาณเล็กน้อยจนมองไม่เห็นด้วยตาเปล่าก็ตาม แม้แต่เชื้อโรคปรมาณูธรรมชาติ ก็ควรจัดว่าเป็นวัตถุที่มีรูปร่างได้<sup>270</sup> ส่วนกระแสรไฟฟ้านั้นแม้จะเห็นด้วยตา จับต้องไม่ได้ แต่ก็ประกอบด้วยพลังอันต่าง ๆ ซึ่งอาจจะพอถือว่าเป็นวัตถุที่มีรูปร่างได้กระมัง<sup>271</sup>

<sup>269</sup> หยุด แสงอุทัย, *กฎหมายอาญา ภาค 2-3* (กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2553), หน้า 430.

<sup>270</sup> เสนีย์ ปราโมช, ม.ร.ว., *อธิบายประมวลกฎหมายแพ่งและพาณิชย์ กฎหมายลักษณะทรัพย์* (กรุงเทพมหานคร: โรงพิมพ์อักษรสาส์น, 2521), หน้า 11; วิริยะ นามศิริพงศ์พันธ์, *เอกสารประกอบการสอนวิชากฎหมายลักษณะทรัพย์* (กรุงเทพมหานคร: คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2524), หน้า 2-4.

<sup>271</sup> บัญญัติ สุชีวะ, *คำอธิบายประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยทรัพย์* (กรุงเทพมหานคร: โรงพิมพ์มหาวิทยาลัยรามคำแหง, 2514), หน้า 6.

ความเห็นที่ 3 มองถึงวิธีการลึกลับว่าต้องมีการพาทรัพย์สินเคลื่อนที่ไป ดังนั้นสิ่งที่จะสามารถลึกลับได้นั้น ต้องเป็น “ทรัพย์สินที่เคลื่อนที่ได้” ซึ่งในประมวลกฎหมายแพ่งและพาณิชย์เดิม มาตรา 101 ได้บัญญัติถึงทรัพย์สินที่เคลื่อนที่ได้ไว้ในคำว่า “สังหาริมทรัพย์ ได้แก่ทรัพย์สินทั้งหลาย อันอาจขนเคลื่อนจากที่หนึ่งไปแห่งอื่นได้ ไม่ว่าเคลื่อนด้วยแรงเดินแห่งตัวทรัพย์สิน หรือเคลื่อนด้วยกำลังภายนอก อนึ่ง คำว่า “สังหาริมทรัพย์ ท่านหมายรวมทั้งกำลังแรงแห่งธรรมชาติอันอาจถือเอาได้...” ดังนั้นจึงหมายความว่ารวมถึงกำลังแรงแห่งธรรมชาติ เช่นแรงไฟฟ้าด้วยนั่นเอง<sup>272</sup>

ความเห็นดังกล่าวนี้มีที่มาจากคำอธิบายของกรรมการร่างประมวลกฎหมายแพ่งและพาณิชย์ ฉบับ พ.ศ. 2466 ได้อธิบายความหมายของคำว่า “ทรัพย์สิน” โดยยกตัวอย่างคำว่า “ทรัพย์สิน ได้แก่ บ้าน ที่ดิน บ่อ เครื่องจักร รถยนต์ เรือยนต์ แรงไฟฟ้า สัตว์ ฯลฯ”<sup>273</sup> ดังนั้น จึงมีความเห็นว่าทรัพย์สินรวมถึงแรงไฟฟ้าด้วย

ความเห็นที่ 4 เห็นว่าไม่ควรนำประมวลกฎหมายแพ่งและพาณิชย์มาใช้ เนื่องจากในประมวลกฎหมายอาญาไม่มีส่วนใดที่บัญญัติให้อนุโลมใช้ประมวลกฎหมายแพ่งและพาณิชย์ ดังเช่นประมวลกฎหมายวิธีพิจารณาความอาญาบัญญัติให้นำประมวลกฎหมายวิธีพิจารณาความแพ่งมาใช้บังคับโดยอนุโลม ดังนั้นจึงควรพิจารณาความหมายจากประมวลกฎหมายลักษณะอาญารัตนโกสินทรศก ซึ่งเป็นประมวลกฎหมายฉบับเดิมก่อนที่จะเปลี่ยนมาเป็นประมวลกฎหมายอาญาในปัจจุบัน ได้เคยมีนิยามคำว่า ทรัพย์สิน ไว้ใน มาตรา 6 (10) ว่าหมายถึง “บรรดาสิ่งของอันบุคคลสามารถมีกรรมสิทธิ์ หรือถืออำนาจเป็นเจ้าของได้ เป็นต้นว่าเงินตรา และบรรดาสิ่งของอันพึงเคลื่อนจากที่ได้ก็ดี และเคลื่อนจากที่มิได้ก็ดี ท่านก็นับว่าเป็นทรัพย์สินอันกล่าวมาในข้อนี้”

จากความเห็นดังกล่าวไม่ได้พิจารณาทรัพย์สินจากลักษณะทางกายภาพ หรือวิธีการพาทรัพย์สินเคลื่อนที่ได้ แต่พิจารณาจากอำนาจเหนือสิ่งของหรือความสามารถในการหวงกันของบุคคลที่มีต่อสิ่งของนั้น ดังนั้นสิ่งใดก็ตามไม่ว่าจะมีรูปร่างหรือไม่ หากเป็นสิ่งที่อยู่ในการควบคุมของบุคคลได้ สิ่งนั้นก็เรียกว่าเป็นทรัพย์สินได้

นอกจากนี้ยังมีคำพิพากษาศาลฎีกาที่ 5161/2547 เกี่ยวข้องกับความหมายของทรัพย์สินอันเป็นวัตถุแห่งการกระทำในความผิดฐานลักทรัพย์ โดยวินิจฉัยว่าการนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ของผู้อื่นโจทก์ร่วม ไม่เป็นความผิดฐานลักทรัพย์ ศาลฎีกาได้ให้เหตุผลว่า ข้อมูล ตามพจนานุกรมให้ความหมายว่า “ข้อเท็จจริง หรือสิ่งที่ถือหรือยอมรับว่าเป็นข้อเท็จจริง สำหรับใช้เป็นหลักฐานหาความจริงหรือการคำนวณ” ส่วน

<sup>272</sup> จิตติ ดิงศภัทย์, *หมายเหตุท้ายคำพิพากษาศาลฎีกา 877/2501*, หน้า 991.

<sup>273</sup> กิตติศักดิ์ ปรกติ, “กฎหมายกับพัฒนาการของสังคมไทย: จากลัทธิกระแสไฟฟ้า มาสู่ลัทธิสัญญาณโทรศัพท์,” *วารสารไทยคดีศึกษา* 2, 2 (เมษายน-กันยายน 2548): 35-54.

ข้อเท็จจริง มีหมายความว่า “ข้อความแห่งเหตุการณ์ที่เป็นมาหรือที่เป็นอยู่ตามจริง ข้อความหรือเหตุการณ์ที่จะต้องวินิจฉัยว่าเท็จหรือจริง” ดังนั้นข้อมูลจึงไม่นับเป็นวัตถุที่มีรูปร่าง สำหรับตัวอักษร ภาพ แผ่นผิง และตราสารเป็นเพียงสัญลักษณ์ที่ถ่ายทอดความหมายของข้อมูลออกจากแผ่นบันทึก ข้อมูลโดยอาศัยเครื่องคอมพิวเตอร์ มิใช่รูปร่างของข้อมูล เมื่อประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 บัญญัติว่า ททรัพย์ หมายความว่า “วัตถุที่มีรูปร่าง” ข้อมูลในแผ่นบันทึกข้อมูลจึงไม่ถือเป็นทรัพย์ การที่จำเลยนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลของโจทก์ร่วม จึงไม่เป็นความผิดฐานลักทรัพย์

จากคำพิพากษาฎีกานี้สรุปได้ว่า ข้อมูลที่ปรากฏโดยอาศัยเครื่องคอมพิวเตอร์ ไม่ถือว่าเป็นวัตถุที่มีรูปร่าง ดังนั้นการนำแผ่นบันทึกข้อมูลเปล่าลอกข้อมูลจากแผ่นบันทึกข้อมูลที่อยู่ในเครื่องคอมพิวเตอร์ แผ่นบันทึกที่มีข้อมูลอยู่ในนั้น ไม่ถือเป็นทรัพย์ที่สามารถลักได้ตามองค์ประกอบความผิดฐานลักทรัพย์

ความเห็นของผู้เขียนมองว่าทรัพย์ที่จะเป็นวัตถุแห่งการกระทำความผิดฐานลักทรัพย์ได้นั้น ต้องเป็นวัตถุที่มีรูปร่างเพื่อจะได้ทราบว่ามี การกระทำที่เป็นการเอาไปอันเป็นองค์ประกอบความผิดฐานลักทรัพย์สำเร็จแล้วหรือไม่ หากเป็นทรัพย์ที่ไม่มีรูปร่างแล้วย่อมไม่สามารถวินิจฉัยองค์ประกอบความรับผิดในการแย่งการครอบครอง และการพาทรัพย์เคลื่อนที่ไปว่าได้เกิดขึ้นเมื่อใด นอกจากนี้ยังต้องปรากฏว่าวัตถุที่มีรูปร่างนั้นต้องเป็นสิ่งที่มิใช่เจ้าของหรืออยู่ในความควบคุมของบุคคลได้ เพราะคุณธรรมทางกฎหมายของความผิดฐานนี้มีได้คุ้มครองตัวทรัพย์แต่คุ้มครองกรรมสิทธิ์และการครอบครองที่บุคคลมีต่อทรัพย์ มิให้ถูกเปลี่ยนแปลงไปโดยมิชอบ ดังนั้นจึงจำเป็นต้องเป็นวัตถุที่มีรูปร่างที่บุคคลสามารถครอบครองและเป็นเจ้าของได้

ดังนั้น สกุลเงินดิจิทัลแม้จะเป็นสิ่งที่มีราคา อาจถือเอาได้ สามารถครอบครองและเป็นเจ้าของได้ แต่สกุลเงินดิจิทัลนั้นเป็นสิ่งที่ไม่มีรูปร่าง จึงไม่เป็นทรัพย์ตามความหมายของความผิดฐานลักทรัพย์ อีกทั้งการไม่รูปร่างนี้ทำให้ไม่มีจุดเกาะเกี่ยวในการพิจารณาองค์ประกอบความผิดฐานลักทรัพย์ที่ได้กำหนดวัตถุแห่งการกระทำไว้ชัดเจนแล้วว่าเป็น ทรัพย์ ซึ่งหมายถึงวัตถุที่มีรูปร่าง ดังนั้นความผิดฐานนี้จึงไม่สามารถปรับใช้กับกรณีการขโมยสกุลเงินดิจิทัลได้

วิเคราะห์ความผิดกรณีขโมยสกุลเงินดิจิทัลกับความผิดฐานทำให้เสียหายซึ่งพินัยกรรมหรือเอกสาร มาตรา 188

จากคำพิพากษาฎีกาที่ 4311/2557 ที่วินิจฉัยให้ข้อมูลคอมพิวเตอร์เป็นเอกสารจึงมีผลทำให้นำความผิดเกี่ยวกับเอกสารมาใช้กับสิ่งที่เป็นข้อมูลคอมพิวเตอร์ได้ จึงมีประเด็นที่ต้องพิจารณาว่าหากสกุลเงินดิจิทัลมีความเป็นข้อมูลคอมพิวเตอร์แล้ว และข้อมูลคอมพิวเตอร์ถือเป็นเอกสาร ดังนั้นสกุลเงินดิจิทัลจะมีสถานะเป็นเอกสารด้วยหรือไม่ ซึ่งจะมีผลทำให้นำความผิดเกี่ยวกับเอกสารมาใช้กับสกุลเงินดิจิทัลได้ด้วย

สำหรับความผิดกรณีการขโมยสกุลเงินดิจิทัลเมื่อนำมาปรับใช้กับมาตรา 188 ซึ่งมีองค์ประกอบความผิด คือ 1) เอาไป 2) ซึ่งเอกสารหรือพินัยกรรมของผู้อื่น (หรือสกุลเงินดิจิทัลของผู้อื่น) 3) โดยเจตนา ก็เป็นความผิดแล้ว เนื่องจากมาตรานี้ไม่มีเจตนาพิเศษเป็นองค์ประกอบความผิด ดังนั้นเพียงแค่มิเจตนาเอาไป แม้จะไม่ได้เอาไปเพื่อแสวงหาประโยชน์ก็เป็นความผิดแล้ว การเอาไปตามมาตรานี้จึงมีความหมายกว้างกว่าการเอาไปตามมาตรา 334 ที่ต้องประกอบด้วยเจตนาพิเศษ (โดยทุจริต) จึงจะเป็นความผิด

อย่างไรก็ตาม แม้การเอาไปเสีย ตามมาตรา 188 จะกว้างจนสามารถครอบคลุมคำว่า เอาไป ในความผิดฐานลักทรัพย์ได้ แต่เมื่อพิจารณาถึงวัตถุประสงค์ของกฎหมายในการกำหนดให้การลักทรัพย์เป็นความผิด คือ กฎหมายต้องการลงโทษผู้ที่เอาทรัพย์ของผู้อื่นไปแสวงหาประโยชน์โดยมิชอบ ซึ่งเป็นการกระทำที่น่าตำหนิ จึงได้กำหนดเจตนาพิเศษเพิ่มเติมขึ้นจากเจตนาธรรมดาเพื่อต้องการแยกให้ชัดเจนว่าผู้นั้นมีเจตนาที่มากกว่าแค่การตั้งใจเอาไปหรือเป็นการเอาไปเพื่อแสวงหาประโยชน์โดยมิชอบซึ่งสมควรจะถูกลงโทษฐานลักทรัพย์ แต่มาตรา 188 เป็นการลงโทษผู้ที่เอาไปทุกกรณีโดยไม่มีแบ่งแยกว่าสมควรถูกลงโทษเพราะขโมยหรือเพราะแค่อายที่

ดังนั้น จะเห็นได้ว่าเจตนาธรรมดากับเจตนาพิเศษ กฎหมายมีขึ้นเพื่อแยกแยะว่าแต่ละความผิดควรลงโทษผู้กระทำความผิดอย่างไร ดังนั้นการนำความผิดตามมาตรา 188 ที่กฎหมายต้องการลงโทษผู้ที่เจตนาเอาไป หรือย้ายที่เอกสาร มาใช้กับฐานความผิดที่กฎหมายต้องการลงโทษผู้ที่มีเจตนาเอาไปเพื่อแสวงหาผลประโยชน์จึงเป็นคนละเรื่องกัน และไม่ควรมานำมาตรา 188 มาใช้กับกรณีการขโมยสกุลเงินดิจิทัล

2) กรณีการใช้ทรัพยากรคอมพิวเตอร์ผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล

(1) บทบัญญัติในประมวลกฎหมายอาญาที่เกี่ยวกับกรณีการใช้ทรัพยากรคอมพิวเตอร์ผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล คือ ความผิดฐานลักทรัพย์ มาตรา 334 จึงมีองค์ประกอบเช่นเดียวกับกรณีการขโมยสกุลเงินดิจิทัลที่ได้กล่าวไว้แล้ว แต่มีความแตกต่างจากกรณีขโมยสกุลเงินดิจิทัลตรงที่กรณีการขโมยสกุลเงินดิจิทัลมีวัตถุประสงค์แห่งการกระทำคือ สกุลเงินดิจิทัลของผู้อื่น แต่กรณีการใช้ทรัพยากรคอมพิวเตอร์ มีวัตถุประสงค์แห่งการกระทำ คือ ทรัพยากรคอมพิวเตอร์ผู้อื่น เพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล

(2) วิเคราะห์กรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัลตามประมวลกฎหมายอาญา

การเอาไปที่จะเป็นความผิดฐานลักทรัพย์ได้นั้นต้องมีลักษณะเป็นการแย่งการครอบครองไปจากเจ้าของเดิม อันมีลักษณะเป็นการตัดกรรมสิทธิ์หรือสิทธิครอบครองโดยเจ้าของเดิมได้ขาดจากการใช้หรือไม่สามารถใช้ประโยชน์จากทรัพย์นั้นได้ แต่การใช้ทรัพยากรผู้อื่นนั้นเป็นการแอบใช้โดยเจ้าของไม่อนุญาต โดยเจ้าของอาจไม่รู้ตัวเพราะยังคงใช้งานได้อยู่แต่

ประสิทธิภาพในการประมวลผลจะช้าลง และทำให้เจ้าของต้องเสียค่าใช้จ่าย ค่าไฟ เพิ่มขึ้นจากเดิม การกระทำดังกล่าวจึงไม่ได้ทำให้เสียหายต่อกรรมสิทธิ์หรือสิทธิครอบครองซึ่งเป็นคุณธรรมทางกฎหมายของความผิดฐานลักทรัพย์ อีกทั้งทรัพย์สินคอมพิวเตอร์ที่เป็นวัตถุแห่งการกระทำนั้นก็มีใช้ทรัพย์สินซึ่งหมายถึงวัตถุที่มีรูปร่าง (ตามที่ได้อธิบายไว้ในหัวข้อทรัพย์สินอันเป็นวัตถุแห่งการกระทำ) ด้วยเหตุที่ลักษณะของการนำไปใช้ที่กรรมสิทธิ์ยังไม่ขาดจากเจ้าของเดิม และทรัพย์สินคอมพิวเตอร์ก็มีใช้วัตถุที่มีรูปร่างอันเป็นองค์ประกอบความผิดฐานลักทรัพย์เช่นเดียวกับกรณีการลักสกุลเงินดิจิทัล ดังนั้นกรณีการใช้ทรัพย์สินคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล จึงอาจไม่นำความผิดฐานลักทรัพย์มาปรับใช้ได้

อย่างไรก็ตามแม้กรณีการใช้ทรัพย์สินคอมพิวเตอร์ของผู้อื่นจะมีบทบัญญัติของกฎหมายที่อาจพอจะเทียบเคียงได้อยู่ คือประมวลกฎหมายอาญาความผิดฐานลักทรัพย์ มาตรา 334 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ความผิดฐาน รบกวน ขัดระบบคอมพิวเตอร์จนไม่สามารถทำงานได้ตามปกติ มาตรา 10 แต่เมื่อนำมาปรับใช้แล้วจะเห็นว่ายังมีข้อจำกัดที่ไม่เป็นไปตามองค์ประกอบความผิดที่กฎหมายกำหนด อีกทั้งการความผิดในกรณีนี้เป็นกรณีก่อให้เกิดไปซึ่งผลประโยชน์โดยมิชอบจึงเป็นการกระทำที่เจตนาจึงสมควรกำหนดให้เป็นความผิดอาญาฐานใหม่เป็นการเฉพาะได้

### 3.4 ความร่วมมือทางอาญาระหว่างประเทศเกี่ยวกับสกุลเงินดิจิทัล

การกระทำความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัลสามารถกระทำได้จากทั่วทุกมุมทั่วโลกที่มีการเชื่อมต่อกับระบบอินเทอร์เน็ต จึงเป็นการก่ออาชญากรรมได้อย่างไรพรมแดน สร้างความเสียหายให้กับผู้ที่อยู่ในประเทศต่าง ๆ ได้พร้อมกันหลายประเทศ อาชญากรรมที่มีลักษณะข้ามชาติเช่นนี้จึงยากแก่การบังคับใช้กฎหมายของประเทศใดประเทศหนึ่ง ดังนั้นความร่วมมือระหว่างประเทศจึงเป็นกลไกสำคัญในการป้องกันและปราบปรามอาชญากรรมดังกล่าว ในหัวข้อนี้จะแบ่งความร่วมมือทางอาญาระหว่างประเทศออกเป็น ความร่วมมือระหว่างประเทศรูปแบบอนุสัญญา และความร่วมมือระหว่างประเทศรูปแบบองค์กร ดังนี้

#### 3.4.1 ความร่วมมือทางอาญาระหว่างประเทศรูปแบบอนุสัญญา

##### 3.4.1.1 อนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ (Convention on Cybercrime)

อนุสัญญาว่าด้วยอาชญากรรมทางคอมพิวเตอร์หรืออนุสัญญากรุงบูดาเปสต์ จัดทำขึ้นโดยสภายุโรป (Council of Europe) ได้มีการเปิดให้ลงนามในเมืองบูดาเปสต์เมื่อวันที่ 23

พฤศจิกายน 2544 และมีผลบังคับใช้เมื่อ 1 กรกฎาคม 2547 ปัจจุบันมี 66 ประเทศที่ให้สัตยาบัน และมี 2 ประเทศที่ลงนามในอนุสัญญาแล้ว แต่ยังไม่ให้สัตยาบัน<sup>274</sup> แม้ประเทศไทยจะไม่เข้าร่วมลงนามในอนุสัญญานี้ แต่ได้นำหลักการที่สำคัญของอนุสัญญาดังกล่าวมาเป็นหนึ่งในต้นแบบของกฎหมายว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ทั้งนี้วัตถุประสงค์ของอนุสัญญาฯ มีสามประการ คือ 1) สร้างนโยบายร่วมกันทางด้านอาชญากรรมทางคอมพิวเตอร์ภายในกลุ่มรัฐภาคีให้มีความสอดคล้องไปในทิศทางเดียวกัน 2) สร้างกระบวนการดำเนินคดีการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ของรัฐภาคี โดยให้อำนาจแก่เจ้าพนักงาน ในการรวบรวมพยานหลักฐานโดยเฉพาะพยานหลักฐานที่อยู่ในรูปของข้อมูลอิเล็กทรอนิกส์ 3) ส่งเสริมความร่วมมือระหว่างประเทศให้เป็นไปตามวัตถุประสงค์ของอนุสัญญา

ทั้งนี้เนื้อหาของอนุสัญญากรุงบูดาเปสต์แบ่งออกเป็น 4 บท โดยบทที่ 1 จะให้คำจำกัดความของคำศัพท์สำคัญในอนุสัญญา ได้แก่ ระบบคอมพิวเตอร์ ข้อมูลคอมพิวเตอร์ ผู้ให้บริการ (Service Provider) และข้อมูลจราจร (Traffic Data) บทที่ 2 กำหนดรายละเอียดเกี่ยวกับการทำกฎหมายภายในรัฐด้านอาชญากรรมทางคอมพิวเตอร์สอดคล้องกัน ทั้งด้านกฎหมายสารบัญญัติและวิธีบัญญัติอนุสัญญากรุงบูดาเปสต์จะกำหนดฐานความผิดสำหรับการกระทำ 9 รูปแบบไว้ในข้อ 2-10 ได้แก่ การเข้าสู่ระบบโดยผิดกฎหมาย การดักจับข้อมูลโดยผิดกฎหมาย การเข้าแทรกแซงข้อมูล การเข้าแทรกแซงระบบ การใช้อุปกรณ์โดยมิชอบ การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์ การฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์การกระทำความผิดเกี่ยวกับสิ่งลามกอนาจารเด็กและการกระทำความผิดเกี่ยวกับทรัพย์สินทางปัญญา การกระทำที่จะตกเป็นความผิดนั้นจะต้องกระทำไปโดยเจตนา และปราศจากสิทธิ และกำหนดรายละเอียดเกี่ยวกับความผิดฐานผู้ใช้ผู้สนับสนุนความรับผิดชอบบุคคลและมาตรการบังคับทางอาญาไว้ด้วย

บทที่ 3 ของอนุสัญญาได้กำหนดหลักเกณฑ์ให้ความร่วมมือทางอาญาระหว่างประเทศโดยให้รัฐภาคีให้ความร่วมมือทางอาญาระหว่างประเทศให้กว้างที่สุดเท่าที่จะทำได้ อีกทั้งให้ลดอุปสรรคในการให้ความร่วมมือ เพื่อให้การดำเนินการต่าง ๆ นั้นสามารถรวบรวมหลักฐานสำคัญได้ทันท่วงที โดยอนุสัญญายังกำหนดให้ความร่วมมือทางอาญาครอบคลุมไปถึงการก่ออาชญากรรมตามฐานความผิดที่กำหนดไว้ในข้อ 2-11 ของอนุสัญญาและอาชญากรรมประเภทอื่น ๆ ที่ใช้คอมพิวเตอร์เป็นเครื่องมือ รวมถึงการรวบรวมหลักฐานที่อยู่ในรูปแบบข้อมูลคอมพิวเตอร์ของอาชญากรรมทุก

---

<sup>274</sup> Council of Europe, **Chart of Signatures and Ratifications of Treaty 185**, Retrieved April 11, 2021 from <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=185>

ประเภท<sup>275</sup> ทั้งนี้การให้ความร่วมมือทางอาญาระหว่างประเทศภายใต้อนุสัญญานี้จะประกอบไปด้วย การส่งตัวผู้ร้ายข้ามแดนและการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย ซึ่งได้มีการจัดตั้ง เครือข่ายจุดติดต่อตลอดเวลา เพื่อเป็นจุดติดต่อประสานงานกันระหว่างรัฐภาคีเพื่อให้ความช่วยเหลือ ในด้านต่าง ๆ ที่เกี่ยวข้องกับอาชญากรรมทางคอมพิวเตอร์ได้อย่างทันที่

ส่วนสุดท้ายของอนุสัญญา (Final Provisions) จะเกี่ยวข้องกับการบริหารอนุสัญญา โดยทั่วไป ได้แก่ บทบัญญัติเกี่ยวกับการเข้าผูกพันตามอนุสัญญาด้วยการลงนามหรือการเข้า ภาควิชาการที่จำกัดผลการบังคับใช้อนุสัญญาด้วยการตั้งข้อสงวน การประกาศเขตแดน บังคับใช้การประกาศตีความรายละเอียดอนุสัญญาบางส่วน รวมถึงการปรับปรุงแก้ไขอนุสัญญา และการระงับข้อพิพาท เป็นต้น

ดังนั้นการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลจำเป็นต้องอาศัยคอมพิวเตอร์เป็น ช่องทางในการกระทำความผิด จึงมีความผิดบางส่วนเกี่ยวข้องกับอาชญากรรมคอมพิวเตอร์ใน ลักษณะข้ามชาติ อนุสัญญาฉบับนี้จึงได้ให้ความสำคัญกับการกระทำความผิดในลักษณะดังกล่าว โดย กำหนดมาตรการความร่วมมือระหว่างประเทศมาใช้ในการป้องกันและปราบปรามการกระทำความผิด ไว้ดังนี้

#### 1) การให้ความช่วยเหลือซึ่งกันและกันทางกฎหมาย

รัฐภาคีต้องให้ความช่วยเหลืออาชญากรรมทุกประเภทที่เกี่ยวข้องกับการใช้ ระบบคอมพิวเตอร์และข้อมูลทางคอมพิวเตอร์ให้มากที่สุดเท่าที่จะทำได้ การให้ความช่วยเหลือจะ ครอบคลุมไปถึงการรวบรวมหลักฐานในรูปแบบอิเล็กทรอนิกส์ในคดีอาชญากรรมต่าง ๆ<sup>276</sup> ทั้งนี้ ขอบเขตดังกล่าวจะกว้างขวางกว่าในกรณีการส่งตัวผู้ร้ายข้ามแดน เพราะการให้ความช่วยเหลือซึ่งกัน และกันทางกฎหมายนั้นเป็นไปเพื่อการแสวงหาหลักฐานเพื่อระบุตัว จับกุม และดำเนินคดีแก่ผู้กระทำ ความผิด<sup>277</sup> จึงเป็นกรณีเร่งด่วนกว่าการส่งตัวผู้ร้ายข้ามแดน ซึ่งได้ตัวผู้กระทำผิดและถูกตัดสินลงโทษ แล้ว ความช่วยเหลือดังกล่าวยังรวมถึงเรื่องการเงินด้วย<sup>278</sup> นอกจากนี้การให้ความช่วยเหลือซึ่งกันและ กันต้องอยู่ภายใต้เงื่อนไขว่าการความผิดทางอาญาที่จะให้ความช่วยเหลือซึ่งกันและกันได้ต้องเป็นความผิดของ ทั้งสองรัฐ ทั้งนี้ไม่ว่าจะกำหนดความผิดไว้เช่นเดียวกัน หรือกำหนดประเภทของความผิดไว้แบบ เดียวกันหรือระบุความผิดโดยใช้คำศัพท์เดียวกับที่รัฐร้องขอหรือไม่ก็ตาม และในอนุสัญญานี้ยังได้

<sup>275</sup> ข้อ 23 Convention on Cybercrime

<sup>276</sup> ข้อ 23 Convention on Cybercrime

<sup>277</sup> ข้อ 25 วรรค 1 Convention on Cybercrime

<sup>278</sup> ข้อ 25 วรรค 4 Convention on Cybercrime

กำหนดเงื่อนไขและกระบวนการสำหรับให้ความช่วยเหลือในกรณีที่รัฐภาคีของอนุสัญญาที่ไม่ได้ทำข้อตกลงด้านการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายไว้ระหว่างกันอีกด้วย<sup>279</sup>

นอกจากนี้ยังมีข้อตกลงในส่วนของ การดำเนินการโดยให้หน่วยงานกลางของรัฐภาคีติดต่อระหว่างกันได้อย่างสะดวกรวดเร็ว อนุสัญญาได้กำหนดให้รัฐภาคีส่งมอบชื่อและที่อยู่ติดต่อของหน่วยงานที่ทำหน้าที่เป็นหน่วยงานกลางไปยังเลขาธิการของสภายุโรป โดยเลขาธิการสภายุโรปจะต้องจัดทำรายชื่อหน่วยงานให้ทันกับข้อมูลที่ได้รับอยู่เสมอ<sup>280</sup> ข้อกำหนดดังกล่าวจึงเป็นการเพิ่มประสิทธิภาพในการดำเนินการความร่วมมือระหว่างประเทศเนื่องจากทำให้รัฐภาคีสามารถทราบได้ว่าตนต้องติดต่อหน่วยงานใดในกรณีไหนบ้าง เพื่อดำเนินการวางแผนรองรับล่วงหน้าได้

## 2) การส่งผู้ร้ายข้ามแดน

ความผิดที่ส่งตัวผู้ร้ายข้ามแดนได้ตามอนุสัญญากรุงบูดาเปสต์นั้น แบ่งออกเป็น 4 ประเภท ดังนี้

(1) ความผิดต่อความลับ ความสมบูรณ์และความพร้อมใช้งานของข้อมูล และระบบคอมพิวเตอร์ (Offences against Confidentiality Integrity and Availability ได้แก่ การเข้าถึงโดยผิดกฎหมาย<sup>281</sup> (Illegal Access) การดักจับข้อมูลโดยผิดกฎหมาย<sup>282</sup> (Illegal Interception) การเข้าแทรกแซงข้อมูลคอมพิวเตอร์<sup>283</sup> (Data Interception) การแทรกแซงระบบคอมพิวเตอร์<sup>284</sup> เป็นต้น

(2) การกระทำผิดที่เกี่ยวข้องกับคอมพิวเตอร์ (Computer-related Offences) การปลอมแปลงที่เกี่ยวข้องกับคอมพิวเตอร์<sup>285</sup> การฉ้อโกงที่เกี่ยวข้องกับคอมพิวเตอร์<sup>286</sup>

(3) การกระทำความผิดที่เกี่ยวข้องกับเนื้อหา (Content-related Offences) ได้แก่การกระทำความผิดเกี่ยวกับวัตถุลามกอนาจารเด็ก<sup>287</sup>

<sup>279</sup> ข้อ 27 Convention on Cybercrime

<sup>280</sup> ข้อ 27 วรรค 2 c Convention on Cybercrime

<sup>281</sup> ข้อ 2 Convention on Cybercrime

<sup>282</sup> ข้อ 3 Convention on Cybercrime

<sup>283</sup> ข้อ 4 Convention on Cybercrime

<sup>284</sup> ข้อ 5 Convention on Cybercrime

<sup>285</sup> ข้อ 7 Convention on Cybercrime

<sup>286</sup> ข้อ 8 Convention on Cybercrime

<sup>287</sup> ข้อ 9 วรรค 2 Convention on Cybercrime

(4) การกระทำผิดที่เกี่ยวข้องกับการละเมิดลิขสิทธิ์และสิทธิข้างเคียง ความผิดเหล่านี้จะต้องเป็นความผิดที่สามารถดำเนินการลงโทษได้ตามกฎหมายภายในของรัฐทั้งสองฝ่าย โดยโทษที่ได้รับสำหรับฐานความผิดเหล่านี้ต้องเป็นการลงโทษด้วยการจำคุก อิสรภาพที่มีระยะเวลา 1 ปีเป็นอย่างน้อย<sup>288</sup> อย่างไรก็ตาม หากรัฐภาคีมีสนธิสัญญาสัญญาส่งตัวผู้ร้ายข้ามแดนหรือมีข้อตกลงที่มีฐานมาจากกฎหมายในลักษณะต่างตอบแทนซึ่งกำหนดมาตรฐานโทษขั้นต่ำไว้เป็นอย่างอื่นหรือเป็นไปตามเงื่อนไขที่กำหนดใน The European Convention on Extradition รัฐภาคีสามารถยึดหลักการตามสนธิสัญญาหรือข้อตกลงเหล่านั้นแทนได้ นอกจากนี้ในการส่งตัวผู้ร้ายข้ามแดนที่แม้จะมีข้อกำหนดเป็นไปตามกฎหมายของรัฐผู้รับคำขอให้ส่งตัวผู้ร้ายข้ามแดนหรือตามสนธิสัญญาด้านการส่งตัวผู้ร้ายข้ามแดนนั้น แต่หากรัฐภาคีมีกฎหมายภายในหรือได้จัดทำสนธิสัญญาที่เอื้ออำนวยให้สามารถส่งตัวผู้ร้ายข้ามแดนได้ในฐานความผิดที่อนุสัญญาฉบับนี้ไม่ครอบคลุมหรือสามารถให้รัฐให้ความช่วยเหลือด้วยวิธีการนอกอนุสัญญาได้ ทั้งนี้รัฐภาคียังคงสามารถดำเนินการตามกฎหมายภายในของตนหรือสนธิสัญญาฉบับอื่น ๆ ได้<sup>289</sup>

อย่างไรก็ตามมาตรการการให้ความช่วยเหลือซึ่งกันและกันทางกฎหมายด้วยวิธีการอื่น ๆ ที่ในอนุสัญญาไม่ได้ระบุไว้ยังสามารถนำมาปรับใช้ได้ภายใต้เงื่อนไขที่รัฐภาคีสามารถปรับใช้กฎหมายที่เกี่ยวข้องและมีผลบังคับใช้กับรัฐภาคีทั้งระดับภายในและระหว่างประเทศได้ควบคู่ไปกับการปฏิบัติตามบทบัญญัติด้านความร่วมมือระหว่างประเทศที่ประเทศนั้น ๆ เป็นภาคี<sup>290</sup>

#### 3.4.1.2 อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย ค.ศ. 1999 (International Convention for the Suppression of the Financing of Terrorism, 1999)

อนุสัญญาฉบับนี้มีวัตถุประสงค์เพื่อสกัดกั้นแหล่งเงินทุนของผู้ก่อการร้าย กลุ่ม หรือองค์กรการก่อการร้ายที่มีการระดมทุนซึ่งการระดมทุนนี้รวมถึงการระดมทุนด้วยสกุลเงินดิจิทัล ซึ่งปัจจุบันสกุลเงินดิจิทัลถูกใช้เป็นช่องทางในการทำธุรกรรมเพื่อสนับสนุนการก่อการร้ายในหลายประเทศทั่วโลก ดังนั้นในอนุสัญญาจึงกำหนดให้การกระทำดังกล่าว เป็นความผิดอาญา (Criminalization Provision) ตามกฎหมายภายในของประเทศสมาชิกและกำหนดบทลงโทษที่เหมาะสม โดยคำนึงถึงความร้ายแรงของความผิดแก่ผู้กระทำความผิดทั้งที่เป็นบุคคลธรรมดาและนิติ

<sup>288</sup> ข้อ 24 วรรค 1 b Convention on Cybercrime

<sup>289</sup> ข้อ 24 วรรค 5 Convention on Cybercrime

<sup>290</sup> ข้อ 23 Convention on Cybercrime

บุคคล<sup>291</sup> และให้แต่ละรัฐดำเนินมาตรการที่เหมาะสมตามหลักกฎหมายภายในของตนเพื่อพิสูจน์ทราบ และอายัดหรือยึดเงิน หรือทุนใด ๆ ซึ่งรวมถึงสกุลเงินดิจิทัลที่ได้ใช้หรือจัดสรรเพื่อมุ่งประสงค์ในการกระทำความผิดสนับสนุนทางการเงินแก่การก่อการร้าย รวมทั้งทรัพย์สินที่ได้จากการกระทำความผิด<sup>292</sup> ทั้งทางตรงและทางอ้อมโดยมีเจตนาระดมทุนเหล่านั้นนำไปใช้หรือรู้ว่าจะถูกนำไปใช้เพื่อการก่อการร้าย ไม่ว่าทั้งหมดหรือบางส่วนถือว่าเป็นความผิด<sup>293</sup> โดยให้แต่ละประเทศร่วมมือกันในการแลกเปลี่ยนข้อมูลข่าวสารที่เกี่ยวข้องและกำหนดมาตรการให้สถาบันการเงินต่าง ๆ มีหน้าที่ต้องรายงานธุรกรรมขนาดใหญ่ หรือธุรกรรมที่น่าสงสัยต่อหน่วยงานที่รับผิดชอบ และเก็บรักษาเอกสารที่เกี่ยวข้องไว้เป็นระยะเวลาไม่น้อยกว่า 5 ปี<sup>294</sup>

อนุสัญญาดังกล่าวยังสอดคล้องกับข้อมติคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ 1267: UNSCR 1267 (1999) ที่กำหนดให้ประเทศต่าง ๆ ยึด และอายัดทรัพย์สินของบุคคลที่ได้รับการระบุชื่อโดยคณะมนตรีฯ และข้อมติคณะมนตรีความมั่นคงแห่งสหประชาชาติที่ 1373: UNSCR 1373 (2001) กำหนดให้ทุกรัฐต้องให้หลักประกันว่าผู้มีส่วนในการสนับสนุนทางการเงิน การวางแผน หรือปฏิบัติการก่อการร้าย หรือให้การสนับสนุนการก่อการร้ายต้องถูกนำตัวมาดำเนินการตามกฎหมายและให้หลักประกันว่ากฎหมายและกฎข้อบังคับภายในรัฐต้องระบุให้การก่อการร้ายเป็นการกระทำที่ผิดกฎหมายอาญาร้ายแรงและต้องกำหนดบทลงโทษตามความร้ายแรงของการกระทำนั้น ๆ รวมถึงการระบุรายชื่อบุคคล (Designated List) โดยประเทศต่าง ๆ สามารถกำหนดและจัดทำรายชื่อบุคคล กลุ่มหรือองค์กรที่เกี่ยวข้องกับการก่อการร้ายของประเทศตนเองได้ เช่น OFAC List เป็นต้น

<sup>291</sup> International Convention for the Suppression of the Financing of Terrorism 1999 Article ข้อ 4 Article 2

<sup>292</sup> Article 8, International Convention for the Suppression of the Financing of Terrorism 1999

<sup>293</sup> Article 3, International Convention for the Suppression of the Financing of Terrorism 1999, “For an act to constitute an offence set forth in paragraph

1, it shall not be necessary that the funds were actually used to carry out an offence referred to in paragraph 1, subparagraphs (a) or (b)”

<sup>294</sup> สำนักงานป้องกันและปราบปรามการฟอกเงิน, **ความเป็นมาและวัตถุประสงค์**, คำนวณที่ 11 เมษายน 2564 จาก <https://www.amlo.go.th/index.php/th/designated-person/2016-05-22-11-51-34>

เพื่อนำไปสู่การอายัดเงินและทรัพย์สินของผู้ก่อการร้าย พยายามก่อการร้ายหรือผู้ที่เข้าร่วม ผู้อำนวยการ ความสะดวกให้แก่การก่อการร้าย และผู้ดำเนินการตามคำสั่งของบุคคลข้างต้น<sup>295</sup>

ความร่วมมือระหว่างประเทศภายใต้อนุสัญญาสหประชาชาติว่าด้วยการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย ค.ศ. 1999

ในส่วนที่เกี่ยวกับการประสานความร่วมมือกันในทางระหว่างประเทศของรัฐภาคีอนุสัญญาฉบับนี้ได้กำหนดไว้ ดังต่อไปนี้

1) การให้ความช่วยเหลือซึ่งกันและกันทางอาญา<sup>296</sup> ได้มีมาตรการในการให้ความร่วมมือกันระหว่างรัฐภาคีในการให้ความช่วยเหลือซึ่งกันและกันในการสืบสวนสอบสวนทางอาญาและการได้มาซึ่งพยานหลักฐานที่จำเป็นต่อการพิจารณาคดี และไม่สามารถปฏิเสธคำร้องขอความช่วยเหลือซึ่งกันและกันทางอาญาด้วยเหตุผลว่าเป็นความลับทางธนาคาร เป็นความผิดทางการเงิน หรือเป็นความผิดทางการเมืองหรือความผิดที่เกี่ยวกับความผิดทางการเมือง หรือความผิดที่เกิดจากแรงจูงใจทางการเมืองทั้งนี้ให้ประเทศต่าง ๆ ที่มีสนธิสัญญาหรือข้อตกลงว่าด้วยความช่วยเหลือซึ่งกันและกันทางอาญาปฏิบัติตามสนธิสัญญา แต่ในกรณีที่ไม่ได้มีสนธิสัญญาหรือข้อตกลงดังกล่าวต่อกันให้มีความร่วมมือช่วยเหลือและปฏิบัติตามกฎหมายภายในของตน<sup>297</sup>

2) การส่งผู้ร้ายข้ามแดน<sup>298</sup> การกระทำความผิดตามอนุสัญญานี้เป็นความผิดที่รัฐภาคีสามารถส่งผู้ร้ายข้ามแดนได้ แต่การส่งผู้ร้ายข้ามแดนโดยหลักแล้วกำหนดข้อยกเว้นไว้ 3 กรณี คือ ความผิดทางการเมือง ความผิดทางการทหาร และความผิดทางการเงิน แต่สำหรับอนุสัญญานี้มิให้นำข้อยกเว้นในการส่งผู้ร้ายข้ามแดนดังกล่าวมาใช้<sup>299</sup> ดังนั้น รัฐภาคีจึงไม่สามารถปฏิเสธคำร้องขอส่งผู้ร้ายข้ามแดนโดยอาศัยเหตุดังกล่าวได้

<sup>295</sup> Article 5, International Convention for the Suppression of the Financing of Terrorism 1999

<sup>296</sup> Article 12–15, International Convention for the Suppression of the Financing of Terrorism 1999

<sup>297</sup> ศิริมาศ สุขประสงค์, **การป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายตามกฎหมายระหว่างประเทศและผลกระทบทางกฎหมายสำหรับประเทศไทย** (วิทยานิพนธ์ปริญญาโทมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2556), หน้า 18.

