บทเรียนจากทศวรรษแรกของคริปโทเคอร์เรนซี

Lessons from the First Decade of Cryptocurrencies

พรชัย ชุนหจินดา[1]

pchunhachinda@hotmail.com

บทคัดย่อ

นับตั้งแต่มีการเปิดเผยแนวคิดในการพัฒนาคริปโทเคอร์เรนซี[2]ชนิดแรก คือ บิทคอยน์ เมื่อปี พ.ศ. 2551 ตลอด 10 ปีที่ผ่านมา ความสนใจในนวัตกรรมนี้ค่อย ๆ ขยายวงจากกลุ่มนักพัฒนาไปสู่ประชาชนทั่วไป โดยการยอมรับ และใช้งานได้เพิ่มมากขึ้นตามลำดับ จากการใช้เป็นสื่อกลางในการแลกเปลี่ยนภายในกลุ่มนักพัฒนา ไปจนถึงการเก็งกำไรในปัจจุบัน นอกจากนี้ เทคโนโลยีเบื้องหลังของคริปโทเคอร์เรนซี คือ บล็อกเชน ยังมีศักยภาพสูง จนกลายเป็นหนึ่งในหัวใจของการสร้างกลุ่มธุรกิจใหม่ ที่คาดว่าจะมีมูลค่ามหาศาล นั่นคือ ธุรกิจเทคโนโลยีทางการเงิน (Financial Technology: FinTech) หรือฟินเทค สิ่งเหล่านี้แสดงถึงความสำคัญของคริปโทเคอร์เรนซีต่อทั้งภาครัฐ และภาคธุรกิจ รวมไปถึงภาคประชาชน ทั้งในปัจจุบันและอนาคต ดังนั้น เพื่อเป็นการส่งเสริมความเข้าใจ และสนับสนุนการพัฒนาของวงการการเงิน บทความนี้ จึงนำเสนอแง่มุมต่าง ๆ ของคริปโทเคอร์เรนซี โดยเน้นประเด็นทางเศรษฐกิจการเงินเป็นสำคัญ

คำสำคัญ: คริปโทเคอร์เรนซี เทคโนโลยีทางการเงิน (ฟินเทค) บิทคอยน์ บล็อกเชน

[1] ศาสตราจารย์ประจำคณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์ คณะพาณิชยศาสตร์และการบัญชี มหาวิทยาลัยธรรมศาสตร์ และภาคีสมาชิกราชบัณฑิต สาขาบริหารธุรกิจ ราชบัณฑิตยสภา

[2] ราชบัณฑิตยสภากำหนดศัพท์บัญญัติของคริปโทเคอร์เรนซีไว้ว่า “สกุลเงินเข้ารหัส”

Abstract

Since its introduction in 2008 as a peer-to-peer electronic cash system, cryptocurrency (Bitcoin) technology has been developed from being a breakthrough network innovation to a worldwide speculative target. Nowadays, not only being widely considered by software developers, cryptocurrency also captures public's attention. Moreover, the backbone of the groundbreaking virtual token (Blockchain) has tremendous potential to disrupt numerous activities. The effect is massive enough to create an advanced business cluster, called financial technology (FinTech). Unfortunately, this complex technology is not flawless. Without a thoughtful protection, some drawbacks may cause vastly difficulties. For these reasons, this paper aims to support a general public's understanding about cryptocurrency, especially from financial viewpoint.

Keywords: Cryptocurrency, Financial technology (FinTech), Bitcoin, Blockchain

บทนำ

วิวัฒนาการของการแลกเปลี่ยนเริ่มต้นจากการแลกสิ่งของที่ตนเองมีกับสิ่งของที่ต้องการ (Barter Trade) โดยนิยมแลกสัตว์ หรือพืชผลทางการเกษตร การทำธุรกรรมในระบบนี้ได้รับการบันทึกไว้เป็นครั้งแรกตั้งแต่สมัยอียิปต์ต่อมาระหว่าง 1,200 ถึง 1,100 ปีก่อนคริสตกาล ผู้คนแถบมหาสมุทรอินเดียใช้เปลือกหอยเบี้ย ขณะที่ชาวจีนใช้ทองสัมฤทธิ์ (Bronze) เป็นสื่อกลางของการแลกเปลี่ยน ทั้งนี้ เงินตราชนิดแรกถูกสร้างขึ้นอย่างเป็นทางการในตุรกีเมื่อ 600 ปีก่อนคริสตกาล โดยจะประทับรูปหน้าสิงโตไว้บนเหรียญ ซึ่งในยุคแรกผลิตจากโลหะมีค่าอย่างทองคำและเงิน ส่วนเงินตราที่ทำจากกระดาษได้รับการพัฒนาขึ้นในจีนเป็นครั้งแรก เมื่อปี พ.ศ. 1833 แต่การพิมพ์ธนบัตรอย่างเป็นทางการเกิดขึ้นที่สวีเดน ในปี พ.ศ. 2204 ภายหลัง ในปี พ.ศ. 2403 บริษัทเวสเทิร์นยูเนียน (Western Union) ให้กำเนิดเงินตราอิเล็กทรอนิกส์ จากการให้บริการโอนเงินทางโทรเลข ส่วนเงินตราพลาสติก หรือบัตรเครดิต (Credit Card) คิดค้นโดย John Biggins ในปี พ.ศ. 2489 และเทคโนโลยีชำระเงินแบบไม่ต้องสัมผัส (Contactless Payment) เกิดขึ้นที่สหราชอาณาจักรเป็นครั้งแรก ในปี พ.ศ. 2551

นอกจากเงินตราจะได้รับการสร้างขึ้นเพื่อเป็นสื่อกลางของการแลกเปลี่ยน เงินตรายังมีหน้าที่อื่น ๆ ได้แก่ เป็นมาตรฐานในการเปรียบเทียบมูลค่า เป็นเครื่องมือเก็บรักษามูลค่า (Store of Value) เป็นหน่วยในการบันทึกบัญชี

และเป็นมาตรฐานในการชำระหนี้ ซึ่งอาจกล่าวได้ว่า เงิน (Money) เป็นหน่วยแสดงอำนาจการซื้อ (Purchasing Power) โดยเงินจะถือเป็นเงินตรา (Currency) เมื่อถูกใช้แสดงมูลค่า และนับตั้งแต่เหรียญชนิดแรกถูกผลิตขึ้นที่ตุรกี มูลค่าของเหรียญก็ได้รับการรับรองจากรัฐบาล ว่ามีมูลค่าตามน้ำหนักของโลหะมีค่าที่ใช้เป็นวัตถุดิบ โดยรัฐบาลเป็นเพียงผู้เดียวที่มีอำนาจออกใช้ จึงสามารถควบคุมอุปทาน (Supply) ของเงินตราได้ทั้งหมด อย่างไรก็ตาม เมื่อโลหะมีค่ามีอยู่อย่างจำกัด (Scarcity) สัดส่วนของโลหะเหล่านี้จึงถูกปรับลดเป็นครั้งแรกในสมัยจักรวรรดิโรมัน ซึ่งใช้ทองคำเพียงครึ่งเดียวของมูลค่าเหรียญ ส่งผลให้ประชาชนขาดความเชื่อมั่น และนับเป็นสาเหตุหนึ่งที่ทำให้จักรวรรดิฯล่มสลาย นอกจากนี้ การกระทำดังกล่าวยังทำให้ทั่วทั้งยุโรปเลิกใช้เหรียญเป็นสื่อกลาง และกลับไปใช้ระบบแลกเปลี่ยนด้วยสิ่งของอีกด้วย

เมื่อเวลาผ่านไป กลุ่มคนที่ไม่เชื่อมั่นในเงินตราสกุลหลัก หรือเงินตราที่ออกโดยรัฐบาลกลางมีมากขึ้น ประกอบกับการขาดประสิทธิภาพของกลไกต่าง ๆ ในระบบการเงิน การพัฒนาและการเข้าถึงเทคโนโลยี รวมทั้งความต้องการใช้ประโยชน์เฉพาะด้าน จึงดึงดูดให้ภาคเอกชนพยายามออกใช้เงินตราลักษณะต่าง ๆ ที่ได้รับการยอมรับ และสามารถใช้เป็นสื่อกลางในการแลกเปลี่ยนภายในเครือข่ายของตนเอง ด้วยเหตุผลเดียวกันนี้ จึงเป็นจุดกำเนิดของคริปโทเคอร์เรนซี ทั้งนี้ เนื่องจากความผันผวนของราคาและโอกาสการใช้ประโยชน์ในด้านอื่น ๆ คริปโทเคอร์เรนซีจึงได้รับความสนใจ และถูกใช้งานเพิ่มขึ้นอย่างมากตลอดระยะเวลา 2 - 3 ปีที่ผ่านมา โดยเทคโนโลยีนี้เป็นนวัตกรรมที่มีศักยภาพในอันที่จะสนับสนุนระบบเศรษฐกิจ และชีวิตประจำวันให้มีประสิทธิภาพสูงขึ้น สอดคล้องกับทิศทางการขับเคลื่อนเศรษฐกิจด้วยนวัตกรรมในยุคประเทศไทย 4.0 (Thailand 4.0) และการพัฒนาเศรษฐกิจดิจิทัล (Digital Economy) ซึ่งระบุไว้ในแผนพัฒนาเศรษฐกิจ และสังคมแห่งชาติ ฉบับที่ 12 (พ.ศ. 2560 - 2564)