<sup>298</sup> Article 11, 13-15, International Convention for the Suppression of the Financing of Terrorism 1999

<sup>299</sup> Article 13-14, International Convention for the Suppression of the Financing of Terrorism 1999

3) การโอนตัวนักโทษ<sup>300</sup> การโอนตัวบุคคลซึ่งอยู่ในระหว่างการควบคุมตัว หรือต้องรับโทษอยู่ในรัฐภาคีใดรัฐหนึ่ง หากมีการร้องขอจากรัฐภาคีอีกรัฐหนึ่งเพื่อให้บุคคลดังกล่าวไปปรากฏตัวในการชี้ตัวให้การ หรือให้ความช่วยเหลืออื่นใดในการให้ได้มาซึ่งพยานหลักฐานสำหรับการสืบสวนสอบสวนหรือฟ้องร้องดำเนินคดีความผิดตามที่กำหนดไว้สามารถกระทำได้ ภายใต้เงื่อนไขต่อไปนี้ (ก) บุคคลนั้นต้องให้ความยินยอมโดยรู้ข้อเท็จจริงและโดยสมัครใจและ (ข) พนักงานเจ้าหน้าที่ของรัฐทั้งสองตกลงกันภายในเงื่อนไขที่รัฐทั้งสองอาจเห็นสมควรเมื่อมีการโอนตัวนักโทษแล้ว ให้รัฐซึ่งได้รับการโอนตัวบุคคลนั้นมีอำนาจและพันธกรณีที่จะควบคุมตัวผู้นั้นไว้ในที่ควบคุม เว้นแต่จะได้รับการร้องขอหรือได้รับมอบอำนาจเป็นอย่างอื่น

4) การแลกเปลี่ยนข้อมูลข่าวสาร<sup>301</sup> 12 อนุสัญญา ได้กำหนดให้บรรดารัฐภาคีจะต้องร่วมมือกันในการป้องกันการกระทำความผิดตามที่กำหนดไว้ในอนุสัญญาโดยการแลกเปลี่ยนข้อมูลข่าวสารที่ถูกต้องและได้รับการพิสูจน์ยืนยันแล้วตามกฎหมายภายในของรัฐนั้น เพื่อป้องกันการกระทำความผิด โดยกำหนดให้มีการจัดตั้งช่องทางการติดต่อระหว่างหน่วยงานที่เกี่ยวข้อง และหน่วยงานที่มีอำนาจในการให้บริการข้อมูลข่าวสาร รวมถึงการแลกเปลี่ยนข้อมูลผ่านองค์กรตำรวจสากล (Interpol)

### 3.4.2 ความร่วมมือทางอาญาระหว่างประเทศรูปแบบองค์กร

#### 3.4.2.1 สำนักงานป้องกันยาเสพติดและปราบปรามอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime (UNODC))

United Nations Office on Drugs and Crime (UNODC) หรือ สำนักงานป้องกันยาเสพติดและปราบปรามอาชญากรรมแห่งสหประชาชาติ มีบทบาทที่สำคัญในการเสริมสร้างความร่วมมือระหว่างประเทศในด้านการป้องกันยาเสพติด อาชญากรรม การก่อการร้าย องค์กรอาชญากรรมข้ามชาติซึ่งรวมถึงอาชญากรรมคอมพิวเตอร์ และต่อต้านการทุจริต<sup>302</sup>

UNODC ได้เห็นความสำคัญเทคโนโลยีที่เกิดขึ้นใหม่ที่เรียกว่า “สกุลเงินดิจิทัล” ซึ่งเป็นสกุลเงินที่ไม่ได้ออกโดยรัฐบาลของประเทศใด ผู้ทำธุรกรรมสามารถทำกันเองได้โดยตรง โดยไม่

<sup>300</sup> Article 16, International Convention for the Suppression of the Financing of Terrorism 1999

<sup>301</sup> Article 18, International Convention for the Suppression of the Financing of Terrorism 1999

<sup>302</sup> United Nations Office on Drugs and Crime, **UNODC Strategy 2021-2025**, Retrieved April 11, 2021 from <https://www.unodc.org/unodc/en/strategy/index.html>

ต้องมีธนาคารหรือตัวกลางใดๆที่ทำหน้าที่ในตรวจสอบและเก็บข้อมูลธุรกรรมดังกล่าว นอกจากนี้การเข้าทำธุรกรรมสามารถทำได้ผ่านระบบอินเทอร์เน็ตโดยไม่มีการเรียกร้องให้เปิดเผยตัวตน จึงสะดวก รวดเร็ว และมีความเป็นส่วนตัวสูง ด้วยคุณลักษณะที่กล่าวมานี้ได้เปิดโอกาสให้อาชญากรอาศัยประโยชน์จากเทคโนโลยีเดียวกันนี้ไปใช้ในการกระทำความผิด ในขณะที่สกุลเงินดิจิทัลพัฒนาขึ้นอย่างรวดเร็วและสามารถใช้เครือข่ายอินเทอร์เน็ตเชื่อมโยงบุคคลข้ามข้อจำกัดทางภูมิศาสตร์ แต่ความแตกต่างของกฎหมายแต่ละประเทศและเขตอำนาจในการบังคับใช้ยังเป็นอุปสรรคต่อป้องกันและปราบปราม UNODC ได้ตระหนักถึงปัญหาดังกล่าวจึงได้จัดการประชุมเชิงปฏิบัติการเพื่อสะท้อนปัญหาและหาแนวทางความร่วมมือระหว่างประเทศ ซึ่งมีสาระสำคัญ<sup>303</sup> ดังนี้

1) สนับสนุนให้มีกฎระเบียบในการขอข้อมูลระดับตัวตนในการทำธุรกรรม (Know Your Customer Rules) และการนำเทคโนโลยีมาใช้ในการวิเคราะห์ธุรกรรมที่ผิดกฎหมาย เพื่อเป็นแนวทางที่จะบรรลุวัตถุประสงค์ทางอาญาในการป้องกันการนำสกุลเงินดิจิทัลไปใช้ในทางที่มีชอบได้

2) พัฒนาเทคนิคการป้องกันและสอบสวนที่มีประสิทธิภาพให้สามารถปรับให้เข้ากับการเปลี่ยนแปลงของเทคโนโลยีและการใช้งานต่าง ๆ ของสกุลเงินดิจิทัลเพื่อลดภัยคุกคามที่เกี่ยวข้องกับการใช้ในทางที่มีชอบ

3) ทั้งสองแนวทางที่ได้นำเสนอมาข้างต้น จะก่อให้เกิดประสิทธิภาพหากมีการเผยแพร่แนวทางดังกล่าวและนำไปปฏิบัติอย่างเป็นรูปธรรม ดังนั้นจึงมีการส่งเสริมให้มีการฝึกอบรมความรู้และทักษะที่จำเป็นแก่ผู้สืบสวนอาชญากรรมสกุลเงินดิจิทัลในการติดตาม ตรวจสอบ การกระทำผิดอย่างมีประสิทธิภาพ ดังจะเห็นได้จากตั้งแต่ปี ค.ศ. 2017 องค์กรสหประชาชาติได้เริ่มมีการจัดอบรมเพื่อส่งเสริมความรู้และทักษะที่จำเป็นเกี่ยวกับสกุลเงินดิจิทัลในองค์กรก่อการร้าย โดย Michael Gronager CEO ของ Chainalysis Inc. กล่าวว่า Chainalysis Inc. ได้ร่วมมือกับ UNODC ในการจัดโครงการฝึกอบรมผู้ฝึกอบรมที่ครอบคลุมเกี่ยวกับการวิเคราะห์ การติดตาม และการตรวจสอบสกุลเงินดิจิทัล ซึ่งเป็นสิ่งที่สำคัญอย่างยิ่ง การใช้สกุลเงินเสมือนมีการเติบโตอย่างต่อเนื่อง ดังนั้นผู้ที่เกี่ยวข้องไม่ว่าจะเป็นนักวิเคราะห์ ผู้บังคับใช้กฎหมาย และอัยการจำเป็นต้องได้รับการฝึกอบรมเพื่อรวบรวมและเผยแพร่ข้อมูลที่ได้จากศูนย์ซื้อขายแลกเปลี่ยน โบรเกอร์ รวมถึง

<sup>303</sup> United Nations, **Workshop 4. Current Crime Trends, Recent**

**Developments and Emerging Solutions, in Particular New Technologies as Means for and Tools against Crime, Background paper prepared by the Secretariat,**

Retrieved January 5, 2023 from [https://documents-dds-ny.un.org/doc/UNDOC/](https://documents-dds-ny.un.org/doc/UNDOC/GEN/V20/005/48/PDF/V2000548.pdf?OpenElement)

[GEN/V20/005/48/PDF/V2000548.pdf?OpenElement](https://documents-dds-ny.un.org/doc/UNDOC/GEN/V20/005/48/PDF/V2000548.pdf?OpenElement)

สนับสนุนความเชี่ยวชาญของหน่วยงานระดับประเทศในการป้องกันการนำเทคโนโลยีที่เป็นนวัตกรรมนี้ไปใช้ในทางที่มีชอบ<sup>304</sup>

จากแนวทางข้างต้นจึงเป็นที่มาของการประชุมสหประชาชาติว่าด้วยการป้องกันอาชญากรรมและความยุติธรรมทางอาญา หรือ United Nations Congress on Crime Prevention and Criminal Justice (The United Nations Congress on Crime Prevention and Criminal Justice-UN Crime Congress) เป็นการประชุมที่รวบรวมผู้เกี่ยวข้องทั้งผู้กำหนดนโยบาย ผู้ปฏิบัติงาน ผู้แทนสหประชาชาติ หน่วยงานรัฐ และหน่วยงานที่ไม่ใช่รัฐ ตลอดจนผู้เชี่ยวชาญด้านการป้องกันอาชญากรรม การบังคับใช้กฎหมาย การลงโทษทางอาญา ระบบศาล และการราชทัณฑ์ และผู้เชี่ยวชาญเกี่ยวกับประเด็นที่เกิดขึ้นใหม่อื่น ๆ มาร่วมประชุมหารือกันเกี่ยวกับปัญหาความท้าทายใหม่ ๆ ในด้านการป้องกันอาชญากรรมและการอำนวยความยุติธรรมทางอาญา ได้จัดให้มีการประชุมระดับภูมิภาคครั้งที่ 14 ที่ประเทศญี่ปุ่น โดยมีชื่อหัวข้อว่า “การส่งเสริมการป้องกันอาชญากรรม ความยุติธรรมทางอาญา และหลักนิติธรรม เพื่อนำไปสู่การบรรลุเป้าหมายการพัฒนาที่ยั่งยืน ค.ศ. 2030”<sup>305</sup> ในการประชุมมีการกล่าวถึงปัญหาของสกุลเงินดิจิทัลที่เริ่มเข้ามาอยู่เบื้องหลังการก่อการร้ายในหลายประเทศ ภูมิภาคเอเชียตะวันออกเฉียงใต้หลายประเทศยังไม่มีกฎหมายเท่าทันกับคดีไซเบอร์หรือคดีที่มีความซับซ้อนทางเทคโนโลยี การร่วมกันหาแนวทางในการรับมือกับปัญหาอาชญากรรมข้ามชาติที่เกี่ยวข้องกับสกุลเงินดิจิทัลอาจเกิดขึ้นได้ในอนาคต ในประเด็นนี้ นายจูเลียน การ์ซานี รองผู้แทนประจำภูมิภาคเอเชียตะวันออกเฉียงใต้และแปซิฟิก สำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (UNODC) มีความเห็นว่า “ปัจจุบันหลายประเทศในเอเชียตะวันออกเฉียงใต้ใช้สกุลเงินดิจิทัลมากติดอันดับต้น ๆ ของโลก เงินมูลค่าหลายพันล้านดอลลาร์ถูกแลกเปลี่ยนข้ามพรมแดนผ่านระบบและการแลกเปลี่ยนด้วยสกุลเงินดิจิทัล จึงจำเป็นต้องหามาตรการในการรับมือกับเรื่องดังกล่าว ซึ่งในปัจจุบันยังไม่มีกฎหมายหรือมาตรการใด ๆ ทางกฎหมายออกมารองรับ และการสั่งห้ามใช้หรือหยุดใช้งานคงจะเป็นไปไม่ได้ เพราะมันเป็นระบบที่เกิดขึ้นออนไลน์”

<sup>304</sup> United Nations Office on Drugs and Crime, **UNODC Launches Training to Tackle Cryptocurrency-Enabled Organized Crime**, Retrieved April 11, 2021 from <https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launches-training-to-tackle-money-laundering-and-bitcoin-banking-fraud.html>

<sup>305</sup> สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน), **บทบาท TIJ ในการประชุม Crime Congress 2021**, ค้นวันที่ 11 เมษายน 2564 จาก <https://www.tijthailand.org/th/highlight/detail/tij-s-role-in-crime-congress-2020>

ดังนั้นการแลกเปลี่ยนความรู้ เทคโนโลยี บทเรียนในการสืบสวนปราบปรามอาชญากรรมดังกล่าวระหว่างหน่วยงานของแต่ละประเทศจึงเป็นสิ่งสำคัญ

จากการประชุมดังกล่าวมีประเด็นสาระสำคัญ ดังนี้

- 1) กำหนดยุทธศาสตร์ที่ครอบคลุมในการป้องกันอาชญากรรมต่อการพัฒนาสังคมและเศรษฐกิจและแนวทาบุรณาการเพื่อท้าทายระบบยุติธรรมทางอาญาเผชิญหน้า
- 2) ส่งเสริมแนวทางหลายมิติของรัฐบาลในการส่งเสริมหลักนิติธรรมโดยให้ทุกคนเข้าถึงความยุติธรรม การสร้างอย่างมีประสิทธิภาพ รับผิดชอบ เป็นกลาง และครอบคลุม สถาบัน; และพิจารณามาตรการทางสังคม การศึกษา และมาตรการอื่น ๆ ที่เกี่ยวข้อง รวมถึงส่งเสริมวัฒนธรรมของความถูกต้องกฎหมายในขณะที่เคารพเอกลักษณ์ทางวัฒนธรรมให้สอดคล้องกับ The Doha Declaration (การประชุมครั้งที่ 13)
- 3) ส่งเสริมให้เกิดความร่วมมือระหว่างประเทศและความช่วยเหลือด้านเทคนิคในการป้องกันและจัดการกับอาชญากรรมทุกรูปแบบไม่ว่าจะเป็นการก่อการร้าย หรืออาชญากรรมที่ใช้เทคโนโลยีรูปแบบใหม่<sup>306</sup>
- 4) ให้ความสำคัญกับแนวโน้มของอาชญากรรมในปัจจุบัน การพัฒนาล่าสุด และแนวทางแก้ไขที่เกิดขึ้นใหม่ โดยเฉพาะอย่างยิ่งการใช้เทคโนโลยีเป็นเครื่องมือในการกระทำความผิดและเครื่องมือในการต่อต้านอาชญากรรม<sup>307</sup>

นอกจากนี้ยังได้มีการยกประเด็นปัญหาอาชญากรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัลซึ่งมีแนวโน้มที่จะขยายวงกว้างมากขึ้น เนื่องจากสกุลเงินดิจิทัลมีลักษณะเป็นการทำงานด้วยเทคนิคการเข้ารหัสและควบคุมการสร้างด้วยระบบดิจิทัล มีการทำธุรกรรมแบบ Peer-to-peer และมีการตรวจสอบดำเนินการโดยไม่ขึ้นกับธนาคารกลาง ด้วยคุณลักษณะดังกล่าวจึงอำนวยความสะดวกในการก่ออาชญากรรมได้มากมาย ไม่ว่าจะเป็นการฟอกเงิน การจัดหาเงินทุนจากการก่อการร้าย

<sup>306</sup> United Nations Office on Drugs and Crime, **Reference: CU 2018/450(A)/DTA0SGB**, Retrieved April 11, 2021 from [https://www.unodc.org/documents/congress//Documentation\\_14th\\_Congress/RPM1Asia/CU\\_2018\\_450\\_A\\_English.pdf](https://www.unodc.org/documents/congress//Documentation_14th_Congress/RPM1Asia/CU_2018_450_A_English.pdf)

<sup>307</sup> United Nations, **Asia and Pacific Regional Preparatory Meeting for the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice Bangkok, 22-24 January 2019**, Retrieved April 11, 2021 from [https://www.unodc.org/documents/congress//Documentation\\_14th\\_Congress/RPM1Asia/ACONF234\\_RPM1\\_L1\\_AP\\_e.pdf](https://www.unodc.org/documents/congress//Documentation_14th_Congress/RPM1Asia/ACONF234_RPM1_L1_AP_e.pdf)

การกรรโชก การฉ้อโกง ดังนั้นการใช้ประโยชน์การสกุลเงินดิจิทัลจึงต้องอยู่ภายใต้กฎระเบียบและความร่วมมือระหว่างที่เหมาะสมโดยคำนึงถึงการใช้เทคโนโลยีสกุลเงินดิจิทัลอย่างถูกกฎหมาย รวมถึงการใช้สกุลเงินดิจิทัลเพื่อทำหน้าที่เก็บมูลค่าและวิธีการชำระสินค้าและบริการที่ถูกต้องตามกฎหมาย ดังนั้นจึงจำเป็นอย่างยิ่งที่รัฐจะต้องพัฒนากลยุทธ์สหสาขาวิชาชีพในการกำหนดนโยบายมาตรการกำกับดูแลไปจนถึงการป้องกัน ตลอดจนการฝึกอบรมหน่วยงานที่เกี่ยวข้องอำนาจเพื่อจัดการกับปัญหาดังกล่าวและพัฒนาความสามารถในการสืบสวนสอบสวนและดำเนินคดีที่เกี่ยวข้องให้มีประสิทธิภาพ สิ่งเหล่านี้จะทำให้บรรลุวัตถุประสงค์ในการบังคับใช้กฎระเบียบได้

ทั้งนี้ UNODC จึงได้วางกรอบแนวทางการพัฒนาหลักสูตรสากลเพื่อฝึกอบรมการสืบสวนของสกุลเงินดิจิทัลและอาชญากรรมทางอินเทอร์เน็ตในภูมิภาคต่าง ๆ<sup>308</sup> โดยมีจุดมุ่งหมายเพื่อยกระดับความสามารถของเจ้าหน้าที่บังคับใช้กฎหมาย นักวิเคราะห์ อัยการและผู้พิพากษาในการทำความเข้าใจแนวคิดของสกุลเงินดิจิทัล การติดตามบิตคอยน์ในการตรวจสอบเส้นทางการเงิน การค้นหาแหล่งข้อมูลเพิ่มเติมต่าง ๆ และการทำงานร่วมกันในคดีระหว่างประเทศ โดย UNODC ยังสร้างความร่วมมือกับภาคเทคโนโลยีการกำกับดูแล “RegTech” และการเงินภาคเทคโนโลยี “FinTech” และร่วมมือกับผู้นำอุตสาหกรรมสกุลเงินดิจิทัลเช่น Chainalysis, Inc. เพื่อช่วยเหลือเจ้าหน้าที่บังคับใช้กฎหมายและนักวิเคราะห์ในการติดตามสิ่งผิดกฎหมาย<sup>309</sup>

การฝึกอบรมทักษะที่จำเป็นให้กับบุคลากรและองค์กรที่เกี่ยวข้องควบคู่ไปกับกฎหมายภายในที่เหมาะสมและความร่วมมือระหว่างประเทศที่มีประสิทธิภาพ จะช่วยลดอาชญากรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัลได้

ดังกรณีตัวอย่างความร่วมมือที่น่าสนใจในปี 2563 ระหว่างสถาบันเพื่อการยุติธรรมแห่งประเทศไทย (Thailand Institute of Justice: TIJ) และสำนักงานว่าด้วยยาเสพติดและอาชญากรรมแห่งสหประชาชาติ (United Nations Office on Drugs and Crime: UNODC) ได้ร่วมลงนามข้อตกลงความร่วมมือระหว่างสององค์กร สำหรับการเสริมสร้างศักยภาพประเทศไทยในการรับมือกับอาชญากรรมไซเบอร์ ผ่านการดำเนินกิจกรรมต่าง ๆ ได้แก่ 1. การจัดการประชุมและ

<sup>308</sup> United Nations Office on Drugs and Crime, **Cryptocurrency Training Course**, Retrieved April 11, 2021 from <https://www.unodc.org/unodc/site-search.html?q=cryptocurrency+training+course>

<sup>309</sup> United Nations, **Fourteenth United Nations Congress on Crime Prevention and Criminal Justice Kyoto, Japan, 20-27 April 2020: Discussion Guide**, Retrieved April 11, 2021 from [https://www.unodc.org/documents/congress/Documentation\\_14th\\_Congress/DiscussionGuide/A\\_CONF234\\_PM1\\_e\\_V1806329.pdf](https://www.unodc.org/documents/congress/Documentation_14th_Congress/DiscussionGuide/A_CONF234_PM1_e_V1806329.pdf)

หารือกับผู้มีส่วนได้เสียในภาคส่วนต่าง ๆ ประเมินสถานการณ์อาชญากรรมไซเบอร์ในประเทศไทย 2. การประชุมของเจ้าหน้าที่ระดับสูงของรัฐ เพื่อสร้างความตระหนักรู้เกี่ยวกับโอกาสและความท้าทายของเทคโนโลยีดิจิทัลต่อเศรษฐกิจและสังคมของประเทศไทย และ 3. การฝึกอบรมเจ้าหน้าที่และผู้ปฏิบัติการเพื่อสร้างกลุ่มผู้เชี่ยวชาญเฉพาะด้านอาชญากรรมไซเบอร์<sup>310</sup> โดยในเดือนมกราคม 2565 UNDOC ร่วมกับสำนักงานป้องกันและปราบปรามยาเสพติด (ป.ป.ส.) จัดฝึกอบรมการสืบสวนสอบสวนเงินตราเข้ารหัสลับและเว็บลับ รุ่นที่ 1 (UNODC Cryptocurrencies and Darknet Investigation Training Course) เพื่อพัฒนาองค์ความรู้ของฝ่ายปฏิบัติการจากผู้เชี่ยวชาญระดับโลกในการเพิ่มศักยภาพและองค์ความรู้ในการทรัพย์สินดิจิทัลหรือขายนักค้ายาเสพติด รวมถึงการดำเนินการกับกลุ่มอาชญากรนักค้ายาเสพติดที่ใช้เทคโนโลยีเช่นสกุลเงินดิจิทัลหรือคริปโตเคอร์เรนซีมาเป็นเครื่องมือในการกระทำโดยอาศัยช่องทางออนไลน์ เพื่อให้มีความสลับซับซ้อนในการติดตามตัวผู้กระทำได้ยากขึ้น<sup>311</sup>

#### 3.4.2.2 คณะทำงานเฉพาะกิจเพื่อดำเนินมาตรการทางการเงินเกี่ยวกับการฟอกเงิน Financial Action Task Force (FATF)

ความร่วมมือระหว่างประเทศนี้อยู่ในรูปแบบของข้อเสนอแนะของคณะทำงานเฉพาะกิจ (Financial Action Task Force-FATF) เป็นองค์การระหว่างรัฐบาลที่รัฐมนตรีของประเทศสมาชิกร่วมกันจัดตั้งขึ้นในปี พ.ศ. 2532 ได้รับการรับรองจากกองทุนการเงินระหว่างประเทศและธนาคารโลกว่าเป็นมาตรฐานระหว่างประเทศในป้องกันปราบปรามการฟอกเงินและการต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย มีอำนาจหน้าที่ในการจัดทำมาตรฐานด้านการป้องกันและปราบปรามการฟอกเงินและการติดตามการสนับสนุนทางการเงินแก่การก่อการร้าย และส่งเสริมให้มีการใช้มาตรการทางกฎหมาย มาตรการด้านการกำกับดูแลและมาตรการด้านปฏิบัติการอย่างบังเกิดผลในการต่อต้านการฟอกเงิน การสนับสนุนทางการเงินแก่การก่อการร้าย (Anti-Money Laundering and the Financing of Terrorism Global Standard: AML/CFT) และการแพร่ขยายอาวุธที่มีอานุภาพทำลายล้างสูง ตลอดจนป้องกันภัยคุกคามอื่น ๆ ที่จะกระทบต่อระบบการเงินระหว่างประเทศ นอกจากนี้ FATF ยังร่วมมือกับองค์กรระหว่างประเทศอื่น ๆ ที่เกี่ยวข้องเพื่อกำหนดจุดอ่อนด้าน

<sup>310</sup> สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน), **เมื่ออาชญากรรมไร้พรมแดน**, ค้นวันที่ 2 พฤษภาคม 2565 จาก <https://tijacademy.org/2022/01/3030/เมื่ออาชญากรไร้พรมแดน>

<sup>311</sup> United Nations, **UNODC Delivered the Cryptocurrencies and Darknet Investigations Training Course**, Retrieved May 2, 2022 from <https://www.unodc.org/roseap/en/2022/02/cryptocurrencies-darknet-investigations/story.html>

AML/CFT ในระดับชาติ โดยมีเป้าหมายเพื่อป้องกันมิให้กลุ่มอาชญากรใช้ระบบการเงินระหว่างประเทศในการกระทำความผิด

FATF ได้ตระหนักถึงปัญหาการฟอกเงินที่มักใช้สกุลเงินดิจิทัลเป็นเครื่องมือในการทำธุรกรรมและการก่อการร้ายที่มีเบื้องหลังมาจากการระดมทุนด้วยสกุลเงินดิจิทัล เพื่อทำให้ยากแก่การตรวจสอบ ดังนั้น FATF จึงได้มีการออกข้อกำหนดเกี่ยวกับสกุลเงินดิจิทัลโดยกำหนดไว้อยู่ในภาพรวมของคำว่า “สินทรัพย์ดิจิทัล” (Virtual Asset) ในข้อ 15 ซึ่งกำหนดให้แต่ละประเทศและสถาบันการเงินต้องระบุและประเมินความเสี่ยงด้านการฟอกเงิน (ML) และการก่อการร้าย (TF) ที่อาจเกิดขึ้นจาก (1) การพัฒนาผลิตภัณฑ์และหลักปฏิบัติทางธุรกิจใหม่ รวมถึงวิธีการในการส่งใหม่ๆ และ (2) การใช้เทคโนโลยีใหม่หรือเทคโนโลยีที่กำลังพัฒนา สำหรับทั้งผลิตภัณฑ์ใหม่และผลิตภัณฑ์ที่มีอยู่ก่อนแล้ว ในกรณีของสถาบันการเงิน การประเมินความเสี่ยงดังกล่าว ต้องดำเนินการตามเงื่อนไขที่กำหนดก่อนการเปิดตัวผลิตภัณฑ์ใหม่ หรือหลักปฏิบัติทางธุรกิจใหม่ หรือการใช้เทคโนโลยีใหม่ หรือเทคโนโลยีที่กำลังพัฒนา สถาบันการเงินต้องใช้มาตรการที่เหมาะสมในการบริหารจัดการและบรรเทาความเสี่ยงดังกล่าว ในการบริหารจัดการและบรรเทาความเสี่ยงที่เกิดจากสินทรัพย์เสมือน แต่ละประเทศต้องมีการกำกับดูแลด้าน AML/CFT กับผู้ให้บริการสินทรัพย์เสมือนรวมทั้งต้องได้รับอนุญาตหรือจดทะเบียนและจะต้องมีระบบการติดตามตรวจสอบที่มีประสิทธิภาพ ตลอดจนการดำเนินการที่สอดคล้องกับข้อเสนอแนะของ FATF<sup>312</sup> ในส่วนของความผิดฐานก่อการร้ายนั้น ครอบคลุมไปถึงบุคคลทุกคนที่ได้จัดหาหรือรวบรวมเงินหรือทรัพย์สินอื่น ๆ ซึ่งหมายความรวมถึงสกุลเงินดิจิทัลด้วย ไม่ว่าจะโดยทางตรงหรือทางอ้อม โดยมีเจตนาละเมิดกฎหมายที่จะให้นำเงินนั้นไปใช้ หรือโดยทราบว่าจะให้นำไปใช้ ไม่ว่าจะเต็มจำนวนหรือบางส่วนเพื่อ (1) กระทำการอันเป็นการก่อการร้าย (2) ให้นำไปใช้โดยองค์กรก่อการร้าย หรือ (3) โดยผู้ก่อการร้ายข้อกำหนดดังกล่าวเกี่ยวข้องกับภาระระดมทุนโดยใช้สกุลเงินดิจิทัล<sup>313</sup>

จากข้อกำหนดดังกล่าวมีผลทำให้แต่ละประเทศต้องออกข้อกำหนดให้ผู้ที่เกี่ยวข้องกับการใช้สกุลเงินดิจิทัล ไม่ว่าจะเป็นผู้ให้บริการ ผู้รวบรวม ผู้ใช้ต้องขึ้นทะเบียนหรือได้รับอนุญาตจากหน่วยงานที่มีหน้าที่กำกับดูแลสกุลเงินดิจิทัลก่อนจึงจะให้หรือรับบริการที่เกี่ยวข้องกับสกุลเงินดิจิทัลได้

ความร่วมมือทางอาญาระหว่างประเทศที่เกี่ยวกับสกุลเงินดิจิทัลภายใต้ Financial Action Task Force (FATF)

<sup>312</sup> ข้อ 15 FATF

<sup>313</sup> ข้อ 5 FATF

### 1) การให้ความช่วยเหลือซึ่งกันและกันทางอาญา<sup>314</sup>

มีข้อกำหนดให้แต่ละประเทศต้องมีวิธีดำเนินการ และความสามารถในการตอบสนองต่อคำร้องขออายัด ยึด และริบทรัพย์สิน ซึ่งรวมทั้งสกุลเงินดิจิทัลที่ได้จากการฟอกเงิน และการก่อการร้ายโดยอาศัยกระบวนการพิจารณาคดีเพื่อริบทรัพย์ทางแพ่ง และมาตรการชั่วคราวที่เกี่ยวข้องเป็นหลัก เว้นเสียแต่ว่าการกระทำดังกล่าวจะไม่สอดคล้องกับหลักการขั้นพื้นฐานของกฎหมายภายในประเทศของ และต้องมีกลไกที่มีประสิทธิภาพในการบริหารจัดการทรัพย์สินดังกล่าว ให้มีการประสานงานด้านการพิจารณาคดีเพื่อการยึดและริบทรัพย์ โดยเฉพาะการร่วมกันริบทรัพย์สินซึ่งสามารถแบ่งกับประเทศอื่น ๆ ได้ และหากเป็นกรณีการร้องขอให้ใช้วิธีการสืบสวนสอบสวนให้ปฏิบัติตามคำร้องขอความช่วยเหลือทางกฎหมายระหว่างกันซึ่งสอดคล้องกับกรอบกฎหมายภายในประเทศของตนก็ให้นำมาใช้ได้

ทั้งนี้การให้ความช่วยเหลือทางกฎหมายระหว่างกันทำได้แม้ไม่มีหลักการการเป็นความผิดเดียวกันของทั้งสองรัฐ ใช้บังคับระหว่างกันอยู่ก็ตาม ถ้าความช่วยเหลือดังกล่าวไม่เกี่ยวกับการใช้กำลังบังคับ แต่ละประเทศต้องพิจารณานำมาตรการต่าง ๆ มาใช้ตามความจำเป็นเพื่อให้ตนสามารถให้ความช่วยเหลือในขอบข่ายที่กว้างขวางแม้ในกรณีไม่มีหลักการการเป็นความผิดเดียวกันของทั้งสองรัฐก็ตาม

ส่วนกรณีที่มีข้อกำหนดให้ต้องเป็นความผิดเดียวกันของทั้งสองรัฐสามารถให้ความช่วยเหลือทางกฎหมายระหว่างกันได้ตามหลักทั่วไป ไม่ว่าทั้งสองประเทศจะกำหนดให้ความผิดดังกล่าวอยู่ในประเภทของความผิดเดียวกันหรือกำหนดชื่อความผิดโดยใช้ศัพท์เดียวกันหรือไม่ก็ตาม ทั้งนี้โดยมีเงื่อนไขว่าทั้งสองประเทศจะต้องกำหนดให้การกระทำความผิดนั้นเป็นความผิดอาญา

### 2) การส่งผู้ร้ายข้ามแดน<sup>315</sup>

เป็นหลักการทั่วไปที่ใช้กับการฟอกเงินและการก่อการร้ายตามข้อเสนอแนะของ FATF แต่หากทั้งสองกรณีที่กล่าวมาเกี่ยวข้องกับสกุลเงินดิจิทัลในการใช้เป็นเครื่องในการกระทำความผิดก็สามารถนำหลักดังกล่าวมาใช้ได้ ไม่ว่าทั้งสองรัฐจะกำหนดให้การกระทำนั้นเป็นความผิดเดียวกัน หรือกำหนดให้อยู่ในประเภทเดียวกัน หรือกำหนดชื่อความผิดโดยใช้ศัพท์เดียวกันหรือไม่ก็ตาม ทั้งนี้โดยมีเงื่อนไขว่าทั้งสองประเทศจะต้องกำหนดให้การกระทำความผิดนั้นเป็นความผิดอาญา

<sup>314</sup> ข้อ 38 FATF, 38 ข้อเสนอแนะเพิ่มเติม

<sup>315</sup> ข้อ 39 FATF

### 3) การแลกเปลี่ยนข้อมูล<sup>316</sup>

FATF มีข้อกำหนดเกี่ยวกับความร่วมมือในการแลกเปลี่ยนข้อมูลโดยกำหนดให้หน่วยงานที่มีอำนาจต้องไม่ปฏิเสธการร้องขอความช่วยเหลือด้วยเหตุผลว่าคำร้องขอนั้นเกี่ยวข้องกับเรื่องการค้าหรือข้อกำหนดของสถาบันการเงินเว้นแต่ข้อมูลที่ต้องการนั้นเก็บรักษาไว้ตามเอกสิทธิ์ทางกฎหมาย หรือการเก็บรักษาความลับทางวิชาชีพตามกฎหมายยังใช้บังคับอยู่นอกจากนี้ยังมีข้อกำหนดการแลกเปลี่ยนข้อมูลระหว่างสถาบันการเงินและการแลกเปลี่ยนข้อมูลโดยหน่วยงานที่บังคับใช้กฎหมายมีข้อกำหนดให้สามารถใช้อำนาจและเทคนิคในการสืบสวนสอบสวนตามกฎหมายภายในประเทศของตนได้ในดำเนินการไต่สวนและขอรับข้อมูลแทนหน่วยงานบังคับใช้กฎหมายต่างประเทศ ระบบหรือหลักปฏิบัติที่ใช้อยู่ในการร่วมมือในการบังคับใช้กฎหมายดังกล่าวนั้น เช่น ข้อตกลงระหว่างตำรวจสากล (Interpol) หรือตำรวจสากลยุโรป (Europol) หรือฝ่ายยุติธรรมสากลยุโรป (Eurojust)

จากข้อกำหนดของ FATF ที่ได้กล่าวมาจะเห็นได้ว่าเป็นข้อกำหนดในการควบคุมการทำธุรกรรมเกี่ยวกับสกุลเงินดิจิทัลที่จะนำไปสู่การกระทำความผิดฟอกเงิน หรือการก่อการร้าย โดยควบคุมตั้งแต่ต้นทางการทำธุรกรรมที่กำหนดให้การให้บริการสินทรัพย์เสมือนต้องมีการขึ้นทะเบียนหรือใบอนุญาตและดำเนินการบรรเทาความเสี่ยงที่จะเป็นป้องกันการฟอกเงินและการจัดหาเงินทุนของผู้ก่อการร้าย และใช้มาตรการป้องกัน AML/CFT จนถึงปลายโดยกำหนดให้มีการรายงานธุรกรรมหากเข้าเงื่อนไข