บทความฉบับนี้ จึงจัดทำขึ้นเพื่อส่งเสริมความเข้าใจเกี่ยวกับคริปโทเคอร์เรนซี โดยรวบรวมประเด็นที่สำคัญต่าง ๆ อย่างรอบด้าน เพื่อให้เป็นฐานข้อมูลที่มีคุณภาพสำหรับทุกฝ่ายที่เกี่ยวข้อง ซึ่งสามารถอ้างอิงได้ทั้งในเชิงวิชาการและในทางปฏิบัติ อันจะนำไปสู่การพัฒนาวงการการเงิน และเศรษฐกิจไทยในอนาคต ทั้งนี้ ลำดับการนำเสนอประกอบด้วยหัวข้อ คริปโทเคอร์เรนซีคืออะไร เส้นทางของบิทคอยน์ ข้อดีและข้อเสียของคริปโทเคอร์เรนซี กลไลการลงทุนในคริปโทเคอร์เรนซี การเสนอขายดิจิทัลโทเคนต่อสาธารณชน การประเมินมูลค่าคริปโทเคอร์เรนซี จุดยืนของประเทศต่าง ๆ ที่มีต่อคริปโทเคอร์เรนซี สถานการณ์ของคริปโทเคอร์เรนซีในประเทศไทย อนาคตของคริปโทเคอร์เรนซี และบทสรุปตามลำดับ

คริปโทเคอร์เรนซีคืออะไร

คริปโทเคอร์เรนซี (Cryptocurrency) เป็นเงินตราดิจิทัล (Digital Currency) หรือเงินตราเสมือน (Virtual Currency) ที่เกิดขึ้นและอยู่ได้ด้วยเครือข่ายคอมพิวเตอร์ (Computer Network) ซึ่งทำงานบนอินเทอร์เน็ต (Internet) คริปโทเคอร์เรนซีไม่มีข้อกำหนดว่าต้องออกโดยธนาคารกลาง และไม่ต้องมีสินทรัพย์หนุนหลัง แต่คุณค่าขึ้นกับความเชื่อมั่นของผู้ใช้ โดยในระยะเริ่มต้น การออกใช้อ้างอิงจากความสามารถในการประมวลผลบนเครือข่ายคอมพิวเตอร์ ซึ่งถูกจำกัดด้วยกลไกที่กำหนดไว้ในระบบ[3] แต่ไม่สามารถระบุผู้ออกที่ชัดเจนได้ นอกจากนี้ คริปโทเคอร์เรนซียังปรับตัวตามกลไกตลาด โดยไม่ถูกรัฐบาลควบคุม จากลักษณะดังกล่าว คริปโทเคอร์เรนซีประเภทแรกจึงจัดเป็นเงินตราแบบกระจายศูนย์ (Decentralized Currency) อย่างไรก็ตาม ธนาคารกลางในหลายประเทศ กำลังศึกษาแนวทางการออกใช้คริปโทเคอร์เรนซีของตัวเอง (Central Bank Digital Currencies: CBDCs) เช่น จีน สวีเดน แคนาดา เป็นต้น ในปัจจุบัน มีคริปโทเคอร์เรนซีอีกกลุ่ม ที่สามารถระบุตัวตนของผู้ออก และมีวัตถุประสงค์ของการออกใช้ที่ชัดเจน ซึ่งเป็นการดำเนินการโดยเอกชน (Private Entity Issued Cryptocurrencies) ทั้งนี้ คริปโทเคอร์เรนซีทุกประเภทล้วนมีลักษณะร่วมกับเงินตราแบบดั่งเดิม (Fiat Currency) คือ ความเชื่อมั่นมีผลอย่างมากต่อทั้งระบบ และการทำธุรกรรมจะต้องได้รับการยอมรับจากคู่สัญญา ซึ่งปัจจุบัน คริปโทเคอร์เรนซีถูกใช้ในระบบชำระเงินเพิ่มขึ้นทั่วโลก ทั้งในและนอกเครือข่ายอินเทอร์เน็ต (Online และ Offline) แต่ก็ยังมีสภาพคล่องน้อยกว่าเงินตราแบบดั่งเดิม

คริปโทเคอร์เรนซีเป็นผลตอบแทนที่ได้รับจากการแก้ปัญหาคณิตศาสตร์ของกระบวนการเข้ารหัสข้อมูลความปลอดภัย (Cryptography) เพื่อรับรองธุรกรรม (Proof-of-Work[4]) ซึ่งมอบให้แก่นักขุด (Miner) คนแรกที่แก้ปัญหาสำเร็จ โดยเทคโนโลยีเบื้องหลังของคริป

[3] Gjermundrød and Dionysiou (2014) และ Saito and Iwamura (2018) เสนอว่า การจำกัดอุปทานสูงสุด และปริมาณการออกใช้ ไว้ตามที่ออกแบบไว้ล่วงหน้า ประกอบกับมีคริปโทเคอร์เรนซีจำนวนมากที่สูญหายไปจากระบบ ทำให้อุปทานของคริปโทเคอร์เรนซีขาดความยืดหยุ่น ไม่สามารถปรับตามอุปสงค์ (Demand) ของตลาด ณ ขณะนั้น ได้อย่างมีประสิทธิภาพ จึงเป็นสาเหตุให้เกิดความผันผวน และความไม่มีเสถียรภาพของราคาคริปโทเคอร์เรนซี

[4] Proof-of-Work หรือการพิสูจน์ด้วยการทำงาน เป็นหลักการที่ถูกนำมาประยุกต์ใช้กับการรับรองธุรกรรม โดยใช้ความสามารถในการประมวลผลบนเครือข่ายคอมพิวเตอร์ในการแก้ปัญหาคณิตศาสตร์ที่เรียกว่า (Proof-of-Work) ด้วยวิธีทดลองสุ่ม (Trial-and-Error: Brute Force Cracking) ซึ่งดำเนินไปพร้อมกับการตรวจสอบ รวบรวม จัดระเบียบ และบันทึกธุรกรรม หรือรวมเรียกว่าการสร้างบล็อกใหม่ โดยนักขุดแต่ละกลุ่มดำเนินกระบวนการทั้งหมดนี้เหมือนกัน แต่แยกกัน ซึ่งผู้ที่สร้างบล็อกใหม่สำเร็จเป็นรายแรก และประกาศบนเครือข่าย จะได้รับผลตอบแทนเป็นคริปโทเคอร์เรนซี ที่ถูกกำหนดปริมาณไว้ล่วงหน้า โดยไม่ขึ้นกับตัวตนของผู้ชนะ ทั้งนี้ เมื่อคริปโทเคอร์เรนซีถูกขุดมากขึ้น ปัญหา

โทเคอร์เรนซี คือ บล็อกเชน (Blockchain) ซึ่งทำหน้าที่เก็บข้อมูลธุรกรรมแบบกระจายศูนย์ (Decentralized Database) ด้วยเทคโนโลยีสมุดบัญชีแยกประเภทแบบกระจายศูนย์ (Distributed Ledger Technology: DLT) โดยโครงสร้างของบล็อกเชนได้รับการออกแบบให้ไม่พึ่งพาการจัดเก็บข้อมูล ณ จุดใดจุดหนึ่งเป็นการเฉพาะ แต่ข้อมูลจะถูกกระจายการจัดเก็บไว้หลายจุด (Nodes) บนเครือข่าย (Network) อย่างอัตโนมัติ บล็อกเชนจึงมีลักษณะเป็นฐานข้อมูลสาธารณะ (Public Database) ทั้งนี้ เมื่อแต่ละจุดสามารถเข้าถึงข้อมูลเพื่อตรวจสอบสถานะของทุกฝ่ายบนเครือข่ายได้อย่างเท่าเทียม ความโปร่งใสของการทำธุรกรรมบนบล็อกเชนทำให้ไม่ต้องอาศัยตัวกลางในการตรวจสอบตัดสินใจ และสร้างความมั่นใจเช่นในอดีต แต่เครือข่ายจะร่วมกันประมวลผล เพื่อรับรองการทำธุรกรรมที่เกิดขึ้น

กิจกรรมที่ได้รับการรับรองบนบล็อกเชน จะถือเป็นธุรกรรม และถูกบันทึกทั้งหมด โดยนักขุดจะรวบรวมธุรกรรมไว้เป็นบล็อก (Block) ตามลำดับเวลา (Chronological Order) ทั้งนี้ การสร้างบล็อกใหม่จะถูกเข้ารหัสความปลอดภัยด้วยปัญหาคณิตศาสตร์ เช่น บิทคอยน์ (Bitcoin) ใช้ ฟังก์ชันแฮช (Hash Function[5]) SHA-256 อีเธอร์ (Ether) ใช้ Keccak แดช (Dash) ใช้ X11 เป็นต้น ซึ่งระบบจะปรับความยากให้สอดคล้องกับพลังการประมวลผลของทั้งเครือข่าย เพื่อให้สร้างบล็อกใหม่ด้วยความเร็ว (Block Time) ที่สม่ำเสมอ เช่น บิทคอยน์ 10 นาที ไลท์คอยน์ (Litecoin) 3 นาที อีเธอร์ 15 วินาที เป็นต้น บล็อกใหม่จะถูก

คณิตศาสตร์จะยิ่งซับซ้อน แต่ผลตอบแทนจะลดลง (ในกรณีบิทคอยน์ รางวัลเริ่มต้นจาก 50 บิทคอยน์ต่อบล็อก และลดครึ่งหนึ่งทุก ๆ 4 ปี ปัจจุบันอยู่ที่ 12.5 บิทคอยน์ต่อบล็อก) นอกจาก Proof-of-Work ยังมีกระบวนการรับรองธุรกรรมอีกประเภท ที่กำลังได้รับความสนใจ ระบบนั้นคือ Proof-of-Stake ซึ่งให้ผลตอบแทนแก่ผู้รับรองธุรกรรม เป็นค่าธรรมเนียม โดยอ้างอิงตามจำนวนคริปโทเคอร์เรนซีที่นักขุดมีอยู่ และผู้ที่จะเข้ามารับรองธุรกรรม จะต้องครอบครองคริปโทเคอร์เรนซีสกุลนั้นอยู่ก่อนหน้า ทั้งนี้ ระบบจะสุ่มเลือกนักขุดที่จะรับผิดชอบการสร้างบล็อกใหม่ จากกรอบเงื่อนไขที่แตกต่างกันของแต่ละสกุล ซึ่งจุดเด่นของระบบ Proof-of-Stake คือ การใช้พลังงานไฟฟ้าที่มีประสิทธิภาพสูงกว่าระบบ Proof-of-Work

[5] Hash Function เป็นกระบวนการทางคณิตศาสตร์ ที่ใช้แปลงข้อมูลให้ได้ผลลัพธ์ขนาดตายตัว แม้ว่าข้อมูลขาเข้าจะมีขนาดต่างกัน การทำงานของฟังก์ชันแฮชสามารถอธิบายอย่างง่าย ด้วยระบบตรวจสอบความถูกต้องของรหัสผ่าน (Password) เช่น การสร้างบัญชีอีเมล์ (e-mail) รหัสผ่านที่เจ้าของบัญชีกำหนด จะถูกแปลงด้วยฟังก์ชันแฮช ซึ่งระบบจะบันทึกผลลัพธ์ที่ได้ โดยในอนาคต เมื่อมีความพยายามเปิดบัญชีอีเมล์นั้น รหัสที่กรอกใหม่ จะถูกแปลงด้วยฟังก์ชันแฮชและเปรียบเทียบกับผลลัพธ์ที่เคยบันทึกไว้ ซึ่งต้องตรงกันทั้งหมดจึงจะเข้าใช้งานได้ ทั้งนี้ แม้ว่าข้อมูลขาเข้าจะแตกต่างกันเพียงเล็กน้อย ฟังก์ชันแฮชก็อาจได้ผลลัพธ์ไม่ใกล้เคียงกันอย่างไรก็ตาม มีความเป็นไปได้ที่ข้อมูลขาเข้าที่แตกต่างกันจะให้ผลลัพธ์เดียวกันจากการแปลงของฟังก์ชันแฮช แต่ความน่าจะเป็นลดลงอย่างมาก เมื่อใช้ฟังก์ชันแฮชที่ซับซ้อน เช่น SHA-256 SHA-512 เป็นต้น

เรียงต่อจากบล็อกเดิมเป็นสายโซ่ (Chain) เมื่อประกอบกับความปลอดภัยจากการบันทึกเวลาของการทำธุรกรรม (Trusted Timestamp) บล็อกเชนจึงถือเป็นแพลตฟอร์มแห่งความไว้วางใจ (Platform of Trust) และคริปโทเคอร์เรนซีเป็นเพียงการใช้ประโยชน์รูปแบบหนึ่งจากเทคโนโลยีนี้ ในปัจจุบัน มีคริปโทเคอร์เรนซีกว่า 1,400 ชนิด ซึ่งสร้างขึ้นด้วยวัตถุประสงค์ต่าง ๆ โดยพัฒนาต่อจากบิทคอยน์ คริปโทเคอร์เรนซีชนิดแรก ซึ่งยังได้รับความนิยมสูงที่สุด

เส้นทางของบิทคอยน์

บิทคอยน์ คิดค้นโดยผู้ใช้อินเทอร์เน็ตชื่อ Satoshi Nakamoto[6] ซึ่งเผยแพร่บทความบนเว็บไซต์ (Website) metzdowd.com ปลายปี พ.ศ. 2551 โดย Nakamoto (2008) เสนอหลักการของบิทคอยน์ ว่าเป็นระบบเงินสดอิเล็กทรอนิกส์ที่ผู้ใช้เครือข่ายสามารถโอนให้กันได้โดยตรง (Peer-to-Peer Electronic Cash) ไม่ต้องดำเนินการผ่านสถาบันการเงินเช่นในอดีต ทั้งยังสามารถป้องกันการจ่ายเงินซ้ำซ้อน[7] (Double Spending) ที่เป็นปัญหาสำคัญของเงินตราดิจิทัลอื่น หลังจากนั้น ต้นปี พ.ศ. 2552 Nakamoto เริ่มแจกจ่ายซอฟต์แวร์ (Software) ที่ใช้สร้างเครือข่าย พร้อมเปิดตัวบิทคอยน์หน่วยแรก เขาตั้งเว็บไซต์ bitcoin.org และร่วมพัฒนาซอฟต์แวร์บิทคอยน์จนถึงปี พ.ศ. 2553 จึงยุติกิจกรรม และมอบอำนาจการดูแลให้กลุ่มนักพัฒนาบิทคอยน์รุ่นบุกเบิก ทั้งนี้ ถึงแม้ว่าตัวตนที่แท้จริงของ Nakamoto จะยังคงเป็นปริศนา แต่คาดกันว่าในปัจจุบันเขามีบิทคอยน์ประมาณ 1 ล้านบิทคอยน์ คิดเป็นมูลค่ามากกว่า 19,000 ล้านดอลลาร์สหรัฐ (เมื่อบิทคอยน์ขึ้นไปถึงจุดสูงสุด ณ วันที่ 16 ธันวาคม พ.ศ. 2560) ซึ่งทำให้เขาติดอันดับ 1 ใน 50 คนรวยที่สุดในโลก

---

[6] เพื่อให้เกียรติแก่ Satoshi Nakamoto หน่วยที่เล็กที่สุดของบิทคอยน์จึงถูกเรียกว่า ซาโตชิ (Satoshi) โดย 1 บิทคอยน์ มีค่าเท่ากับ 100 ล้านซาโตชิ ด้วยลักษณะดังกล่าว บิทคอยน์จึงลดข้อจำกัดของเงินตราแบบดั้งเดิม ซึ่งมีหน่วยย่อยหยาบกว่านี้มาก ทำให้ระบบราคามีประสิทธิภาพ สร้างความเป็นธรรมในการทำธุรกรรมมากขึ้น นอกจากนี้ การมีหน่วยย่อยที่เล็กมาก ๆ ยังช่วยลดปัญหาจากการที่ระบบจำกัดปริมาณอุปทานสูงสุดของบิทคอยน์ไว้ที่ 21 ล้านหน่วย

[7] ระบบฐานข้อมูลกระจายศูนย์ และการตรวจสอบ รับรองภายในเครือข่าย ลดปัญหาที่เกิดจากความล่าช้าในการประมวลผลข้อมูลแบบรวมศูนย์ (Centralized Data Processing) อีกทั้งโครงสร้างการทำงานของบล็อกเชน ยังป้องกันการทำซ้ำ และดัดแปลงข้อมูลบนระบบคอมพิวเตอร์ให้ทำได้ยากขึ้น จนแทบจะเรียกว่าเป็นไปไม่ได้ เมื่อมีผู้ใช้งานและจำนวนธุรกรรมเพิ่มขึ้น เนื่องจาก ทุกจุดบนเครือข่ายเข้าถึงข้อมูลได้เหมือนกัน จึงสามารถตรวจสอบ และยืนยันการทำธุรกรรม โดยไม่ต้องรอตัวกลางในระบบเดิม ซึ่งการฉ้อโกง จำเป็นต้องแก้ไขฐานข้อมูลทุกจุดที่กระจายการบันทึกไว้บนเครือข่าย และต้องแก้ไขได้เร็วกว่าการเกิดขึ้นของบล็อกใหม่ เพราะบล็อกใหม่ทำให้การแก้ไขข้อมูลซับซ้อนขึ้น อย่างไรก็ตาม ด้วยพลังการประมวลผลของเครือข่ายทั่วโลกในปัจจุบัน อาจพูดได้ว่าอาชญากรไม่มีโอกาสที่จะดำเนินการได้สำเร็จ