ดังนั้นความร่วมมือระหว่างประเทศที่เกิดขึ้นภายใต้แนวปฏิบัติ FATF จึงเน้นไปที่การวางมาตรฐานการป้องกันอาชญากรรมเกี่ยวข้องกับการฟอกเงินและการก่อการร้ายที่ใช้สกุลเงินดิจิทัลเป็นเครื่องมือในการกระทำความผิด โดยเป็นต้นแบบให้แต่ละประเทศที่สมาชิกได้มีมาตรการที่ใกล้เคียงกันในการป้องกันอาชญากรรมที่เกิดขึ้น โดยจะเห็นว่า FATF ได้คำนึงถึงปัญหาในการปราบปรามอาชญากรรมที่เริ่มมีการนำสกุลเงินดิจิทัลมาเป็นเครื่องมือในการกระทำความผิดโดยถือว่าสกุลเงินดิจิทัลเป็นสินทรัพย์สำคัญที่เชื่อมโยงทั้งการฟอกเงินและการก่อการร้าย และเป็นความผิดที่มีลักษณะข้ามชาติ จึงกำหนดให้มีกลไกความร่วมมือระหว่างประเทศที่แต่ละประเทศมีหน้าที่ต้องให้ความร่วมมืออย่างกว้างขวางที่สุดเท่าที่จะทำได้ด้วยความรวดเร็ว เป็นไปในทางสร้างสรรค์และมีประสิทธิผลในส่วนที่เกี่ยวข้องกับการฟอกเงิน ความผิดมูลฐาน และการสนับสนุนทางการเงินแก่การก่อการร้ายที่เกี่ยวกับสินทรัพย์เสมือน โดยเฉพาะอย่างยิ่งหน่วยงานกำกับดูแลผู้ให้บริการฯ การทำธุรกรรมต้องสามารถแลกเปลี่ยนข้อมูลกับหน่วยงานประเภทเดียวกันในต่างประเทศได้รวดเร็วโดยไม่ต้องคำนึงถึงลักษณะหรือสถานะของหน่วยงานกำกับและความแตกต่างในการเรียกชื่อหรือสถานะของ

<sup>316</sup> ข้อ 40 FATF

ผู้ให้บริการ ข้อกำหนดต่าง ๆ จึงเป็นมาตรฐานสากลที่ให้แต่ละประเทศนำไปปรับใช้ในทิศทางเดียวกัน แม้ว่าข้อเสนอ FATF จะไม่มีสถานะเป็นอนุสัญญาและไม่มีสภาพบังคับในทางกฎหมายระหว่างประเทศ แต่เป็นข้อเสนอที่ได้รับการยอมรับในระดับสากลที่นานาประเทศนำมาปฏิบัติ อีกทั้งมีสภาพบังคับทางอ้อม (Soft Law) โดยผ่านกระบวนการประเมินผลการปฏิบัติตามมาตรฐานสากลของสมาชิก FATF หรือกลุ่มเครือข่ายต่อต้านการฟอกเงินของ FATF ซึ่งรวมถึงกลุ่มความร่วมมือเพื่อต่อต้านการฟอกเงินเอเชียแปซิฟิก (Asia Pacific Group on Money Laundering-APG) ที่ประเทศไทยเป็นสมาชิกอยู่ โดยหากประเมินแล้วพบว่าประเทศสมาชิกมีข้อบกพร่องจำนวนมากในการปฏิบัติตามมาตรการด้านการป้องกันและปราบปรามการฟอกเงิน เช่น กฎหมายที่มีอยู่ไม่สอดคล้องกับมาตรฐานสากล การกำกับดูแลและการบังคับใช้กฎหมายไม่มีประสิทธิภาพ และไม่มีการประสานความร่วมมือกับต่างประเทศอย่างเพียงพอ อาจส่งผลให้ประเทศนั้นถูกกำหนดให้เป็นรายชื่อประเทศที่มีความเสี่ยงด้านการฟอกเงินได้

#### 3.4.2.3 ตำรวจสากล (Interpol)

องค์การตำรวจสากล มีชื่อว่า “The International Criminal Police Organization” (คำย่อว่า I.C.P.O. หรือที่เรียกสั้น ๆ ว่า Interpol) สำนักงานใหญ่ตั้งอยู่ที่กรุงปารีส ประเทศฝรั่งเศส มีสมาชิก 194 ประเทศ รวมทั้งประเทศไทย<sup>317</sup> องค์การสหประชาชาติได้รับรององค์การตำรวจสากลในฐานะเทียบเท่าองค์การในเครือองค์การสหประชาชาติ โดยมีฐานะเป็นองค์การที่ปรึกษาคณะมนตรีเศรษฐกิจและสังคมอันมีบทบาทสำคัญในกิจกรรม ดังต่อไปนี้

- 1) การต่อต้านการก่อการร้าย เพื่อป้องกันและขัดขวางกิจกรรมการก่อการร้ายโดยการระบุมหาชิกของเครือข่ายผู้ก่อการร้ายและบริษัทในเครือ และจัดการกับปัจจัยหลักที่ทำให้กิจกรรม: การเดินทางและการเคลื่อนไหว การปรากฏตัวทางออนไลน์ อาวุธและวัสดุ และการเงิน
- 2) อาชญากรรมทางอินเทอร์เน็ต โดยเน้นไปที่อาชญากรรมทางอินเทอร์เน็ตที่บริสุทธิ์ (อาชญากรรมต่อคอมพิวเตอร์และระบบสารสนเทศ) และอาชญากรรมที่กระทำผ่านทางไซเบอร์ โดยใช้เทคโนโลยีขยายขอบเขตการก่ออาชญากรรม เช่น การฉ้อโกงทางการเงินและการใช้สื่อโซเชียลของผู้ก่อการร้าย

---

<sup>317</sup> Interpol, **We have 194 Member Countries; Together they Create a Truly Global Network of Police**, Retrieved April 11, 2021 from <https://www.interpol.int/en/Who-we-are/Member-countries>

3) องค์กรและอาชญากรรมที่เกิดขึ้นใหม่โดยมุ่งเน้นการปราบปรามองค์กรข้ามชาติและเครือข่ายอาชญากร ภัยคุกคามและอาชญากรรมที่เกิดขึ้นใหม่<sup>318</sup> เช่น การก่อการร้าย การค้ามนุษย์ การค้ายาเสพติด อาชญากรรมทางการเงิน อาชญากรรมคอมพิวเตอร์ อาชญากรรมสงคราม รวมถึงอาชญากรรมเทคโนโลยีทางการเงินที่เรียกว่าสกุลเงินดิจิทัล ซึ่งเป็นอาชญากรรมไร้พรมแดน และสร้างเครือข่ายเป็นองค์กรอาชญากรรมข้ามชาติได้จึงอยู่ในอำนาจของตำรวจสากลเช่นกัน

#### ความร่วมมือระหว่างประเทศภายใต้บทบาทของตำรวจสากล

##### 1) การส่งผู้ร้ายข้ามแดน

เป็นไปตามหลักทั่วไปของกฎหมายระหว่างประเทศ กล่าวคือ ความผิดซึ่งบุคคลผู้ถูกขอให้ส่งตัวได้กระทำไปนั้น ต้องเป็นความผิดต่อกฎหมายอาญาของทั้งสองประเทศ คือ ประเทศผู้ร้องขอและประเทศผู้รับคำขอ (Principle of Double Criminality) โดยคดีนั้นต้องมีมูลที่จะนำตัวผู้ต้องหาขึ้นฟ้องร้องต่อศาลได้ และต้องเป็นความผิดที่กฎหมายกำหนดโทษจำคุกไม่ต่ำกว่าหนึ่งปี (ตามอนุสัญญา Montevideo ค.ศ. 1933) ที่ยังไม่ขาดอายุความซึ่งกฎหมายไทยก็ยึดถือหลักเกณฑ์ดังกล่าวนี้เช่นกัน เมื่อบุคคลผู้ถูกขอตัวได้ปรากฏตัวอยู่ในประเทศที่ถูกร้องขอให้ส่งตัว (ประเทศผู้รับคำขอ) ให้ประเทศผู้ร้องขอเป็นผู้ดำเนินการร้องขอให้ส่งตัวโดยปฏิบัติตามพิธีการต่าง ๆ ให้ครบถ้วนดังที่กำหนดไว้ในสนธิสัญญาหรือตามกฎหมายว่าด้วยการนั้น

##### 2) การโอนตัวนักโทษ

การโอนตัวนักโทษจะต้องได้รับความเห็นชอบจากรัฐผู้โอน รัฐผู้รับ และจากตัวนักโทษเอง ความผิดที่นักโทษได้กระทำ ต้องเป็นความผิดทางอาญาที่ลงได้ทั้งในรัฐผู้รับ และรัฐผู้โอนซึ่งเงื่อนไขของโทษที่จะโอนได้นั้นต้องเป็นโทษจำคุกที่ยังเหลือไม่ต่ำกว่า 1 ปี โดยรัฐผู้โอนอาจจะกำหนดระยะเวลาขั้นต่ำที่นักโทษจะต้องรับโทษก่อนได้รับการพิจารณาให้โอนตัวไว้ตามกฎหมายภายในได้ และสามารถเปลี่ยนแปลง แก้ไข ยกเลิกคำพิพากษาของตนได้ วิธีการลงโทษนักโทษที่ถูกโอนตัวให้เป็นไปตามกฎหมายและระเบียบปฏิบัติของรัฐผู้รับ<sup>319</sup> ทั้งนี้ภาคีแต่ละฝ่ายมีสิทธิกำหนดหลักเกณฑ์ต่าง ๆ เพื่อพิจารณาว่าจะให้ความเห็นชอบการโอนตัวนักโทษหรือไม่

<sup>318</sup> Interpol, **Interpol: An Overview**, Retrieved April 11, 2021 from <https://www.interpol.int/en/Who-we-are/What-is-INTERPOL>

<sup>319</sup> ลาวัญย์ ถนัดศิลปกุล, วิมาน กฤตพลวิมาน, จตุรงค์ บุญยรัตนสุนทร, ชูเกียรติ น้อยฉิม และชนันภรณ์ บุญเกิดทรัพย์, **การศึกษา วิเคราะห์ และแนวทางในการแก้ไขปัญหาการค้ามนุษย์ในมิติกฎหมายของประเทศในพื้นที่ระเบียงเศรษฐกิจตะวันออก – ตะวันตก, เหนือ – ใต้ (EWEC –**

เหตุในการปฏิเสธการโอนตัวนักโทษมีสองกรณีหลักด้วยกันคือ 1) เหตุอันเนื่องมาจากสัญชาติ กล่าวคือหากนักโทษมีสัญชาติของรัฐผู้โอนอยู่ด้วย รัฐผู้โอนอาจปฏิเสธการโอนตัวได้ และ 2) เหตุอันเนื่องมาจากความผิดต่อความมั่นคงภายในและภายนอกของรัฐต่อประมุขของรัฐหรือเกี่ยวกับกฎหมายคุ้มครองวัตถุประสงค์โบราณจะไม่ได้รับการโอนตัว

ดังนั้นบทบาทความร่วมมือระหว่างประเทศของตำรวจสากลจะเกิดขึ้นได้จะต้องเป็นไปตามหลักเกณฑ์ทางกฎหมายความร่วมมือระหว่างประเทศในเรื่องนั้น ๆ เสียก่อนจึงจะนำมาสู่การประสานงานเพื่อปราบปรามอาชญากรรมระหว่างประเทศโดยตำรวจสากล

กรณีศึกษาการปราบปรามอาชญากรรมที่เกี่ยวข้องกับ Cryptocurrency โดยตำรวจสากลได้ใช้กลไกความร่วมมือระหว่างประเทศในการจับตัวผู้กระทำความผิด

คดี AlphaBay: ประเทศไทยได้มีการประสานงานร่วมกับ Interpol ในการปราบปรามอาชญากรรม Cryptocurrency คดีเว็บไซต์ AlphaBay เป็นการจับกุมผู้ดูแลเว็บไซต์ใต้ดิน (Darknet) ที่เปิดให้บริการซื้อขายยาเสพติด อาวุธ มัลแวร์ ของผิดกฎหมายอื่น ๆ โดยใช้สกุลเงินดิจิทัลในฟอกเงิน ซึ่งผู้กระทำได้เข้ามาอาศัยอยู่ในประเทศไทย โดยอัยการแห่งสหรัฐอเมริกาอาศัยอำนาจตามประมวลกฎหมายแห่งสหรัฐอเมริกา มาตรา 981 (a) (1) (A) และ (C) 201 ลักษณะ 18 ยื่นฟ้องบรรดาทรัพย์สินที่ได้มาจากการกระทำผิดจากการเป็นผู้ดูแลเว็บไซต์ AlphaBay โดย นายอเล็กซานเดอร์ แคลส ต่อศาลแขวงแห่งรัฐแคลิฟอร์เนีย เขตตะวันออก เพื่อทำการยึดอายัดทางแพ่ง (Civil Forfeiture) สืบเนื่องมาจากวันที่ 4 กรกฎาคม 2560 FBI, DEA ได้ร่วมมือสำนักงานตำรวจแห่งชาติของไทยจับกุมและตรวจยึดอายัดทรัพย์สินของนายอเล็กซานเดอร์ แคลส เพื่อส่งตัวเป็นผู้ร้ายข้ามแดนไปดำเนินคดีที่สหรัฐอเมริกาตามพระราชบัญญัติส่งผู้ร้ายข้ามแดน พ.ศ. 2551 ภายใต้ปฏิบัติการที่ชื่อว่า “Operation Bayonet” พบว่าจำเลยได้กบดานอยู่ที่ประเทศไทย โดยจากการเข้าค้นฝ่ายจับกุมสามารถเข้าสู่ระบบของ AlphaBay ผ่านชื่อผู้ใช้ Admin ที่ถูกทิ้งไว้ในคอมพิวเตอร์ส่วนตัวซึ่งไม่ได้เข้ารหัสไว้ ฝ่ายจับกุมสามารถค้นหาเจอรหัสผ่านในการเข้าถึงเซิร์ฟเวอร์ AlphaBay และสามารถยึดเงินสกุลดิจิทัล จำนวน 255,700,000 บาท ยึดเงินสกุลดิจิทัล ประเทศลิทัวเนีย จำนวน 57,600,000 บาท โดยมีการทำการโอนย้าย Cryptocurrency ยัง Digital Wallet ของหน่วยงานของสหรัฐอเมริกา ยึดอุปกรณ์คอมพิวเตอร์ รวมถึง เซิร์ฟเวอร์ที่เกี่ยวข้องกับการกระทำความผิดเกี่ยวกับเครือข่ายเว็บไซต์ออนไลน์ รวม 39 รายการ เพื่อไว้ตรวจสอบ อายัดเงินในบัญชีในประเทศไทย 46 ล้านบาท รวมมูลค่าทรัพย์สินกว่า 726,300,000 บาท โดยก่อนนำตัวจำเลยส่งมอบ

ตามพระราชบัญญัติส่งผู้ร้ายข้ามแดนพบว่าจำเลยได้ฆ่าตัวตายก่อนดำเนินการทางกฎหมาย อย่างไรก็ตาม รัฐบาลสหรัฐอเมริกายังคงดำเนินการยึดสินทรัพย์ที่เกี่ยวข้องกับ AlphaBay ต่อไป

นอกจากกลไกความร่วมมือระหว่างประเทศที่ตำรวจสากลใช้ในการป้องกันและปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินดิจิทัลแล้ว ยังได้ให้ความสำคัญกับการพัฒนาทักษะเชิงเทคนิคในการสืบหา พยานหลักฐานในการติดตามผู้กระทำความผิดมาดำเนินคดี โดยได้มีการจัดการประชุมนานาชาติ การประชุมระดับโลกครั้งที่ 5 เรื่อง Criminal Finances and Cryptocurrencies เมื่อวันที่ 7-8 ธันวาคม พ.ศ. 2564 ซึ่งจัดโดย Basel Institute on Governance, Interpol และ Europol โดยได้เน้นย้ำถึงแนวทางในการติดตามธุรกรรมสกุลเงินดิจิทัล ซึ่งมี 7 ข้อแนะนำ<sup>320</sup> ดังนี้

1) การใช้เครื่องมือเพื่อเพิ่มขีดความสามารถในการตรวจสอบสินทรัพย์ดิจิทัล (Virtual Assets) (VAs) ประเทศ/รัฐสมาชิกทั้งหมดจะต้องดำเนินการริเริ่มเสริมสร้างขีดความสามารถในด้านบัญชีแยกประเภทเทคโนโลยีตลอดจนบทบาทในการป้องกันการฟอกเงินหรือการก่อการร้ายการจัดการจัดหาเงินทุน การผลิตคู่มือและความคิดริเริ่มการฝึกอบรม การจัดโครงการแลกเปลี่ยนและการประชุมระดับนานาชาติตลอดจนการพัฒนาความร่วมมือภาครัฐภาคเอกชน

2) ใช้กฎหมายเพื่อควบคุมผู้ให้บริการสินทรัพย์ดิจิทัล (VASP) เพื่อป้องกันเงินซั๊กฟอกสนับสนุนให้ทุกประเทศ/รัฐสมาชิกกำหนดกรอบและกระบวนการกำกับดูแลที่ชัดเจนเพื่อสนับสนุนการลงทะเบียนและการกำกับดูแล AML/CFT ของ VASP เช่นการแลกเปลี่ยนสกุลเงินดิจิทัล ผู้ให้บริการกระเป๋าสตางค์และหน่วยงานอื่น ๆ ที่ออกหรือส่งสินทรัพย์ดิจิทัลตามการดำเนินการทางการเงินข้อเสนอแนะของ Task Force (FATF) ผู้ให้บริการสินทรัพย์ดิจิทัลควรได้รับการควบคุมในลักษณะเดียวกับการเงินอื่น ๆ ตัวกลางและควรมีส่วนร่วมในความพยายามระดับโลกต่อ AML/CFT โดยการดำเนินการโปรแกรมการปฏิบัติตาม, การตรวจสอบวิเคราะห์สถานะตามความเสี่ยง, การรายงาน ฯลฯ ผู้ให้บริการสินทรัพย์ดิจิทัลควรอยู่ภายใต้ระเบียบ AML/CFT เพื่อรายงานรายงานธุรกรรมที่น่าสงสัยและดำเนินการตรวจสอบวิเคราะห์ลูกค้าและธุรกรรมเชิงเทคนิคด้วยเช่นกัน

3) ใช้กลยุทธ์ “ตามเงิน” ทุกประเทศ/รัฐสมาชิกควรใช้กลยุทธ์ในการติดตามสินทรัพย์ดิจิทัล ควรจัดการเช่นเดียวกับทรัพย์สินอื่นในแง่ของการรับและการสอบสวน การตรวจสอบธุรกรรมทางการเงิน

---

<sup>320</sup> Basel Institute on Governance, **Thousands Gather Virtually to Share Knowledge of Virtual Assets-based Money Laundering and Other Crypto-enabled Crimes**, Retrieved July 17, 2021 from <https://baselgovernance.org/news/5CrC>

4) เสริมสร้างความร่วมมือระหว่างประเทศความร่วมมือและการแลกเปลี่ยนข้อมูลเป็นสิ่งสำคัญในการปราบปรามองค์กรอาชญากรรม สมาชิกทั้งหมดตั้งนั้นจึงแนะนำให้ประเทศ/รัฐใช้แพลตฟอร์มระดับโลกที่มีอยู่สำหรับระหว่างประเทศการสืบสวนเช่น Interpol, Europol, Egmont Group และ FIU.net

5) นำแนวทางสหสาขาวิชาชีพมาใช้ในการสืบสวนที่เกี่ยวข้องกับ ซึ่งรวมถึงความเชี่ยวชาญในอาชญากรรมไซเบอร์และการสอบสวนทางการเงิน จำเป็นต้องทำงานร่วมกันระหว่างผู้ตรวจสอบทางการเงินและผู้เชี่ยวชาญด้านคอมพิวเตอร์

6) ส่งเสริมเทคโนโลยีใหม่ ๆ ที่ใช้กับการตรวจสอบทางการเงินสินทรัพย์ดิจิทัล เทคโนโลยีใหม่ ๆ ที่นำมาใช้ในการสืบสวนมีความสำคัญอย่างยิ่งต่อการช่วยเพิ่มประสิทธิภาพของการตรวจสอบทางการเงิน และเพื่อลดความเสี่ยงที่เกี่ยวข้อง การวิจัยและนวัตกรรมเกี่ยวกับเครื่องมือที่สามารถอำนวยความสะดวกในการตรวจสอบและป้องกันการฟอกเงินและการก่อการร้ายได้

7) ปรับกลยุทธ์การสืบสวนแผนการทางอาญาทุกรูปแบบที่ละเมิดสินทรัพย์ดิจิทัล การติดตามธุรกรรมควรมุ่งเน้นไปที่การเชื่อมโยงระหว่างผู้ต้องสงสัยกับกระเป๋าเงิน<sup>321</sup>

นอกจากนี้ Interpol ยังเป็นหนึ่งใน 15 องค์กรร่วมกับ Europol ได้มีการก่อตั้งโครงการวิจัยที่ชื่อว่า Titanium มีจุดมุ่งหมายเพื่อพัฒนาทักษะทางเทคนิคในการติดตามสกุลเงินเสมือนและระบบนิเวศของตลาดที่มีการซื้อขายสิ่งผิดกฎหมาย โดยวิเคราะห์ธุรกรรมผ่านบัญชีแยกประเภทสกุลเงินเสมือนต่าง ๆ ที่ได้รับการออกแบบให้สอดคล้องกับระเบียบข้อบังคับด้านการปกป้องข้อมูลระดับประเทศ และนำเครื่องมือนี้มาสนับสนุนหน่วยงานบังคับใช้กฎหมายในการตรวจสอบและบรรเทาอาชญากรรม การก่อการร้ายที่เกี่ยวข้องกับสกุลเงินเสมือนจริงและธุรกรรมในตลาดใต้ดิน โดยมีเทคนิคที่เกี่ยวข้องกับการตรวจสอบธุรกรรมและการสืบหาพยานหลักฐาน ดังนี้<sup>322</sup>

- 1) การติดตามเว็บไซต์ที่ใช้สกุลเงินดิจิทัลชื่อของสิ่งผิดกฎหมาย<sup>323</sup>
- 2) การสำรวจเครือข่าย Bitcoin จากที่อยู่หนึ่งไปยังอีกที่อยู่หนึ่งเพื่อตรวจสอบลิงก์ที่น่าสงสัยและติดตามตัวตนที่แท้จริง<sup>324</sup>

<sup>321</sup> Recommendations 4<sup>th</sup> Global Conference on Criminal Finances and Cryptocurrencies by Interpol, Europol and Basel Institute on Governance

<sup>322</sup> Titanium, **Titanium Project**, Retrieved July 17, 2021 from <https://www.titanium-project.eu/>

<sup>323</sup> Titanium, **Monitoring the Dark Web**, Retrieved July 17, 2021 from <https://www.titanium-project.eu/news/articles/darkwebmonitor1/>

3) จัดทำเครื่องมือตรวจสอบกระเป๋าเงิน เพื่อวิเคราะห์ร่องรอยที่อาจทิ้งไว้โดยเครื่องมือนี้จะใช้ได้กับกระเป๋าเงินที่ติดตั้งในเดสก์ท็อปและมือถือ และทำการตรวจสอบตามข้อมูลบล็อกเชนโดยอัตโนมัติ และอาจต้องใช้เทคนิคเฉพาะในการเข้าถึงกระเป๋าเงินเพื่อตรวจสอบข้อมูล<sup>325</sup>

4) การจัดทำ Software ที่ชื่อว่า GraphSense เป็นเครื่องมือวิเคราะห์สำรวจธุรกรรมซึ่งรองรับได้สกุลเงินดิจิทัล คือ Bitcoin, Litecoin, BitcoinCash และ Zcash GraphSense ยังสามารถใช้ในการวิเคราะห์เหตุการณ์ในบล็อกเชน Bitcoin ที่เกี่ยวข้องกับอาชญากรรม เช่น การยกยอก การฟอกเงิน การแฮ็ก และแรนซัมแวร์ โดยแสดงให้เห็นว่าอาชญากรรมทางอินเทอร์เน็ตสามารถทำงานอย่างไร<sup>326</sup>

จากที่ได้ศึกษาถึงหลักกฎหมายที่เกี่ยวข้องกับการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลของต่างประเทศมาแล้ว จะเห็นได้ว่ามีกฎหมายของสหรัฐอเมริกา และสหราชอาณาจักร (อังกฤษ) มีกฎหมายที่สามารถนำมาปรับใช้กับกรณีการขโมยสกุลเงินดิจิทัลและกรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นโดยมิชอบได้โดยตรง ในขณะที่ประเทศไทยนั้นยังไม่มีกฎหมายเฉพาะสำหรับกรณีดังกล่าว มีเพียงบางฐานความผิดในประมวลกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ที่ใกล้เคียงกับกรณีดังกล่าว และในบทนี้ยังได้ทำการศึกษาถึงมาตรการความร่วมมือทางอาญาระหว่างประเทศทั้งรูปแบบอนุสัญญาและรูปแบบองค์กร ซึ่งเป็นอีกกลไกที่สำคัญในการควบคุมการกระทำความผิดที่มีลักษณะที่ไร้พรมแดนให้ได้ อย่างมีประสิทธิภาพ จากการศึกษาทั้งหมดที่ได้กล่าวมาผู้เขียนได้นำมาวิเคราะห์โดยตั้งประเด็นปัญหาทางกฎหมายเพื่อแสวงหามาตรการที่เหมาะสมในการควบคุมการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลไว้ในบทต่อไป

---

<sup>324</sup> Titanium, **TITANIUM Tool Cointel: Cryptocurrency Analytics Functionality**, Retrieved July 17, 2021 from <https://www.titanium-project.eu/news/articles/cointel1/>

<sup>325</sup> Titanium, **TITANIUM Tool Dence Wallet Investigator**, Retrieved July 17, 2021 from [https://www.titanium-project.eu/news/articles/wallet\\_investigator/](https://www.titanium-project.eu/news/articles/wallet_investigator/)

<sup>326</sup> Titanium, **TITANIUM Tool GraphSense**, Retrieved July 17, 2021 from <https://www.titanium-project.eu/news/articles/graphsense1/>

## บทที่ 4

### วิเคราะห์ปัญหาทางกฎหมายเกี่ยวกับการกระทำความผิดอาญา ที่เกี่ยวกับสกุลเงินดิจิทัล

จากการศึกษาลักษณะของสกุลเงินดิจิทัล ความผิดทางอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล และหลักเกณฑ์การบัญญัติความผิดทางอาญาของบุคคล ในบทนี้ผู้เขียนจะนำหลักการดังกล่าวมาวิเคราะห์ให้เห็นถึงปัญหาทางกฎหมายในการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล ซึ่งจะนำไปสู่การแสวงหามาตรการทางกฎหมายที่เหมาะสมในการควบคุมการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัลซึ่งเป็นวัตถุประสงค์ของงานวิจัยนี้ ทั้งนี้ผู้เขียนได้แบ่งออกเป็นสามประเด็นปัญหา ดังนี้

#### 4.1 ปัญหาเกี่ยวกับสถานะของสกุลเงินดิจิทัล

ปัจจุบันกฎหมายไทยยังไม่มีข้อกำหนดสถานะทางกฎหมายที่ชัดเจนให้กับสกุลเงินดิจิทัล ดังนั้น หากมีการกระทำความผิดที่เกี่ยวกับสกุลเงินดิจิทัล จะทำให้เกิดความไม่ชัดเจนว่าจะนำกฎหมายใดที่มีอยู่มาบังคับใช้และจะมีขอบเขตการตีความในการบังคับใช้อย่างไร ปัญหาดังกล่าวยังส่งผลต่อการกำหนดความรับผิดทางอาญาของบุคคล เนื่องจากกฎหมายอาญาจะลงโทษบุคคลได้ก็ต่อเมื่อมีกฎหมายบัญญัติว่าการกระทำนั้นเป็นความผิดและกำหนดโทษไว้อย่างชัดเจน<sup>327</sup> ซึ่งหลักการนี้เป็นหลักการสำคัญของกฎหมายอาญาอันเป็นหลักประกันสิทธิเสรีภาพของบุคคล ดังนั้นหากไม่มีกฎหมายบัญญัติว่าการกระทำนั้นเป็นความผิด จะลงโทษทางอาญาแก่บุคคลนั้นมิได้

ด้วยเหตุนี้จึงจำเป็นต้องกำหนดสถานะทางกฎหมายของสกุลเงินดิจิทัลให้ชัดเจนเสียก่อน โดยพิจารณาจากลักษณะทางกายภาพ ลักษณะความผิดที่เกิดขึ้นได้กับสกุลเงินดิจิทัล นิยามทางกฎหมายและข้อจำกัดทางกฎหมายของแต่ละสถานะที่ใกล้เคียงเมื่อนำมาปรับใช้กับสกุลเงินดิจิทัลเพื่อวิเคราะห์และกำหนดสถานะทางกฎหมายที่เหมาะสมแก่สกุลเงินดิจิทัล ทั้งนี้ผู้เขียนได้นำสถานะต่าง ๆ ซึ่งมีลักษณะใกล้เคียงกับสกุลเงินดิจิทัลมาพิจารณา ดังนี้

---

<sup>327</sup> มาตรา 2 แห่งประมวลกฎหมายอาญา

1) สถานะทรัพย์สิน ตามประมวลกฎหมายแพ่งและพาณิชย์ได้นิยามคำว่า “ทรัพย์สิน” ไว้ในมาตรา 138 ว่า “ทรัพย์สิน” หมายความว่ารวมทั้งทรัพย์สินซึ่งหมายถึงวัตถุที่มีรูปร่าง<sup>328</sup> และวัตถุไม่มีรูปร่าง ซึ่งอาจมีราคาและอาจถือเอาได้ ซึ่งเมื่อพิจารณาจากลักษณะทางกายภาพของสกุลเงินดิจิทัล จะเห็นได้ว่าเป็นสิ่งที่บุคคลคิดค้นขึ้นเพื่อเป็นสื่อกลางในการแลกเปลี่ยนสินค้าและบริการต่าง ๆ โดยใช้กลไกทางคณิตศาสตร์ซึ่งประมวลผลด้วยระบบคอมพิวเตอร์และมีวิธีการใช้ในรูปแบบดิจิทัลในช่องทางออนไลน์เท่านั้น และมีได้มีลักษณะเป็นธนบัตรที่ทำมาจากกระดาษหรือเหรียญโลหะที่รัฐบาลของประเทศได้รับรองให้ใช้แต่อย่างใด ลักษณะดังกล่าวจึงเป็นสิ่งที่ไม่มีรูปร่างที่อาจถือเป็นทรัพย์สินได้ตามนิยามของกฎหมายแพ่ง นอกจากนี้หากพิจารณาถึงความสามารถในการถือครองหรือเป็นความเจ้าของของสกุลเงินดิจิทัล จะเห็นว่าแม้จะเป็นสิ่งที่ไม่มีรูปร่างแต่ก็สามารถสร้างมูลค่าทางเศรษฐกิจได้<sup>329</sup> อีกทั้งในการบังคับคดีหากลูกหนี้ตามคำพิพากษาได้มีการถือครองสกุลเงินดิจิทัลไว้ก็สามารถถูกยึดเพื่อออกขายทอดตลาด นำเงินมาชำระหนี้ให้แก่เจ้าหนี้ตามคำพิพากษาได้ ในฐานะเป็นทรัพย์สินเช่นเดียวกับ สิทธิการเช่าทรัพย์สินทางปัญญา สิทธิของลูกหนี้ตามคำพิพากษา หรือสิทธิอย่างอื่นที่มีลักษณะคล้ายคลึงหรือเกี่ยวเนื่องกับสิทธิดังกล่าว<sup>330</sup> ซึ่งสิทธิต่าง ๆ เหล่านี้แม้เป็นสิ่งที่ไม่มีรูปร่างแต่มีมูลค่าที่สามารถนำมาบังคับชำระหนี้ได้ตามกฎหมาย ดังนั้นในทางแพ่งจึงมองว่าสกุลเงินดิจิทัลมีสถานะเป็นทรัพย์สินได้

นอกจากนี้หน่วยงาน The UK Taskforce’s Legal Statement ของสหราชอาณาจักร (อังกฤษ) ได้ตีความว่า Cryptoasset เป็นทรัพย์สิน (Property) ชนิดหนึ่งโดยพิจารณาถึงความสัมพันธ์ทางกฎหมายในลักษณะกรรมสิทธิ์ที่มีขึ้นระหว่างบุคคลกับทรัพย์สิน ซึ่งหมายถึงสิทธิในการครอบครองตามกฎหมายแพ่งที่อาจได้รับการเยียวยา (Civil Remedy) หากถูกละเมิดผู้เป็นเจ้าของมีอำนาจที่จะติดตามเอาคืนได้<sup>331</sup> และสามารถถูกประทุษร้ายเป็นคดีความทางอาญาได้ เหมือนกับการถูกขโมยและถูกฉ้อโกงได้<sup>332</sup> อีกทั้งใน Theft Act 1968 ความผิดฐานขโมยได้กำหนดวัตถุแห่งการกระทำให้เป็นทรัพย์สินซึ่งหมายความว่ารวมถึงวัตถุที่ไม่มีรูปร่าง<sup>333</sup> ไว้อย่างชัดเจน ดังนั้น

<sup>328</sup> มาตรา 137 แห่งประมวลกฎหมายแพ่งและพาณิชย์

<sup>329</sup> Jonathan Chiu and Thorsten V. Koepl, **The Economics of Cryptocurrencies-Bitcoin and Beyond** (Ontario, Bank of Canada, 2018), p. 2.

<sup>330</sup> พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายวิธีพิจารณาความแพ่ง (ฉบับที่ 30) พ.ศ. 2560

<sup>331</sup> UK Jurisdiction Taskforce, *op. cit.*, p. 11.

<sup>332</sup> *Ibid.*, p. 11.

<sup>333</sup> Section 4, The Theft Act 1968

ความผิดฐานขโมยนี้จึงอาจนำมาปรับใช้กับการขโมยสกุลเงินดิจิทัลได้โดยไม่จำเป็นต้องบัญญัติกฎหมายเฉพาะขึ้นมาใหม่

อย่างไรก็ตาม จากการศึกษาพบว่าแม้สกุลเงินดิจิทัลจะมีสถานะเป็นทรัพย์สินตามกฎหมายแพ่งและพาณิชย์ของไทยและกฎหมาย the Theft Act ของประเทศอังกฤษก็ตาม แต่ในทางกฎหมายอาญาของไทยนั้น ยังคงมีปัญหาในส่วนของวัตถุแห่งการกระทำที่แบ่งออกเป็นทรัพย์สิน และทรัพย์สินตามแต่ละฐานความผิด ซึ่งฐานความผิดที่จะนำมาใช้กับสกุลเงินดิจิทัลได้นั้น เมื่อพิจารณาจากลักษณะภายนอกของสกุลเงินดิจิทัลจะเห็นได้ว่าสกุลเงินดิจิทัลเป็นวัตถุที่ไม่มีรูปร่าง ดังนั้นจึงใช้ได้กับความผิดที่กำหนดให้วัตถุแห่งการกระทำเป็นทรัพย์สินเท่านั้น อันได้แก่ ความผิดฐานกรรโชก รีดเอาทรัพย์สิน ฉ้อโกง ในขณะที่ความผิดฐานอื่นที่กำหนดให้วัตถุแห่งการกระทำเป็นทรัพย์สินที่แม้จะมีลักษณะทางกายภาพที่ไม่ตรงกับสกุลเงินดิจิทัล แต่ก็มีความผิดที่อาจเกิดขึ้นกับสกุลเงินดิจิทัลได้ เช่น ความผิดฐานลักทรัพย์ ชิงทรัพย์ ปล้นทรัพย์ ยักยอกทรัพย์ ดังนั้นหากมีการกระทำความผิดตามฐานที่กล่าวมานี้ จะเกิดปัญหาว่าไม่อาจนำกฎหมายที่มีอยู่มาใช้เพื่อลงโทษผู้กระทำความผิดได้เนื่องจากขาดองค์ประกอบความผิดในส่วนที่เป็นวัตถุแห่งการกระทำไป

2) สถานะเงินตรา เป็นการพิจารณาในแง่ของการทำหน้าที่บางประการได้เสมือนเงินตรา ได้แก่ 1) หน้าที่ในการเป็นสื่อกลางการแลกเปลี่ยน แม้ปัจจุบันสำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ หรือ ก.ล.ต. ได้ออกเกณฑ์กำกับกับการให้บริการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ไม่สนับสนุนการใช้สินทรัพย์ดิจิทัลเป็นสื่อกลางชำระค่าสินค้าหรือบริการก็ตาม โดยคำนึงถึงประโยชน์และความเสี่ยงของสินทรัพย์ดิจิทัลจากความผันผวนของราคา ความเสี่ยงจากการถูกโจรกรรมทางไซเบอร์ ความเสี่ยงข้อมูลส่วนบุคคลรั่วไหล หรือการถูกใช้เป็นเครื่องมือของการฟอกเงิน จึงได้ออกประกาศให้ผู้ประกอบธุรกิจสามารถให้บริการเพื่อการลงทุนได้ แต่ห้ามมิให้บริการนำสินทรัพย์ดิจิทัลมาใช้เป็นสื่อกลางชำระค่าสินค้าและบริการ<sup>334</sup> ซึ่งประกาศดังกล่าวเป็นการกำกวมดูแลผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลเท่านั้น จึงไม่กระทบกับภาคประชาชนที่ยังสามารถใช้และถือครองสกุลเงินดิจิทัลในฐานะเป็นสื่อกลางการแลกเปลี่ยนระหว่างผู้ใช้ด้วยกันได้โดยไม่ต้องผ่านตัวแทนหรือผู้ประกอบธุรกิจสินทรัพย์ดิจิทัลแต่อย่างใด 2) หน้าที่ในการเป็นมาตรฐานการวัดมูลค่าสินค้าและบริการ แม้มูลค่าของสกุลเงินดิจิทัลจะไม่ได้อิงตามค่าเงินของสกุลใดแต่มีมูลค่าขึ้นลงจากความต้องการของผู้ใช้โดยแท้ก็ตาม และมูลค่านั้นสามารถเทียบได้กับสกุลเงินตราของประเทศอื่นได้เช่นกัน ดังนั้น

<sup>334</sup> สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, ก.ล.ต. ออกเกณฑ์กำกับ การให้บริการของผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล ไม่สนับสนุนการใช้สินทรัพย์ดิจิทัลเป็นสื่อกลาง, ค้นวันที่ 5 มกราคม 2565 จาก[https://www.sec.or.th/TH/Pages/News\\_Detail.aspx?SECID=9353](https://www.sec.or.th/TH/Pages/News_Detail.aspx?SECID=9353)

สกุลเงินดิจิทัลจึงสามารถทำหน้าที่เป็นมาตรฐานการวัดมูลค่าได้เสมือนเงินตรา และ3) หน้าที่ในการสะสมมูลค่าหรือเก็งกำไร แม้สกุลเงินดิจิทัลมีความผันผวนสูงซึ่งอาจถือเป็นข้อควรระวังในการลงทุน แต่มูลค่าที่เพิ่มขึ้นอย่างรวดเร็วก็เป็นสิ่งจูงใจให้ผู้ใช้บางกลุ่มนิยมการเก็งกำไรที่มีความเสี่ยงสูงเช่นกัน

อย่างไรก็ตามแม้สกุลเงินดิจิทัลจะทำหน้าที่ได้ใกล้เคียงกับเงินตราก็ตาม แต่เมื่อพิจารณาความหมายทางกฎหมายคำว่าเงินตราหมายถึง เหรียญกษาปณ์และธนบัตร<sup>335</sup> ซึ่งสองสิ่งนี้เป็นสิ่งที่มีรูปร่าง ดังนั้นความผิดเกี่ยวกับเงินตราจึงเป็นความผิดที่ต้องกระทำต่อวัตถุที่มีรูปร่าง เช่น ความผิดฐานปลอมเงินตรา ความผิดฐานแปลงเงินตรา ความผิดฐานทำให้เหรียญกษาปณ์น้ำหนักลดลง ในขณะที่สกุลเงินดิจิทัลถูกสร้างขึ้นในรูปแบบสถาปัตยกรรมระบบคอมพิวเตอร์<sup>336</sup> จึงเป็นวัตถุที่ไม่มีรูปร่าง ดังนั้นสกุลเงินดิจิทัลจึงไม่ต้องตามความหมายคำว่าเงินตราและไม่สามารถนำความผิดเกี่ยวกับเงินตรามาปรับใช้ได้เหมาะสม

3) สถานะข้อมูลคอมพิวเตอร์ หมายถึง ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์<sup>337</sup> จากนิยามดังกล่าว สกุลเงินดิจิทัลได้จัดเก็บอยู่ในระบบคอมพิวเตอร์ซึ่งสามารถประมวลผลและปรากฏให้เห็นได้ในรูปแบบดิจิทัล ดังนั้นสกุลเงินดิจิทัลจึงมีสถานะเป็นข้อมูลคอมพิวเตอร์ได้ตามความหมายข้างต้น จากการศึกษาพบว่าแม้สกุลเงินดิจิทัลจะอยู่ในความหมายของสถานะข้อมูลคอมพิวเตอร์ได้ก็ตาม แต่ลักษณะการกระทำความผิดบางประการที่ใช้กับข้อมูลคอมพิวเตอร์ไม่อาจเกิดขึ้นกับสกุลเงินดิจิทัลได้ เช่น ความผิดฐานดักจับข้อมูลคอมพิวเตอร์ของผู้อื่นที่อยู่ระหว่างการส่งในระบบคอมพิวเตอร์ ความผิดฐานส่งข้อมูลคอมพิวเตอร์โดยปกปิดหรือปลอมแปลงแหล่งที่มาของการส่ง เป็นต้น ดังนั้นสถานะข้อมูลคอมพิวเตอร์จึงไม่เหมาะสมกับสกุลเงินดิจิทัล

4) สถานะเอกสาร เป็นการวิเคราะห์โดยผลของคำพิพากษาศาลฎีกาที่ 4311/2557 ซึ่งได้วินิจฉัยว่าการพิมพ์ข้อความลงบนเครื่องคอมพิวเตอร์เป็นการทำให้ปรากฏความหมายบนวัตถุอื่นใด เช่นเดียวกับการกระทำลงบนเอกสาร ส่วนคำว่า “เอกสาร” หมายความว่า

<sup>335</sup> มาตรา 6 แห่งพระราชบัญญัติเงินตรา พ.ศ. 2501

<sup>336</sup> Sessa Kethineni, Ying Cao and Cassandra Dodge, “Use of Bitcoin in Darknet Market: Examining Facilitative Factors on Bitcoin-Related Crimes,” *American Journal of Criminal Justice* 43 (2018): 142.