อย่างไรก็ตาม ก่อนที่จะเกิดบิทคอยน์ นักพัฒนามีความพยายามที่จะสร้างเงินตราบนระบบเครือข่ายด้วยแนวคิดคล้ายกัน เช่น บีมันนี (B-money) ของ Wei Dai และบิทโกลด์ (Bit Gold) ของ Nick Szabo ซึ่งนำเสนอหลักการไว้ตั้งแต่ปี พ.ศ. 2541 แต่แนวคิดเหล่านั้นไม่ได้รับการพัฒนาต่อให้สำเร็จ และไม่ได้รับการยอมรับอย่างบิทคอยน์ ทั้งนี้ หลังการเกิดขึ้นของบิทคอยน์หน่วยแรก ในวันที่ 3 มกราคม พ.ศ. 2552 การขุดก็ดำเนินไปอย่างต่อเนื่อง ในระยะแรกปัญหาคณิตศาสตร์ยังไม่ซับซ้อน ทำให้นักขุดสามารถขุดบิทคอยน์จำนวนมากจากคอมพิวเตอร์ส่วนบุคคล และทุกจุดบนเครือข่ายยังเป็นนักขุดกันหมด แต่เนื่องจากไม่มีสินทรัพย์อ้างอิงที่ชัดเจน จึงยากที่จะประเมินมูลค่าที่แท้จริง แม้เวลาจะผ่านไปกว่าหนึ่งปี ก็ยังไม่มีการซื้อขายด้วยบิทคอยน์ จนกระทั่งวันที่ 22 พฤษภาคม พ.ศ. 2553 การซื้อขายสินค้าด้วยบิทคอยน์จึงเกิดขึ้นเป็นครั้งแรก โดย 10,000 บิทคอยน์ แลกพิซซ่า (Pizza) ได้ 2 ถาด (คิดเป็นมูลค่ามากกว่าถาดละ 50 ล้านดอลลาร์สหรัฐ ณ วันที่ 18 กุมภาพันธ์ พ.ศ. 2561)

เป็นเวลานานกว่า 2 ปี ที่บิทคอยน์เป็นคริปโทเคอร์เรนซีเพียงสกุลเดียวในตลาด จนกระทั่งปี พ.ศ. 2554 คริปโทเคอร์เรนซีสกุลอื่นจึงเริ่มเปิดตัว ซึ่งเรียกรวม ๆ ว่า อัลต์คอยน์ (Alternative Coins: Altcoins) โดยอัลต์คอยน์ที่สำคัญในยุคแรก เช่น เนมคอยน์ (Namecoin ใช้ Decentralized Domain Name System) ไลท์คอยน์ (ใช้ scrypt แทน SHA-256[8]) เพียร์คอยน์ (Peercoin ใช้ Proof-of-Stake ร่วมกับ Proof-of-Work) เป็นต้น ทั้งนี้ อัลต์คอยน์ได้รับการพัฒนาให้สามารถลดจุดอ่อนต่าง ๆ ของบิทคอยน์ เช่น ลดระยะเวลาการทำธุรกรรมให้เร็วขึ้น เพิ่มความเป็นส่วนตัวของเครือข่ายให้ระบุตัวตนยากขึ้น เพิ่มประสิทธิภาพการใช้พลังงานในการรับรองธุรกรรม เป็นต้น ต่อมาราคาบิทคอยน์ได้ปรับขึ้นไปถึง 1,000 ดอลลาร์สหรัฐ เป็นครั้งแรกในเดือนพฤศจิกายน พ.ศ. 2556 แต่เพียงปีกว่า ๆ หลังจากนั้น ราคากลับลดลงอย่างรุนแรง จนต่ำกว่าระดับ 200 ดอลลาร์สหรัฐ ในเดือนมกราคม พ.ศ. 2558 และต้องใช้เวลาอีกประมาณ 2 ปี ราคาจึงสามารถกลับขึ้นไปที่ 1,000 ดอลลาร์สหรัฐ ได้อีกครั้งในเดือนมกราคม พ.ศ. 2560

การเสนอขายดิจิทัลโทเคนต่อสาธารณชน (Initial Coin Offering: ICO) เริ่มต้นในปี พ.ศ. 2556 โดย มาสเตอร์คอยน์ (Mastercoin) แต่ไอซีโอยุคแรกที่ประสบความสำเร็จในระดับสูง คือ อีเธอร์ โดย อีเธอร์เรียม (Ethereum) ซึ่งระดมทุนได้ 18 ล้านดอลลาร์สหรัฐ ในปี พ.ศ. 2557 อย่างไรก็ตาม จุดเด่นเรื่องการตัดตัวกลางทางการเงิน และการปราศจากการควบคุม กลายเป็นประเด็นปัญหาที่

[8] การใช้ scrypt เป็นกลไกเข้ารหัสในกิจกรรม Proof-of-Work ทำให้ต้องใช้หน่วยความจำในการประมวลผลมากกว่า SHA-256 ของบิทคอยน์ ซึ่งส่งผลต่อเครื่องขุดที่ต้องมีโครงสร้างซับซ้อน และราคาแพงกว่าเดิม

สั่นคลอนคริปโทเคอร์เรนซีทั้งระบบ เพราะในเดือนมกราคม พ.ศ. 2557 เพียง 2 เดือนหลังจากราคาบิทคอยน์ปรับตัวสูงขึ้นไปถึง 1,000 ดอลลาร์สหรัฐ เมาท์ก๊อก (Mt.Gox) ซึ่งเป็นตลาดซื้อขายแลกเปลี่ยนบิทคอยน์ที่ใหญ่ที่สุดในโลก โดยมีธุรกรรมบิทคอยน์มากกว่าร้อยละ 70 ต้องหยุดการซื้อขาย ปิดเว็บไซต์ และปิดทำการ เนื่องจากบิทคอยน์ประมาณ 850,000 บิทคอยน์ที่ฝากไว้กับตลาดนี้สูญหายไป (แต่ค้นพบ 200,000 บิทคอยน์ ในอีกหนึ่งเดือนต่อมา) คิดเป็นมูลค่าความเสียหายมากกว่า 450 ล้านดอลลาร์สหรัฐ จากราคา ณ ขณะนั้น เหตุการณ์ดังกล่าวทำให้ราคาบิทคอยน์ลดลงร้อยละ 50 ภายในเวลาเพียง 2 เดือน จนถึงปัจจุบันนี้ ยังไม่สามารถสรุปหาสาเหตุที่แท้จริงของการสูญหายได้[9]

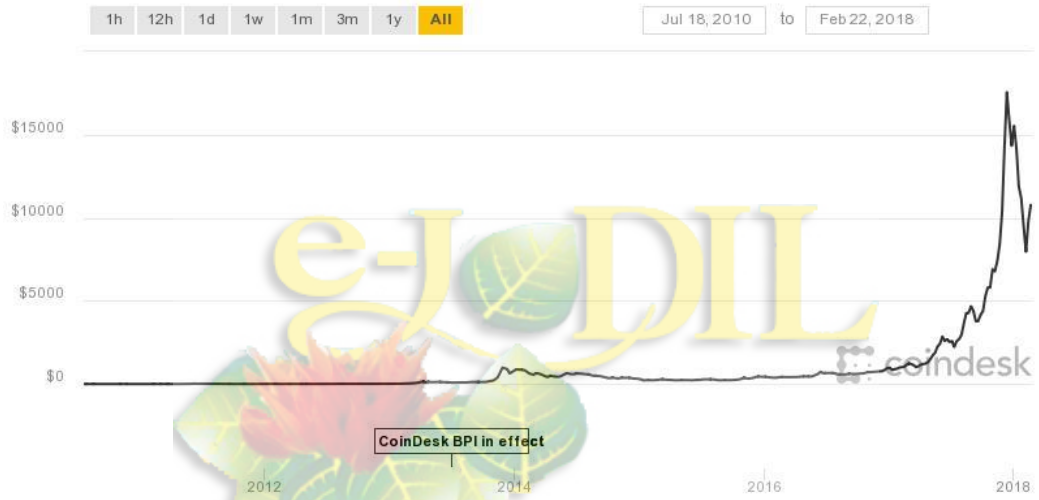
ในปี พ.ศ. 2558 บิทคอยน์จำนวน 19,000 บิทคอยน์ ถูกขโมยไปจากตลาดบิทแสตมป์ (Bitstamp) ปีถัดมา บิทคอยน์หายไป 120,000 บิทคอยน์ จากตลาดบิทฟินเน็กซ์ (Bitfinex) อย่างไรก็ตาม ความสนใจ และการยอมรับคริปโทเคอร์เรนซีกลับเพิ่มขึ้นตามลำดับ โดยในปี พ.ศ. 2559 วารสารเลดเจอร์ (Ledger) ซึ่งเป็นวารสารวิชาการ (Peer-Reviewed Academic Journal) เกี่ยวกับคริปโทเคอร์เรนซีและบล็อกเชน ได้เริ่มตีพิมพ์ฉบับแรก ต่อมาในปี พ.ศ. 2560 การเก็งกำไรทำให้ราคาบิทคอยน์ผันผวนอย่างมาก[10] โดยราคาขึ้นไปกว่า 10 เท่าระหว่างเดือนมกราคม ถึงพฤศจิกายน และด้วยระยะเวลาเพียงครึ่งเดือนหลังจากนั้น ราคาก็ขึ้นไปสูงกว่า 19,000 ดอลลาร์สหรัฐ ก่อนจะลงไปต่ำกว่า 7,000 ดอลลาร์สหรัฐต่อบิทคอยน์ ในเดือนกุมภาพันธ์ พ.ศ. 2561 นอกจากนี้ การจำกัดจำนวนธุรกรรมที่สามารถประมวลผลบนระบบบิทคอยน์ ไว้ที่ 7 ธุรกรรมต่อวินาที ทำให้เกิดคอขวด การทำธุรกรรมช้าลง และต้องจ่าย

[9] คาดว่าเกิดจากการโจมตีแบบ DDoS (Distributed Denial-of-Service) ซึ่งอาชญากร (Hacker) กระจายระดมโจมตีตลาดเมาท์ก๊อก จากต้นทางหลายแหล่งพร้อม ๆ กัน เพื่อให้ทรัพยากรของตลาดไม่เพียงพอรองรับการใช้งาน จนต้องหยุดให้บริการในที่สุด ทั้งนี้ แม้ว่าบล็อกเชนจะสามารถป้องกันการฉ้อโกงภายในเครือข่ายได้เป็นอย่างดี แต่จะเห็นได้ว่า ปัญหาดังกล่าวอยู่นอกเหนือการควบคุม เมื่อต้องออกจากระบบบล็อกเชน เช่นในกรณีนี้ ซึ่งเป็นการฝากคริปโทเคอร์เรนซีไว้กับตลาดซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซี

[10] Cocco, Concas, and Marchesi (2017) พบปัญหา Autocorrelation ระหว่างค่าสัมบูรณ์ของผลตอบแทนจากการเปลี่ยนแปลงราคาบิทคอยน์ (Absolute หรือ Squared Return) ซึ่งแสดงถึงปรากฏการณ์ Volatility Clustering ในตลาดบิทคอยน์ ซึ่งความผันผวนที่รุนแรงมีแนวโน้มที่จะจับกลุ่มอยู่ในช่วงเวลาไล่เลี่ยกัน เช่นเดียวกับการเปลี่ยนแปลงราคาในกรอบแคบ ๆ ที่มักจะรวมตัวในช่วงเวลาที่ต่างออกไป ทั้งนี้ Urquhart (2016) และ Nadarajah and Chu (2017) รายงานผลการศึกษาว่าตลาดบิทคอยน์เป็นตลาดที่ไม่มีประสิทธิภาพ (Inefficient Market) เนื่องจากพบว่าราคาบิทคอยน์เปลี่ยนแปลงอย่างมีแบบแผน (Non-Randomness) หรือราคาในอดีตสามารถใช้คาดการณ์ราคาในอนาคตได้ แต่งานทั้งสองชิ้นก็ยังแสดงให้เห็นว่าตลาดบิทคอยน์น่าจะมีประสิทธิภาพดีขึ้นในอนาคต

ค่าธรรมเนียมสูงขึ้นถ้าต้องการความรวดเร็ว บิทคอยน์จึงถูกแบ่ง (Hard Fork) ออกเป็น 2 สกุล ในปี พ.ศ. 2560 คือ บิทคอยน์ (BTC) ที่ใช้ขนาดบล็อก 1 MB และบิทคอยน์แคช (Bitcoin Cash: BCH) ที่ใช้ขนาดบล็อก 8 MB

สถานการณ์ราคาบิทคอยน์ตั้งแต่อดีตจนถึงปัจจุบัน (ดอลลาร์สหรัฐ)[11]



แม้ว่าบิทคอยน์จะถูกพัฒนาอย่างต่อเนื่อง แต่การแก้ไขทุกครั้งจำเป็นต้องได้รับความเห็นชอบจากเครือข่าย ซึ่งใช้เวลาในการพิจารณา และมักมีมุมมองแตกต่างกันในรายละเอียด ทั้งนี้ ระยะเวลาการสร้างบล็อกใหม่ทุก 10 นาที[12] เป็นปัญหาที่มีมาอย่างยาวนาน เพราะเมื่อมีธุรกรรมเพิ่มมากขึ้น ปริมาณข้อมูลที่รับได้ต่อบล็อก และระยะเวลาที่ต้องรอก่อนจะสร้างบล็อกใหม่ ทำให้ประสิทธิภาพของการทำธุรกรรมลดลง ในปี พ.ศ. 2560 จึงเกิดข้อตกลง

[11] ข้อมูลจาก CoinDesk.com ตั้งแต่วันที่ 18 กรกฎาคม พ.ศ. 2553 ถึง 22 กุมภาพันธ์ พ.ศ. 2561 เนื่องจากราคาบิทคอยน์ในแต่ละตลาดมักจะแตกต่างกันเล็กน้อย CoinDesk.com จึงคำนวณราคาเฉลี่ยด้วยราคาปิดจากตลาดซื้อขายแลกเปลี่ยนบิทคอยน์ชั้นนำหลายแห่ง ทั้งนี้ Pieters and Vivanco (2017) พบว่าตลาดที่ไม่มีระเบียบให้ผู้ทำธุรกรรมเปิดเผยตัวตน มีแนวโน้มที่ราคาจะแตกต่างจากตลาดอื่นมากขึ้น

[12] Nakamoto คาดว่า 10 นาที หรือ 6 บล็อกต่อชั่วโมง เป็นระยะเวลาที่ให้ประสิทธิภาพสูงที่สุดในการตรวจสอบ และสร้างบล็อกใหม่ โดยหนึ่งในเหตุผลที่เขาใช้พิจารณา คือ สัดส่วนความสูญเสีย (Waste) จากกิจกรรมที่ซ้ำซ้อน อยู่ในระดับที่ยอมรับได้ เมื่อใช้ระยะเวลาสร้างบล็อกใหม่ที่ 10 นาที ซึ่งแน่นอนว่าเป็นที่ถกเถียงอย่างมากถึงความเหมาะสมของระยะเวลาดังกล่าว

ระหว่างนักขุด ที่จะสร้างบล็อกเชนใหม่ ที่พัฒนาจากบิทคอยน์ โดยเพิ่มความจุข้อมูลให้บล็อกสามารถบันทึกได้ 8 MB[13] จนเกิดเป็น บิทคอยน์แคช (BCH) ซึ่งในปัจจุบันมีมูลค่าตามราคาตลาดมากกว่า 25,000 ล้านดอลลาร์สหรัฐ (ปริมาณการซื้อขาย 700 ล้านดอลลาร์สหรัฐต่อวัน) และไลท์คอยน์ เปิดตัวในปี พ.ศ. 2554 มีการออกแบบคล้ายคลึงกับบิทคอยน์ แต่กำหนดระยะเวลาการสร้างบล็อกใหม่ที่ 2.5 นาที และกำหนดอุปทานสูงสุดไว้ที่ 84 ล้านไลท์คอยน์ ปัจจุบันมีมูลค่าตามราคาตลาด 13,000 ล้านดอลลาร์สหรัฐ (ปริมาณการซื้อขาย 1,400 ล้านดอลลาร์สหรัฐต่อวัน)

มูลค่าตลาดคริปโทเคอร์เรนซีรวมกันทั้งหมด ขึ้นไปสูงกว่า 300,000 ล้านดอลลาร์สหรัฐ ในปี พ.ศ. 2560 และ Jesse Powell ประธานเจ้าหน้าที่บริหารของตลาดคราเคน (Kraken) คาดว่ามูลค่าจะขึ้นไปถึง 1 ล้านล้านดอลลาร์สหรัฐ ในปี พ.ศ. 2561 โดยบิทคอยน์ได้รับการยอมรับในระดับที่ตลาดอนุพันธ์ระดับโลกอย่าง Chicago Board Options Exchange (CBOE) และ Chicago Mercantile Exchange (CME) Group เปิดตัวสัญญาซื้อขายล่วงหน้าที่อ้างอิงราคาบิทคอยน์[14] เมื่อเดือนธันวาคม พ.ศ. 2560 ทั้งนี้ อ้างอิงข้อมูลจากเว็บไซต์ CoinMarketCap (ณ วันที่ 20 กุมภาพันธ์ พ.ศ. 2561) บิทคอยน์ (BTC) เป็นคริปโทเคอร์เรนซีที่มีมูลค่าตามราคาตลาด (Market Capitalization) และปริมาณการซื้อขาย (Trading Volume) สูงที่สุด ประมาณ 195,000 และ 9,000 ล้านดอลลาร์สหรัฐ ตามลำดับ เนื่องจากความสนใจจากสาธารณชน และนักลงทุนที่เพิ่มขึ้น การได้รับการยอมรับจากรัฐบาลในหลายประเทศ และการเกิดสัญญาซื้อขายล่วงหน้า ทั้ง ๆ ที่ราคาบิทคอยน์ผันผวนอย่างมาก และมีปัญหาเรื้อรังเรื่องความเร็วของการทำธุรกรรม กับค่าธรรมเนียมในการทำธุรกรรมที่เพิ่มขึ้น

ตามมาด้วยอีเธอร์ (ETH) มูลค่าตามราคาตลาด และปริมาณการซื้อขาย ประมาณ 92,000 และ 2,300 ล้านดอลลาร์สหรัฐ ตามลำดับ อีเธอร์ใช้ประโยชน์บล็อกเชนในด้านอื่นควบคู่ไปกับการเป็นระบบชำระเงิน คือ การเป็นแพลตฟอร์มสำหรับพัฒนาซอฟต์แวร์แบบ

[13] การเพิ่มความจุบล็อกมีข้อเสียที่สำคัญ คือ ลดความสามารถในการแข่งขันของนักขุดรายย่อย เพราะพวกเขาจะไม่สามารถรองรับการประมวลผลข้อมูลปริมาณมากได้อย่างมีประสิทธิภาพ ด้วยเหตุนี้ จึงเพิ่มความเสี่ยงที่จะถูกควบคุมโดยนักขุดรายใหญ่ไม่กี่ราย ซึ่งลดการกระจายอำนาจอันเป็นจุดเด่นของบล็อกเชน ตัวอย่างคริปโทเคอร์เรนซีที่แยกตัวจากบิทคอยน์ เช่น Bitcoin XT Bitcoin Unlimited Bitcoin Gold เป็นต้น