<sup>337</sup> มาตรา 3 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.

“กระดาษหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น”<sup>338</sup> ดังนั้นการทำข้อมูลคอมพิวเตอร์ให้ปรากฏความหมายบนหน้าจอคอมพิวเตอร์ ไม่ว่าจะป็นรูปแบบของตัวอักษร ตัวเลข ผัง หรืออย่างอื่น ย่อมมีผลทางกฎหมายเท่ากับเป็นการกระทำลงบนเอกสารและสิ่งนั้นมีสถานะเป็นเอกสาร

จากคำวินิจฉัยของคำพิพากษานี้แม้จะมีผลเป็นการยอมรับสถานะข้อมูลคอมพิวเตอร์ให้มีความเท่าเทียมกับสถานะเอกสารก็ตาม แต่ผู้เขียนเห็นว่าคำพิพากษาดังกล่าวจะเป็นการตีความโดยนำหลักความเท่าเทียมกันในการทำหน้าที่ (Functional-Equivalent Approach) ซึ่งหลักดังกล่าวเป็นการรับรองธุรกรรมทางแพ่งและพาณิชย์มาใช้ในการปรับบทกฎหมาย กล่าวคือ เมื่อการใดกระทำลงโดยใช้วิธีการติดต่อสื่อสารแบบดั้งเดิมแล้วสามารถทำหน้าที่ได้และมีผลสมบูรณ์ตามกฎหมายหากการนั้นได้กระทำลงโดยใช้ข้อมูลอิเล็กทรอนิกส์แทนเอกสารปกติธรรมดา การนั้นก็ต้องทำหน้าที่ได้อย่างเดียวกันกับการที่กระทำลงโดยวิธีการดั้งเดิมและต้องมีผลทางกฎหมายอย่างเดียวกัน ซึ่งการหลักการดังกล่าวนั้นเป็นการรองรับความเท่าเทียมของสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์และเอกสารในการทำธุรกรรมทางแพ่งและพาณิชย์เท่านั้น แต่สำหรับในทางอาญามีได้พิจารณาความเท่าเทียมกันในการหน้าที่เหมือนเช่นกฎหมายแพ่ง ซึ่งความเท่าเทียมกันหรืออาจแทนที่กันได้นั้นจะต้องพิจารณาจากความหมายและลักษณะของการกระทำมีความผิดต้องมีลักษณะเดียวกัน ดังจะเห็นได้ว่าความผิดเกี่ยวกับเอกสารที่บัญญัติไว้ในประมวลกฎหมายอาญามีลักษณะความผิดที่กระทำต่อวัตถุที่มีรูปร่างและมีคุณธรรมทางกฎหมายเพื่อคุ้มครองความน่าเชื่อถือของเอกสารและการใช้เอกสารเป็นพยานหลักฐาน และเป็นหลักประกันความแท้จริงของเอกสาร ในขณะที่สกุลเงินดิจิทัลเป็นวัตถุที่ไม่มีรูปร่างและไม่ได้มีวัตถุประสงค์เพื่อคุ้มครองความน่าเชื่อถือในฐานะที่เป็นพยานหลักฐานแต่มีขึ้นเพื่อคุ้มครองความเป็นเจ้าของ รักษาเป็นส่วนตัว และสร้างความเชื่อมั่นให้กับผู้ใช้และผู้ถือครองสกุลเงินดิจิทัล ดังนั้นสถานะเอกสารจึงไม่สามารถนำมาปรับใช้กับสกุลเงินดิจิทัลได้อย่างเหมาะสม

จากการวิเคราะห์สถานะทรัพย์สิน เงินตรา ข้อมูลคอมพิวเตอร์ และเอกสาร ในการนำมาปรับใช้กับสกุลเงินดิจิทัล สามารถสรุปเป็นตารางได้ดังนี้

<sup>338</sup> มาตรา 1 (7) แห่งประมวลกฎหมายอาญา

ตารางที่ 4.1 ตารางสรุปความแตกต่างของสถานะทรัพย์สิน เงินตรา ข้อมูลคอมพิวเตอร์ เอกสารและสกุลเงินดิจิทัล

สถานะ	ทรัพย์สิน	เงินตรา	ข้อมูลคอมพิวเตอร์	เอกสาร	สกุลเงินดิจิทัล
1. ลักษณะ	วัตถุไม่มีรูปร่าง	เหรียญกษาปณ์และธนบัตร	วัตถุไม่มีรูปร่าง มีลักษณะเป็นข้อมูลที่สามารถประมวลผลได้ด้วยระบบคอมพิวเตอร์	กระดาษหรือวัตถุอื่นใดซึ่งสามารถปรากฏความหมายได้	วัตถุไม่มีรูปร่าง มีลักษณะเป็นข้อมูลที่สามารถประมวลผลได้ด้วยระบบคอมพิวเตอร์ ซึ่งใช้เป็นสื่อกลางในการแลกเปลี่ยนและการลงทุน
2. นิยามกฎหมาย	ประมวลกฎหมายแพ่งและพาณิชย์ มาตรา 137 “วัตถุไม่มีรูปร่าง” มาตรา 138 “ทรัพย์สิน หมายความรวมถึงทรัพย์สินและรูปร่าง ซึ่งอาจมีราคาและอาจถือเอาได้”	พระราชบัญญัติ พระราชบัญญัติ เงินตรา พ.ศ. 2501 มาตรา 6 “เหรียญกษาปณ์และธนบัตร”	พระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 มาตรา 3 “ข้อมูล ข้อความ คำสั่ง ชุดคำสั่ง หรือสิ่งอื่นใดบรรดาที่อยู่ในระบบคอมพิวเตอร์ในสภาพที่ระบบคอมพิวเตอร์อาจประมวลผลได้ และให้หมายความรวมถึง ข้อมูลอิเล็กทรอนิกส์ ตามกฎหมายว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์”	ประมวลกฎหมายอาญา มาตรา 1 (7) “กระดาศหรือวัตถุอื่นใดซึ่งได้ทำให้ปรากฏความหมายด้วยตัวอักษร ตัวเลข ผัง หรือแผนแบบอย่างอื่น จะเป็นโดยวิธีพิมพ์ ถ่ายภาพ หรือวิธีอื่นอันเป็นหลักฐานแห่งความหมายนั้น”	พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 มาตรา 3 “สินทรัพย์ดิจิทัล หมายถึง ทรัพย์สินหรือโทเคนดิจิทัล” “คริปโทเคอร์เรนซี หมายถึง หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นสื่อกลางในการแลกเปลี่ยน การแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์



สถานะ	ทรัพย์สิน	เงินตรา	ข้อมูลคอมพิวเตอร์	เอกสาร	สกุลเงินดิจิทัล
3. ผิดโง่			<p>ขอบมาตรา 7</p> <p>2. ตักรับข้อมูลคอมพิวเตอร์โดยมิชอบมาตรา 8</p> <p>3. ทำให้ข้อมูลคอมพิวเตอร์เสียหายมาตรา 9</p> <p>4. ปกปิดหรือปลอมแปลงแหล่งที่มาการส่งข้อมูลคอมพิวเตอร์มาตรา 11</p>	มาตรา 264 - 269	
5. ข้อจำกัดในการนำไปใช้กับสกุลเงินดิจิทัล	<p>ความผิดเกี่ยวกับสกุลเงินดิจิทัลทั้งความผิดที่เกี่ยวข้องกับทรัพย์สินและทรัพย์สิน แต่จะนำมาใช้ได้เฉพาะฐานความผิดที่เกี่ยวข้องกับทรัพย์สินเท่านั้น</p>	<p>เป็นการกระทำต่อวัตถุที่มีรั้วรัวซึ่งเป็นที่หรือธนบัตร ลักษณะความผิดที่ใช้ในการควบคุมเงินตรา ไม่สามารถนำมาใช้กับความผิดเกี่ยวกับสกุลเงินดิจิทัล</p>	<p>ความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์นำมาใช้กับสกุลเงินดิจิทัลได้บางส่วน</p> <p>ความผิด ดังนี้</p> <p>1. ความผิดเกี่ยวกับระบบคอมพิวเตอร์ 5, 6 ได้ แต่ใช้มาตรา 10 ไม่ได้</p> <p>2. ความผิดเกี่ยวกับข้อมูลคอมพิวเตอร์ 7, 9 ได้ ส่วนมาตราอื่น ๆ ที่เป็นข้อมูลคอมพิวเตอร์ไม่ได้มีลักษณะความผิดที่นำมาใช้กับสกุลเงินดิจิทัลได้</p>	<p>เป็นการกระทำต่อวัตถุที่มีรูปร่าง</p> <p>ความผิดตามมาตรา 188 มิได้มีเจตนาจะนำไปใช้กับความผิดฐานขโมยสกุลเงินดิจิทัล เนื่องจากไม่ได้กำหนดเจตนาพิเศษ และความผิดอื่น ๆ ที่เกี่ยวกับเอกสารเป็นการกระทำต่อวัตถุที่มีรูปร่าง</p>	<p>เป็นความผิดที่อาจนำฐานความผิดเกี่ยวกับทรัพย์สินและข้อมูลคอมพิวเตอร์มาใช้ได้ในบางฐาน และมีลักษณะเฉพาะอื่น ๆ ที่กฎหมายยังไม่ครอบคลุม</p>

จากตารางข้างต้นแสดงให้เห็นถึงลักษณะเฉพาะและข้อจำกัดทางกฎหมายของแต่ละสถานะที่ไม่สามารถนำมาปรับกับความผิดเกี่ยวกับสกุลเงินดิจิทัลได้อย่างเป็นระบบ อีกทั้งกฎหมายอาญาของไทยยังมีได้มีการกำหนดสถานะของสกุลเงินดิจิทัลไว้อย่างชัดเจน ปัญหาดังกล่าวจึงก่อให้เกิดช่องว่างทางกฎหมายในความรับผิดชอบทางอาญาของบุคคลตามมา กล่าวคือเมื่อมีการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลเกิดขึ้นแต่กฎหมายมิได้มีการกำหนดให้สกุลเงินดิจิทัลมีสถานะหรือมีการกำหนดให้เป็นองค์ประกอบความผิดของกฎหมายอาญาดังกล่าวไว้อย่างชัดเจนแล้ว ย่อมไม่อาจลงโทษบุคคลนั้นได้ และจะนำบทบัญญัติกฎหมายใกล้เคียงอย่างอื่นมาปรับใช้หรือตีความขยายความในลักษณะที่แตกต่างจากถ้อยคำที่เป็นบัญญัติไว้เป็นลายลักษณ์อักษรไม่ได้ ทั้งนี้เป็นไปตามหลักประกันกฎหมายอาญาที่ต้องมีความชัดเจนภายใต้กฎหมายที่ประกาศให้ประชาชนรับรู้ทั่วกันแล้ว อย่างไรก็ตามได้มีการตีความคำพิพากษาศาลฎีกาตัดสินลงโทษทางอาญาแก่บุคคลโดยมิได้มีบทบัญญัติกำหนดความผิดไว้อย่างชัดเจน ซึ่งผู้เขียนได้นำคดีลักกระแสไฟฟ้า<sup>339</sup> มาเป็นกรณีศึกษา ด้วยเหตุที่การลักกระแสไฟฟ้ามิได้มีการกำหนดว่ากระแสไฟฟ้าซึ่งเป็นสิ่งที่มีรูปร่างอันจะเป็นวัตถุแห่งการกระทำในองค์ประกอบความผิดฐานลักทรัพย์ได้ เช่นเดียวกับการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลที่เกิดขึ้นในปัจจุบัน โดยในคำพิพากษาได้มีการลงมติในที่ประชุมแต่เพียงว่าการลักกระแสไฟฟ้าเป็นความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา มาตรา 334 โดยมีได้ให้เหตุผลในการวินิจฉัยว่ากระแสไฟฟ้าเป็นทรัพย์อันเป็นวัตถุที่มีรูปร่างหรือไม่ เพียงแต่กล่าวว่ากระแสไฟฟ้าให้ลงโทษความผิดฐานลักทรัพย์ได้เท่านั้น ดังนั้นประเด็นที่ว่าวัตถุแห่งการกระทำในความผิดฐานลักทรัพย์ที่ใช้คำว่า “ทรัพย์” นั้น รวมถึง “กระแสไฟฟ้า” ด้วยหรือไม่นั้น จึงยังเป็นที่ยกเถียงในวงการวิชาการจนถึงปัจจุบัน ซึ่งเป็นผลมาจากความไม่ชัดเจนกรณีที่มีการขโมยหรือเอาไปซึ่งวัตถุที่ไม่มีรูปร่างของผู้อื่นนั้นจะถือเป็นความผิดฐานลักทรัพย์ด้วยหรือไม่ และด้วยเหตุที่กฎหมายอาญาของไทยยังไม่มีบทบัญญัติกำหนดให้การลักกระแสไฟฟ้าเป็นความผิดไว้เป็นการเฉพาะ จึงส่งผลให้ศาลต้องตีความโดยปรับใช้กับกฎหมายเท่าที่มีอยู่ (ความผิดฐานลักทรัพย์) มาลงโทษผู้ที่ลักกระแสไฟฟ้า อย่างไรก็ตามแนวทางการตัดสินกรณีดังกล่าวแม้จะมีเหตุผลในแง่ของการกระทำที่สมควรถูกลงโทษก็ตาม แต่เมื่อพิจารณาถึงหลักประกันของกฎหมายอาญาที่ต้องมีความชัดเจนแน่นอนแล้วย่อมขัดต่อหลักการดังกล่าว ดังนั้นเพื่อให้ข้อถกเถียงที่ว่าความผิดฐานลักทรัพย์นั้นให้หมายรวมถึงกระแสไฟฟ้าหรือพลังงานด้วยหรือไม่นั้นเป็นที่ยุติ ได้มีนักวิชาการเห็นว่าควรมีแก้ไขกฎหมายในส่วนนี้ให้เกิดความชัดเจน<sup>340</sup> อีกทั้งประเทศไทยอยู่ในระบบซีวิลลอว์ซึ่งใช้กฎหมายจากบทบัญญัติที่เป็นลายลักษณ์จึง

<sup>339</sup> คำพิพากษาศาลฎีกาที่ 877/ 2501

<sup>340</sup> ทวีเกียรติ มีนะกนิษฐ, **กฎหมายกับสังคม** (กรุงเทพมหานคร: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2552), หน้า 149.

ต้องตีความอย่างเคร่งครัด และหลีกเลี่ยงการปรับใช้กฎหมายและการตีความโดยเทียบบทกฎหมายที่ใกล้เคียงอย่างยิ่ง

อย่างไรก็ตามสำหรับกรณีลักขโมยกระแสไฟฟ้าหรือพลังงานในต่างประเทศได้มีบทบัญญัติดังกล่าวไว้เป็นการเฉพาะเพื่อหลีกเลี่ยงปัญหาการไม่มีบทบัญญัติที่ชัดเจนในการลงโทษ สหรัฐอเมริกาได้กำหนดความผิดฐานลักทรัพย์ไว้ใน Model Penal Code มาตรา 223.2 โดยกำหนดวัตถุประสงค์ของการกระทำที่จะเป็นความผิดฐานลักทรัพย์ได้นั้น ได้แก่ ทรัพย์สินที่เคลื่อนที่ได้ และ ทรัพย์สินที่เคลื่อนที่ไม่ได้ และได้มีการนิยามคำว่าทรัพย์สินให้หมายความถึงกระแสไฟฟ้าไว้ในมาตรา 223.0.(6) ไว้อย่างชัดเจน ส่วนประเทศอังกฤษโดยบัญญัติความผิดฐานลักกระแสไฟฟ้า (Abstracting of Electricity) ไว้เป็นการเฉพาะใน Theft Act 1968 ความผิดซึ่งมีโทษจำคุกไม่เกินห้าปีและ หรือปรับ สำหรับการลักใช้ไฟฟ้า พลังงานที่สิ้นเปลือง หรือเปลี่ยนทิศทางกระแสไฟฟ้าโดยทุจริต รวมถึงการกระทำโดยการเสียดใช้มิเตอร์ไฟฟ้าของตนหรือต่อมิเตอร์ไฟฟ้าที่ติดการเชื่อมต่อใหม่ หรือใช้โทรศัพท์โดยไม่เสียค่าใช้จ่ายอย่างผิดกฎหมาย ประเทศเยอรมนีก็ได้มีการบัญญัติความผิดฐานใช้กระแสไฟฟ้าของผู้อื่นโดยไม่ได้รับอนุญาตเป็นความผิดอีกฐานหนึ่งในประมวลกฎหมายอาญา<sup>341</sup> ประเทศฝรั่งเศสได้มีการกำหนดไว้เป็นลายลักษณ์อักษรให้การลักใช้กระแสไฟฟ้าของผู้อื่นเป็นความผิดเช่นเดียวกับความผิดฐานลักทรัพย์<sup>342</sup>

อย่างไรก็ตามแม้ประเทศทั้งสองจะใช้ระบบคอมมอนลอว์ซึ่งศาลสามารถตีความและปรับใช้กฎหมายเพื่อให้เกิดความยุติธรรมได้ แต่ก็ได้มีบทบัญญัติเป็นลายลักษณ์อักษรที่มีความชัดเจนเพื่อเป็นขอบเขตในการตีความได้อย่างเหมาะสมยิ่งขึ้น ดังนั้นเพื่อเป็นการหลีกเลี่ยงปัญหาความไม่ชัดเจนของกฎหมายอันเนื่องมาจากการไม่มีบทบัญญัติที่จะลงโทษผู้กระทำผิด จึงควรมีบัญญัติกฎหมายที่ใช้กับการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลไว้เป็นการเฉพาะ โดยกำหนดสถานะทางกฎหมายให้กับสกุลเงินดิจิทัลเพื่อเป็นองค์ประกอบความผิดอาญาในฐานความผิดนั้น ๆ ได้อย่างชัดเจน เพื่อเป็นการป้องกันไม่ให้เกิดปัญหาการตีความหรือการปรับใช้กฎหมายโดยนำบทกฎหมายใกล้เคียงอย่างยิ่งมาใช้ ก่อให้เกิดการบังคับใช้กฎหมายที่ขาดเอกภาพและขัดต่อหลักประกันของกฎหมายอาญา

<sup>341</sup> Gerold Harfst, **German Criminal Law** (Germany: Rosch-Buch Scheblitz, 1998), p. 156.

<sup>342</sup> Code Penal 1992 Article 311-2 “Dishonest appropriation of energy to prejudice of another person is assimilated to theft”

## 4.2 ปัญหาฐานความผิดเกี่ยวกับสกุลเงินดิจิทัล

ความผิดตามประมวลกฎหมายอาญาและความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 แม้จะมีบางฐานความผิดอาจนำมาปรับใช้กับความผิดเกี่ยวกับสกุลเงินดิจิทัลได้ก็ตาม แต่จากการศึกษาลักษณะการกระทำความผิดที่เกิดขึ้นกับสกุลเงินดิจิทัลในบทที่ 2 พบว่ายังมีความผิดบางลักษณะที่ไม่สามารถนำฐานความผิดตามกฎหมายที่มีอยู่เดิมมาปรับใช้ได้ ได้แก่ การขโมยสกุลเงินดิจิทัล และการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นโดยมิชอบ เนื่องจากความผิดเกี่ยวกับสกุลเงินดิจิทัลเป็นความผิดที่เกี่ยวข้องกับอาชญากรรมพื้นฐานผนวกกับเทคโนโลยี จึงมีลักษณะเฉพาะทางเทคนิค ซึ่งฐานความผิดในกฎหมายอาญาและพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ ที่มีอยู่ยังไม่สามารถรองรับการกระทำความผิดอันเกิดจากเทคโนโลยีในลักษณะดังกล่าวได้ ทั้งสองกรณีนี้จึงยังเป็นช่องว่างทางกฎหมายที่ยังสามารถลงโทษผู้กระทำความผิดได้ ในหัวข้อนี้จะกล่าวถึงปัญหาฐานความผิดที่เกี่ยวข้องกับทั้งสองกรณี ดังนี้

1) กรณีการขโมยสกุลเงินดิจิทัล สามารถแบ่งกระทำออกเป็นสามขั้นตอนด้วยกัน คือ ขั้นตอนแรกมีการเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ขั้นตอนที่สอง คือการเข้าไปใน Wallet ที่เก็บสกุลเงินดิจิทัล และขั้นตอนสุดท้าย คือทำการโอนสกุลเงินดิจิทัลจากบัญชี Wallet ของผู้เสียหายไปยังบัญชีอื่น ซึ่งการกระทำขั้นตอนนี้จึงยังเป็นความผิดตามองค์ประกอบความผิดฐานเข้าถึงระบบคอมพิวเตอร์ของผู้อื่นที่มีวิธีการป้องกันการเข้าถึงโดยเฉพาะ ตามมาตรา 5 แห่งพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้ เว้นแต่ระบบคอมพิวเตอร์ของผู้เสียหายไม่มีมาตรการป้องกันการเข้าถึงไว้ เช่นนี้ผู้กระทำจะไม่มีผิด ส่วนขั้นตอนที่สองเป็นการเข้าไปยังwalletที่เก็บสกุลเงินดิจิทัล หากมองว่าที่เก็บสกุลเงินดิจิทัลเป็นข้อมูลคอมพิวเตอร์ การเข้าถึงที่ดังกล่าวจึงเป็นความผิดตามมาตรา 7 ได้ แต่สำหรับส่วนที่ยังเป็นช่องว่างทางกฎหมายคือขั้นตอนที่ 3 การโอนสกุลเงินดิจิทัลของผู้เสียหายไปยังบัญชีอื่น ซึ่งมีฐานความผิดที่เกี่ยวข้อง ดังนี้

(1) ความผิดฐานลักทรัพย์ มาตรา 334 แห่งประมวลกฎหมายอาญา ได้กำหนดองค์ประกอบความผิดไว้ ดังนี้ 1) ผู้ใด 2) การเอาไป การแย่งการครอบครองและเข้ายึดถือเพื่อพาทรัพย์ของผู้อื่น “เคลื่อนที่” ไปจากการครอบครองอันมีลักษณะเป็นการตัดกรรมสิทธิ์เจ้าของเดิมออกจากตัวทรัพย์อย่างถาวร 3) ทรัพย์ของผู้อื่นหรือผู้อื่นเจ้าของรวมอยู่ด้วยนั้น ทั้งนี้มีประเด็นปัญหาที่ต้องพิจารณา คือ องค์ประกอบความผิด ข้อ 3) คำว่า “ทรัพย์” อันเป็นวัตถุแห่งการกระทำในความผิดฐานลักทรัพย์นั้นรวมถึงวัตถุที่ไม่มีรูปร่าง เช่น กระแสไฟฟ้า และในอนาคตอาจรวมถึงสกุลเงินดิจิทัลซึ่งไม่มีรูปร่างด้วยได้หรือไม่ ผู้เขียนเห็นว่าต้องพิจารณาจากถ้อยคำที่กฎหมายกำหนดไว้เป็นสำคัญ ด้วยเหตุที่ประเทศไทยอยู่ในระบบประมวลกฎหมายจึงควรยึดถ้อยคำจากบทบัญญัติแห่ง

กฎหมายมากกว่าการสร้างกฎหมาย (Judge Made Law) โดยการตีความจากศาล<sup>343</sup> ดังนั้นจึงต้องพิจารณาคำว่าทรัพย์สินจากถ้อยคำในกฎหมาย แม้ในบทนิยามแห่งประมวลกฎหมายอาญาจะไม่ได้บัญญัติความหมายของคำว่าทรัพย์สินไว้ ก็สามารถหาความหมายได้จากบทบัญญัติในประมวลกฎหมายแพ่งและพาณิชย์ตามหลักกฎหมายย่อมเกี่ยวข้องซึ่งกันและกันอยู่ เว้นแต่ตามบทบัญญัตินั้นจะแสดงว่าจะไม่ประสงค์ให้ความหมายดังที่ปรากฏตามกฎหมายอื่น<sup>344</sup> ซึ่งในมาตรา 137 ได้นิยามไว้ว่าทรัพย์สิน หมายถึง “วัตถุที่มีรูปร่าง” ดังนั้นสิ่งที่จะเป็นวัตถุแห่งการกระทำในความผิดฐานลักทรัพย์ได้นั้นจะต้องเป็นสิ่งที่มีการรูปร่าง ประกอบกับเมื่อพิจารณาถึงองค์ประกอบความผิดข้อ 2) การเอาไปจะต้องมีการพาทรัพย์สินเคลื่อนที่จากความครอบครองของเจ้าของเดิมไปสู่การครอบครองของบุคคลอื่น โดยมีเจตนาแสวงหาประโยชน์โดยมิชอบนั้นจำเป็นต้องเป็นการกระทำกับวัตถุที่มีรูปร่าง เพราะหากเป็นวัตถุที่ไม่มีรูปร่างแล้วจะไม่สามารถทราบได้ว่าการเอาไปแล้วหรือไม่ ซึ่งจะมีผลต่อการวินิจฉัยความรับผิดว่าการกระทำนั้นเป็นความผิดสำเร็จหรือเป็นเพียงการพยายามการทำความผิด

ดังนั้นเมื่อความผิดฐานลักทรัพย์ได้กำหนดให้วัตถุแห่งการกระทำไว้เป็น “ทรัพย์สิน” ซึ่งหมายถึงวัตถุที่มีรูปร่างไว้อย่างชัดเจนแล้ว จึงไม่มีความจำเป็นต้องตีความขยายถ้อยคำให้รวมไปถึงวัตถุที่ไม่มีรูปร่างด้วย ดังนั้นความผิดฐานลักทรัพย์ซึ่งกำหนดวัตถุแห่งการกระทำให้เป็นวัตถุที่มีรูปร่างจึงไม่อาจนำมาใช้กับได้กรณีการขโมยสกุลเงินดิจิทัลซึ่งเป็นวัตถุคนละประเภทได้

(2) ความผิดฐานทำให้เสียหายซึ่งพินัยกรรมหรือเอกสาร มาตรา 188 แห่งประมวลกฎหมายอาญา ความผิดฐานนี้ถูกนำมาเชื่อมโยงกับการขโมยสกุลเงินดิจิทัลด้วยเหตุที่มีคำพิพากษาได้วินิจฉัยให้ข้อมูลคอมพิวเตอร์เป็นเอกสาร<sup>345</sup> ซึ่งมีผลทำให้นำความผิดที่กำหนดให้วัตถุแห่งการกระทำเป็นเอกสารมาใช้แทนหรือมีค่าเท่ากับข้อมูลคอมพิวเตอร์ได้ จึงมีประเด็นปัญหาว่าหากพิจารณาว่าสกุลเงินดิจิทัลมีความเป็นข้อมูลคอมพิวเตอร์ในตัวแล้วก็อาจนำความผิดเกี่ยวกับเอกสารมาใช้กับสกุลเงินดิจิทัลได้ด้วย ดังนั้นความผิดฐานเอาไปซึ่งเอกสารจึงอาจนำมาปรับใช้กับการขโมยสกุลเงินดิจิทัลได้ ความผิดฐานนี้มีองค์ประกอบความผิด คือ 1) เอาไป 2) ซึ่งเอกสารหรือพินัยกรรมของผู้อื่น 3) โดยเจตนา 4) ในประการที่น่าจะเกิดความเสียหายแก่ผู้อื่นหรือประชาชน ความผิดฐานนี้แม้จะมีการกำหนดให้ “การเอาไป” มีลักษณะ เช่นเดียวกับความผิดฐานลักทรัพย์ก็ตาม แต่เมื่อพิจารณาเจตนาประกอบกับการเอาไป จะเห็นได้ว่าการเอาไปในความผิดตามมาตรา 188 นี้เพียงผู้กระทำมีเจตนา (ธรรมดา) ในการย้ายที่เอกสารจากที่เดิมที่เคยวางอยู่โดยมิพพฤติการณ์

<sup>343</sup> Joel Sarmaha, **Criminal Law**, 11<sup>th</sup> ed. (Belmont, CA: Wadsworth Learning, 2014), p. 16.

<sup>344</sup> กิตติศักดิ์ ปรกติ, *เรื่องเดิม*, หน้า 47.

<sup>345</sup> คำพิพากษาฎีกาที่ 4311/2557

ประกอบความเสียหายว่าน่าจะเสียหายอย่างไรก็เพียงพอแล้วโดยไม่จำเป็นต้องเกิดความเสียหายขึ้นจริง ลักษณะของการเอาไปดั่งกล่าวจึงกว้างจนสามารถครอบคลุมคำว่า เอาไปในความผิดฐานลักทรัพย์ได้ก็ตาม แต่สำหรับกรณีการเอาไปซึ่งสกุลเงินดิจิทัลหรือการขโมยสกุลเงินดิจิทัลนั้น การเอาไปที่จะเป็นความผิดได้นั้นจะต้องเป็นการเอาไปเพื่อแสวงหาประโยชน์โดยมิชอบ(ต้องมีเจตนาพิเศษโดยทุจริต) อันมีลักษณะเช่นเดียวกับการลักทรัพย์ ดังนั้นจะเห็นได้ว่าความผิดตามมาตรา 188 กับความผิดกรณีการขโมยสกุลเงินดิจิทัลนั้น แม้จะมีการเอาไปเช่นเดียวกัน แต่เจตนาอันเป็นองค์ประกอบภายในกำหนดไว้แตกต่างกัน อีกทั้งกฎหมายมีวัตถุประสงค์ในการคุ้มครองที่แตกต่างกัน กล่าวคือมาตรา 188 ความผิดเกี่ยวกับเอกสารนั้นกฎหมายมุ่งคุ้มครองความน่าเชื่อถือของเอกสารในฐานะที่เป็นพยานหลักฐานในกระบวนการยุติธรรม เนื่องจากเป็นความผิดที่อยู่ในหมวดความผิดต่อเจ้าพนักงานในการยุติธรรม ส่วนการขโมยเป็นความผิดที่ประมวลกฎหมายอาญาจัดไว้ในลักษณะ 12 ความผิดเกี่ยวกับทรัพย์ ย่อมแสดงให้เห็นว่ามุมมองของกฎหมายต่อทรัพย์มุ่งคุ้มครองตัวทรัพย์ในฐานะที่เป็นวัตถุแห่งกรรมสิทธิ์หรือคุ้มครองความเป็นกรรมสิทธิ์ต่อทรัพย์นั้น กฎหมายจึงมีวัตถุประสงค์ในการคุ้มครองที่แตกต่างกันและผู้กระทำมีเจตนาที่แตกต่างกัน ดังนั้นการนำมาตรา 188 มาปรับใช้กับการขโมยสกุลเงินดิจิทัลจึงมิได้สะท้อนให้เห็นถึงเจตนาที่แท้จริงของผู้กระทำที่แตกต่างกันซึ่งควรมีบทลงโทษที่ต่างกัน บทบัญญัตินี้จึงไม่เหมาะสมที่จะนำมาใช้กับกรณีการขโมยสกุลเงินดิจิทัล

(3) ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ มาตรา 7 แห่งพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ประเด็นปัญหาที่ต้องพิจารณาในความผิดฐาน “เข้าถึง” ข้อมูลคอมพิวเตอร์นี้ ซึ่งจะมีลักษณะเช่นเดียวกับการที่บุคคลหนึ่งเอาไปซึ่งสกุลเงินดิจิทัลของผู้อื่นไปหรือไม่ ความหมายของคำว่า “เข้าถึง” หมายถึงมีขอบเขตของการกระทำที่สามารถเข้าไปดำเนินการต่าง ๆ เกี่ยวกับข้อมูลคอมพิวเตอร์นั้นได้ ไม่ว่าจะทางกายภาพ ทางไกล หรือการควบคุมข้อมูลคอมพิวเตอร์จากระยะไกล รวมถึงเข้าถึงข้อมูลคอมพิวเตอร์ทั้งหมดหรือแต่บางส่วนก็ได้<sup>346</sup> ไม่จำเป็นว่าการแสดงข้อมูลโดยคอมพิวเตอร์หรือการประมวลผลของข้อมูลคอมพิวเตอร์ หรือการคัดลอกหรือย้ายข้อมูลไปยังที่อื่นในคอมพิวเตอร์ หรือไปยังอุปกรณ์จัดเก็บข้อมูล<sup>347</sup> ดังนั้นจะเห็นได้ว่าการเข้าถึงข้อมูลคอมพิวเตอร์กระทำด้วยวิธีการใด ๆ ที่เป็นการเข้าถึงโดยปราศจากอำนาจ เช่น การแอบเข้าไปดูข้อมูลคอมพิวเตอร์แล้วจดจำออกมา หรือเข้าถึงแล้วแอบถ่ายรูปรูปด้วยโทรศัพท์มือถือไว้ หรือทำสำเนาข้อมูล แม้จะไม่กระทบต่อข้อมูลต้นฉบับก็ตาม ก็อยู่ในความหมายของความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ทั้งสิ้น นอกจากนี้การขโมยหรือการเอาไปซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ

<sup>346</sup> พรเพชร วิชิตชลชัย, *เรื่องเดิม*.

<sup>347</sup> สาวตรี สุขศรี, *เรื่องเดิม*, หน้า 163.

ยังเป็นความผิดที่ใช้ความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ลงโทษผู้กระทำความผิดได้ เนื่องจากกฎหมายไทยมองว่าการเอาไปซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นได้นั้น เป็นการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบอยู่ในตัว ดังนั้นจึงไม่จำเป็นต้องมีบทบัญญัติว่าด้วยการเอาไปซึ่งข้อมูลคอมพิวเตอร์อีกบทหนึ่งแยกต่างหากจากการเข้าถึงข้อมูลคอมพิวเตอร์ ดังนั้นบทบัญญัติความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 นี้จึงมีขอบเขตกว้างจนสามารถครอบคลุมถึงกรณีการขโมยหรือการเอาไปซึ่งข้อมูลคอมพิวเตอร์ได้ ทั้งนี้แนวคิดในการกำหนดขอบเขตการเข้าถึงข้อมูลคอมพิวเตอร์ของพระราชบัญญัตินี้มีที่มาจาก Convention on Cybercrime<sup>348</sup> ซึ่งได้กำหนดต้นแบบความผิดฐานเข้าถึงระบบคอมพิวเตอร์ไว้ซึ่งเปิดโอกาสให้ประเทศสมาชิกสามารถกำหนดรายละเอียดเพิ่มเติมจากที่อนุสัญญาที่กำหนดไว้ได้ ดังนั้นประเทศไทยจึงเลือกที่จะกำหนดให้การเข้าถึงระบบคอมพิวเตอร์โดยมิชอบเป็นความผิดตามมาตรา 5 และการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบเป็นความผิดตามมาตรา 7 อันเป็นการกำหนดขอบเขตการเข้าถึงไว้อย่างกว้าง โดยมีได้มีการกำหนดให้กระทำให้มีลักษณะเป็นการเอาไปเป็นความผิดได้อีก และหากกฎหมายประสงค์จะให้การกระทำใดเป็นความผิดที่อยู่ นอกเหนือขอบเขตการเข้าถึงแล้วก็จะมิบทบัญญัติให้การกระทำนั้นเป็นความผิดไว้เฉพาะแยกต่างหากจากมาตรา 7 การจากศึกษาพบว่ามีเพียง 3 ฐานความผิดนี้เท่านั้น ซึ่งเป็นการกระทำที่กฎหมายกำหนดให้เป็นความผิดและเป็นขั้นตอนหลังจากที่ได้มีการเข้าถึงข้อมูลคอมพิวเตอร์โดยมิชอบมาแล้ว ดังนี้

ก) ความผิดฐานดักจับข้อมูลคอมพิวเตอร์ที่อยู่ระหว่างการส่ง มาตรา 8 เป็นกรณีดักจับข้อมูลที่อยู่ระหว่างการส่ง (Intercept) โดยไม่มีสิทธิและข้อมูลนั้นไม่ได้มีไว้เพื่อประโยชน์สาธารณะ ไม่ว่าจะเป็นภาพ เสียง ข้อมูล รหัส ฯลฯ เช่น สร้างเว็บไซต์ปลอมเพื่อดักข้อมูลหรือรหัสลับของลูกค้าธนาคาร การแอบฟังข้อความเสียงของบุคคลอื่นที่สื่อสารผ่าน VoicelP MSN

ข) ความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลงหรือเพิ่มเติมซึ่งข้อมูลคอมพิวเตอร์ มาตรา 9 ความผิดฐานนี้กฎหมายมีวัตถุประสงค์ในการคุ้มครองความสมบูรณ์ ครบถ้วนและถูกต้องของข้อมูล (Integrity of Data) ให้อยู่ในสภาพที่พร้อมใช้งาน ซึ่งจะคุ้มครองสองส่วนด้วยกันคือ คุ้มครองไม่ให้ข้อมูลถูกแก้ไข เปลี่ยนแปลง และคุ้มครองความน่าเชื่อถือของแหล่งที่มา ความผิดฐานนี้ ได้แก่ การแก้ไขเปลี่ยนแปลงข้อมูลคอมพิวเตอร์ การปล่อยไวรัสตั้งเวลาให้โปรแกรมทำลายข้อมูลคอมพิวเตอร์ เป็นต้น

อย่างไรก็ตามแม้การขโมยสกุลเงินดิจิทัลด้วยวิธีการส่งต่อหรือถ่ายโอนข้อมูลคอมพิวเตอร์จะมีลักษณะคล้ายกับการแก้ไขหรือเปลี่ยนแปลงซึ่งข้อมูลคอมพิวเตอร์อันเป็นความผิดตามพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ มาตรา 9 ก็ตาม

<sup>348</sup> Article 2, Convention on Cybercrime

แต่ผู้เขียนมีความเห็นว่า ความผิดตามมาตรา 9 มีลักษณะของการกระทำและเจตนาธรรมณ์เช่นเดียวกับการทำให้เสียหายทำลายทำให้เสื่อมค่าหรือทำให้ไร้ประโยชน์อันเป็นความผิดฐานทำให้เสียหายตามประมวลกฎหมายอาญามาตรา 358 ซึ่งมีเจตนาธรรมณ์ในการคุ้มครองความสมบูรณ์ของตัวทรัพย์สินหรือข้อมูลคอมพิวเตอร์ซึ่งเป็นวัตถุแห่งการกระทำ การกำหนดความผิดตามมาตรา 9 แห่งพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ จึงเป็นเรื่องของการเอาผิดกับผู้ที่มีเจตนาทำให้เสียหายหรือทำลายแก้ไขเปลี่ยนแปลง ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่น มิใช่เป็นการเอาผิดกับผู้ที่มีเจตนาเอาไปซึ่งสกุลเงินดิจิทัลของผู้อื่น ดังนั้นการเอาไปซึ่งสกุลเงินดิจิทัลของผู้อื่น จึงไม่อาจเป็นความผิดตามมาตรา 9 ได้

ค) ความผิดฐานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์รบกวนการใช้ระบบคอมพิวเตอร์โดยปกติสุขหรือก่อให้เกิดความเดือดร้อนรำคาญ มาตรา 11 เช่น การทำสแปม (Spamming) ปกปิดหรือปลอมแปลงแหล่งที่มา การส่ง e-Mail ขยายสินค้าหรือแจ้งข่าวสารไปยังลูกค้า สมาชิก โดยไม่เปิดโอกาสให้ยกเลิกการรับข้อมูล เป็นต้น

ดังนั้นจะเห็นได้ว่ามีเพียงสามฐานความผิดข้างต้นนี้เท่านั้นที่เป็นบทบัญญัติแยกออกมาอีกส่วนหลังจากที่ได้มีการกระทำอันเข้าถึงโดยปราศจากอำนาจ ส่วนกระทำอันมีลักษณะเป็นการส่งต่อข้อมูล การถ่ายโอนข้อมูลคอมพิวเตอร์ การเอาไปหรือการขโมยซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยไม่ได้รับอนุญาตนั้น มิได้มีบทบัญญัติที่แยกเฉพาะออกมา ดังนั้นการกระทำดังกล่าวจึงรวมอยู่ในความผิดฐานเข้าถึงโดยมิชอบทั้งสิ้น<sup>349</sup>

สำหรับกรณีการขโมยสกุลเงินดิจิทัลนั้นจะนำความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมาตรา 7 มาปรับใช้เช่นเดียวกับการขโมยข้อมูลคอมพิวเตอร์นั้น เห็นว่าการขโมยข้อมูลคอมพิวเตอร์และการขโมยสกุลเงินดิจิทัลมีลักษณะการกระทำความผิดที่แตกต่างในสาระสำคัญ คือ การขโมยข้อมูลคอมพิวเตอร์นั้นมิได้หลายรูปแบบ เช่น การทำสำเนาและนำข้อมูลออกมาหรือส่งต่อได้โดยไม่กระทบกับต้นฉบับ<sup>350</sup> ในขณะที่การขโมยสกุลเงินดิจิทัลนั้นไม่สามารถขโมยได้ด้วยการทำสำเนา ดังนั้นการขโมยสกุลเงินดิจิทัลจึงมีลักษณะเช่นเดียวกับความผิดฐานลักทรัพย์ตามประมวลกฎหมายอาญา มาตรา 334 มากกว่าจะเป็นความผิดในลักษณะของการเข้าถึงข้อมูลคอมพิวเตอร์ กล่าวคือเป็นการเอาไปซึ่งมีลักษณะเป็นการแย่งการครอบครองและทำลายกรรมสิทธิ์เจ้าของเดิม เนื่องจากเมื่อมีการเอาไปซึ่งสกุลเงินดิจิทัลแล้วจะไม่มีสกุลเงินดิจิทัลอีกชุดหนึ่งอยู่ที่เจ้าของเดิม แต่สกุลเงินดิจิทัลจะถูกย้ายไปอยู่ที่กระเป๋าเงินของผู้อื่น เนื่องจากสกุลเงินดิจิทัลได้ถูกออกแบบระบบ

<sup>349</sup> คณาธิป ทองรวีวงศ์, *เรื่องเดิม*, หน้า 110.

<sup>350</sup> สาวตรี สุขศรี, *เรื่องเดิม*, หน้า 164.

ป้องกันการโอนซ้ำซ้อน (Double Spending)<sup>351</sup> มาเป็นอย่างดี จึงไม่มีกรณีที่สกุลเงินดิจิทัลชุดเดียวกันจะอยู่ที่เจ้าของบัญชีและอยู่ที่บัญชีของผู้ที่ขโมยไปพร้อมกันได้ กรณีจึงต่างจากการทำสำเนาข้อมูลคอมพิวเตอร์ที่ข้อมูลคอมพิวเตอร์จะยังอยู่ที่เจ้าของเดิมและผู้ที่เขาไปได้ ดังนั้นความเสียหายอันเกิดจากได้ไปซึ่งสกุลเงินดิจิทัลจึงมีความแตกต่างจากการได้ไปซึ่งข้อมูลคอมพิวเตอร์ อีกทั้งการใช้งานและการถือครองสกุลเงินดิจิทัลมีลักษณะคล้ายเงินตราซึ่งมีมูลค่าและนำไปใช้ในระบบเศรษฐกิจได้จริง ดังนั้นผู้เขาไปโดยมิเจตนาเพื่อแสวงหาประโยชน์โดยมิชอบจากผู้อื่นจึงไม่ควรนำความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ที่ผู้กระทำความผิดเจตนาในการเข้าถึงมาใช้กับการขโมยสกุลเงินดิจิทัล

2) การใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล (Cryptojacking) คือ การนำพลังงานคอมพิวเตอร์ของผู้อื่นมาใช้ในการตรวจสอบธุรกรรมการโอนสกุลเงินดิจิทัลเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล ซึ่งเป็นความผิดเฉพาะที่เกิดขึ้นกับสกุลเงินดิจิทัลที่ยังมีช่องว่างทางกฎหมายที่ไม่มีความผิดฐานนำมาปรับใช้ได้อย่างเหมาะสม ทั้งนี้มีความผิดที่เกี่ยวข้อง ดังนี้

(1) ความผิดฐานกระทำเพื่อให้การทำงานของระบบคอมพิวเตอร์ไม่สามารถทำงานตามปกติ มาตรา 10 แห่งพระราชบัญญัติว่าด้วยความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ได้กำหนดองค์ประกอบความผิดให้ผู้กระทำต้องมีเจตนาพิเศษ กล่าวคือ นอกจากผู้กระทำจะต้องมีเจตนาในการกระทำอันมิชอบต่อระบบคอมพิวเตอร์ของผู้อื่นแล้ว ยังต้องประกอบด้วยเจตนาพิเศษที่กระทำไปนั้นเพื่อทำให้ระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานตามปกติได้ ดังนั้นความมุ่งหมายของมาตรานี้มีขึ้นเพื่อคุ้มครองระบบคอมพิวเตอร์ มิให้ถูกรบกวน ชัดขวาง จากการกระทำที่ไม่ปลอดภัย ในขณะที่การใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นนั้นผู้กระทำไม่ได้มีเจตนาพิเศษที่จะทำให้ระบบคอมพิวเตอร์ของผู้อื่นไม่สามารถใช้งานได้ตามปกติ แต่มีความมุ่งหมายหรือเจตนาพิเศษคือกระทำเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล ดังนั้น เจตนาพิเศษอันเป็นองค์ประกอบความผิดในมาตรา 10 จึงเป็นเจตนาที่มุ่งหมายต่อประโยชน์หรือวัตถุประสงค์เฉพาะกับการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่น ฐานความผิดดังกล่าวจึงไม่อาจนำมาปรับใช้ได้อย่างเหมาะสม

(2) ความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 334 มีองค์ประกอบ 4 ส่วน คือ

- ก) ผู้กระทำ
- ข) ลักษณะการกระทำ (การเอาไป)
- ค) วัตถุแห่งการกระทำ (ทรัพย์ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย)
- ง) เจตนาพิเศษ (โดยทุจริต)

<sup>351</sup> Satoshi Nakamoto, *op. cit.*, p. 2.

สำหรับกรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่น หมายถึง การใช้พลังงานไฟฟ้าของผู้อื่นโดยมิชอบ ซึ่งสามารถพิจารณาเทียบเคียงกับกรณีการเอาไปซึ่งกระแสไฟฟ้าของผู้อื่นโดยมิชอบ แม้กฎหมายไทยจะไม่มีบทบัญญัติให้การเอากระแสไฟฟ้าของผู้อื่นไปเป็นความผิดทางอาญาไว้โดยตรง แต่ศาลฎีกาได้เคยมีคำวินิจฉัยเกี่ยวกับการลักกระแสไฟฟ้าของผู้อื่นว่าการกระทำดังกล่าวเป็นความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญา มาตรา 334 อย่างไรก็ตามการเอาไปซึ่งทรัพย์ที่ไม่มีรูปร่างที่มีลักษณะใกล้เคียงกันนี้ยังมีแนวคำพิพากษาศาลฎีกาบางส่วนวินิจฉัยว่าไม่เป็นความผิดฐานลักทรัพย์ แต่เป็นความผิดตามพระราชบัญญัติเฉพาะ ในส่วนนี้ผู้เขียนขอแยกพิจารณาให้เห็นถึงความแตกต่างของแนวคำวินิจฉัยทั้งสองแนวทาง ดังนี้

(1) แนวคำวินิจฉัยที่เป็นความผิดฐานลักทรัพย์

คำพิพากษาศาลฎีกาที่ 877/2501 จำเลยกับพวกร่วมกันทำการต่อสายไฟฟ้าของกรุงเทพมหานคร กรมโยธาเทศบาล เข้ากับสายไฟฟ้าในบ้าน เป็นการกระทำผิดฐานลักทรัพย์

คำพิพากษาศาลฎีกาที่ 1880/2542 คำว่า “โทรศัพท์” สารานุกรมไทยสำหรับเยาวชนอธิบายว่า โทรศัพท์เป็นวิธีแปลงเสียงพูดให้เป็นกระแสไฟฟ้าแล้วส่งกระแสไฟฟ้าให้กลับเป็นเสียงพูดอีกครั้งหนึ่ง สัญญาณโทรศัพท์จึงเป็นกระแสไฟฟ้าที่แปลงมาจากเสียงพูดเคลื่อนที่ไปตามสายลวดตัวนำจากที่หนึ่งไปยังอีกที่หนึ่ง การที่จำเลยลักเอาสัญญาณโทรศัพท์จากตู้โทรศัพท์แห่งประเทศไทยไปใช้เพื่อประโยชน์ของจำเลยโดยทุจริตจึงเป็นความผิดฐานลักทรัพย์เช่นเดียวกับการลักกระแสไฟฟ้า

คำพิพากษาศาลฎีกาที่ 2286/2545 สัญญาณโทรศัพท์เป็นกรรมวิธีแปลงเสียงพูดให้เป็นกระแสไฟฟ้าแล้วส่งกระแสไฟฟ้านั้นไปในสายลวดไปเข้าเครื่องที่ศูนย์ชุมสายประจำภูมิภาคของการสื่อสารแห่งประเทศไทยผู้เสียหาย แล้วแปลงสัญญาณไฟฟ้าเป็นคลื่นวิทยุส่งไปยังเครื่องรับปลายทางในต่างประเทศ เครื่องรับปลายทางจะแปลงสัญญาณกลับเป็นเสียงพูดอีกครั้งหนึ่ง สัญญาณโทรศัพท์จึงเป็นกระแสไฟฟ้าที่แปลงมาจากเสียงพูดเคลื่อนที่ไปตามสายลวดที่จำเลยต่อพ่วงเป็นตัวนำจากที่หนึ่งไปยังอีกที่หนึ่ง การที่จำเลยลักเอาสัญญาณโทรศัพท์จากสายโทรศัพท์ซึ่งอยู่ในความครอบครองของผู้เสียหายไปใช้เพื่อประโยชน์ของจำเลยโดยทุจริต จึงเป็นความผิดฐานลักทรัพย์

คำพิพากษาศาลฎีกาที่ 481/2549 จำเลยกับพวกร่วมกันแก้ไขตัดแปลงมิเตอร์ไฟฟ้าที่ติดตั้งในบ้านไม่ให้หมุน ทำให้ตัวเลขวัดการใช้กระแสไฟฟ้าชำรุดเสียหายไม่เคลื่อนที่ เพื่อให้ได้ใช้ไฟฟ้าโดยไม่เสียค่าไฟฟ้า เป็นความผิดฐานลักทรัพย์

จากแนวคำพิพากษาข้างต้น แม้ศาลฎีกาจะมีได้ให้เหตุผลและวินิจฉัยว่ากระแสไฟฟ้าคือทรัพย์ที่เป็นวัตถุที่มีรูปร่างอันเป็นวัตถุแห่งการกระทำในความผิดฐานลักทรัพย์ได้ก็ตาม แต่ศาลได้วินิจฉัยในส่วนของลักษณะของการกระทำว่ามีการเอาไปตามองค์ประกอบความผิดฐานลักทรัพย์แล้ว และแนววินิจฉัยดังกล่าวนี้ถูกนำมาเป็นบรรทัดฐานในการวินิจฉัยการกระทำที่มี

ลักษณะคล้ายเคียงกันอีกหลายคดี เช่น การลักลอบเอาสัญญาณโทรศัพท์จากตู้โทรศัพท์สาธารณะไปใช้เพื่อประโยชน์ส่วนตนหรือผู้อื่นเป็นความผิดฐานลักทรัพย์ได้เช่นเดียวกัน โดยศาลมองว่ากลไกหรือกระบวนการของสัญญาณโทรศัพท์มีลักษณะเช่นเดียวกับกระแสไฟฟ้า คือ การเริ่มต้นจากการแปลงเสียงพูดให้เป็นกระแสไฟฟ้า แล้วส่งกระแสไฟฟ้าไปตามสายไฟฟ้าไปยังคู่สนทนาแล้วจึงเปลี่ยนเป็นเสียงพูดอีกครั้งหนึ่ง สัญญาณโทรศัพท์จึงเป็นกระแสไฟฟ้าที่แปลงมาจากเสียงพูดเคลื่อนที่ไปตามสายโทรศัพท์จากที่หนึ่งไปยังอีกที่หนึ่ง อีกทั้งยังมีกรณีการใช้สายลวดพ่วงต่อสัญญาณจากศูนย์ชุมสายประจำภูมิภาคของการสื่อสารแห่งประเทศไทยเข้ากับสายโทรศัพท์ของผู้กระทำเพื่อโทรออกไปยังเครื่องรับปลายทางในต่างประเทศ ดังนั้นกรณีการลักลอบใช้สัญญาณโทรศัพท์นี้จึงเป็นความผิดฐานลักทรัพย์ตามแนวฎีกาที่เคยตัดสินไว้ นอกจากนี้ยังมีกรณีการแก้ไขตัดแปลงมิเตอร์ไฟฟ้าที่ติดตั้งในบ้านไม่ให้หมุน ทำให้สามารถใช้ไฟฟ้าได้โดยตัวเลขวัดการใช้กระแสไฟฟ้าไม่เคลื่อนที่ (เป็นการกระทำกับมิเตอร์ไฟฟ้า) เพื่อให้ใช้ไฟฟ้าโดยไม่เสียค่าไฟฟ้าตามจริง สำหรับกรณีนี้จะเห็นได้ว่าศาลฎีกาได้พิจารณาว่าแม้จะไม่มี การเอาไปที่มีลักษณะเป็นการต่อสายไฟจากจุดหนึ่งไปยังอีกจุดหนึ่งก็ตาม แต่หากวัตถุประสงค์แห่งการกระทำ (กระแสไฟฟ้า) สามารถถูกบังคับทิศทาง การเคลื่อนที่ได้หรือถูกควบคุมปริมาณได้ จากบุคคลอื่นการกระทำนั้นก็ถือเป็นการเอาไปตามความหมายของความผิดฐานลักทรัพย์แล้ว ดังนั้นเมื่อกระแสไฟฟ้าส่วนที่ไหลผ่านไปตามสายลวดเส้นใด ย่อมเท่ากับว่าเป็นสิ่งที่สามารถถูกทำให้เปลี่ยนทิศทางหรือเปลี่ยนการถ่ายเทจากที่หนึ่งไปยังอีกที่หนึ่งได้ ไม่ว่าจะเป็นการกระทำต่อสายลวดโดยตรง เช่น การพ่วงสายต่อสายไฟ การพ่วงต่อสัญญาณโทรศัพท์ หรือวิธีการอื่น เช่น การแก้ไขมิเตอร์ไฟฟ้า อันมีผลให้กระแสไฟฟ้าตกมาอยู่ในความครอบครองของผู้อื่นโดยทุจริต ย่อมถือเป็นการเอาไปตามความผิดฐานลักทรัพย์แล้วทั้งสิ้น

(2) แนวคำวินิจฉัยที่ไม่เป็นความผิดฐานลักทรัพย์

คำพิพากษาฎีกาที่ 5354/2539 จำเลยนำโทรศัพท์มือถือมาปรับจูนและก๊อปปี้คลื่นสัญญาณโทรศัพท์ของผู้เสียหายแล้วใช้รับส่งวิทยุคมนาคมโดยไม่ได้รับอนุญาตเป็นเพียงการแย่งใช้คลื่นสัญญาณโทรศัพท์ของผู้เสียหายโดยไม่มีสิทธิ มิใช่เป็นการเอาทรัพย์สินของผู้อื่นไปโดยทุจริต ไม่เป็นความผิดฐานลักทรัพย์แม้จำเลยให้การรับสารภาพก็ต้องพิพากษายกฟ้อง

คำพิพากษาฎีกาที่ 8177/2543 การกระทำของจำเลยตามฟ้องที่ระบุว่า จำเลยร่วมกับพวกลักเอาคลื่นแม่เหล็กไฟฟ้าอันเป็นทรัพย์สินของผู้เสียหายที่ผลิตขึ้นเพื่อใช้กับวิทยุคมนาคม โดยจำเลยกับพวกนำเครื่องโทรศัพท์เคลื่อนที่ที่ปรับคลื่นสัญญาณและรหัสเลขหมายของโทรศัพท์ผู้อื่นมาใช้ติดต่อสื่อสารโทรออกหรือรับการเรียกเข้าผ่านสถานีและชุมสายโทรศัพท์ระบบเซลลูลาร์ของผู้เสียหายนั้น เป็นเพียงการรับส่งวิทยุคมนาคมหรือกล่าวอีกนัยหนึ่งว่า เป็นการแย่งใช้คลื่นสัญญาณโทรศัพท์โดยไม่มีสิทธิของตนเอง จึงมิใช่เป็นการเอาไปซึ่งทรัพย์สินของผู้อื่นโดยทุจริต การกระทำของ

จำเลยจึงไม่เป็นความผิดตามประมวลกฎหมายอาญามาตรา 335 (1) (7) วรรคสอง แต่จำเลยคงมีความผิดตามพระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498

จากแนวคำพิพากษาศาลฎีกาข้างต้นจะเห็นว่าการปรับจูนสัญญาณคลื่นโทรศัพท์เคลื่อนที่ด้วยการคัดลอกคลื่นสัญญาณโทรศัพท์ผู้อื่น เพื่อนำมาใช้รับส่งวิทยุคมนาคมโดยไม่ได้รับอนุญาต ศาลฎีกากลับวินิจฉัยว่า เป็นเพียงการแย่งใช้คลื่นสัญญาณโทรศัพท์โดยไม่มีสิทธิ เช่นเดียวกับการนำเครื่องโทรศัพท์เคลื่อนที่ไปปรับคลื่นสัญญาณและรหัสเลขหมายของโทรศัพท์เคลื่อนที่ผู้อื่นมาใช้ติดต่อสื่อสาร โทรออกหรือรับการเรียกเข้าผ่านสถานีชุมสายโทรศัพท์ระบบเซลลูลาร์ ศาลฎีกาได้วินิจฉัยว่า เป็นการแย่งใช้คลื่นสัญญาณโทรศัพท์โดยไม่มีสิทธิ เนื่องจากคลื่นสัญญาณโทรศัพท์จับต้องไม่ได้ จึงไม่อาจมีพฤติการณ์การเคลื่อนที่หรือถูกบังคับให้เปลี่ยนทิศทางของคลื่นสัญญาณโทรศัพท์ซึ่งเป็นวัตถุแห่งการกระทำได้ กรณีจึงขาดองค์ประกอบการเอาไปโดยทุจริตในความผิดฐานลักทรัพย์ ตามประมวลกฎหมายอาญา อย่างไรก็ตามการกระทำในลักษณะดังกล่าวก็ยังคงมีความผิดตามพระราชบัญญัติวิทยุคมนาคม พ.ศ. 2498

ผู้เขียนจึงขอแนะนำคำวินิจฉัยตามคำพิพากษาของศาลฎีกาดังกล่าวมาวิเคราะห์เปรียบเทียบกับประเด็นการนำพลังงานคอมพิวเตอร์ของผู้อื่นไปใช้โดยมิชอบว่า กรณีดังกล่าวนี้จะเป็นความผิดฐานลักทรัพย์ด้วยหรือไม่ ดังนี้

สาระสำคัญของคำวินิจฉัยตามแนวคำพิพากษาของศาลฎีกาทั้งสองแนว ศาลฎีกาวินิจฉัยโดยหยิบยกองค์ประกอบความผิดในส่วนของวัตถุแห่งการกระทำว่าเป็นทรัพย์หรือทรัพย์สินที่อาจถือเอาได้หรือไม่ หากวัตถุแห่งการกระทำสามารถถือเอาได้ย่อมเป็นสิ่งที่สามารถถูกลักได้เช่นกัน ส่วนข้อเท็จจริงที่แสดงให้เห็นว่าพลังงานไฟฟ้าเป็นทรัพย์หรือทรัพย์สินที่อาจถือเอาได้หรือไม่นั้นก็พิจารณาจากข้อเท็จจริงที่ว่า การนำพลังงานไฟฟ้าของผู้อื่นไปใช้โดยวิธีการเชื่อมต่อสาย (Bypass) เพื่อเคลื่อนพลังงานไฟฟ้าออกจากที่หนึ่งไปยังอีกที่หนึ่ง แสดงให้เห็นว่าพลังงานไฟฟ้าก็เป็นวัตถุที่ถือเอาและเข้าครอบครองได้ ซึ่งสอดคล้องกับแนวคำพิพากษาของศาลฎีกากลุ่มแรกที่วินิจฉัยว่าการลักกระแสไฟฟ้าเป็นความผิดฐานลักทรัพย์ ไม่ว่าจะเป็นการต่อสายไฟฟ้าของการไฟฟ้าแห่งประเทศไทยเข้าไปใช้ในบ้านโดยไม่ผ่านมิเตอร์ไฟฟ้า หรือการต่อสายสัญญาณโทรศัพท์จากตู้โทรศัพท์แห่งประเทศไทยเพื่อใช้โทรออกโดยไม่เสียค่าใช้จ่าย การกระทำดังกล่าวล้วนแต่เป็นใช้กระแสไฟฟ้าของผู้อื่นโดยมิสายเชื่อมต่อทั้งสิ้น นอกจากนี้การใช้สายเชื่อมต่อยังแสดงให้เห็นว่าวัตถุแห่งการกระทำที่ทำการลักนั้นได้มีการเคลื่อนที่ออกจากจุดเดิมที่เจ้าของครอบครองอยู่ไปยังอีกจุดหนึ่งด้วย ดังนั้นจึงเป็นการเอาไปตามองค์ประกอบความผิดในส่วนของลักษณะการกระทำว่า การกระทำความผิดเกิดขึ้นแล้วได้อย่างชัดเจนยิ่งขึ้น ในขณะที่แนวคำพิพากษาศาลฎีกากรณีการปรับจูนคลื่นสัญญาณโทรศัพท์เคลื่อนที่วินิจฉัยว่า ไม่เป็นความผิดฐานลักทรัพย์ ศาลพิจารณาโดยใช้หลักเกณฑ์เดียวกันคือ หากวัตถุแห่งการกระทำเป็นสิ่งที่ล่องลอยอยู่ในอากาศ เช่น สัญญาณโทรศัพท์เคลื่อนที่ สัญญาณคลื่นวิทยุ ที่ไม่มี

ลักษณะที่แสดงให้เห็นว่าคลื่นสัญญาณโทรศัพท์เคลื่อนที่หรือสัญญาณคลื่นวิทยุได้เปลี่ยนทิศทางหรือเคลื่อนที่จากที่หนึ่งไปยังอีกที่หนึ่งเพื่อนำไปใช้อย่างไร กรณีจึงไม่มีลักษณะการกระทำเอาไปซึ่งทรัพย์สินที่มีการหวงกันหรืออาจถือเอาได้ เป็นผลให้ไม่สามารถรับรู้ได้ว่าวัตถุแห่งการกระทำที่จะเอาไปนั้นคือวัตถุใดและมีการเคลื่อนที่จากการครอบครองเมื่อใด การกระทำจึงขาดองค์ประกอบความผิดฐานลักทรัพย์ทั้งในส่วนของลักษณะการกระทำ (การเอาไป) และวัตถุแห่งการกระทำ (ทรัพย์สินของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วย) อย่างไรก็ตามการกระทำดังกล่าวก็อาจมีความผิดตามกฎหมายอื่นได้

สำหรับความผิดฐานใช้พลังงานคอมพิวเตอร์ของผู้อื่นนั้น หมายถึง การนำทรัพย์สินคอมพิวเตอร์ของผู้อื่นในการนำมาเพิ่มกำลังการตรวจสอบธุรกรรมเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล กล่าวคือ เป็นการนำพลังงานคอมพิวเตอร์หรือกระแสไฟฟ้าของผู้อื่นโดยทุจริตนั่นเอง เพียงแต่ผู้กระทำความผิดมิได้ใช้วิธีการเชื่อมต่อสาย (Bypass) เพื่อเคลื่อนพลังงานคอมพิวเตอร์หรือกระแสไฟฟ้าออกจากที่หนึ่งไปยังอีกที่หนึ่งและแย่งพลังงานคอมพิวเตอร์จากผู้เสียหายไปใช้หรือไปอยู่ที่คอมพิวเตอร์ของผู้กระทำ แต่ผู้กระทำความผิดในลักษณะนี้กลับใช้วิธีการกระทำในระบบออนไลน์ซึ่งมีลักษณะไร้สายด้วยการฝังมัลแวร์ไว้กับโปรแกรมต่าง ๆ หรืออาจฝังไว้กับอีเมลที่ส่งไปยังผู้เสียหาย เมื่อผู้เสียหายเปิดโปรแกรมหรืออีเมลดังกล่าว มัลแวร์ที่ฝังไว้จะทำงานโดยอัตโนมัติออกคำสั่งให้เครื่องคอมพิวเตอร์ของผู้เสียหายทำการเปิดโปรแกรมสำหรับการตรวจสอบธุรกรรมเกี่ยวกับสกุลเงินดิจิทัล และเริ่มกระบวนการตรวจสอบธุรกรรมเกี่ยวกับสกุลเงินดิจิทัล โดยหากตรวจสอบธุรกรรมสำเร็จจะได้สกุลเงินดิจิทัลตอบแทนเข้าบัญชีสกุลเงินดิจิทัลของผู้กระทำความผิด ด้วยวิธีดังกล่าวนี้ผู้กระทำความผิดจึงมิได้มีการต่อสายใดเพื่อทำการแย่งพลังงานคอมพิวเตอร์ของผู้เสียหายหรือทำให้พลังงานคอมพิวเตอร์เปลี่ยนทิศทางไปอยู่ที่คอมพิวเตอร์ของผู้กระทำแต่อย่างใด ดังนั้นหากพิจารณาตามแนวคำพิพากษาฎีกาในเรื่องการลักกระแสไฟฟ้าหรือปรับจนสัญญาณคลื่นโทรศัพท์เคลื่อนที่ การใช้พลังงานคอมพิวเตอร์ของผู้อื่นในลักษณะนี้ก็จะไม่เป็นความผิดฐานลักทรัพย์ เนื่องจากไม่มีลักษณะของการกระทำใดที่เป็นการถ่ายโอนพลังงานคอมพิวเตอร์ออกไปยังผู้กระทำผิดหรือผู้อื่น อย่างไรก็ตามแม้พลังงานคอมพิวเตอร์หรือกระแสไฟฟ้าที่ถูกแย่งใช้นั้น ไม่ได้ถูกแย่งใช้พลังงานคอมพิวเตอร์หรือกระแสไฟฟ้าทั้งหมด โดยยังคงมีพลังงานคอมพิวเตอร์หรือกระแสไฟฟ้าบางส่วนที่ยังทำหน้าที่เป็นพลังงานให้แก่คอมพิวเตอร์ของผู้เสียหายอยู่ แต่กระบวนการตรวจสอบธุรกรรมเกี่ยวกับสกุลเงินดิจิทัลจำเป็นต้องใช้พลังงานคอมพิวเตอร์หรือกระแสไฟฟ้าจำนวนมากในการทำงาน ดังนั้นการนำพลังงานคอมพิวเตอร์หรือกระแสไฟฟ้าของผู้อื่นไปใช้ในการตรวจสอบธุรกรรมเกี่ยวกับสกุลเงินดิจิทัลจึงส่งผลให้ประสิทธิภาพในการทำงานของเครื่องคอมพิวเตอร์ผู้เสียหายลดน้อยลง อีกทั้งผู้เสียหายยังคงต้องเสียค่าไฟฟ้าเพิ่มมากขึ้น การกระทำในลักษณะนี้แม้จะไม่ได้เป็นการเอาไปจากการครอบครองอันมีลักษณะเป็นการตัดกรรมสิทธิ์จากเจ้าของเดิมตามความหมายของความผิดฐานลักทรัพย์ก็ตาม แต่ก็ถือ

ได้ว่าการกระทำในลักษณะนี้เป็นการล่วงละเมิดต่อผู้อื่น และเป็นการไม่สมควรที่จะให้มีการกระทำในลักษณะนี้เกิดขึ้นโดยไม่มีคามผิดตามกฎหมายอาญา และปัจจุบันก็ยังไม่มีความหมายอาญาใดที่ครอบคลุมถึงการกระทำในลักษณะดังกล่าวว่าเป็นความผิด จึงยังเป็นช่องว่างทางกฎหมายที่สมควรมีบทบัญญัติที่ครอบคลุมถึงความผิดในลักษณะนี้ให้ชัดเจน

นอกจากนี้ในการบัญญัติความผิดเกี่ยวกับสกุลเงินดิจิทัลขึ้นมาใหม่ต้องพิจารณาถึงความจำเป็นในการกำหนดความผิดอาญาที่จะมีได้ก็ต่อเมื่อเป็น “ความผิดร้ายแรง”<sup>352</sup> ที่มีรากฐานมาจากการกระทำที่ก่อให้เกิดผลเสียหายกับสังคม และเป็นการกระทำที่เป็นอันตรายอันส่งผลกระทบต่อประโยชน์ที่มีความใกล้ชิดกับ “ระดับมาตรฐานการดำรงชีวิตของปัจเจกชน (The Degree to which the Living Standard)” แล้ว การกระทำนั้นย่อมมีความร้ายแรงอันสมควรจะถูกกำหนดเป็นความผิดอาญา<sup>353</sup> และหากจะบัญญัติเป็นกฎหมายอาญาในอนาคตจะต้องเป็นการกระทำที่กระทบต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชนอย่างร้ายแรงและมีผลกระทบต่อส่วนรวม ซึ่งที่ไม่สามารถใช้มาตรการอื่นเพื่อบังคับใช้กฎหมายอย่างได้ผลหรือมีประสิทธิภาพเพียงพอ<sup>354</sup> ดังนั้นสำหรับความผิดเกี่ยวกับสกุลเงินดิจิทัลที่ยังเป็นช่องว่างทางกฎหมายทั้งกรณีการขโมยสกุลเงินดิจิทัล และกรณีการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัลนั้นมีลักษณะเป็นการกระทำที่ร้ายแรงด้วยวิธีการแสวงหาผลประโยชน์โดยมิชอบและเป็นการเอาเปรียบผู้อื่น ซึ่งถือเป็นการละเมิดต่อกติกาการอยู่ร่วมกันในสังคม จึงสมควรจะใช้มาตรการทางอาญาในการกำหนดบทบัญญัติเป็นการเฉพาะไว้ในประมวลกฎหมายอาญาการเช่นเดียวกับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ความผิดเกี่ยวกับหนังสือเดินทาง และความผิดเกี่ยวกับศพ ซึ่งเหตุผลในการแก้ไขเพิ่มเติม คือ ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์เป็นความผิดที่มีลักษณะเป็นการกระทำซ้ำหรือแอบดูรหัสข้อมูลผู้อื่นและนำไปใช้โดยไม่กระทบกับกรรมสิทธิ์และการแย่งการครอบครองของเจ้าของข้อมูล อีกทั้งมีคำพิพากษากฎีกาวินิจฉัยว่า ข้อมูลไม่ใช่วัตถุที่มีรูปร่าง จึงไม่ใช่ทรัพย์สินตามมาตรา 137 ประมวลกฎหมายแพ่งและพาณิชย์ เมื่อไม่ใช่ทรัพย์สินก็ไม่อาจเป็นวัตถุแห่งกระทำในความผิดฐานลักทรัพย์ได้<sup>355</sup> ทำให้ความผิดฐานลักทรัพย์ที่มีอยู่ไม่อาจครอบคลุมกรณีนี้ได้ ความผิดเกี่ยวกับหนังสือเดินทางเป็นกรณีที่มีความผิดฐานปลอมหนังสือเดินทางของไทยเป็นซึ่งเอกสารราชการมีโทษหนักกว่าการปลอมเอกสารทั่วไป

<sup>352</sup> มาตรา 77 วรรคท้าย ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

<sup>353</sup> Andrew Ashworth, *Principles of Criminal Law*, 5<sup>th</sup> ed. (Oxford: Oxford University Press, 2006), p. 25, 37.

<sup>354</sup> คำแนะนำของคณะกรรมการพัฒนากฎหมาย เรื่อง การกำหนดโทษอาญาในกฎหมาย, *ราชกิจจานุเบกษา* 136, 132 (27 พฤศจิกายน 2562): หน้า 18.

<sup>355</sup> คำพิพากษากฎีกา 5161/2547

อาจส่งผลให้มีการกระทำความผิดฐานปลอมหนังสือเดินทางต่างประเทศในประเทศไทยเป็นจำนวนมาก<sup>356</sup> และความผิดเกี่ยวกับศพ ซึ่งเดิมกฎหมายมองว่ากระทำต่อศพนั้นเป็นการกระทำต่อสิ่งที่ไม่มีความผิดตามกฎหมายอาญาเพราะ ขาดองค์ประกอบความผิดในส่วนของวัตถุหรือกรรมของการกระทำ แต่เมื่อคำนึงถึงการกระทำอันมิบังควรต่อศพซึ่งถือเป็นการล่วงละเมิดต่อบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ของผู้ตายและญาติของผู้ตายจึงเป็นการกระทำที่ขัดต่อความสงบเรียบร้อย ศีลธรรมอันดีของประชาชน<sup>357</sup> ศักดิ์ศรีของเป็นมนุษย์<sup>358</sup> และสิทธิของบุคคลในครอบครัว เกียรติยศ ชื่อเสียง ตลอดจนความเป็นส่วนตัว<sup>359</sup> จึงมีความจำเป็นต้องมีบทบัญญัติดังกล่าวขึ้นมาใหม่

จากที่ได้กล่าวถึงแนวคิดในการกำหนดความผิดอาญาของกฎหมายทั้งสามลักษณะนี้จะเห็นได้ว่ามีที่มาจากกรกระทำที่ก่อให้เกิดความเสียหายต่อสังคมเป็นวงกว้างอันขัดต่อความสงบเรียบร้อยของสังคม ซึ่งเป็นการกระทำที่มีความน่าตำหนิจากสังคม ซึ่งยังไม่มีกฎหมายกำหนดให้การกระทำนั้นเป็นความผิด เช่นเดียวกับการขโมยสกุลเงินดิจิทัล และการใช้พลังงานคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัลซึ่งมีข้อจำกัดในเรื่องขององค์ประกอบความผิดซึ่งฐานความผิดที่มีอยู่ไม่ว่าจะเป็นความผิดเกี่ยวกับทรัพย์สินหรือความผิดเกี่ยวกับเอกสารไม่สามารถนำมาใช้กับสกุลเงินดิจิทัลซึ่งเป็นวัตถุที่ไม่มีรูปร่างที่มีลักษณะเฉพาะได้ ดังนั้นเพื่อเป็นการแก้ไขช่องว่างทางกฎหมายนี้ จึงควรกำหนดสถานะที่ชัดเจนให้เหมาะสมกับสภาพและลักษณะการกระทำของสกุลเงินดิจิทัล โดยการกำหนดนิยามสกุลเงินดิจิทัลไว้ในมาตรา 1 ในประมวลกฎหมายอาญาเช่นเดียวกับ “บัตรอิเล็กทรอนิกส์” และ “หนังสือเดินทาง” และกำหนดบทบัญญัติขึ้นมาใหม่ให้ครอบคลุมกับกรณีเพื่อเป็นการอุดช่องว่างทางกฎหมายที่จะก่อให้เกิดความเสียหายแก่ประชาชนได้ นอกจากนี้ในส่วนการกำหนดโทษสำหรับความผิดกรณีขโมยสกุลเงินดิจิทัลและการใช้พลังงานคอมพิวเตอร์ของผู้อื่นโดยทุจริตนั้น จะเป็นการกำหนดความผิดขึ้นใหม่โดยให้การขโมยและการใช้ประโยชน์จากวัตถุที่ไม่มีรูปร่างผู้อื่นเป็นความผิดอาญา ดังนั้นจึงต้องพิจารณาลักษณะของทรัพย์สินที่นำมาใช้ในการกำหนดโทษ จากการศึกษาพบว่ากรกำหนดอัตราโทษความผิดฐานลักทรัพย์มิได้ใช้เกณฑ์รูปร่างของวัตถุ แต่กฎหมายคำนึงถึงความสำคัญ

<sup>356</sup> พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 18) พ.ศ. 2550, **ราชกิจจานุเบกษา** 124, 42 ก (15 สิงหาคม 2550), หน้า 1.