[14] Nikolaos Panigirtzoglou ผู้บริหารของ JPMorgan Chase มองว่าคริปโทเคอร์เรนซีเป็นสินทรัพย์ประเภทใหม่ (Emerging Asset Class) ซึ่งการเกิดขึ้นของสัญญาซื้อขายล่วงหน้าที่อ้างอิงราคาบิทคอยน์ในตลาด CBOE และ CME จะทำให้นักลงทุนสถาบันเข้ามาลงทุนในตลาดคริปโทเคอร์เรนซีมากขึ้น จากเดิมที่เน้นการใช้ประโยชน์ในเชิงระบบ

กระจายศูนย์ (Distributed Software Development Platform) เพื่อลดความสำคัญของแอพพลิเคชันจากบุคคลที่สาม (Third Party Application) รวมทั้งการสร้างสัญญาอัจฉริยะ (Smart Contract[15]) โดยใช้ภาษาโปรแกรมที่เข้าถึงง่ายกว่าเมื่อเปรียบเทียบกับบิทคอยน์ สำหรับริปเปิล (Ripple: XRP) มีมูลค่าตามราคาตลาดเป็นอันดับสาม ราว ๆ 44,000 ล้านดอลลาร์สหรัฐ (ปริมาณการซื้อขาย 700 ล้านดอลลาร์สหรัฐต่อวัน) ริปเปิลเป็นตัวกลางในระบบชำระเงินประสิทธิภาพสูง (ใช้พลังงานต่ำและทำธุรกรรมได้เร็วในระดับวินาที) แต่ค่าธรรมเนียมต่ำ ซึ่งแตกต่างจากทั้งบิทคอยน์และอีเธอร์ เป็นอย่างมาก เพราะการขุด (บริษัทขุดไว้ล่วงหน้าทั้งหมด) และอุปทานส่วนใหญ่ควบคุมโดยบริษัทริปเปิล นอกจากนี้ ริปเปิลยังถูกใช้งานโดยสถาบันการเงินขนาดใหญ่หลายแห่ง ซึ่งกลายเป็นจุดที่สร้างความน่าเชื่อถือให้แก่ริปเปิล

ข้อดีและข้อเสียของคริปโทเคอร์เรนซี

คริปโทเคอร์เรนซีช่วยเพิ่มประสิทธิภาพของระบบแลกเปลี่ยนเงินตรา ทำให้การโอนเงินระหว่างกันภายในเครือข่ายสะดวก รวดเร็ว และต้นทุนต่ำลง โดยฐานข้อมูล และระบบรับรองธุรกรรมของคริปโทเคอร์เรนซี ยังเพิ่มความโปร่งใส ให้ความเป็นส่วนตัว ลดโอกาสผิดพลาดและการฉ้อโกง ซึ่งสร้างความเชื่อมั่นให้คู่สัญญามากขึ้น ทั้งนี้ United Nations Research Institute for Social Development (UNRISD) โดย Scott (2016) รายงานว่า การใช้งานคริปโทเคอร์เรนซีส่งผลดีต่อสังคมอีกหลายประการ เช่น ทุกคนสามารถใช้ได้จากทุกที่ ๆ มีอินเทอร์เน็ตด้วยอุปกรณ์ที่หลากหลาย ขยายการเข้าถึงบริการทางการเงิน (Financial Inclusion) ทำธุรกรรมระหว่างประเทศได้โดยไม่ถูกแทรกแซงการดำเนินการมีความเป็นประชาธิปไตย และใช้มาตรฐานเดียวกันทั่วโลก ลดปัญหาอัตราแลกเปลี่ยน อัตราดอกเบี้ย และค่าธรรมเนียมที่แตกต่างกันในแต่ละประเทศ สนับสนุนความรู้เรื่องทางการเงิน (Financial Literacy) เป็นต้น นอกจากนี้ เทคโนโลยีบล็อกเชน ยังสามารถใช้กับกิจกรรมอื่น เช่น การลงคะแนนเลือกตั้ง การเชื่อมต่อฐานข้อมูลลูกค้า (Know Your Client: KYC) ระบบสัญญาอัจฉริยะ เป็นต้น

อย่างไรก็ตาม เนื่องจากคริปโทเคอร์เรนซีไม่มีลักษณะทางกายภาพ โดยต้องจัดเก็บไว้บนเครือข่าย หรือบันทึกไว้ในอุปกรณ์อิเล็กทรอนิกส์ ความเสียหายจึงรุนแรงเมื่อระบบและอุปกรณ์เหล่านั้นมีปัญหา หรือแม้กระทั่งความผิดพลาดส่วนบุคคล เช่น เผลอลบข้อมูลในระบบ ลืมสื่อบันทึกข้อมูล (Bitcoin Wallet) การเปิดเผยบัญชีโดยบังเอิญ (QR Code) เป็นต้น นอกจากนี้ คริป

[15] สัญญาอัจฉริยะ เป็นข้อตกลงที่ถูกสร้างขึ้นบนบล็อกเชน ซึ่งจะถูกบังคับใช้โดยอัตโนมัติ เมื่อเครือข่ายตรวจสอบ และรับรองว่าสถานการณ์ปัจจุบัน เป็นไปตามเงื่อนไขที่ระบุไว้ในสัญญาโดยสมบูรณ์แล้ว

โทเคอร์เรนซียังประเมินมูลค่าได้ยาก เพราะไม่มีสินทรัพย์อ้างอิง ราคาคริปโทเคอร์เรนซีจึงปรับตามมุมมองผู้ใช้งานในเครือข่าย และนักเก็งกำไรจากการคาดการณ์ระดับอุปสงค์อุปทาน เมื่อประกอบกับการไม่ได้ถูกควบคุมจากส่วนกลาง ทำให้ราคาผันผวนเป็นอย่างมาก ถือเป็นการลงทุนที่มีความเสี่ยงสูง ทั้งนี้ แม้แต่คริปโทเคอร์เรนซีสกุลหลักก็ยังไม่สามารถใช้แลกเปลี่ยนสินค้าและบริการได้อย่างกว้างขวาง อีกทั้งร้านค้าที่รับชำระด้วยคริปโทเคอร์เรนซี ยังนิยมปรับเพิ่มส่วนต่างเพื่อป้องกันความเสี่ยงจากความผันผวนของราคา ลูกค้าจึงต้องซื้อสินค้าแพงขึ้น ยิ่งไปกว่านั้น การไม่ระบุตัวตนของผู้ทำธุรกรรม ทำให้คริปโทเคอร์เรนซีกลายเป็นแหล่งฟอกเงินของอาชญากร[16] และการหลีกเลี่ยงภาษี

กลไลการลงทุนในคริปโทเคอร์เรนซี

การครอบครองคริปโทเคอร์เรนซีสามารถทำได้ 3 วิธี คือ ซื้อขายแลกเปลี่ยน การขุด (Mining) และวิธีอื่น ๆ เช่น รางวัลจากเกมส์ (Games) ผลตอบแทนจากการลงทุนที่ได้ผลตอบแทนสูง (High Yield Investment Program: HYIP) เป็นต้น ผู้ทำธุรกรรมด้วยคริปโทเคอร์เรนซีสามารถเป็นได้ทั้งบุคคลธรรมดา นิติบุคคล อุปกรณ์ที่เชื่อมต่ออินเทอร์เน็ต (Internet of Things: IoT) หรือแม้แต่อัลกอริทึม (Algorithm) ที่ไม่มีลักษณะและที่ตั้งทางกายภาพ อย่างไรก็ตาม ผู้ใช้งานคริปโทเคอร์เรนซียังคงมีลักษณะร่วมกัน คือ จะต้องเป็นส่วนหนึ่งของเครือข่าย ซึ่งเชื่อมต่อกับระบบอินเทอร์เน็ต โดยในปัจจุบันสามารถดำเนินการผ่านอุปกรณ์หลากหลายชนิด ไม่จำกัดเฉพาะเครื่องคอมพิวเตอร์ หรือโทรศัพท์ที่รองรับระบบปฏิบัติการ (Smartphone) ส่วนการเข้าร่วมเครือข่าย เพื่อซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซีในตลาด เป็นไปตามขั้นตอนการสร้างกระเป๋าคริปโทเคอร์เรนซี (Cryptocurrency Wallet[17]) ดังต่อไปนี้ สมัครสมาชิกตลาดซื้อขาย