<sup>357</sup> อริยพร โพธิ์ใส, “การกระทำผิดต่อศพ: ปัญหาที่รอการแก้ไข,” **จุลนิติ** (มกราคม-กุมภาพันธ์ 2558): 176.

<sup>358</sup> มาตรา 4 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

<sup>359</sup> มาตรา 35 ของรัฐธรรมนูญแห่งราชอาณาจักรไทย พุทธศักราช 2560

ของลักษณะทรัพย์สินที่มีจำเป็นต่ออาชีพการกรรม<sup>360</sup> ได้แก่ ทรัพย์สินที่เป็นผลิตภัณฑ์ พืชพันธุ์ สัตว์หรือเครื่องมืออันมีไว้สำหรับประกอบกิจการหรือได้มาจากกิจการ<sup>361</sup> และทรัพย์สินที่เป็นโค กระบือ เครื่องกลหรือเครื่องจักรที่มีอาชีพการกรรมไว้หรือประกอบกิจการ<sup>362</sup> (เหตุผลกรจ) ดังนั้นการกระทำต่อทรัพย์สินดังกล่าวนี้ผู้กระทำจะต้องรับโทษหนักกว่าการลักทรัพย์อื่น ๆ<sup>363</sup> จะเห็นว่าแนวคิดของกฎหมายไทยไม่ได้มีการนำลักษณะของวัตถุที่มีรูปร่างกับวัตถุที่ไม่มีรูปร่างมาเป็นข้อพิจารณาในการกำหนดอัตราโทษ ดังนั้นผู้เขียนจึงนำแนวคิดของกฎหมายดังกล่าวมากำหนดอัตราโทษสำหรับความผิดกรณีขโมยสกุลเงินดิจิทัลและการใช้ทรัพย์สินคอมพิวเตอร์ของผู้อื่นโดยทุจริต โดยให้มีอัตราโทษเช่นเดียวกับการลักทรัพย์ทั่วไป และกรณีการขโมยสกุลเงินดิจิทัลที่มีการใช้กำลังประทุษร้ายให้มีอัตราโทษเช่นเดียวกับการชิงทรัพย์หรือปล้นทรัพย์ แล้วแต่กรณี และด้วยเหตุที่ความผิดเกี่ยวกับสกุลเงินดิจิทัลเป็นความผิดที่ไร้พรมแดนจึงควรนำความผิดนี้มาบัญญัติเพิ่มเติมใน มาตรา 8 เพื่อคุ้มครองประเทศไทยหรือคนไทยอาจตกเป็นผู้เสียหายได้จากการกระทำที่มีลักษณะข้ามชาติได้ โดยกำหนดให้ผู้กระทำผิดเกี่ยวกับสกุลเงินดิจิทัลที่กระทำนอกราชอาณาจักรต้องรับโทษในราชอาณาจักร

#### 4.3 ปัญหาความร่วมมือทางอาญาระหว่างประเทศเกี่ยวกับการกระทำความผิดอาญาที่เกี่ยวข้องกับสกุลเงินดิจิทัล

คุณสมบัติเฉพาะที่โดดเด่นของสกุลเงินดิจิทัล คือ การทำธุรกรรมการโอนมูลค่าได้โดยตรงไปยังผู้รับโดยไม่ผ่านการกำกับดูแลของตัวกลาง และการรักษาความเป็นส่วนตัวของผู้ใช้งานโดยไม่ต้องระบุตัวตน และสามารถทำธุรกรรมในระบบออนไลน์โดยอาศัยเครือข่ายอินเทอร์เน็ตสามารถเชื่อมโยงคอมพิวเตอร์ต่าง ๆ จากทั่วทุกมุมโลกเข้าไว้ด้วยกัน ความเชื่อมโยงทางเทคโนโลยีนี้จึงเป็นลักษณะของธุรกรรมที่ไร้พรมแดน ด้วยเหตุนี้สกุลเงินดิจิทัลจึงเอื้อต่อการกระทำผิด และแพร่กระจายไปอย่างรวดเร็วทั้งยังสร้างมูลค่าความเสียหายมหาศาล ความเสียหายไม่ได้จำกัดอยู่ในประเทศใดประเทศหนึ่งเท่านั้น การกระทำดังกล่าวจึงเป็นปัญหาอาชญากรรมที่มีมิติข้ามชาติ ส่งผลให้การปราบปรามการกระทำความผิดทำได้ยาก เนื่องจากต้องอาศัยความร่วมมือระหว่างรัฐในการประสานงานขอความ

<sup>360</sup> คณิต ฌ นคร, กฎหมายอาญา ภาคความผิด, พิมพ์ครั้งที่ 9 (กรุงเทพมหานคร: วิญญูชน, 2549), หน้า 322.

<sup>361</sup> มาตรา 335 (12) แห่งประมวลกฎหมายอาญา

<sup>362</sup> มาตรา 335 วรรค 3 แห่งประมวลกฎหมายอาญา

<sup>363</sup> มาตรา 334 แห่งประมวลกฎหมายอาญา

ร่วมมือไปยังหน่วยงานต่างประเทศเพื่อรวบรวมพยานหลักฐานและติดตามผู้กระทำความผิดมาลงโทษ ซึ่งแต่ละประเทศมีข้อจำกัดในเรื่องของกฎหมายภายในของแต่ละประเทศ รวมถึงความแตกต่างของ กฎเกณฑ์ภายในในการควบคุมและกำกับธุรกรรมสกุลเงินดิจิทัล กล่าวคือ บางประเทศไม่ให้การ ยอมรับสกุลเงินดิจิทัล และถือว่าธุรกรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัลเป็นสิ่งที่ผิดกฎหมาย เช่น ประเทศจีน บางประเทศยอมรับเงินสกุลเงินดิจิทัลเป็นเงินตรา เช่น สาธารณรัฐเอลซัลวาดอร์และบาง ประเทศกำกับดูแลอย่างเคร่งครัด เช่น ประเทศไทย ดังนั้นอาชญากรรมสกุลเงินดิจิทัลจึงกลายเป็น โอกาสให้ผู้กระทำความผิดใช้ความแตกต่างนี้เป็นช่องว่างทางกฎหมายในการเลือกสถานที่หรือประเทศที่จะ กระทำความผิดหรือหลบหนีได้ นอกจากนี้แล้วแต่ละประเทศยังมีความแตกต่างในเรื่องของขั้นตอนและ วิธีการปฏิบัติตามกระบวนการยุติธรรมในการพิสูจน์ข้อเท็จจริง ซึ่งต้องอาศัยเจ้าหน้าที่ที่มีความรู้ความ เชี่ยวชาญด้านพยานหลักฐานดิจิทัลร่วมด้วย ปัญหาต่าง ๆ เหล่านี้ส่งผลให้การปราบปราม อาชญากรรมที่เกี่ยวข้องกับสกุลเงินดิจิทัลไม่สามารถกระทำได้อย่างทันที่

ปัจจุบันทั่วโลกได้ตระหนักถึงแนวทางการปราบปรามปัญหาดังกล่าวด้วยการนำกลไกความ ร่วมมือทางอาญาระหว่างประเทศมาใช้ให้เกิดประสิทธิภาพ โดยมีทั้งความร่วมมือระหว่างประเทศ รูปแบบอนุสัญญาและความร่วมมือระหว่างประเทศรูปแบบองค์กร จากการศึกษาพบว่ายังมีปัญหา บางประการ ดังนี้

1) ความร่วมมือระหว่างประเทศรูปแบบอนุสัญญา ปัจจุบันมีอนุสัญญาว่าด้วย อาชญากรรมคอมพิวเตอร์ (Convention on Cybercrime) อนุสัญญาสหประชาชาติว่าด้วยการ ต่อต้านการสนับสนุนทางการเงินแก่การก่อการร้าย ค.ศ. 1999 (International Convention for the Suppression of the Financing of Terrorism, 1999) ทั้งสองอนุสัญญามีมาตรการความ ร่วมมือในประเด็นการให้ความช่วยเหลือทางอาญาซึ่งกันและกัน การส่งผู้ร้ายข้ามแดน การ แลกเปลี่ยนข้อมูลข่าวสารในระหว่างรัฐภาคี โดยมีข้อกำหนดในเรื่องการประสานขอความร่วมมือ ลักษณะผ่อนปรนข้อจำกัดอำนาจอธิปไตยเท่าที่จะเป็นไปได้ และมีข้อกำหนดที่ยืดหยุ่นหลักความผิด ของทั้งสองประเทศในการส่งผู้ร้ายข้ามแดน เพื่อเป็นการขจัดอุปสรรคในเรื่องความแตกต่างของ กฎหมายภายในแต่ละประเทศ โดยเฉพาะอนุสัญญาว่าด้วยอาชญากรรมคอมพิวเตอร์ได้มีการจัดตั้ง หน่วยงานกลางในการประสานขอความร่วมมือระหว่างประเทศที่สามารถติดต่อกันได้โดยตรง รวมถึง สามารถประสานงานผ่านองค์การตำรวจสากลได้เช่นกัน อย่างไรก็ตามแม้แนวทางการร่วมมือ ระหว่างประเทศดังกล่าวจะมีความหลากหลายและมีความเป็นรูปธรรมแต่ทั้งสองอนุสัญญามีได้เป็น อนุสัญญาที่ก่อตั้งโดยมีวัตถุประสงค์ในการป้องกันหรือปราบปรามความผิดอาญาเกี่ยวกับสกุลเงินไว้ โดยเฉพาะ แต่มีเพียงบางส่วนที่เกี่ยวข้องพอนำมาปรับใช้กับอาชญากรรมที่มีลักษณะข้ามชาติได้ อีกทั้งมาตรการต่าง ๆ ที่มีขึ้นนั้นเพื่อให้ความช่วยเหลือในการค้นหาพยานหลักฐาน หรือการส่งผู้ตัว กระทำความผิดมาดำเนินคดีต่างรัฐในคดีทั่วไปภายใต้หลักเกณฑ์ของกฎหมายภายในแต่ละประเทศ

ซึ่งความแตกต่างของกฎหมายภายในก็ยังคงเป็นอุปสรรคที่สำคัญอย่างหลีกเลี่ยงไม่ได้ แม้ว่าปัจจุบันจะมีแนวปฏิบัติมาตรฐานในการขอความร่วมมือทางคดีอาญาระหว่างประเทศอยู่แล้ว แต่ขั้นตอนการประสานงานต่าง ๆ มีลักษณะที่เป็นทางการเกี่ยวข้องกับหลายหน่วยงาน จึงค่อนข้างใช้เวลานาน ปัญหาเหล่านี้อาจทำให้การอำนวยความสะดวกไม่ทันต่อสถานการณ์ที่เปลี่ยนแปลงไป ดังนั้นการสร้างกรอบความร่วมมือเฉพาะในการปราบปรามการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลจะเป็นเครื่องมือที่สำคัญในการเสริมประสิทธิภาพการประสานงานระหว่างรัฐได้เท่าทันต่อการเปลี่ยนแปลงทางเทคโนโลยี<sup>364</sup>

2) ความร่วมมือระหว่างประเทศรูปแบบองค์กร เป็นแนวทางความร่วมมือที่มีลักษณะไม่เป็นทางการ จึงสามารถลดขั้นตอนการประสานงานระหว่างรัฐได้และการจัดตั้งองค์กรมีวัตถุประสงค์ในการปราบปรามการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลไว้โดยเฉพาะมากกว่าความร่วมมือระหว่างประเทศรูปแบบอนุสัญญา ปัจจุบันมีองค์กรระหว่างประเทศที่เกี่ยวข้องกับการปราบปรามสกุลเงินดิจิทัล ได้แก่ United Nations Office on Drugs and Crime (UNODC) Financial Action Task Force (FATF) และ Interpol ซึ่งทั้งสององค์กรนี้ได้ให้ความสำคัญกับการถ่ายทอดความรู้ การพัฒนาเทคนิคในการป้องกันและสอบสวน ในรูปแบบของการจัดอบรม แลกเปลี่ยนทักษะที่จำเป็นให้แก่บุคลากรที่เกี่ยวข้องที่เน้นเนื้อหาในเชิงปฏิบัติ การพัฒนาความรู้เชิงเทคนิคในการสืบสวนหาพยานหลักฐานดิจิทัลและการสอบสวนทางการเงินซึ่งเป็นสิ่งสำคัญในการปราบปรามองค์กรอาชญากรรมและจำเป็นต้องทำงานร่วมกันระหว่างผู้ตรวจสอบทางการเงินและผู้เชี่ยวชาญด้านคอมพิวเตอร์ ทั้งนี้การพัฒนาความรู้ในด้านนี้จำเป็นต้องศักยภาพในการเข้าถึงเทคโนโลยีที่ตอบสนองกับสภาพการณ์ที่เปลี่ยนแปลงไปอย่างรวดเร็ว เช่น การพัฒนาเครื่องมือทางเทคโนโลยีที่ใช้ในการวิเคราะห์สำนวนธุรกรรมที่ผิดปกติ การจัดทำ Software ที่สามารถใช้ในการวิเคราะห์เหตุการณ์ในบล็อกเชนที่อาจเกี่ยวข้องกับอาชญากรรมได้ ซึ่งเครื่องมือต่าง ๆ เหล่านี้อาจเป็นการสร้างภาระให้แก่ประเทศที่ด้อยพัฒนาในด้านการเงินและเทคโนโลยีที่ไม่สามารถบรรลุวัตถุประสงค์ของความร่วมมือได้อย่างแท้จริง

ดังนั้นเพื่อให้การปราบปรามอาชญากรรมที่เกี่ยวกับสกุลเงินดิจิทัลเป็นไปอย่างมีประสิทธิภาพจึงจำเป็นต้องสร้างความร่วมมือระหว่างประเทศในการส่งเสริมความรู้ ความเชี่ยวชาญเทคโนโลยีทางการเงินให้แก่เจ้าหน้าที่ที่เกี่ยวข้องโดยการส่งต่อข้อมูลและแบ่งปันเทคโนโลยีที่จำเป็นอย่างทั่วถึงไปยังประเทศที่ด้อยพัฒนา เพราะความเหลื่อมล้ำทางด้านเทคโนโลยีที่มากเกินไปอาจกลายเป็นอุปสรรคต่อการแก้ไขปัญหาการกระทำความผิดข้ามพรมแดนได้ ประกอบกับแต่ละประเทศควรมีกฎหมายสาร

<sup>364</sup> Petra Kodysova and Miroslav Kastyl, *Combating Cryptomarkets: Cross-Border Cooperation and Investigation* (N.P.: n.p., 2018), p. 17.

บัญญัติที่มีความใกล้เคียงกัน ตลอดจนมีการประชาสัมพันธ์ให้ประชาชนตระหนักถึงวิธีใช้อย่างปลอดภัย วิธีป้องกันอันตรายจากความเสี่ยงที่จะเกิดความเสียหาย และรูปแบบการการกระทำผิดที่เกี่ยวข้อง สิ่งต่าง ๆ เหล่านี้จะเป็นเครื่องมือที่สำคัญในการเสริมประสิทธิภาพปราบปรามการกระทำ ความผิดเกี่ยวกับสกุลเงินดิจิทัลได้อย่างทันที่



## บทที่ 5

### บทสรุปและข้อเสนอแนะ

#### 5.1 บทสรุป

วิจัยนี้มีวัตถุประสงค์มีวัตถุประสงค์หลักคือ ศึกษาและวิเคราะห์สถานะทางกฎหมายของสกุลเงินดิจิทัลและรูปแบบการกระทำความผิดที่ยังเป็นช่องว่าง ตลอดจนปัญหาข้อจำกัดของกฎหมายไทย และความจำเป็นที่ควรกำหนดให้การกระทำรูปแบบที่ยังเป็นช่องว่างนั้นเป็นความผิดอาญา เพื่อนำมาสู่การแสวงหามาตรการที่เหมาะสมจะนำมาใช้ในการควบคุมการกระทำความผิดที่เป็นกฎหมายสารบัญญัติและได้กำหนดองค์ประกอบสำหรับความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลไว้อย่างชัดเจน ตามหลักเกณฑ์ของกฎหมายอาญา ซึ่งจะส่งผลให้ผู้กระทำไม่สามารถอ้างความไม่มีกฎหมายมาเป็นเหตุให้การกระทำนั้นไม่เป็นความผิดและไม่ต้องรับโทษได้ และยังก่อให้เกิดความเป็นเอกภาพในการวินิจฉัยความรับผิดซึ่งสอดคล้องกับหลักเกณฑ์ความชัดเจนแน่นอนของกฎหมายอาญาซึ่งจะส่งผลให้การบังคับใช้กฎหมายมีประสิทธิภาพต่อการป้องกันและปราบปรามอาชญากรรมสกุลเงินดิจิทัล การศึกษาวิจัยนี้ผู้เขียนได้ทำการวิเคราะห์และสังเคราะห์ข้อมูลตามวิธีวิทยาการวิจัยเพื่อให้ได้ข้อมูลที่ถูกต้อง เหมาะสมในการกำหนดมาตรการควบคุมการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัลที่เหมาะสม และได้ดำเนินการจนบรรลุเป้าหมายตามวัตถุประสงค์ดังกล่าว โดยสรุปผลได้ดังนี้

การศึกษาวิจัยได้ศึกษาสถานะที่เกี่ยวข้องกับสกุลเงินดิจิทัล โดยแต่ละสถานะจะมีความเกี่ยวข้องกับสกุลเงินดิจิทัลในแง่มุมที่แตกต่างกันออกไป ได้แก่ สถานะทรัพย์สิน สถานะเงินตรา สถานะข้อมูลคอมพิวเตอร์ และสถานะเอกสาร เพื่อแสดงให้เห็นว่าสกุลเงินดิจิทัลมีความใกล้เคียงและเกี่ยวข้องกับทุกสถานะที่ได้กล่าวมา :ซึ่งแต่ละสถานะมีข้อจำกัด ดังนี้

- 1) สถานะทรัพย์สิน ตามประมวลกฎหมายอาญา ลักษณะ 12 ความผิดเกี่ยวกับทรัพย์สิน กำหนดองค์ประกอบความผิดโดยมีคำว่าทรัพย์สินและทรัพย์สิน ปะปนกัน เนื่องจากสกุลเงินดิจิทัลเป็นวัตถุที่ไม่มีรูปร่าง ดังนั้นหากกำหนดให้สกุลเงินดิจิทัลมีสถานะเป็นทรัพย์สินแล้ว จะนำกฎหมายมาใช้ได้เฉพาะในส่วนที่มีองค์ประกอบเป็นทรัพย์สินเท่านั้น ได้แก่ ความผิดฐานกรรโชก ริดเอาทรัพย์สิน ฉ้อโกง ส่วนฐานความผิดที่มีองค์ประกอบความผิดเป็นทรัพย์สิน ได้แก่ ลักทรัพย์ ชิงทรัพย์

ปล้นทรัพย์ ยักยอกทรัพย์ ไม่อาจนำมาใช้ได้ ทั้งที่ฐานความผิดเหล่านี้เป็นความผิดที่เกิดขึ้นกับสกุลเงินดิจิทัลได้เช่นกัน

2) สถานะเงินตรา จากพระราชบัญญัติเงินตรา พ.ศ. 2501 ได้ให้ความหมายคำว่า เงินตรา หมายถึง เหรียญกษาปณ์และธนบัตรที่ได้รับอนุญาตให้ทำ จำหน่าย ใช้ จากรัฐมนตรี แต่สกุลเงินดิจิทัลนั้นถูกสร้างขึ้นในรูปแบบสมการดิจิทัลในระบบคอมพิวเตอร์จึงไม่ได้มีลักษณะเป็นเหรียญกษาปณ์หรือธนบัตรที่ได้รับอนุญาตให้ออกให้ใช้โดยรัฐบาลของประเทศใด จึงไม่มีสถานะทางกฎหมายเป็นเงินตรา อีกทั้งเมื่อพิจารณาถึงลักษณะความผิดที่เกี่ยวข้องกับเงินตราตามประมวลกฎหมายอาญา จะเห็นได้ว่าความผิดฐานปลอม การแปลง การทำให้น้ำหนักลดลง ต้องเป็นการกระทำต่อวัตถุที่มีรูปร่าง ดังนั้นกฎหมายที่ใช้กับสถานะเงินตราจึงไม่เหมาะสมจะนำมาใช้กับสกุลเงินดิจิทัล

3) สถานะข้อมูลคอมพิวเตอร์ แม้สกุลเงินดิจิทัลจะมีลักษณะที่อาจเป็นข้อมูลคอมพิวเตอร์ได้ตามความหมายของพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 และพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 ก็ตาม แต่เมื่อพิจารณาถึงฐานความผิดอาญาที่กำหนดไว้ในพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ฯ พบว่ายังมีความผิดบางฐานยังไม่เหมาะสมที่จะนำมาใช้กับความผิดเกี่ยวกับสกุลเงินดิจิทัลได้ เนื่องจากมีการกำหนดองค์ประกอบความผิดและมีลักษณะความผิดที่ต่างจากความผิดที่เกี่ยวข้องกับสกุลเงินดิจิทัลจึงไม่เหมาะสมที่จะนำมาปรับใช้ได้ เช่น ความผิดฐานทำให้เสียหาย ทำลาย แก้ไข เปลี่ยนแปลง ซึ่งข้อมูลคอมพิวเตอร์ของผู้อื่นโดยมิชอบ ความผิดฐานทำให้การทำงานของระบบคอมพิวเตอร์ของผู้อื่นถูกระงับ ชะลอ ชัดขวาง หรือรบกวนจนไม่สามารถทำงานได้ตามปกติ และความผิดฐานส่งข้อมูลคอมพิวเตอร์หรือจดหมายอิเล็กทรอนิกส์แก่บุคคลอื่น อันเป็นการรบกวนการใช้ระบบคอมพิวเตอร์ของบุคคลอื่นโดยปกติสุข

4) สถานะเอกสาร มีที่มาจากจากคำพิพากษาฎีกาที่ 4311/2557 ที่มีผลเป็นการยอมรับความเท่าเทียมกันในการทำหน้าที่ของสถานะข้อมูลคอมพิวเตอร์และสถานะเอกสาร ซึ่งเป็นการรับรองสถานะทางกฎหมายของข้อมูลอิเล็กทรอนิกส์ในการทำธุรกรรมทางแพ่งและพาณิชย์เท่านั้น แต่ในทางอาญาความเท่าเทียมทางสถานะจะต้องพิจารณาจากลักษณะความผิดและองค์ประกอบที่กฎหมายกำหนดด้วย ซึ่งความผิดเกี่ยวกับเอกสารนั้นเป็นความผิดที่กระทำต่อวัตถุที่มีรูปร่าง แต่สกุลเงินดิจิทัลเป็นวัตถุที่ไม่มีรูปร่าง อีกทั้งความผิดเกี่ยวกับเอกสารตามที่บัญญัติไว้ในประมวลกฎหมายอาญามีวัตถุ ประสงค์ ค้ำครองเอกสารในฐานะพยานหลักฐานที่ต้องมีความน่าเชื่อถือ แต่ข้อมูลคอมพิวเตอร์ค้ำครองความเป็นเจ้าของและความเป็นส่วนตัว ดังนั้นความผิดเกี่ยวกับเอกสารจึงไม่สามารถนำมาปรับใช้กับสกุลเงินดิจิทัลได้อย่างเหมาะสม

ข้อจำกัดดังกล่าวนำมาสนับสนุนประเด็นความไม่ชัดเจนของสถานะทางกฎหมายของสกุลเงินดิจิทัลซึ่งส่งผลกระทบต่อกฎหมายอาญาไทย ที่ต้องมีความชัดเจนแน่นอนในการกำหนดสถานะอัน

เป็นองค์ประกอบความผิด ดังนั้นหากไม่กำหนดสถานะที่ให้ชัดเจนให้กับสกุลเงินดิจิทัลย่อมส่งผลให้เกิดความไม่แน่นอนว่าจะนำกฎหมายของสถานะใดมาบังคับใช้กับความผิดที่เกิดขึ้น และอาจเกิดปัญหาการปรับใช้กฎหมาย และการตีความกฎหมายที่แตกต่างกันทั้งที่เป็นความผิดเกี่ยวกับสกุลเงินดิจิทัลลักษณะเดียวกัน ในประเด็นดังกล่าวยังได้ทำการศึกษากฎหมายของสหรัฐอเมริกา ประเทศอังกฤษ พบว่าแม้ทั้งสองประเทศจะใช้ระบบกฎหมายคอมมอนลอว์ศาลที่สามารถปรับใช้กฎหมายกับข้อเท็จจริงได้ แต่ก็ไม่มีบทบัญญัติที่ชัดเจนที่จะนำมาใช้กับความผิดเกี่ยวกับสกุลเงินดิจิทัลได้ โดยไม่กระทบต่อกฎหมายอาญาเดิมและนิติวิธีในการใช้กฎหมายแต่อย่างใด

นอกจากนี้ผู้เขียนได้ศึกษาองค์ประกอบความผิดกรณีการเอาไปหรือการชิงทรัพย์หรือเอกสารของผู้อื่นและแนวคำพิพากษาของศาลฎีกาที่เกี่ยวข้อง เพื่อนำมาวิเคราะห์ประเด็นรูปแบบการกระทำ ความผิดเกี่ยวกับสกุลเงินดิจิทัลที่เป็นช่องว่างทางกฎหมาย ซึ่งกฎหมายและคำพิพากษาศาลฎีกาที่มีอยู่ยังไม่ครอบคลุมกับความผิดบางลักษณะของสกุลเงินดิจิทัล ได้แก่ การขโมยสกุลเงินดิจิทัลและการใช้ทรัพยากรคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล และได้ทำการศึกษาแนวคิดในการควบคุมการกระทำผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล และหลักเกณฑ์การบัญญัติความผิดอาญา โดยนำสาระสำคัญของหลักเกณฑ์วิเคราะห์สนับสนุนประเด็นความจำเป็นในการกำหนดให้ความผิดทั้งสองรูปแบบที่กล่าวมาข้างต้นให้เป็นความผิดอาญา มี 4 ประการด้วยกัน คือ 1) เป็นการกระทำที่น่าตำหนิ และขัดต่อความสงบเรียบร้อยหรือศีลธรรมอันดีของประชาชน 2) การกระทำนั้นก่อให้เกิดอันตรายต่อประโยชน์หรือความสงบสุขของบุคคล หรือก่อให้เกิดอันตรายแก่ประโยชน์ของสังคมหรือประโยชน์ของรัฐ 3) หากการกำหนดให้การกระทำนั้นเป็นความผิดอาญาจะก่อให้เกิดผลดีมากกว่าการปล่อยทิ้งไว้โดยไม่กำหนดให้เป็นความผิด 4) การกำหนดให้การกระทำนั้นเป็นความผิดอาญาจะต้องเป็นทางเลือกสุดท้าย เมื่อไม่มีทางอื่นที่จะแก้ไขการกระทำดังกล่าวได้แล้ว นอกจากนี้ในการวิเคราะห์ความจำเป็นในการกำหนดความผิดอาญานั้น ยังได้ศึกษาแนวคิดการกำหนดความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ความผิดเกี่ยวกับหนังสือเดินทางและความผิดเกี่ยวกับศพที่ได้มีการบัญญัติให้เป็นความผิดไว้ในประมวลกฎหมายอาญาเพื่อนำมาเป็นแนวทางในการกำหนดความผิดเกี่ยวกับสกุลเงินดิจิทัลในประมวลกฎหมายอาญา และได้ทำการศึกษาแนวทางความร่วมมือทางอาญาระหว่างประเทศที่เป็นรูปแบบที่ก่อตั้งโดยอนุสัญญาและรูปแบบที่ก่อตั้งโดยองค์กร เพื่อนำมาวิเคราะห์ประเด็นความร่วมมือทางอาญาระหว่างประเทศในการปราบปรามการกระทำผิดสกุลเงินดิจิทัล ซึ่งเป็นโจทย์สำคัญในการควบคุมความผิดเกี่ยวกับสกุลเงินดิจิทัล เนื่องจากผู้กระทำผิดสามารถกระทำได้จากทั่วทุกมุมทั่วโลกที่มีการเชื่อมต่อกับระบบอินเทอร์เน็ต จึงเป็นการก่ออาชญากรรมได้อย่างไร้พรมแดนสร้างความเสียหายให้กับผู้ที่อยู่ในประเทศต่าง ๆ ได้พร้อมกันหลายประเทศ อาชญากรรมที่มีลักษณะข้ามชาติเช่นนี้จึงยากแก่การบังคับใช้กฎหมายของประเทศใดประเทศหนึ่ง: ดังนั้นปัจจุบันแนวทางความร่วมมือทางอาญาระหว่างประเทศจะมีข้อกำหนดที่ยืดหยุ่นหลักความผิดของทั้งสอง

ประเทศในการส่งผู้ร้ายข้ามแดน เพื่อเป็นการขจัดอุปสรรคในเรื่องความแตกต่างของกฎหมายภายในแต่ละประเทศ และยังได้ให้ความสำคัญกับการถ่ายทอดองค์ความรู้ เทคนิคในการสืบสวนหาพยานหลักฐานจากผู้เชี่ยวชาญและหน่วยงานที่เกี่ยวข้องในรูปแบบของการจัดอบรมสัมมนาออนไลน์ และออฟไลน์ ซึ่งแนวทางดังกล่าวนี้มีส่วนสำคัญในการเพิ่มพูนประสิทธิภาพในการป้องกันและปราบปรามการกระทำความผิดให้ทันต่อสถานการณ์ของเทคโนโลยีที่เปลี่ยนแปลงอย่างรวดเร็ว

เมื่อนำข้อมูลดังกล่าวมาศึกษาและวิเคราะห์ตามวิทยาการวิจัยที่ได้กำหนดไว้ ทำให้ได้ข้อค้นพบนำมาสู่คำตอบของงานวิจัย คือ สถานะของสกุลเงินดิจิทัล คือองค์ประกอบความผิดที่จะนำมาวินิจฉัยความรับผิดทางอาญาของบุคคล หากจุดเริ่มต้นในการวินิจฉัยความรับผิดไม่ชัดเจนแล้วย่อมส่งผลต่อการวินิจฉัยและการปรับใช้กฎหมายอย่างหลีกเลี่ยงไม่ได้ ดังนั้นจึงจำเป็นต้องกำหนดสถานะทางกฎหมายที่ชัดเจนให้กับสกุลเงินดิจิทัล เมื่อพิจารณาสถานะต่าง ๆ ที่ใกล้เคียงกับสกุลเงินดิจิทัล ได้แก่ สถานะทรัพย์สิน เงินตรา ข้อมูลคอมพิวเตอร์ และเอกสาร พบว่าแม้จะแนวคิดในการสนับสนุนให้เป็นสถานะต่าง ๆ ได้ แต่เมื่อพิจารณาทั้งความหมาย ลักษณะการกระทำความผิดกฎหมายอาญาที่ใช้ในการควบคุม รวมถึงคุณธรรมทางกฎหมายแล้ว จะเห็นว่าทุกสถานะที่กล่าวมายังมีข้อจำกัดบางประการยังไม่เหมาะสมจะนำมาปรับใช้กับสกุลเงินดิจิทัลได้ ดังนั้นในการกำหนดสถานะของสกุลเงินดิจิทัล นอกจากจะต้องมีความชัดเจนแล้วยังต้องมีความเหมาะสมกับลักษณะความผิดของสกุลเงินดิจิทัล จึงควรกำหนดสถานะของสกุลเงินดิจิทัลขึ้นมาใหม่ โดยกำหนดให้มีสถานะสกุลเงินดิจิทัล ซึ่งพิจารณาตามความเป็นจริงและสามารถครอบคลุมกับรูปแบบการกระทำความผิดที่มีลักษณะเฉพาะซึ่งอาศัยเทคโนโลยีในการกระทำความผิดมากกว่าที่จะกำหนดให้มีสถานะต่าง ๆ ตามที่ได้กล่าวมา ทั้งนี้จากการศึกษาวิเคราะห์พบว่ามีกรกระทำเกี่ยวกับสกุลเงินดิจิทัลอีก 2 รูปแบบ คือ การขโมยสกุลเงินดิจิทัลและการใช้พลังงานคอมพิวเตอร์ของผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัล ซึ่งทั้งสองรูปแบบนี้ยังไม่สามารถปรับใช้กับองค์ประกอบความผิดฐานลักทรัพย์ ความผิดฐานเอาไปซึ่งเอกสารตามประมวลกฎหมายอาญา และความผิดฐานเข้าถึงข้อมูลคอมพิวเตอร์ตามมีพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ได้ อีกทั้งการกระทำดังกล่าวยังมีลักษณะเป็นการกระทำที่น่าตำหนิและเป็นอันตรายต่อความสงบสุขและสวัสดิภาพของประชาชน ดังนั้นจึงควรกำหนดให้มีเป็นความผิดอาญาขึ้นมาใหม่ ตามหลักเกณฑ์การบัญญัติความผิดอาญา เช่นเดียวกับความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ ความผิดเกี่ยวกับหนังสือเดินทาง ที่ได้มีการบัญญัติให้เป็นความผิดไว้ในประมวลกฎหมายแล้ว

ท้ายที่สุดนี้ประเด็นสำคัญของควบคุมการกระทำความผิดอาญาที่เกี่ยวกับสกุลเงินดิจิทัล จะสัมฤทธิ์ผลไปไม่ได้หากปราศจากความร่วมมือทางอาญาระหว่างประเทศ ซึ่งปัจจุบันนี้มีความร่วมมือระหว่างประเทศในรูปแบบอนุสัญญาและความร่วมมือระหว่างประเทศรูปแบบองค์กร จากการศึกษาพบว่าความร่วมมือระหว่างประเทศรูปแบบอนุสัญญามีกลไกที่หลากหลายและเป็นรูปธรรม แต่ยังมี

ข้อจำกัดเรื่องความแตกต่างของกฎหมายภายในและกฎเกณฑ์การกำกับดูแลสกุลเงินดิจิทัลของแต่ละประเทศ อีกทั้งกลไกต่างๆ มิได้มีขึ้นเพื่อนำมาใช้กับความผิดเกี่ยวกับสกุลเงินดิจิทัลโดยเฉพาะ ส่วนความร่วมมือระหว่างประเทศรูปแบบขององค์กรนั้น จัดตั้งขึ้นมาเพื่อวัตถุประสงค์ที่เกี่ยวข้องกับการป้องกันและปราบปรามสกุลเงินดิจิทัลมากขึ้น โดยให้ความสำคัญกับมาตรการในการเรียนรู้ ถ่ายทอดเทคนิคในการสืบสวน สอบสวน การค้นหาพยานหลักฐานดิจิทัลและทักษะที่เกี่ยวข้องโดยผู้เชี่ยวชาญ มาตรการเหล่านี้เทคโนโลยีเป็นสิ่งสำคัญในการขับเคลื่อนการแก้ไขปัญหา ซึ่งทำให้ประเทศที่ด้อยพัฒนาทางการเงินและเทคโนโลยีไม่สามารถพัฒนาศักยภาพได้อย่างเต็มที่ ดังนั้นในการแก้ไขปัญหาการกระทำความผิดที่มีลักษณะข้ามพรมแดนเช่นนี้ ทั่วโลกจำเป็นต้องลดความเหลื่อมล้ำในการเข้าถึงเทคโนโลยีที่จำเป็นและร่วมมือกันแบ่งปันความรู้ก็จะช่วยเพิ่มประสิทธิภาพในการป้องกันและปราบปรามได้อย่างแท้จริง

สรุปผลการวิจัยข้างต้นเป็นไปตามสมมติฐานที่ได้กำหนดว่า การใช้สกุลเงินดิจิทัลมีแนวโน้มเพิ่มมากขึ้น ปัจจุบันยังไม่มีกฎหมายควบคุมการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลไว้เป็นการเฉพาะ หากมีการกระทำความผิดเกิดขึ้นจะต้องนำบทบัญญัติของสถานะที่ใกล้เคียงมาปรับใช้ในการลงโทษผู้กระทำความผิด ซึ่งการปรับใช้กฎหมายดังกล่าวขัดกับหลัก ความชัดเจนแน่นอนของกฎหมายอาญา ก่อให้เกิดความสับสนและขาดมาตรฐานในการบังคับใช้กฎหมายไปในทิศทางเดียวกัน อีกทั้งการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัลยังมีลักษณะเฉพาะทางเทคนิคจึงทำให้การกระทำความผิดบางกรณีเกิดช่องว่างทางกฎหมายไทย จึงจำเป็นต้องมีกฎหมายสารบัญญัติกำหนดความผิดเกี่ยวกับสกุลเงินดิจิทัล ไว้เป็นการเฉพาะเพื่อให้ สอดคล้องและครอบคลุมกับกรณีความผิดที่อาจเกิดขึ้นได้อย่างเหมาะสม ควบคู่ไปกับความร่วมมือทางอาญาระหว่างประเทศ เพื่อบังคับใช้ในการป้องกันและปราบปรามการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลได้อย่างมีประสิทธิภาพ

## 5.2 ข้อเสนอแนะ

1) จากปัญหาสถานะทางกฎหมายของสกุลเงินดิจิทัลและข้อจำกัดทางกฎหมายของสถานะอื่น ๆ ที่ได้ทำการวิเคราะห์และนำมาสู่บทสรุปที่ไม่มีกฎหมายของสถานะใดสามารถมาปรับใช้ได้เหมาะสมนั้น ผู้เขียนเห็นว่าควรกำหนดนิยามของสกุลเงินดิจิทัลให้เกิดความชัดเจนโดยพิจารณาตามสภาพความเป็นจริงและลักษณะเฉพาะของสกุลเงินดิจิทัล ซึ่งจะทำให้กฎหมายสามารถรองรับเทคโนโลยีแบบเดียวกันในอนาคตได้อย่างเหมาะสมมากกว่าการเทียบเคียงให้มีสถานะอื่น โดยกำหนดไว้ในประมวลกฎหมายอาญามาตรา 1 (19) ดังนี้