[16] ในปี พ.ศ. 2556 รัฐบาลสหรัฐอเมริกาปิดเว็บไซต์ตลาดซื้อขายแลกเปลี่ยนสิ่งผิดกฎหมาย ซิลค์โรด (Silk Road) ซึ่งสมาชิกไม่จำเป็นต้องเปิดเผยตัวตน และผู้ก่อตั้งถูกตัดสินจำคุกตลอดชีวิต ทั้งนี้ บิทคอยน์มีส่วนเกี่ยวข้องในฐานะที่เป็นสื่อกลางซึ่งอาชญากรนิยมใช้ในการซื้อขาย อย่างไรก็ตาม อาชญากรมีแนวโน้มที่จะเปลี่ยนไปใช้คริปโทเคอร์เรนซีที่ถูกพัฒนาให้ระบุตัวตนได้ยากกว่า เช่น แดช (Dash) มันเนโร (Monero: XMR) เป็นต้น การศึกษาของ Brenig, Accorsi, and Müller (2015) เสนอแนวทางควบคุมปัญหาการฟอกเงิน โดยแบ่งการดำเนินการออกเป็น 3 ช่วง ได้แก่ ก่อนทำธุรกรรม (ระบุตัวตนผู้ทำธุรกรรม และผู้มีส่วนได้ส่วนเสีย, สร้างฐานข้อมูลผู้ใช้เครือข่าย, ห้ามผู้ใช้เครือข่ายที่น่าสงสัยทำธุรกรรม) ระหว่างทำธุรกรรม (แยกแยะธุรกรรม, ตรวจจับธุรกรรมที่น่าสงสัย, ปรับปรุงฐานข้อมูลเครือข่าย) และหลังทำธุรกรรม (บันทึกข้อมูลเพื่อใช้ตรวจสอบในอนาคต)

[17] การเก็บคริปโทเคอร์เรนซีไว้ในคอมพิวเตอร์ส่วนบุคคล (Personal Computer) เพียงอย่างเดียว อาจไม่ใช้ทางเลือกที่เหมาะสมเสมอไป เนื่องจากข้อบกพร่องของอุปกรณ์โดยเฉพาะอย่างยิ่งฮาร์ดดิสก์ (Hard Disk Drive) ที่อาจทำให้ทรัพย์สินสูญหาย ดังเกิดขึ้นกับข้อมูลทั่วไป เพราะฉะนั้น จึงควรใช้ทางเลือกการจัดเก็บอื่น ๆ ร่วมกับการเก็บในคอมพิวเตอร์ส่วนบุคคล เช่น หน่วยความจำแฟลช (Flash

แลกเปลี่ยนคริปโทเคอร์เรนซี (Cryptocurrency Exchange) ยืนยันตัวตน ยืนยันบัญชีธนาคาร และโอนเงินเข้าสู่ระบบตลาด

การขุดคริปโทเคอร์เรนซี เป็นการแข่งขันกันแก้ปัญหาคณิตศาสตร์เพื่อรับรองธุรกรรม และสร้างบล็อก ซึ่งผู้ชนะจะได้รับคริปโทเคอร์เรนซีที่มีอยู่อย่างจำกัดเป็นผลตอบแทน โดยคริปโทเคอร์เรนซีเหล่านี้เป็นการออกใหม่แตกต่างจากตลาดซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซีที่เป็นตลาดรอง (Secondary Market) ทั้งนี้ บิทคอยน์ถูกขุดไปแล้วประมาณ 17 ล้านบิทคอยน์ และคาดว่าจะครบ 21 ล้านบิทคอยน์[18] ภายในปี พ.ศ. 2683 ทั้งนี้ การขุดคริปโทเคอร์เรนซีสามารถทำได้ 2 วิธี คือ การสร้างและจัดการเครื่องขุดส่วนบุคคล และการร่วมลงทุนโดยทำสัญญาซื้อกำลังขุด (Cloud Mining) ซึ่งในระบบนี้ ผู้ให้บริการจะจัดหา และจัดการเครื่องขุดด้วยเงินลงทุนที่รวบรวมได้ อย่างไรก็ตาม แม้ว่าระบบร่วมลงทุนจะช่วยลดค่าใช้จ่าย และความรับผิดชอบที่มีต่อกระบวนการขุดอันซับซ้อน แต่ก็ต้องแลกมาด้วยการเสียค่าธรรมเนียม ผลกำไรที่ลดลง ความเสี่ยงจากการฉ้อโกง และการยกเลิกสัญญาเมื่อราคาคริปโทเคอร์เรนซีตกต่ำในระดับที่ผู้ให้บริการพิจารณาว่าควรเลิกขุด ทั้งนี้ ขั้นตอนการขุดคริปโทเคอร์เรนซีด้วยตัวเอง มีรายละเอียดโดยสรุปดังต่อไปนี้

- จัดหาเครื่องขุด ระดับการแข่งขันในปัจจุบันทำให้ไม่คุ้มค่าที่จะใช้คอมพิวเตอร์ทั่วไป (ขุดด้วย CPU และ Graphic Card) ซึ่งประสิทธิภาพต่ำ โดยผู้ขุดต้องลงทุนกับเครื่องขุดประสิทธิภาพสูง เช่น Application-Specific Integrated Circuit (ASIC) Miner หรือ Field-Programmable Gate Array (FPGA) Miner เป็นต้น ที่ออกแบบขึ้นเป็นการเฉพาะ และต้องเชื่อมต่อกับเครือข่ายอินเทอร์เน็ตความเร็วสูงตลอดเวลา แม้ว่าเครื่องขุดเหล่านี้จะได้รับการออกแบบให้ใช้พลังงานอย่างมีประสิทธิภาพกว่าคอมพิวเตอร์ทั่วไป แต่การขุดคริปโทเคอร์เรนซีก็ยังคงใช้ไฟฟ้ามหาศาล ทั้งในส่วนเครื่องขุด และระบบทำความเย็น โดยในเดือนธันวาคม พ.ศ. 2560 สภาเศรษฐกิจโลก (World Economic Forum: WEF) ประเมินว่าความสิ้นเปลืองพลังงานไฟฟ้าจากการขุดบิทคอยน์ทั่วโลก มีอัตราการเติบโตร้อยละ 25 ต่อเดือน และอาจเทียบเท่ากับการใช้ไฟฟ้าของทั้งประเทศสหรัฐอเมริกา ภายในปี พ.ศ. 2562 เมื่อมีเครื่องขุดแล้ว ผู้ขุดต้องดาวน์โหลด (Download) ซอฟท์แวร์สำหรับการขุด ซึ่งในปัจจุบันมีซอฟท์แวร์ฟรีให้เลือกมากมายบนอินเทอร์เน็ต

Memory) กระเป๋าคริปโทเคอร์เรนซีบนเครือข่าย (Cloud Wallet) การพิมพ์ QR Code เป็นต้น

[18] ยังคงเป็นคำถามว่า เมื่อบิทคอยน์ถูกขุดครบทุกหน่วยแล้ว จะใช้วิธีการใดดึงดูดให้นักขุดยังคงประมวลผล เพื่อตรวจสอบและรับรองธุรกรรมบนเครือข่ายต่อไป ซึ่งทางเลือกหนึ่ง คือ การใช้ระบบค่าธรรมเนียม อันย้อนกลับไปสู่ระบบเดียวกับการทำธุรกรรมผ่านสถาบันการเงิน

- สร้างกระเป๋าคริปโทเคอร์เรนซี ซึ่งเข้ารหัส 2 ระดับ (Private-Encryption Key และ Public-Encryption Key) ด้วยลายเซ็นอิเล็กทรอนิกส์ (Digital Signature) โดยเครือข่ายจะเข้าถึงข้อมูลการทำธุรกรรมทั้งหมดของเจ้าของบัญชี เพื่อตรวจสอบ และยืนยันการทำธุรกรรมที่เกิดขึ้น ผ่าน Public-Encryption Key ส่วน Private-Encryption Key จะรับรู้และใช้งานโดยเจ้าของบัญชีเท่านั้น นอกจากนี้ กระเป๋าคริปโทเคอร์เรนซียังสร้างไว้เพื่อรองรับผลตอบแทนจากการขุด และแลกเปลี่ยน หรือทำกำไรจากผลตอบแทนเหล่านั้น ภายในตลาดซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซี

- เข้าร่วมกลุ่มนักขุด (Mining Pool) เพื่อเพิ่มประสิทธิภาพของการแก้ปัญหาคณิตศาสตร์ โดยร่วมกันขุดเป็นเครือข่าย แต่แน่นอนว่าวิธีการนี้จะต้องแบ่งคริปโทเคอร์เรนซีกันภายในกลุ่ม นอกจากนี้ กลุ่มยังใช้เป็นช่องทางสื่อสาร และติดตามข้อมูลทางเทคนิคที่เกี่ยวข้องกับการขุด และแนวโน้มราคาคริปโทเคอร์เรนซี เพื่อสนับสนุนการตัดสินใจให้ทันท่วงทีด้วย