มาตรา 1 (19) “สกุลเงินดิจิทัล” หมายความว่า “สิ่งที่ใช้เป็นตัวกลางในการแลกเปลี่ยนสินค้า บริการ มีมูลค่าทางการเงินและทำหน้าที่เสมือนเป็นเงินตราที่อยู่ในรูปแบบดิจิทัลซึ่งไม่ใช่เหรียญหรือ ธนบัตรในสกุลเงินบาทของประเทศไทยหรือของประเทศอื่น”

2) สมควรกำหนดกรณีการขโมยสกุลเงินดิจิทัลและกรณีการใช้ทรัพยากรคอมพิวเตอร์ของ ผู้อื่นเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัลเป็นฐานความผิดใหม่ในประมวลกฎหมายอาญา เนื่องจากกฎหมาย ที่มีอยู่ไม่สามารถนำมาปรับใช้ได้เหมาะสม การกระทำดังกล่าวจึงยังเป็นช่องว่างทางกฎหมายที่ ไม่สามารถลงโทษผู้กระทำได้ จึงสมควรบัญญัติให้เป็นความผิดตามหลักเกณฑ์การบัญญัติความผิด อาญา

ผู้เขียนเห็นว่าควรกำหนดความผิดฐานใหม่ไว้ในประมวลกฎหมายอาญาลักษณะ 12 ความผิด เกี่ยวกับทรัพย์ เนื่องจากจากการศึกษาพบว่าการกระทำความผิดเกี่ยวกับสกุลเงินดิจิทัลมีลักษณะ ความใกล้เคียงกับความผิดเกี่ยวกับทรัพย์ตามประมวลกฎหมายอาญามากกว่าความผิดเกี่ยวกับ เงินตรา ข้อมูลคอมพิวเตอร์ หรือเอกสาร โดยเพิ่มบทบัญญัติดังนี้

(1) เพิ่มบทบัญญัติเกี่ยวกับการขโมยสกุลเงินดิจิทัลไว้เป็นการเฉพาะ ไว้ในวรรค 2 ของ ความผิดฐานลักทรัพย์ มาตรา 334 แห่งประมวลกฎหมายอาญา โดยความผิดฐานลักทรัพย์นี้ ให้หมายความรวมถึงสกุลเงินดิจิทัล จากเดิมที่กฎหมายกำหนดให้การขโมยกำหนดมีวัตถุแห่งการ กระทำเป็นคำว่า “ทรัพย์” ซึ่งหมายถึงวัตถุที่มีรูปร่างเท่านั้น จึงไม่สามารถนำมาใช้กับวัตถุที่ไม่มี รูปร่างเช่นสกุลเงินดิจิทัลได้ ดังนั้นเมื่อบทบัญญัติใหม่นี้กำหนดให้วัตถุแห่งการกระทำให้หมายความ รวมถึง “สกุลเงินดิจิทัล” ก็จะมีผลครอบคลุมถึงวัตถุที่ไม่มีรูปร่างดังเช่นสกุลเงินดิจิทัลได้ นอกจากนี้ เมื่อการลักสกุลเงินดิจิทัลเป็นความผิดอาญาเช่นเดียวกับการลักทรัพย์แล้ว จะส่งผลให้ความผิดฐาน อื่น ๆ ที่มีพื้นฐานมาจากการลักทรัพย์เป็น อันได้แก่ ความผิดฐานวิ่งราวทรัพย์ ความผิดฐานชิงทรัพย์ ความผิดฐานปล้นทรัพย์ ที่กระทำต่อสกุลเงินดิจิทัลสามารถนำมาปรับใช้ได้โดยไม่จำเป็นต้องแก้ไข บทบัญญัติที่มีอยู่แต่อย่างใด

มาตรา 334 ผู้ใดเอาทรัพย์ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปโดยทุจริต ผู้นั้น กระทำความผิดฐานลักทรัพย์ ต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกหมื่นบาท

“การกระทำตามวรรคหนึ่ง หากกระทำต่อสกุลเงินดิจิทัล ให้ถือเป็นการลักทรัพย์”

อย่างไรก็ตามการเพิ่มเติมบทบัญญัติสกุลเงินดิจิทัลในความผิดฐานลักทรัพย์ ยังไม่ ครอบคลุมกับการกระทำที่มีลักษณะเป็นการยกยอก เนื่องจากทั้งสองฐานความผิดมีองค์ประกอบใน ส่วนของการกระทำที่แตกต่างกัน อีกทั้งความผิดฐานยกยอกนั้นมิได้มีพื้นฐานมาจากความผิดฐานลัก ทรัพย์ ดังนั้นจึงต้องเพิ่มเติมบทบัญญัติเกี่ยวกับสกุลเงินดิจิทัลในความผิดฐานยกยอกไว้ในวรรค 3 ของ มาตรา 352 ดังนี้

## มาตรา 352

ผู้ใดครอบครองทรัพย์สินซึ่งเป็นของผู้อื่น หรือซึ่งผู้อื่นเป็นเจ้าของรวมอยู่ด้วย เบียดบังเอาทรัพย์สินนั้นเป็นของตนหรือบุคคลที่สามโดยทุจริต ผู้นั้นกระทำความผิดฐานลักยอก ต้องระวางโทษจำคุกไม่เกินสามปี หรือปรับไม่เกินหกหมื่นบาทหรือทั้งจำทั้งปรับ

ถ้าทรัพย์สินนั้นได้ตกมาอยู่ในความครอบครองของผู้กระทำความผิด เพราะผู้อื่นส่งมอบให้โดยสำคัญผิดไปด้วยประการใด หรือเป็นทรัพย์สินหายซึ่งผู้กระทำความผิดเก็บได้ ผู้กระทำต้องระวางโทษแต่เพียงกึ่งหนึ่ง

“การกระทำตามวรรคหนึ่ง หากกระทำต่อสกุลเงินดิจิทัล ให้ถือเป็นการลักยอก”

(2) เพิ่มบทบัญญัติความผิดฐานนำพลังงานไฟฟ้าหรือพลังงานของผู้อื่นไปใช้โดยมิชอบไว้ในประมวลกฎหมายอาญาลักษณะ 12 หมวด 1 ความผิดฐานลักทรัพย์และวิ่งราวทรัพย์ เป็นความผิดฐานลักทรัพย์ วิ่งราวทรัพย์และความผิดฐานนำพลังงานไฟฟ้าหรือพลังงานของผู้อื่นไปใช้โดยมิชอบ ดังนี้

มาตรา 336 ตร “ผู้ใดนำพลังงานไฟฟ้าหรือพลังงานอื่นใดซึ่งอาจมีราคาและอาจถือเอาได้ของผู้อื่นหรือที่ผู้อื่นเป็นเจ้าของรวมอยู่ด้วยไปใช้โดยทุจริต ผู้นั้นกระทำความผิดฐานใช้พลังงานของผู้อื่นโดยมิชอบ ต้องระวางโทษต้องระวางโทษจำคุกไม่เกินสามปี และปรับไม่เกินหกหมื่นบาท”

ความผิดฐานนี้ได้กำหนดวัตถุประสงค์แห่งการกระทำให้เป็นคำว่า “พลังงานไฟฟ้าหรือพลังงานอื่นใด” แทนคำว่า “พลังงานคอมพิวเตอร์” เนื่องจากการใช้พลังงานคอมพิวเตอร์ของผู้อื่นในการประมวลผลเพื่อให้ได้มาซึ่งสกุลเงินดิจิทัลมีความหมายเช่นเดียวกับการใช้พลังงานไฟฟ้า ดังนั้นการเพิ่มเติมบทบัญญัติเช่นนี้จึงไม่เพียงแต่นำไปใช้กับความผิดกรณีการใช้พลังงานคอมพิวเตอร์ของผู้อื่นได้เท่านั้น แต่ยังสามารถรองรับความผิดกรณีการใช้พลังงานไฟฟ้า หรือพลังงานของผู้อื่นในรูปแบบอื่น ๆ ซึ่งกระทำโดยทุจริตที่อาจเกิดขึ้นในอนาคตได้อีก ซึ่งแม้จะมีได้เป็นการเอาไปในลักษณะที่ตัดกรรมสิทธิ์และมีได้เป็นการกระทำที่จำกัดเฉพาะวัตถุประสงค์ที่มีรูปร่างก็เป็นความผิดอาญาได้เช่นกัน นอกจากนี้การบทบัญญัติดังกล่าวยังส่งผลให้ประเทศไทยซึ่งอยู่ในระบบประมวลกฎหมายมีบทบัญญัติที่ชัดเจนตามหลักเกณฑ์ความรับผิดชอบอาญาของบุคคลอีกด้วย

3) ด้วยเหตุที่เป็นการกระทำผิดเกี่ยวกับสกุลเงินดิจิทัลมีลักษณะข้ามพรมแดน ซึ่งประเทศไทยหรือคนไทยอาจตกเป็นผู้เสียหายได้ จึงควรบัญญัติให้ผู้กระทำความผิดที่กระทำนอกราชอาณาจักรต้องรับโทษตามกฎหมายไทยไว้ในมาตรา 8 แห่งประมวลกฎหมายอาญา ทั้งนี้การเพิ่มเติมบทบัญญัติความผิดฐานขโมยสกุลเงินดิจิทัลที่อยู่ในวรรค 2 ของ มาตรา 334 เป็นความผิดที่รวมอยู่ในมาตรา 8 (8) และการเพิ่มความผิดฐานลักยอกสกุลเงินดิจิทัลที่อยู่ในวรรค 3 ของมาตรา 352 เป็นความผิดที่รวมอยู่ในมาตรา 8 (11) ไว้แล้ว ดังนั้นหากเป็นการกระทำที่เข้าเงื่อนไของค์ประกอบความผิดตามมาตรา 8 ก็สามารถลงโทษผู้กระทำผิดได้ โดยไม่ต้องแก้ไขอนุมาตราดังกล่าวอีก แต่สำหรับความผิดฐานนำ

พลังงานไฟฟ้าหรือพลังงานของผู้อื่นไปใช้โดยมิชอบนั้นมาตรา 8 อาจยังไม่ครอบคลุมถึง ดังนั้นเพื่อให้สอดคล้องกับฐานความผิดใหม่ที่ได้นำเสนอไว้ซึ่งอยู่ในหมวด 1 ความผิดฐานลักทรัพย์ วิ่งราว และการนำพลังงานไฟฟ้าหรือพลังงานของผู้อื่นไปใช้โดยมิชอบ จึงขอเสนอให้แก้ไข โดยเพิ่มความผิดฐานนำพลังงานไฟฟ้าหรือพลังงานของผู้อื่นไปใช้โดยมิชอบ ตามมาตรา 336 ตร. ให้รวมอยู่ใน (8) ดังนี้

มาตรา 8 ผู้ใดกระทำความผิดนอกราชอาณาจักร และ

(1) ผู้กระทำความผิดนั้นเป็นคนไทย และรัฐบาลแห่งประเทศที่ความผิดได้เกิดขึ้น หรือผู้เสียหายได้ร้องขอให้ลงโทษ หรือ

(2) ผู้กระทำความผิดนั้นเป็นคนต่างด้าว และรัฐบาลไทยหรือคนไทยเป็นผู้เสียหาย และผู้เสียหายได้ร้องขอให้ลงโทษ

ถ้าความผิดนั้นเป็นความผิดดังระบุไว้ต่อไปนี้ จะต้องรับโทษภายในราชอาณาจักร คือ

(1) ความผิดเกี่ยวกับการก่อให้เกิดอันตรายต่อประชาชน ตามที่บัญญัติไว้ในมาตรา 217 มาตรา 218 มาตรา 221 ถึงมาตรา 223 ทั้งนี้ เว้นแต่กรณีเกี่ยวกับมาตรา 220 วรรคแรก และมาตรา 224 มาตรา 226 มาตรา 228 ถึงมาตรา 232 มาตรา 237 และมาตรา 233 ถึงมาตรา 236 ทั้งนี้ เฉพาะเมื่อเป็นกรณีต้องระวางโทษตามมาตรา 238

(2) ความผิดเกี่ยวกับเอกสาร ตามที่บัญญัติไว้ในมาตรา 264 มาตรา 265 มาตรา 266 (1) และ (2) มาตรา 268 ทั้งนี้ เว้นแต่กรณีเกี่ยวกับมาตรา 267 และมาตรา 269

ก) ความผิดเกี่ยวกับบัตรอิเล็กทรอนิกส์ตามที่บัญญัติไว้ในมาตรา 269/1 ถึงมาตรา 269/7

ข) ความผิดเกี่ยวกับหนังสือเดินทางตามที่บัญญัติไว้ในมาตรา 269/8 ถึงมาตรา 269/15

(3) ความผิดเกี่ยวกับเพศ ตามที่บัญญัติไว้ในมาตรา 276 มาตรา 280 และมาตรา 285 ทั้งนี้ เฉพาะที่เกี่ยวกับมาตรา 276

(4) ความผิดต่อชีวิต ตามที่บัญญัติไว้ในมาตรา 288 ถึงมาตรา 290

(5) ความผิดต่อร่างกาย ตามที่บัญญัติไว้ในมาตรา 295 ถึงมาตรา 298

(6) ความผิดฐานทอดทิ้งเด็ก คนป่วยเจ็บหรือคนชรา ตามที่บัญญัติไว้ในมาตรา 306 ถึงมาตรา 308

(7) ความผิดต่อเสรีภาพ ตามที่บัญญัติไว้ในมาตรา 309 มาตรา 310 มาตรา 312 ถึงมาตรา 315 และมาตรา 317 ถึงมาตรา 320

(8) ความผิดฐานลักทรัพย์ วิ่งราวทรัพย์ และการนำพลังงานไฟฟ้าหรือพลังงานของผู้อื่นไปใช้โดยมิชอบ ตามที่บัญญัติไว้ในมาตรา 334 ถึงมาตรา 336 ตร.

(9) ความผิดฐานกรรโชก ริดเอาทรัพย์ ชิงทรัพย์ และปล้นทรัพย์ ตามที่บัญญัติไว้ใน มาตรา 337 ถึงมาตรา 340

(10) ความผิดฐานฉ้อโกง ตามที่บัญญัติไว้ในมาตรา 341 ถึงมาตรา 344 มาตรา 346 และมาตรา 347

(11) ความผิดฐานยักยอก ตามที่บัญญัติไว้ในมาตรา 352 ถึงมาตรา 354

(12) ความผิดฐานรับของโจร ตามที่บัญญัติไว้ในมาตรา 357

(13) ความผิดฐานทำให้เสียทรัพย์ ตามที่บัญญัติไว้ในมาตรา 358 ถึงมาตรา 360

### 5.3 ข้อเสนอแนะอื่น

1) ควรส่งเสริมให้มีแลกเปลี่ยนความรู้ ทักษะที่จำเป็นในการป้องกันและปราบปราม อาชญากรรมสกุลเงินดิจิทัล ให้แก่เจ้าหน้าที่ที่เกี่ยวข้องทั้งในเชิงทฤษฎีและเชิงปฏิบัติ โดยเฉพาะด้าน การสืบสวนสอบสวนอาชญากรรมสกุลเงินดิจิทัล การค้นหาพยานหลักฐานดิจิทัล และสร้างองค์ ความรู้ในการพัฒนากฎหมาย ข้อบังคับ และพัฒนาบุคลากรด้านการปราบปรามให้มีความรู้ ความ เข้าใจเกี่ยวกับการปราบปรามอาชญากรรมสกุลเงินดิจิทัลผ่านการฝึกอบรม อบรม รวมทั้งการส่ง บุคลากรเข้าร่วมสัมมนาปฏิบัติการระหว่างประเทศจะเป็นประเด็นสำคัญที่พัฒนาให้บุคลากรใน ประเทศไทยมีศักยภาพ ดังที่ได้มีการศึกษาแนวทางการป้องกันและปราบปรามอาชญากรรมสกุลเงิน ดิจิทัลของ UNODC ที่ได้ให้ความสำคัญกับการแลกเปลี่ยนความรู้ในรูปแบบของการจัดกิจกรรม สัมมนาโดยเชิญโดยผู้ที่มีความรู้ความเชี่ยวชาญทางด้านเทคนิคจากภาครัฐและภาคเอกชน นักวิชาการ นักกฎหมาย ทั้งในและต่างประเทศ ร่วมกันระดมความคิด หาทางออกถึงประเด็นปัญหาอาชญากรรม สกุลเงินดิจิทัลโดยเฉพาะเทคนิคการติดตามสืบค้นพยานหลักฐาน การยึดสกุลเงินดิจิทัลที่ได้จาก ธุรกรรมที่ผิดกฎหมาย ซึ่งสิ่งเหล่านี้ล้วนเป็นองค์ความรู้ที่จะนำไปพัฒนาปรับปรุงมาตรฐานในการ ป้องกันและปราบปรามของแต่ละประเทศให้มีความใกล้เคียงกัน และสร้างความเชื่อมั่นกับประเทศที่ อยู่ในกลุ่มความร่วมมือว่าสามารถดำเนินปฏิบัติการหรือให้ความร่วมมือให้บรรลุเป้าหมายได้

ทั้งนี้ผู้เขียนมีความเห็นเพิ่มเติม ในส่วนประเทศกลุ่มอาเซียนควรสร้างความมีส่วนร่วมใน รูปแบบทางการในภูมิภาคให้มากขึ้นเนื่องจาก โครงสร้างสังคม วัฒนธรรม ภาษา ใกล้เคียงกัน การ เกิดความร่วมมือในการประสานงานและดำเนินปฏิบัติการระหว่างประเทศสามารถดำเนินการได้ คล่องตัวกว่า โดยจัดทำในรูปแบบการเข้าร่วมอภิปรายหาแนวปฏิบัติและหาแนวทางป้องกันและ ปราบปรามอาชญากรรมสกุลเงินดิจิทัลที่มีระบบและเข้มแข็งภายใต้กรอบความร่วมมือระหว่าง อาเซียน ทั้งนี้กลุ่มประเทศอาเซียนอาจเชิญประเทศนอกกลุ่มที่มีมุมมองในการร่วมกันปราบปราม อาชญากรรมดังกล่าวในทิศทางเดียวกันเข้าร่วมในลักษณะ ASEAN Plus เช่นการเรียกร้องให้ ASEAN

ประเทศออสเตรเลียและประเทศนิวซีแลนด์ (ASEAN Plus Two) เข้าร่วมเป็นพันธมิตรและผลักดันการป้องกันและปราบปรามสกุลเงินดิจิทัลให้มีประสิทธิภาพยิ่งขึ้น

2) ควรส่งเสริมการให้ความรู้และความเข้าใจให้แก่ประชาชนเกี่ยวกับการใช้งานและการถือครองสกุลเงินดิจิทัลอย่างปลอดภัย เช่น การใช้งานกระเป๋าเงินคริปโทเคอร์เรนซีให้ปลอดภัย การให้ความรู้เกี่ยวกับการใช้งานตัวกลางแลกเปลี่ยนสกุลเงินดิจิทัลที่กฎหมายรับรอง การสร้างความตระหนักว่าการทำธุรกรรมผ่านระบบบล็อกเชนไม่มีการคุ้มครองหลังจากการทำธุรกรรมเสร็จสิ้นและไม่สามารถยกเลิกหรือย้อนคืนได้ ผู้ใช้บริการจะไม่มีตัวกลางในการตรวจสอบและให้ความปลอดภัยในการทำธุรกรรมต่างๆ ผู้ใช้จะต้องดูแลธุรกรรมของตัวเองเสมือนตนเองเป็นธนาคารของทรัพย์สินดิจิทัล (Be Your Own Bank) รวมถึงให้ความรู้เกี่ยวกับรูปแบบอาชญากรรมสกุลเงินดิจิทัลที่มีองค์ประกอบทางอาชญากรรมรูปแบบเดิมแต่ใช้ช่องทางเทคโนโลยีที่เกิดขึ้นใหม่มาเป็นเครื่องมือในการหลอกลวงหรืออำนวยความสะดวกในการกระทำผิดได้ง่ายขึ้น ดังนั้นเพื่อให้การส่งเสริมความรู้ดังกล่าวเกิดผลอย่างเป็นรูปธรรม ผู้เขียนเห็นว่าควรมีการจัดทำคู่มือหรือสื่อประชาสัมพันธ์แก่ประชาชนทั่วไปเพื่อสร้างความรู้ ความเข้าใจที่ถูกต้องถึงภัยซ่อนเร้นต่าง ๆ และความเสี่ยงจากการใช้สกุลเงินดิจิทัลและวิธีการป้องกันตนเองเบื้องต้น เช่น การเก็บสกุลเงินดิจิทัลอย่างไรให้ปลอดภัยในส่วนออนไลน์และออฟไลน์ อุปกรณ์และระบบความปลอดภัยทางเลือกที่เหมาะสมในการเก็บเงินดิจิทัล ระบบป้องกันหรือโปรแกรมป้องกันภัยจากการโจมตีทางคอมพิวเตอร์ที่เหมาะสม เช่น Security Program หรือ Scan Virus เป็นต้น รวมถึงกลไกของภาครัฐในการคุ้มครองประชาชนเมื่อตกเป็นผู้เสียหายสามารถดำเนินการร้องทุกข์ ขอความช่วยเหลือหรือขอคำแนะนำในการดำเนินคดีได้จากหน่วยงานใดในช่องทางใด จะเป็นการสร้างมาตรฐานความปลอดภัยและความเชื่อมั่นให้กับผู้ใช้ ผู้ประกอบธุรกิจ และผู้ลงทุนที่เข้ามาทำธุรกรรมสกุลเงินดิจิทัล

ผู้เขียนมีความเห็นว่าการเพิ่มประสิทธิภาพในแก่ผู้บังคับใช้กฎหมายเป็นองค์ประกอบอีกด้านที่สำคัญ การจัดทำคู่มือประกอบการปฏิบัติงานการปราบปรามอาชญากรรมสกุลเงินดิจิทัลสามารถช่วยกำหนดแนวทางในการปฏิบัติงานของพนักงานเจ้าหน้าที่ให้เป็นไปในทิศทางเดียวกันอย่างมีประสิทธิภาพภายใต้ขอบเขตอำนาจหน้าที่ตามกฎหมาย และควรพัฒนาระบบการสืบค้นเส้นทางการเงินผ่านเครือข่ายธนาคารและตัวกลางแลกเปลี่ยนเงินดิจิทัลให้แก่พนักงานเจ้าหน้าที่ แม้ว่าระบบของบล็อกเชนจะเป็นการหลีกเลี่ยงการใช้คนกลางในการทำธุรกรรม จึงมีความเสี่ยงที่จะเลี่ยงการตรวจสอบโดยภาครัฐจากการที่ระบบไม่เปิดเผยตัวตนของผู้ใช้ แต่อย่างไรก็ตามเทคโนโลยีบล็อกเชนจะเก็บข้อมูลประวัติการทำธุรกรรมอันเป็นปัจจัยสำคัญที่จะช่วยในการติดตามและระบุตัวอาชญากรได้ ดังนั้นหากระบบการติดตาม และขอพยานหลักฐานเกี่ยวกับธนาคารหรือตัวกลางแลกเปลี่ยนเงินดิจิทัลมีประสิทธิภาพ การติดตามร่องรอยเพื่อจับกุมตัวอาชญากรก็สามารถทำได้อย่างมีประสิทธิภาพ

3) ควรมีการรวบรวมแนวปฏิบัติความร่วมมือทางอาญาระหว่างประเทศในการกระทำความผิดอาญาเกี่ยวกับสกุลเงินดิจิทัล จากทั้งความร่วมมือทั้งในรูปแบบทางการและไม่เป็นทางการของหน่วยงานปราบปรามอาชญากรรมเกี่ยวกับสกุลเงินดิจิทัล เช่น การให้ความช่วยเหลือซึ่งกันและกันในด้านกฎหมาย (Mutual Legal Assistance) ที่อาจดำเนินการในรูปแบบของการแบ่งปันข้อมูลระหว่างเจ้าหน้าที่ (Police to Police Disseminations) เช่น การให้ความช่วยเหลือทางอาญาซึ่งกันและกัน การส่งผู้ร้ายข้ามแดน การแลกเปลี่ยนข้อมูลข่าวสารในระหว่างรัฐภาคี เป็นต้น เนื่องจากอาชญากรรมสกุลเงินดิจิทัลสามารถก่ออาชญากรรมได้อย่างไรพรหมแดน ประเทศไทยจึงอาจอยู่ในฐานะที่เป็นได้ทั้งประเทศที่ตกเป็นผู้เสียหาย ประเทศที่มีคนไทยเป็นผู้กระทำความผิด หรืออาจเป็นประเทศที่ผู้กระทำความผิดเลือกหนีมาพำนักจากการก่ออาชญากรรมได้ทั้งสิ้น ดังนั้นแนวปฏิบัติดังกล่าวควรมีการแบ่งแยกลักษณะของการเกี่ยวข้องกับอาชญากรรมให้ชัดเจนและกำหนดมีสาระสำคัญเกี่ยวกับองค์ประกอบและฐานความผิดหน่วยงานที่มีหน้าที่ในการรับคำร้องทุกข์ และหน่วยงานที่มีหน้าที่ดำเนินคดีและประสานความร่วมมือกับต่างประเทศ ดังนั้นหากมีการรวบรวมแนวทางปฏิบัติความร่วมมือทางอาญาระหว่างประเทศที่ชัดเจน จะทำให้กระบวนการในการป้องกันและปราบปรามสกุลเงินดิจิทัลได้อย่างเป็นระบบ ทั้งในส่วนของกฎหมาย หน่วยงานที่เกี่ยวข้อง ความพร้อมของเครื่องมือและนวัตกรรมที่ใช้ดำเนินปฏิบัติการและสนับสนุนให้ไปอย่างมีประสิทธิภาพได้ทันทั่วถึง

## บรรณานุกรม

- กระทรวงการคลัง. **ภารกิจ และหน้าที่รับผิดชอบของหน่วยงาน**. ค้นวันที่ 30 พฤษภาคม 2564 จาก <https://www.mof.go.th/th/detail/2018-12-21-15-00-10/2018-12-21-17-48-06>
- กฤษฎา สังขมณี. **การเงินและการธนาคาร**. กรุงเทพมหานคร: ศูนย์หนังสือมหาวิทยาลัยราชภัฏสวนสุนันทา, 2550.
- กษิตศ ทองวิเศษสุข. **ปัญหาทางกฎหมายเกี่ยวกับการป้องกันและปราบปรามการฟอกเงินโดยใช้ระบบปิดคอยน์**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ สถาบันบัณฑิตพัฒนบริหารศาสตร์, 2558.
- กองกษาปณ์. **เงินตรา**. ค้นวันที่ 22 กันยายน 2562 จาก [www.royalthaimint.net/ewtadmin/ewt/mint\\_web/ewt\\_news.php?nid=46&filename=index](http://www.royalthaimint.net/ewtadmin/ewt/mint_web/ewt_news.php?nid=46&filename=index)
- กันตภณ ศรีชาติ. **เงินเสมือน (Virtual Currency) ต่างจากเงินจริงอย่างไร**. กรุงเทพมหานคร. (20 สิงหาคม 2556). ค้นวันที่ 22 กันยายน 2562 จาก <http://www.bangkokbi2news.com/blog/detail/523725>
- กิตติศักดิ์ ปรกติ. **กฎหมายกับพัฒนาการของสังคมไทย: จากลัทธิกระแสไฟฟ้า มาสู่ลัทธิสัญญาณโทรศัพท์**. **วารสารไทยคดีศึกษา**. 2, 2 (เมษายน-กันยายน 2548): 35-54.
- เกียรติกร เทียนธรรมชาติ. **อิทธิพลต่อการตัดสินใจยอมรับใช้เงินดิจิทัล (ปิดคอยน์) ของผู้บริโภคกลุ่ม Millennials ในกรุงเทพมหานคร**. การค้นคว้าอิสระปริญญาโทบริหารธุรกิจ วิทยาลัยนวัตกรรม มหาวิทยาลัยธรรมศาสตร์, 2561.
- เกียรติขจร วัจนะสวัสดิ์. **กฎหมายอาญาภาคความผิด เล่ม 1**. พิมพ์ครั้งที่ 5 ฉบับแก้ไขเพิ่มเติม. กรุงเทพมหานคร: พลสยามพริ้นติ้ง, 2553.
- เกียรติขจร วัจนะสวัสดิ์. **คำอธิบายกฎหมายอาญา ภาค 1**. พิมพ์ครั้งที่ 10. กรุงเทพมหานคร: พลสยามพริ้นติ้ง, 2551.
- คณาธิป ทองรวีวงศ์. **กฎหมายความผิดเกี่ยวกับคอมพิวเตอร์ เล่ม 1**. กรุงเทพมหานคร: นิติธรรม, 2563.
- คณิต ณ นคร. **กฎหมายอาญา ภาคความผิด**. พิมพ์ครั้งที่ 9. กรุงเทพมหานคร: วิญญูชน, 2549.
- คณิต ณ นคร. **กฎหมายอาญาภาคทั่วไป**. พิมพ์ครั้งที่ 4. กรุงเทพมหานคร: วิญญูชน, 2554.
- คณิต ณ นคร. **ปรัชญาและแนวความคิดของการกำหนดความผิดอันยอมความได้**. **วารสารกฎหมายธุรกิจบัณฑิตย์**. 1, 4 (มกราคม-มิถุนายน 2547): 1-2.
- คำแนะนำของคณะกรรมการพัฒนากฎหมาย เรื่อง การกำหนดโทษอาญาในกฎหมาย. **ราชกิจจา**

นุเบกษา. 136, 132 (27 พฤศจิกายน 2562).

- ศิริมาศ สุขประสงศ์. **การป้องกันและปราบปรามการสนับสนุนทางการเงินแก่การก่อการร้ายตามกฎหมายระหว่างประเทศและผลกระทบทางกฎหมายสำหรับประเทศไทย**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2556.
- จิตติ ดิงศภัทย์. **คำอธิบายประมวลกฎหมายอาญา ภาค 1**. พิมพ์ครั้งที่ 10. กรุงเทพมหานคร: สำนักอบรมศึกษากฎหมายแห่งเนติบัณฑิตยสภา, 2546.
- จิตติ ดิงศภัทย์. **รวมผลงานทางวิชาการของศาสตราจารย์จิตติ ดิงศภัทย์ เล่มที่ 1**. กรุงเทพมหานคร: สำนักงานศาลยุติธรรม, 2562.
- ชวกร เลิศรุ่งศรี. **วิวัฒนาการของเงิน (Evolution of Money)**. ค้นวันที่ 12 พฤษภาคม 2563 จาก <https://medium.com/bitkub/evolution-money-barter-digital-cryptocurrency-84c740329328>
- ฐิติมา ชูเชิด. **สกุลเงินดิจิทัล ใกล้เคียงแค่ไหน?**. ค้นวันที่ 22 ตุลาคม 2562 จาก [https://www.bot.or.th/Thai/ResearchAndPublications/articles/Pages/Article\\_01Feb2019.aspx](https://www.bot.or.th/Thai/ResearchAndPublications/articles/Pages/Article_01Feb2019.aspx)
- ณภัทร สรอรรถ. **ความเหมาะสมในการกำหนดความผิดและโทษทางอาญา: ศึกษากรณีกฎหมายการแข่งขันทางการค้า**. สารนิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.
- ดลพร ประสงค์สุทธิพร. **แนวทางการกำกับดูแลการใช้เงินเสมือน: กรณีศึกษาบิตคอยน์**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2557.
- ทพพล น้อยปัญญา. **กฎหมายเรื่อง Bitcoin Blockchain ICO and etc**. กรุงเทพมหานคร: วิทยุชุมชน, 2561.
- ทวีเกียรติ มีนะกนิษฐ. **กฎหมายกับสังคม**. กรุงเทพมหานคร: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2552.
- ทวีเกียรติ มีนะกนิษฐ. **คำอธิบายกฎหมายอาญาภาคทั่วไป**. พิมพ์ครั้งที่ 9. กรุงเทพมหานคร: วิทยุชุมชน, 2551.
- ทวีเกียรติ มีนะกนิษฐ. **รายงานวิจัยเรื่องความผิดฐานลักทรัพย์**. กรุงเทพมหานคร: โครงการวิจัยเสริมหลักสูตร มหาวิทยาลัยธรรมศาสตร์, 2529.
- ธนากร อุทยานิชย์. **การจารกรรมข้อมูลทางคอมพิวเตอร์กับความรับผิดทางอาญา**. **วารสารเทคโนโลยีสารสนเทศ**. 6, 12 (กรกฎาคม-ธันวาคม 2553): 61.
- ธนากรแห่งประเทศไทย. **ข้อมูลเกี่ยวกับบิตคอยน์และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่น ๆ ที่มีลักษณะใกล้เคียงกัน**. **ข่าวของธนาคารแห่งประเทศไทย**. 8 (2557).

ธนาคารแห่งประเทศไทย. **คำอธิบายสรุปสาระสำคัญ พระราชบัญญัติธนาคารแห่งประเทศไทย**

**พุทธศักราช 2485.** ค้นวันที่ 3 พฤศจิกายน 2563 จาก <https://www.bot.or.th/Thai/AboutBOT/LawsAndRegulations/Documents/SUMLAW01.pdf>

ธนาคารแห่งประเทศไทย. **ธนบัตรแบบ 3.** ค้นวันที่ 12 พฤษภาคม 2563 จาก

[https://www.bot.or.th/Thai/Banknotes/HistoryAndSeriesOfBanknotes/Pages/Banknote\\_Series03.aspx](https://www.bot.or.th/Thai/Banknotes/HistoryAndSeriesOfBanknotes/Pages/Banknote_Series03.aspx)

ธนาคารแห่งประเทศไทย. **บทบาทหน้าที่ ธปท.** ค้นวันที่ 8 กรกฎาคม 2563 จาก

<https://www.bot.or.th/Thai/AboutBOT/RolesAndHistory/Pages/RolesAndResponsibility.aspx>

ธนาคารแห่งประเทศไทย. **วิวัฒนาการเงินตราไทย.** ค้นวันที่ 22 กันยายน 2562 จาก

[https://www.bot.or.th/Thai/Banknotes/HistoryAndSeriesOfBanknotes/Pages/Evolution\\_of\\_Thai\\_Banknotes.aspx](https://www.bot.or.th/Thai/Banknotes/HistoryAndSeriesOfBanknotes/Pages/Evolution_of_Thai_Banknotes.aspx)

ธนาคารแห่งประเทศไทย. **25 ปี โรงพิมพ์ธนบัตร 2512-2537.** กรุงเทพมหานคร: โรงพิมพ์ธนบัตรธนาคารแห่งประเทศไทย, 2537.

ธปท.เตือนประชาชนห้ามใช้เงินบิตคอยน์. **กรุงเทพธุรกิจออนไลน์.** (18 มีนาคม 2557). อ้างถึงใน กัทธพร สหกิจพิจารณ์. **ปัญหาการจัดเก็บภาษีเงินได้บุคคลธรรมดาจากบิตคอยน์: การรับรู้เงินได้.** วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ สาขาเศรษฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2559.

ธรรมรักษ์ หมื่นจักร; รัชพร วงศาโรจน์; กษิตติ์ ต้นสงวน และเกวลี สันตโยดม. FAQ

Cryptocurrencies and Friends: พัฒนาการ ความเสี่ยงและการกำกับดูแล. **Digital Currency Series.** 2 (7 มีนาคม 2563): 1.

นวรรตน์ เลชะกุล. **เบี้ย บาท กษาปณ์ แบงก์.** กรุงเทพมหานคร: สารคดี, 2542.

นันทน์ภัส พูลเพิ่ม. **ผลกระทบจากการทำธุรกรรมเกี่ยวกับคริปโตเคอร์เรนซี: กรณีศึกษาธุรกรรมซื้อขาย.** วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ สาขาเศรษฐศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2560.

บัญญัติ สุชีวะ. **คำอธิบายประมวลกฎหมายแพ่งและพาณิชย์ว่าด้วยทรัพย์.** กรุงเทพมหานคร: โรงพิมพ์มหาวิทยาลัยรามคำแหง, 2514.

ปกป้อง ศรีสนิท. **กฎหมายอาญาขั้นสูง.** พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: วิญญูชน, 2563.

ประธาน วัฒนวาณิชย์. การปฏิรูประบบการลงโทษ แนวทางสหวิทยาการโดยเน้นทางด้านอาชญาวิทยา. **บทบัณฑิตย.** 54, 4 (ธันวาคม 2541): 12.

ปาริชาติ มั่นสกุล. **การกำหนดมาตรการทางอาญาเกี่ยวกับการโจมตีค่าเงินบาท.** วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ สาขาเศรษฐศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2546.

- พงศ์บวร ควะชาติ. **สกุลเงินเสมือนจริงปลอดภัยการควบคุมบนเครือข่ายอินเทอร์เน็ต**. วิทยานิพนธ์  
ปริญญาโทบริหารธุรกิจ สาขาบริหารธุรกิจ คณะบริหารศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2558.
- พรชัย บุญบวรรัตนกุล. **การศึกษารูปแบบและการควบคุมการใช้เครือข่ายระบบเงินดิจิทัลเพื่อ  
ป้องกันการฟอกเงิน**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ สาขาบริหารศาสตร์  
มหาวิทยาลัยธรรมศาสตร์, 2561.
- พรเพชร วิชิตชลชัย. **คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ.  
2550**. กรุงเทพมหานคร: สำนักงานศาลยุติธรรม, 2550.
- พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561. **ราชกิจจานุเบกษา**. 135, 33ก (13  
พฤษภาคม 2561).
- พระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19) พ.ศ. 2561. **ราชกิจจานุเบกษา**. 135, 33  
ก (13 พฤษภาคม 2561).
- พระราชบัญญัติการป้องกันและปราบปรามการฟอกเงิน พ.ศ. 2542. **ราชกิจจานุเบกษา**. 116, 29ก  
(21 เมษายน 2542).
- พระราชบัญญัติแก้ไขเพิ่มเติมประมวลกฎหมายอาญา (ฉบับที่ 18) พ.ศ. 2550. **ราชกิจจานุเบกษา**.  
124, 42 ก (15 สิงหาคม 2550).
- พระราชบัญญัติควบคุมการแลกเปลี่ยนเงิน พ.ศ. 2485. **ราชกิจจานุเบกษา**. 59, 7 (1 กุมภาพันธ์  
2485).
- พระราชบัญญัติเงินตรา พ.ศ. 2471. **ราชกิจจานุเบกษา**. 45 (15 เมษายน 2471).
- พระราชบัญญัติเงินตรา พ.ศ. 2501. **ราชกิจจานุเบกษา**. 75, 65 (26 สิงหาคม 2501).
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ พ.ศ. 2544. **ราชกิจจานุเบกษา**. 118, 112ก (4  
ธันวาคม 2544).
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 2) พ.ศ. 2551. **ราชกิจจานุเบกษา**. 125,  
33ก (13 กุมภาพันธ์ 2551).
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 3) พ.ศ. 2562. **ราชกิจจานุเบกษา**. 136,  
49ก (14 เมษายน 2562).
- พระราชบัญญัติว่าด้วยธุรกรรมทางอิเล็กทรอนิกส์ (ฉบับที่ 4) พ.ศ. 2562. **ราชกิจจานุเบกษา**. 136,  
67ก (22 พฤษภาคม 2562).
- พินัย ฌ นคร. **กฎหมายเกี่ยวกับธุรกรรมทางอิเล็กทรอนิกส์ในยุคดิจิทัล**. กรุงเทพมหานคร: วิญญูชน,  
2561.
- ภัทรพร สหกิจพิจารณ์. **ปัญหาการจัดเก็บภาษีเงินได้บุคคลธรรมดาจากบิตคอยน์: การรับรู้เงินได้**.  
วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ สาขาบริหารศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2559.

มูลนิธิอนุรักษ์โบราณสถานในพระราชวังเดิมพระราชวังเดิม. **เงินตราโบราณของไทย**. ค้นวันที่ 22 กันยายน 2563 จาก [http://www.wangdermpalace.org/Pod%20Duang%20Money\\_th.html](http://www.wangdermpalace.org/Pod%20Duang%20Money_th.html)

เมธี กุศลสร้าง. **กฎหมายป้องกันและปราบปรามการฟอกเงินกับบทบาทและภาระหน้าที่ของสถาบันการเงิน**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ สาขาบริหารธุรกิจ คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2539.

เมธี ดุยจินดา. **วิวัฒนาการของระบบธนาคารของโลก**. กรุงเทพมหานคร: ดวงกมล, 2519.

ราชบัณฑิตยสถาน. **พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554**. พิมพ์ครั้งที่ 2.

กรุงเทพมหานคร: นานมีบุ๊คส์, 2556.

ลาวัญญ์ ถนัดศิลป์กุล; วิมาน กฤตพลวิมาน; จตุรงค์ บุญยรัตนสุนทร; ชูเกียรติ น้อยฉิม และชนันภรณ์ บุญเกิดทรัพย์. **การศึกษา วิเคราะห์ และแนวทางในการแก้ไขปัญหาการค้ามนุษย์ในมิติกฎหมายของประเทศในพื้นที่ระเบียงเศรษฐกิจตะวันออก – ตะวันตก, เหนือ – ใต้ (EWEC – NSEC – SEC)**. กรุงเทพมหานคร: สำนักงานคณะกรรมการส่งเสริมวิทยาศาสตร์ วิจัยและนวัตกรรม, 2561.

ลีตาร์, เบอร์นาร์ด. **เงินตราแห่งอนาคต: วิถีใหม่สู่การรังสรรค์ความมั่งคั่ง งาน และโลกอันชาญฉลาด**. แปลโดย จินตลา วิเศษกุล. กรุงเทพมหานคร: สวนเงินมีมา, 2547.

วสุ สุวรรณวิท. **ระบบมาตรฐานทองคำ**. ค้นวันที่ 7 พฤษภาคม 2563 จาก

<https://www.stou.ac.th/stouonline/LOM/data/sec/Lom20/01-01.html>

วารี พงษ์เวช. **การเงินและการธนาคาร**. กรุงเทพมหานคร: อุตสาหกรรมกรรมการพิมพ์, 2502.

วินัย แทนประเสริฐกุล. **ความสมบูรณ์ของระบบการชำระเงิน: ศึกษากรณีผลกระทบที่เกิดขึ้นจากหลักการนับเวลาที่ศูนย์นาฬิกา**. วิทยานิพนธ์ปริญญาโทบริหารธุรกิจ สาขาบริหารธุรกิจ มหาวิทยาลัยธรรมศาสตร์, 2547.

วิริยะ นามศิริพงศ์พันธ์. **เอกสารประกอบการสอนวิชากฎหมายลักษณะทรัพย์**. กรุงเทพมหานคร: คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2524.

วิโรจน์ กลั่นเปา. **เรื่องของเงินและธนาคาร**. กรุงเทพมหานคร: เคล็ดไทย, 2517.

ศิริพล กุศลศิลป์วุฒิ. **กฎหมายอาชญากรรมทางเศรษฐกิจของประเทศสหรัฐอเมริกา**.

ค้นวันที่ 24 มีนาคม 2564 จาก <https://siriphonku.wordpress.com/2008/08/27/กฎหมายอาชญากรรมทางเศรษฐกิจ/>

ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย. **รายงานโครงการศึกษาเรื่องการบังคับคดีกับสินทรัพย์ดิจิทัล**. กรุงเทพมหานคร: ศูนย์วิจัยกฎหมายและการพัฒนา คณะนิติศาสตร์ จุฬาลงกรณ์มหาวิทยาลัย, 2561.

สกล นิคาร์ตัน. **กฎหมายอาญาและการลงโทษที่เหมาะสม: แนวความคิดทางด้านปรัชญาและความยุติธรรมทางสังคม.** วิทยานิพนธ์ปริญญาโทมหาบัณฑิต คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2545.

สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน). **บทบาท TIJ ในการประชุม Crime Congress 2021.** ค้นวันที่ 11 เมษายน 2564 จาก <https://www.tijthailand.org/th/highlight/detail/tij-s-role-in-crime-congress-2020>

สถาบันเพื่อการยุติธรรมแห่งประเทศไทย (องค์การมหาชน). **เมื่ออาชญากรรมไร้พรมแดน.** ค้นวันที่ 2 พฤษภาคม 2565 จาก <https://tijacademy.org/2022/01/3030/เมื่ออาชญากรรมไร้พรมแดน>

สภานิติบัญญัติแห่งชาติ. **เอกสารประกอบการพิจารณา ร่างพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ (ฉบับที่...) พ.ศ.... (คณะรัฐมนตรีเป็นผู้เสนอ) อ.พ28/2559.** (เอกสารไม่ตีพิมพ์เผยแพร่)

สรารุช ปิตยาศักดิ์. **คำอธิบายพระราชบัญญัติว่าด้วยการกระทำความผิดเกี่ยวกับคอมพิวเตอร์ พ.ศ. 2550 และ (ฉบับที่ 2) พ.ศ. 2560.** พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: นิติธรรม, 2561.

สาวตรี สุขศรี. **กฎหมายว่าด้วยอาชญากรรมคอมพิวเตอร์และอาชญากรรมไซเบอร์.** กรุงเทพมหานคร: โครงการตำราและเอกสารประกอบการสอน คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2563.

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. **ก.ล.ต.กล่าวโทษกรรมการผู้จัดการหรือบุคคลที่ได้รับมอบหมายให้เก็บรักษา Private Key ของ BX พร้อมแจ้งเบาะแสบุคคลที่อาจเข้าข่ายเป็นผู้กระทำความผิด กรณีโอนสินทรัพย์ดิจิทัลของลูกค้ำที่อยู่ในความดูแลหรือครอบครองของ BX ออกไปยัง Wallet ที่ไม่ได้มีไว้เพื่อเก็บสินทรัพย์ดิจิทัลของลูกค้ำ.** ค้นวันที่ 14 มกราคม 2564 จาก [https://www.sec.or.th/TH/Pages/News\\_Detail.aspx?SECID=8695](https://www.sec.or.th/TH/Pages/News_Detail.aspx?SECID=8695)

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. **ก.ล.ต. ใช้มาตรการลงโทษทางแพ่งกับผู้กระทำความผิด 3 ราย กรณีสร้างปริมาณเทียมสินทรัพย์ดิจิทัลจำนวน 18 เหรียญในศูนย์ซื้อขายสินทรัพย์ดิจิทัลของบริษัท บิทคับ ออนไลน์ จำกัด.** ค้นวันที่ 30 ธันวาคม 2565 จาก [https://www.sec.or.th/TH/Pages/News\\_Detail.aspx?SECID=9793&NewsNo=9793&NewsYear=9793&Lang=9793](https://www.sec.or.th/TH/Pages/News_Detail.aspx?SECID=9793&NewsNo=9793&NewsYear=9793&Lang=9793)

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. **ก.ล.ต. ใช้มาตรการลงโทษทางแพ่งกับผู้กระทำความผิด 4 ราย กรณีสร้างปริมาณเทียมสินทรัพย์ดิจิทัลจำนวน 3 เหรียญ**

ในศูนย์ซื้อขายสินทรัพย์ดิจิทัลของบริษัท สตางค์ คอร์ปอเรชั่น จำกัด.

เมื่อวันที่ 30 ธันวาคม 2565 จาก [https://www.sec.or.th/TH/Pages/News\\_Detail.aspx?SECID=9794&NewsNo=9794&NewsYear=9794&Lang=9794](https://www.sec.or.th/TH/Pages/News_Detail.aspx?SECID=9794&NewsNo=9794&NewsYear=9794&Lang=9794)

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. ก.ล.ต. ออกเกณฑ์กำกับการให้บริการ

ของผู้ประกอบการธุรกิจสินทรัพย์ดิจิทัล ไม่สนับสนุนการใช้สินทรัพย์ดิจิทัลเป็นสื่อกลาง.

เมื่อวันที่ 5 มกราคม 2565 จาก [https://www.sec.or.th/TH/Pages/News\\_Detail.aspx?SECID=9353](https://www.sec.or.th/TH/Pages/News_Detail.aspx?SECID=9353)

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. ผู้ประกอบธุรกิจที่ได้รับใบอนุญาต

นายหน้าสินทรัพย์ดิจิทัล (Digital Asset Broker). เมื่อวันที่ 25 กุมภาพันธ์ 2563 จาก

<https://www.sec.or.th/TH/Pages/LawandRegulations/DigitalAssetBusiness.aspx>

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. ผู้ประกอบธุรกิจที่ได้รับใบอนุญาต

ศูนย์ซื้อขายสินทรัพย์ดิจิทัล. เมื่อวันที่ 25 พฤษภาคม 2564 จาก

<https://www.sec.or.th/digitalasset#EBD>

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. ผู้ประกอบธุรกิจที่ได้รับใบอนุญาต

ศูนย์ซื้อขายสินทรัพย์ดิจิทัล. เมื่อวันที่ 25 พฤษภาคม 2564 จาก

<https://www.sec.or.th/digitalasset#K>

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. ผู้ประกอบธุรกิจที่ได้รับใบอนุญาต

ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Digital Asset Exchange). เมื่อวันที่ 2 มิถุนายน 2564 จาก

<https://www.sec.or.th/digitalasset#K>

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. ผู้ประกอบธุรกิจสินทรัพย์ดิจิทัล. วันที่

2 มิถุนายน 2564 จาก <https://www.sec.or.th/TH/pages/lawandregulations/digitalassetbusiness.aspx>

สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์. สรุปสาระสำคัญของพระราช

กำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล. กรุงเทพมหานคร: สำนักงานคณะกรรมการ

กำกับหลักทรัพย์และตลาดหลักทรัพย์, 2561. เมื่อวันที่ 4 สิงหาคม 2562 จาก

[https://www.sec.or.th/TH/Documents/DigitalAsset/digitalasset\\_summary.pdf](https://www.sec.or.th/TH/Documents/DigitalAsset/digitalasset_summary.pdf)

สำนักงานป้องกันและปราบปรามการฟอกเงิน. ความเป็นมาและวัตถุประสงค์. เมื่อวันที่ 11 เมษายน

2564 จาก <https://www.amlo.go.th/index.php/th/designated-person/2016-05-22-11-51-34>

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. สถานการณ์ Cryptocurrency ของประเทศไทย.

เมื่อวันที่ 25 เมษายน 2563 จาก <https://www.eta.or.th/th/Useful-Resource/knowledge-sharing/articles/index-article-other-p1/สถานการณ์-Cryptocurrency-ของประเทศไทย.aspx>

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. สถานการณ์ Cryptocurrency ของประเทศไทย.

เมื่อวันที่ 25 เมษายน 2563 จาก <https://www.eta.or.th/th/Useful-Resource/knowledge-sharing/articles/index-article-other-p1/สถานการณ์-Cryptocurrency-ของประเทศไทย.aspx>

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์. สถานการณ์ Cryptocurrency ของประเทศไทย.

เมื่อวันที่ 25 เมษายน 2563 จาก <https://www.eta.or.th/th/Useful-Resource/knowledge-sharing/articles/index-article-other-p1/สถานการณ์-Cryptocurrency-ของประเทศไทย.aspx>

- สำนักงานส่งเสริมเศรษฐกิจดิจิทัล. **เทคโนโลยีที่สำคัญในยุคดิจิทัล: รู้จักกับเงินสกุลดิจิทัล Getting to Know Cryptocurrency.** ค้นวันที่ 25 เมษายน 2663 จาก <https://www.depa.or.th/th/article-view/article-getting-know-cryptocurrency>
- สำนักบริหารเงินตรา. **เหรียญในรัชกาลปัจจุบัน.** ค้นวันที่ 7 พฤษภาคม 2563 จาก <https://www.treasury.go.th/th/medal-in-the-present-reign/>
- สุรสิทธิ์ แสงวิโรจน์พัฒน์. การกำหนดความผิดอาญาตามกฎหมายเยอรมัน. **ข่าวเนติบัณฑิตยสภา.** 16, 192 (กรกฎาคม 2548): 11-12.
- เสนีย์ ปราโมช, ม.ร.ว. **อธิบายประมวลกฎหมายแพ่งและพาณิชย์ กฎหมายลักษณะทรัพย์.** กรุงเทพมหานคร: โรงพิมพ์อักษรสาส์น, 2521.
- หยุด แสงอุทัย. **กฎหมายอาญา ภาค 1.** พิมพ์ครั้งที่ 21. กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2556.
- หยุด แสงอุทัย. **กฎหมายอาญา ภาค 2-3.** กรุงเทพมหานคร: สำนักพิมพ์มหาวิทยาลัยธรรมศาสตร์, 2553.
- อภิรัตน์ เพ็ชรศิริ. **ทฤษฎีอาญา.** พิมพ์ครั้งที่ 3. กรุงเทพมหานคร: วิญญูชน, 2556.
- อมราวดี อังคสุวรรณ. กฎหมายอาญาและอำนาจรัฐในการรักษาความสงบเรียบร้อยของสังคม. **วารสารกฎหมาย.** 2, 12 (ตุลาคม 2531): 112.
- อริยพร โพธิ์ใส. การกระทำผิดต่อศพ: ปัญหาที่รอการแก้ไข. **จลนิตี.** (มกราคม-กุมภาพันธ์ 2558).
- อัจฉรา หล่อตระกูล. เงิน: ความหมายและความสำคัญ. **วารสารวิจัยราชภัฏกรุงเทพฯ.** 2, 1 (มกราคม 2558).
- อัญญา ชันธวิทย์. **กลไกตลาดการเงินในระบบเศรษฐกิจไทย: ตลาดหลักทรัพย์แห่งประเทศไทย พ.ศ. 2546.** พิมพ์ครั้งที่ 2. กรุงเทพมหานคร: ตลาดหลักทรัพย์แห่งประเทศไทย, 2546.
- A \$568 Million Hack of Binance Coin Roils Crypto Sector Anew.** Retrieved December 31, 2022 from <https://www.bloomberg.com/news/articles/2022-10-06/bnb-chain-says-bsc-temporarily-paused-on-irregular-activity>
- Adler, Jason. **Protecting your Devices from Cryptojacking.** Retrieved April 11, 2021 from <https://www.consumer.ftc.gov/blog/2018/06/protecting-your-devices-cryptojacking>
- Admin Intrend. **ย้อนรอยประวัติศาสตร์ 5 อันดับการแฮ็คคริปโตที่ปริมาณมากที่สุดในโลก.** ค้นวันที่ 25 พฤศจิกายน 2565 จาก <https://cryptointrend.com/top-5-biggest-crypto-exchange-heists-in-history/>

- Alkadri, Susan. Defining and Regulating Cryptocurrency: Fake Internet Money or Legitimate Medium of Exchange?. **Duke Law & Technology Review**. 17, 1 (December 2018): 71-98.
- Ashworth, Andrew. **Principles of Criminal Law**. 5<sup>th</sup> ed. Oxford: Oxford University Press, 2006.
- Bains, Parma, Ismail, Arif, Melo, Fabiana, and Sugimoto, Nobuyasu. **Regulating the Crypto Ecosystem the Case of Unbacked Crypto Assets**. Washington: International Monetary Fund, 2022.
- Ball, Laurence M. **Money, Banking and Financial Markets**. New York: Worth Publishers, 2009.
- Bambrough, Billy. Exclusive: Leak Reveals Surprising Reason Major Bitcoin Exchange Luno Is Adding Ripple's XRP. **Forbes**. (28 March 2020). Retrieved May 15, 2020 from <https://www.forbes.com/sites/billybambrough/2020/02/28/exclusive-leak-reveals-surprising-reason-major-bitcoin-exchange-luno-is-adding-ripples-xrp/#434f2e8f4de4>
- Basel Institute on Governance. **Thousands Gather Virtually to Share Knowledge of Virtual Assets-based Money Laundering and Other Crypto-enabled Crimes**. Retrieved July 17, 2021 from <https://baselgovernance.org/news/5CrC>
- Basen, Stanley M. **Introduction to Monetary Economics**. New York: Harper & Row, 1993.
- Bitcoin Mining. **Best Bitcoin Cloud Mining Contract Reviews and Comparisons**. Retrieved April 16, 2020 from <https://www.bitcoinmining.com/best-bitcoin-cloud-mining-contract-reviews/>
- Burniske, Chris and Tatar, Jack. **Cryptoassets: The Innovative Investor's Guide to Bitcoin and Beyond**. New York: McGraw-Hill, 2017.
- Carlin, Domhnall; Burgess, Jonah; OKane, Philip and Sezer, Sakir. You could be Mine(d): The Rise of Cryptojacking. **IEEE Security & Privacy Magazine**. 99 (2019): 1.
- Castronova, Edward. **The Price of 'Man' and 'Woman': A Hedonic Pricing Model of Avatar Attributes in a Synthetic World**. (June 2003). Retrieved November 26, 2019 from <https://ssrn.com/abstract=415043>

Chinhengo, Austin M. **Essential Jurisprudence**. London: Cavendish Publishing Limited, 1995.

Chiu, Jonathan and Koepl, Thorsten V. **The Economics of Cryptocurrencies-Bitcoin and Beyond**. Ontario, Bank of Canada, 2018.

Chromium Blog. **Protecting Users from Extension Cryptojacking**. Retrieved June 7, 2021 from <https://blog.chromium.org/2018/04/protecting-users-from-extension-cryptojacking.html>

CNBC. **El Salvador Looks to Become the World's First Country to Adopt Bitcoin as Legal Tender**. Retrieved June 7, 2021 from <https://www.cnn.com/2021/06/05/el-salvador-becomes-the-first-country-to-adopt-bitcoin-as-legal-tender.html>

Corporate Finance Institute. **Wire Fraud**. Retrieved January 12, 2021 from <https://corporatefinanceinstitute.com/resources/knowledge/other/wire-fraud/>

Council of Europe. **Chart of Signatures and Ratifications of Treaty 185**. Retrieved April 11, 2021 from <https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatyid=185>

Cryptocurrency Prices. **Charts and Market Capitalizations**. Retrieved December 31, 2022 from <https://coinmarketcap.com/>

**Customer Advisory: Understand the Risks of Virtual Currency Trading**. Retrieved July 17, 2021 from [https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory\\_urvct121517.pdf](https://www.cftc.gov/sites/default/files/idc/groups/public/@customerprotection/documents/file/customeradvisory_urvct121517.pdf)

Diamond, Chirs. The History of Money and Banking No One Ever Told You. **Economic History Report**. (June 13, 2014). Retrieved May 8, 2020 from <https://www.scribd.com/book/229908625/The-History-Of-Money-and-Banking-No-One-Ever-Told-You-Economic-History-Report>

Douglas, Laura. **The Virtual Currency Regulation Review: United Kingdom**. Retrieved November 27, 2021 from <https://thelawreviews.co.uk/title/the-virtual-currency-regulation-review/united-kingdom>

The Fast Code. **Cryptojacking คืออะไรและคุณจะสามารถป้องกันตัวเองได้อย่างไร?** คำนวณที่ 14

มกราคม 2564 จาก <https://www.thefastcode.com/th-thb/article/what-is-cryptojacking-and-how-can-you-protect-yourself>

Ffrench, Andrew. **Gang Targeting Bitcoin Traders Fled Empty-handed**. Retrieved March 12, 2021 from <https://www.oxfordmail.co.uk/news/15907000.gangtargeting-bitcoin-traders-fled-empty-handed/>

Financial Action Task Force. **Virtual Currencies: Key Definitions and Potential AML/CFT Risks**. Paris, France: FATF, 2014. Retrieved September 22, 2019 from <http://www.fatf-gafi.org/publications/methodsandtrends/documents/virtual-currency-definitions-aml-cft-risk.html>

Financial Conduct Authority. **Guidance on Cryptoassets: Feedback and Final Guidance to CP 19/3**. Retrieved July 18, 2022 from <https://www.fca.org.uk/publication/policy/ps19-22.pdf>

**FTX Has Been Hacked': Crypto Disaster Worsens as Exchange Sees Mysterious Outflows Exceeding \$600M**. Retrieved December 30, 2022 from <https://www.coindesk.com/business/2022/11/12/ftx-crypto-wallets-see-mysterious-late-night-outflows-totalling-more-than-380m/>

Galbraith, John Kenneth and Galbraith, James K. **Money: Whence it came, where it went**. Princeton: Princeton University Press, 2017.

Galluzzo, Matthew J. **Federal Wire Fraud Charges (18 USC 1343 and 1349)**. Retrieved January 12, 2021 from <https://www.gjllp.com/news/federal-wire-fraud-charges-18-usc-1343-and-1349/>

The Guardian. **Bitcoin Worth £900,000 Seized from Hacker to Compensate Victims**. Retrieved March 4, 2021 from <https://www.theguardian.com/technology/2019/aug/23/bitcoin-seized-hacker-grant-west-uk-compensate-victims>

Guo, Yuanjing and Dong, Tommy. **Several Cryptojacking Apps Found on Microsoft Store**. Retrieved May 19, 2021 from <https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/cryptojacking-apps-microsoft-store>

Harfst, Gerold. **German Criminal Law**. Germany: Rosch-Buch Scheblitz, 1998.

Husak, Douglas. **Overcriminalization: The Limits of the Criminal Law**. Oxford: Oxford

University Press, 2008.

**In the High Court of Justice Business & Property Courts of England and Wales**

**Commercial Court (QBD).** Retrieved January 1, 2023 from

<https://www.judiciary.uk/wp-content/uploads/2020/02/AA-v-Persons-Unknown-summary-case-note-SB-amended.pdf>

Interpol. **Cryptojacking Makes Money for Criminal Monitor your Device's**

**Performance and Power Use.** Retrieved January 12, 2021 from

<https://www.interpol.int/en/Crimes/Cybercrime/Cryptojacking>

Interpol. **Interpol: An Overview.** Retrieved April 11, 2021 from

<https://www.interpol.int/en/Who-we-are/What-is-INTERPOL>

Interpol. **We have 194 Member Countries; Together they Create a Truly Global**

**Network of Police.** Retrieved April 11, 2021 from

<https://www.interpol.int/en/Who-we-are/Member-countries>

Jeerichuda. **นักเทรด Bitcoin บนเว็บเทรดไทยแห่งหนึ่งเผยถูกแฮค ชุมชนคาดเป็นความผิดพลาด  
ผู้ใช้งานมากกว่า.** ค้นวันที่ 7 พฤษภาคม 2563 จาก

<https://siamblockchain.com/2020/04/22/user-on-bitkub-was-hacked-lost-8000-thb/>

Jefferson, Michael. **Criminal Law.** 8<sup>th</sup> ed. London: Pearson Education, 2007.

Jessel, Ben. What Stellar's Investment in Abra Means for the 'Robinhood of  
Cryptocurrency.' **Forbes.** (6 May 2020). Retrieved May 23, 2020 from

<https://www.forbes.com/sites/benjessel/2020/05/06/what-stellars-investment-in-abra-means-for-the-robinhood-of-cryptocurrency/#50159a0fd155>

Keatinge, Tom; Carlisle, David and Keen, Florence. **Virtual Currencies and Terrorist  
Financing: Assessing the Risks and Evaluating Responses.** Washington:

European Parliament, 2018. Retrieved September 22, 2019 from

[https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL\\_S\\_TU\(2018\)604970\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_S_TU(2018)604970_EN.pdf)

Kethineni, Sessa, Cao, Ying and Dodge, Cassandra. Use of Bitcoin in Darknet Market:

Examining Facilitative Factors on Bitcoin-Related Crimes. **American Journal  
of Criminal Justice.** 43 (2018): 141-157.

Kodysova, Petra and Kasty, Miroslav. **Combating Cryptomarkets: Cross-Border Cooperation and Investigation.** N.P.: n.p., 2018.

Krone, Mark J.; Lukes, Emily M. and McKibbin, Chris. Tales from the Crypt: Cryptocurrency is here--how will Crime Insurers Respond?. **Fidelity Law Journal.** 24 (November 2018): 1-83.

Lake, Josh. **What is Cryptojacking (With Examples) and How do you Stop it?** Retrieved May 16, 2021 from [https://www.comparitech.com/blog/informationsecurity/cryptojacking/#Other\\_examples\\_of\\_cryptojacking](https://www.comparitech.com/blog/informationsecurity/cryptojacking/#Other_examples_of_cryptojacking)

Lansky, Jan. Possible State Approaches to Cryptocurrencies. **Journal of Systems Integration.** 9, 1 (January 2018): 19-31.

The Law Library of Congress. **Regulation of Cryptocurrency Around the World.** Retrieved November 26, 2019 from <https://www.loc.gov/law/help/cryptocurrency/cryptocurrency-world-survey.pdf>

Marr, Bernard. Bitcoin and Litecoin-What's The Difference?. **Forbes.** (21 March 2018). Retrieved December 23, 2020 from <https://www.forbes.com/sites/bernardmarr/018/03/21/bitcoin-and-litecoin-whats-the-difference/#758bd0d05664>

McAfee. **McAfee Labs Threats Report'2018.** Retrieved July 5, 2021 from <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-jun2018.pdf>

McKinney, Jr., Ralph E.; Baker, Casey W.; Shao, Lawrence P. and Forrest, Jeff Y. L., Cryptocurrency: Utility Determines Conceptual Classification Despite Regulatory Uncertainty. **USF Intellectual Property and Technology Law Journal.** 25, 1 (Fall 2020): 1-18.

McLeod, Patrick. Taxing and Regulation Bitcoin: The Government's Game of Catch Up. **Common Law Conspectus.** 22 (2014): 389.

Merza, Janet. **Money: from Barter to Online Banking.** USA: Squirrelstore, 2015.

Nakamoto, Satoshi. **Bitcoin: A Peer-to-Peer Electronic Cash System.** Retrieved October 18, 2020 from [https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging\\_Tech\\_Bitcoin\\_Crypto.pdf](https://www.ussc.gov/sites/default/files/pdf/training/annual-national-training-seminar/2018/Emerging_Tech_Bitcoin_Crypto.pdf)

**Notice 2014-21.** Retrieved July 17, 2021 from <https://www.irs.gov/pub/irs-drop/n-14-21.pdf>

The Open Government Licence. **Cryptoassets Taskforce: Final Report.** Retrieved March 3, 2021 from [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/752070/cryptoassets\\_taskforce\\_final\\_report\\_final\\_web.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/752070/cryptoassets_taskforce_final_report_final_web.pdf)

Organization of Economic Co-operation and Development (OECD). **The OECD Definitions of Internet and E-commerce Transactions.** Retrieved July 18, 2021 from <https://www.oecd.org/internet/ieconomy/2771174.pdf>

Ormerod, David. **Criminal Law.** 13<sup>th</sup> ed. New York: Oxford University Press, 2011.

Packer, Herbert L. **The Limits of the Criminal Sanction.** California: Stanford University Press, 1968.

Packer, Herbert L. Two Models of the Criminal Process. **University of Pennsylvania Law Review.** 113, 1 (November 1964): 1-68.

Partz, Helen. **Bitcoin and ETH Are Commodities, While XRP's Status Is Unclear, CFTC Says.** Retrieved July 17, 2021 from <https://cointelegraph.com/news/bitcoin-and-eth-are-commodities-while-xrps-status-is-unclear-cftc-says>

Prosecuting Cryptocurrency Theft with the Defend Trade Secrets Act of 2016.

**University of Pennsylvania Law Review.** 167 (2018): 239-259.

Pyskell. Ethereum and Ethereum Classic: What's the difference?. **Ethereum Classic News.** Retrieved May 2, 2020 from <https://medium.com/@pyskell/ethereum-and-classic-e0102dead543>

Ravelli, Rahman. **Cryptocurrency: Theft and Asset Recovery.** Retrieved April 5, 2021 from <https://www.lexology.com/library/detail.aspx?g=db7e8959-b309-4495-8b3e-200124dd07fb>

Samuelson, Paul A. **Economics.** 11<sup>st</sup> ed. New York: McGraw-Hill, 1980.

Sarmaha, Joel. **Criminal Law.** 11<sup>th</sup> ed. Belmont, CA: Wadsworth Learning, 2014.

**Securities and Exchange Commission Securities Exchange Act of 1934.** Retrieved July 17, 2021 from <https://www.sec.gov/litigation/investreport/34-81207.pdf>

Sloan, William M. Mail and Wire Fraud. **American Criminal Law Review.** 48, 2 (Spring 2011): 906-928.

- SonicWall. **Cryptojacking Reaches Record High**. Retrieved December 31, 2022 from <https://www.sonicwall.com/2022-cyber-threat-report/>
- Stark, Josh and Van Ness, Evan. **“The Year in Ethereum 2019” in Ethereum Guides & Resources**. Retrieved March 6, 2020 from <https://ethereum.org/what-is-ethereum/>
- Statista. **Number of Cryptocurrencies Worldwide from 2013 to 2021**. Retrieved July 25, 2021 from <https://www.statista.com/statistics/863917/number-crypto-coins-tokens/>
- Taylor, Alex and O’Flynn, Micheal. Bitcoin Burglaries and the Theft Act 1968. **Criminal Law Review**. 3 (2021): 163-190.
- Treasury Financial Crimes Enforcement Network. **Application of Fincen’s Regulations to Persons Administering, Exchanging, or Using Virtual Currencies**. Retrieved September 22, 2019 from <https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering>
- Thailand-option Team. **สกุลเงินเสมือนคืออะไร? คำนวณที่ 3 กุมภาพันธ์ 2563** จาก <https://thailand-option.com/cryptocurrency/>
- Thanon. **อัปเดตรายชื่อผู้ประกอบการในไทยที่เปิดรับ Bitcoin**. คำนวณที่ 7 พฤษภาคม 2563 จาก <https://siamblockchain.com/2021/04/01/entrepreneurs-name-list-in-thailand-accepting-bitcoin/>
- Timberlake, Jr., Richard H. and Dowd, Kenvin. Eds. **Money and the Nation State: The Financial Revolution, Government, and the World Monetary System**. U.S.A: Transaction Publishers, 1998.
- Titanium. **Monitoring the Dark Web**. Retrieved July 17, 2021 from <https://www.titanium-project.eu/news/articles/darkwebmonitor1/>
- Titanium. **Titanium Project**. Retrieved July 17, 2021 from <https://www.titanium-project.eu/>
- Titanium. **TITANIUM Tool Cointel: Cryptocurrency Analytics Functionality**. Retrieved July 17, 2021 from <https://www.titanium-project.eu/news/articles/cointel1/>
- Titanium. **TITANIUM Tool Dence Wallet Investigator**. Retrieved July 17, 2021 from

- [https://www.titanium-project.eu/news/articles/wallet\\_investigator/](https://www.titanium-project.eu/news/articles/wallet_investigator/)  
Titanium. **TITANIUM Tool GraphSense**. Retrieved July 17, 2021 from  
<https://www.titanium-project.eu/news/articles/graphsense1/>
- UK Jurisdiction Taskforce. **Legal Statement on Cryptoassets and Smart Contracts**.  
London: The LawTech Delivery Panel, 2009. Retrieved December 28, 2021  
from [https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056\\_JO\\_Cryptocurrencies\\_Statement\\_FINAL\\_WEB\\_111119-1.pdf](https://35z8e83m1ih83drye280o9d1-wpengine.netdna-ssl.com/wp-content/uploads/2019/11/6.6056_JO_Cryptocurrencies_Statement_FINAL_WEB_111119-1.pdf)
- United Nations. **Asia and Pacific Regional Preparatory Meeting for the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice Bangkok, 22-24 January 2019**. Retrieved April 11, 2021 from  
[https://www.unodc.org/documents/congress//Documentation\\_14th\\_Congress/RPM1Asia/ACONF234\\_RPM1\\_L1\\_AP\\_e.pdf](https://www.unodc.org/documents/congress//Documentation_14th_Congress/RPM1Asia/ACONF234_RPM1_L1_AP_e.pdf)
- United Nations. **Fourteenth United Nations Congress on Crime Prevention and Criminal Justice Kyoto, Japan, 20-27 April 2020: Discussion Guide**.  
Retrieved April 11, 2021 from [https://www.unodc.org/documents/congress//Documentation\\_14th\\_Congress/DiscussionGuide/A\\_CONF234\\_PM1\\_e\\_V1806329.pdf](https://www.unodc.org/documents/congress//Documentation_14th_Congress/DiscussionGuide/A_CONF234_PM1_e_V1806329.pdf)
- United Nations. **UNODC Delivered the Cryptocurrencies and Darknet Investigations Training Course**. Retrieved May 2, 2022 from  
<https://www.unodc.org/roseap/en/2022/02/cryptocurrencies-darknet-investigations/story.html>
- United Nations. **Workshop 4. Current Crime Trends, Recent Developments and Emerging Solutions, in Particular New Technologies as Means for and Tools against Crime, Background paper prepared by the Secretariat**.  
Retrieved January 5, 2023 from <https://documents-dds-ny.un.org/doc/UNDOC/GEN/V20/005/48/PDF/V2000548.pdf?OpenElement>
- United Nations Office on Drugs and Crime. **Cryptocurrency Training Course**.  
Retrieved April 11, 2021 from <https://www.unodc.org/unodc/site-search.html?q=cryptocurrency+training+course>
- United Nations Office on Drugs and Crime. **Reference: CU 2018/450(A)/DTA0SGB**.

Retrieved April 11, 2021 from [https://www.unodc.org/documents/congress//Documentation\\_14th\\_Congress/RPM1Asia/CU\\_2018\\_450\\_A\\_English.pdf](https://www.unodc.org/documents/congress//Documentation_14th_Congress/RPM1Asia/CU_2018_450_A_English.pdf)

United Nations Office on Drugs and Crime. **UNODC Launches Training to Tackle Cryptocurrency-Enabled Organized Crime.** Retrieved April 11, 2021 from <https://www.unodc.org/unodc/en/frontpage/2017/May/unodc-launches-training-to-tackle-money-laundering-and-bitcoin-banking-fraud.html>

United Nations Office on Drugs and Crime. **UNODC Strategy 2021-2025.** Retrieved April 11, 2021 from <https://www.unodc.org/unodc/en/strategy/index.html>

The United States Attorney's Office, Eastern District of New York. **Defendant Sentenced to 86 Months in Prison for Defrauding Investors in Binary Options and Cryptocurrency Scheme.** Retrieved March 8, 2021 from <https://www.justice.gov/usao-edny/pr/defendant-sentenced-86-months-prison-defrauding-investors-binary-options-and>

The United States Attorney's Office, Northern District of Illinois. **Chicago Trader Facing Federal Fraud Charge for Allegedly Misappropriating \$2 Million in Cryptocurrencies.** Retrieved April 21, 2021 <https://www.justice.gov/usao-ndil/pr/chicago-trader-facing-federal-fraud-charge-allegedly-misappropriating-2-million>

The United States Attorney's Office, Western District of Washington. **Former Seattle Tech Worker Indicted on Federal Charges for Wire Fraud and Computer Data Theft.** Retrieved June 21, 2021 <https://www.justice.gov/usao-wdwa/pr/former-seattle-tech-worker-indicted-federal-charges-wire-fraud-and-computer-data-theft>

United States Department of Justice. **Attorney General's Cyber-Digital Task Force: Cryptocurrency: An Enforcement Framework 2020.** Retrieved November 28, 2020 from <https://www.justice.gov/archives/ag/page/file/1326061>

The United States Department of Justice. **Massachusetts Man Pleads Guilty to Operating Nationwide Scheme to Steal Social Media Accounts and Cryptocurrency.** Retrieved April 21, 2021 from <https://www.justice.gov/>

opa/pr/massachusetts-man-pleads-guilty-operating-nationwide-scheme-steal-social-media-accounts-and 9

The United States Department of Justice. **Russian Project Lakhta Member Charged with Wire Fraud Conspiracy.** Retrieved April 18, 2021 from <https://www.justice.gov/opa/pr/russian-project-lakhta-member-charged-wire-fraud-conspiracy>

Walker, Nigel. **Punishment, Danger and Stigma: The Morality of Criminal Justice.** New York: Basic Books, 1980. อ้างถึงใน ฅภัทร สรธัฒ. **ความเหมาะสมในการกำหนดความผิดและโทษทางอาญา: ศึกษากรณิกฎหมายการแข่งขันทางการค้า.** สารนิพนธ์ปริญญาโทบริหารธุรกิจ คณะนิติศาสตร์ มหาวิทยาลัยธรรมศาสตร์, 2548.

Wan, Tiffany and Hoblitzell, Max. **Bitcoin Fact. Fiction. Future.** Retrieved July 25, 2021 from <https://www2.deloitte.com/us/en/insights/topics/emerging-technologies/bitcoin-fact-fiction-future.html>

Winck, Ben. **One Cryptocurrency Investor Reportedly Lost \$24 Million Worth of Bitcoin in a SIM Swap Attack.** Retrieved March 12, 2021 from <https://markets.businessinsider.com/currencies/news/bitcoin-investor-loses-24-million-of-crypto-sim-swaphackers-2019-11-1028677818>

Wired. **UK Government Websites Were Caught Cryptomining. But it could have been a Lot Worse.** Retrieved December 31, 2022 from <https://www.wired.co.uk/article/browsealoud-ico-texthelp-cryptomining-how-cryptomining-work>

Zaytoun, Henry S. Cyber Pickpockets: Blockchain, Cryptocurrency, and the Law of Theft. **North Carolina Law Review.** 97, 2 (2019): 395-431.

## ประวัติผู้เขียน

ชื่อ-นามสกุล นางสาวพงศ์จิรา เชิดชู  
ประวัติการศึกษา นิติศาสตรบัณฑิต  
จุฬาลงกรณ์มหาวิทยาลัย  
ปีที่สำเร็จการศึกษา พ.ศ. 2545  
นิติศาสตรมหาบัณฑิต  
จุฬาลงกรณ์มหาวิทยาลัย  
ปีที่สำเร็จการศึกษา พ.ศ. 2553  
ประสบการณ์การทำงาน พ.ศ. 2553-ปัจจุบัน  
อาจารย์ประจำ  
สาขาวิชานิติศาสตร์  
มหาวิทยาลัยสุโขทัยธรรมาธิราช