เว็บไซต์ CoinMarketCap จัดอันดับตลาดซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซี จากปริมาณการซื้อขายต่อวัน (ณ วันที่ 20 กุมภาพันธ์ พ.ศ. 2561) ซึ่งมีลำดับดังต่อไปนี้ ตลาดบิทเม็กซ์ (BitMEX) 2,700 ล้านดอลลาร์สหรัฐต่อวัน ตลาดไบแนนซ์ (Binance) 2,000 ล้านดอลลาร์สหรัฐต่อวัน ตลาดโอเคเอ็กซ์ (OKEx) 1,900 ล้านดอลลาร์สหรัฐต่อวัน ตลาดอัพบิท (Upbit) 1,600 ล้านดอลลาร์สหรัฐต่อวัน ตลาดบิทฟินเน็กซ์ (Bitfinex) 1,300 ล้านดอลลาร์สหรัฐต่อวัน นอกจากนี้ นิตยสารฟอร์บส (Forbes) ยังจัดอันดับมหาเศรษฐีคริปโทเคอร์เรนซี[19] ประจำปี พ.ศ. 2561 โดยรายนาม 5 ลำดับแรก ได้แก่ Chris Larsen (ผู้ก่อตั้งริปเปิล) 7,500 – 8,000 ล้านดอลลาร์สหรัฐ Joseph Lubin (ผู้ก่อตั้งอีเธอร์เรียม) 1,000 – 1,500 ล้านดอลลาร์สหรัฐ Changpeng Zhao (ประธานเจ้าหน้าที่บริหารของตลาดไบแนนซ์) 1,100 – 2,000 ล้านดอลลาร์สหรัฐ Cameron และ Tyler Winklevoss (ผู้ก่อตั้งตลาดจีมิไน หรือ Gemini) 900 – 1,100 ล้านดอลลาร์สหรัฐ Matthew Mellon (นักลงทุนอิสระ) 900 – 1,000 ล้านดอลลาร์สหรัฐ

[19] นิตยสารฟอร์บส ประเมินจากคริปโทเคอร์เรนซีที่ครอบครอง กำไรหลังหักภาษีจากทรัพย์สินและธุรกิจที่เกี่ยวข้องกับคริปโทเคอร์เรนซี โดยอ้างอิงราคา ณ วันที่ 19 มกราคม พ.ศ. 2561 ทั้งนี้ นิตยสารฟอร์บสยังระบุด้วยว่าข้อมูลของผู้เกี่ยวข้องกับคริปโทเคอร์เรนซีมักไม่เปิดเผย การจัดอันดับจึงอาจไม่สมบูรณ์ และรายงานมูลค่าทรัพย์สินอาจไม่แม่นยำ

การเสนอขายดิจิทัลโทเคนต่อสาธารณชน (Initial Coin Offering: ICO)

ICO หรือ IPCO (Initial Public Coin Offering) เป็นการระดมทุนรูปแบบใหม่ ซึ่งกำลังได้รับความสนใจไม่แพ้การซื้อขายคริปโทเคอร์เรนซี ทั้งนี้ ICO มักดำเนินการโดยบริษัทเกิดใหม่ (Startup) ด้านเทคโนโลยี ที่ต้องการต่อยอดแนวคิดทางธุรกิจให้เกิดขึ้นจริง โดยบริษัทเหล่านี้เลือกใช้ดิจิทัลโทเคน (Digital Token) เป็นสื่อกลาง แทนการระดมทุนรูปแบบเดิมที่ถูกควบคุมด้วยกฎระเบียบเข้มงวด และมีลักษณะความสัมพันธ์ระหว่างธุรกิจและนักลงทุนที่ต่างออกไป ซึ่งล้วนแต่ทำให้ต้นทุนการระดมทุนเพิ่มขึ้น ในการทำ ICO นั้น บริษัทจะเขียนสมุดปกขาว (Whitepaper) ซึ่งระบุรายละเอียดต่าง ๆ เช่น ข้อมูลทางเทคนิคของโครงการอ้างอิง แผนธุรกิจ คุณสมบัติต่าง ๆ ของดิจิทัลโทเคนที่จะเสนอขาย เป็นต้น ดิจิทัลโทเคนจะขายให้แก่นักลงทุน โดยนิยมแลกเปลี่ยนกับคริปโทเคอร์เรนซีสกุลหลัก ทั้งนี้ ดิจิทัลโทเคนสามารถเป็นได้ทั้งตัวแทนที่แสดงถึงสิทธิในการเข้าถึงกิจกรรมที่บริษัทระบุไว้ (อาจกลายเป็นคริปโทเคอร์เรนซีหรือสื่อกลางในการแลกเปลี่ยน ถ้าได้รับการยอมรับ) และเปิดโอกาสในการทำกำไรจากการเปลี่ยนแปลงราคาดิจิทัลโทเคน

ICO แบ่งได้เป็น 2 รูปแบบหลัก ตามคุณสมบัติของดิจิทัลโทเคนที่นำเสนอขาย ได้แก่ โทเคนหลักทรัพย์ (Securities Token) เช่น tZERO KODAKOne Polymath เป็นต้น สร้างขึ้นเพื่อเพิ่มความสามารถในการซื้อขายสินทรัพย์ชนิดต่าง ๆ (Tradable Assets) โดยอ้างอิงกับสินทรัพย์ของกิจการ ซึ่งทำให้ราคาของโทเคนชนิดนี้ขึ้นอยู่กับสินทรัพย์เหล่านั้น และผลตอบแทนของผู้ลงทุนเชื่อมโยงกับผลประกอบการของกิจการ ด้วยลักษณะดังกล่าว โทเคนชนิดนี้จึงสุ่มเสี่ยงที่จะถูกควบคุมด้วยกฎหมายหลักทรัพย์ ในขณะที่ โทเคนแสดงสิทธิการใช้งาน (Utility Token) เช่น Bitcoin Basic Attention Token (BAT) Filecoin เป็นต้น เป็นโทเคนที่ผู้ครอบครองสามารถเข้าถึงแพลตฟอร์มของโครงการ รวมถึงสินค้าและบริการของกิจการ ทั้งนี้ โทเคนรูปแบบนี้ยังไม่ถูกควบคุมจากกฎหมายของประเทศส่วนใหญ่ในปัจจุบัน

ICO สามารถให้ผลตอบแทนได้หลายด้าน โดยผู้ลงทุนมีโอกาสเก็บเกี่ยวผลประโยชน์ได้อย่างต่อเนื่องจากโครงการที่ประสบความสำเร็จ อีกทั้ง การทำ ICO ยังเป็นการสร้างเครือข่ายผู้ใช้งานและประชาสัมพันธ์โครงการคล้ายกับการเก็บค่าสมัครสมาชิก ทั้งนี้ ฝ่ายกำกับนโยบายในบางประเทศเริ่มควบคุมการระดมทุนสาธารณะ (Crowdfunding) โดยจำกัดทั้งลักษณะของนักลงทุน และจำนวนเงินลงทุน ในขณะที่ ICO ซึ่งมีลักษณะคล้ายกัน แต่เกิดขึ้นทีหลัง หลายประเทศจึงอยู่ระหว่างการพัฒนามาตรการควบคุม จากช่องโหว่ดังกล่าว ICO จึงถูกใช้เป็นช่องทางในการฉ้อโกง ด้วยการสร้างโครงการที่ไม่ตั้งใจจะดำเนินการจนสำเร็จ ด้วยเหตุนี้ เมื่อประกอบกับความกังวลถึงผลกระทบ

ต่อเสถียรภาพทางเศรษฐกิจ ธนาคารแห่งประเทศจีนจึงห้ามการทำ ICO ในเดือนกันยายน พ.ศ. 2560

เมื่อเปรียบเทียบ ICO กับการเสนอขายหุ้นใหม่แก่ประชาชนทั่วไปเป็นครั้งแรก (Initial Public Offering: IPO) จะพบว่ามีข้อแตกต่างดังต่อไปนี้ ผู้ซื้อ ICO จะได้รับดิจิทัลโทเคนเป็นหลักไม่ใช่หุ้น จึงไม่มีอำนาจควบคุมกิจการ แต่ชดเชยด้วยสิทธิที่หลากหลายของดิจิทัลโทเคนนั้น ๆ ขณะที่บริษัทที่ขาย IPO มักเป็นกิจการที่ดำเนินงานมาอย่างยาวนาน จึงมีผลประกอบการรองรับชัดเจน ตรวจสอบได้ ต่างจากบริษัทที่ขาย ICO ซึ่งมีโอกาสล้มเหลวสูง นอกจากนี้ การทำ IPO ยังมีกฎหมายควบคุมหลายด้าน ทั้งกำหนดให้มีหนังสือชี้ชวนที่ได้รับการรับรองเพื่อประกอบการเสนอขาย มีหน่วยงานกำกับดูแลเพื่อคุ้มครองนักลงทุนตลอดกระบวนการ แตกต่างจากสมุดปกขาวของ ICO ที่ขึ้นกับบริษัทที่เสนอขาย แต่ไม่มีมาตรฐาน และยังไม่มีกฎหมายรองรับ นักลงทุนจึงยังไม่ได้รับการคุ้มครอง อย่างไรก็ตาม ผู้ลงทุนและบริษัทที่ขาย ICO มีแนวโน้มที่จะติดต่อกันโดยตรงมากกว่าการระดมทุนด้วย IPO ที่ดำเนินการผ่านตัวกลาง ยิ่งไปกว่านั้น ICO ยังสามารถเข้าถึงนักลงทุนในต่างประเทศได้ง่ายกว่า IPO

ICO เริ่มต้นอย่างเป็นทางการในปี พ.ศ. 2556 โดยมาสเตอร์คอยน์ ซึ่งระดมทุนได้ประมาณ 5,000 บิทคอยน์ เทียบเป็นมูลค่ามากกว่า 500,000 ดอลลาร์สหรัฐ ณ ขณะนั้น ทั้งนี้ ICO ได้รับความนิยมอย่างมากในปี พ.ศ. 2560 ICOdata รายงานว่า มีมูลค่ารวม 6,000 ล้านดอลลาร์สหรัฐ เพิ่มขึ้นกว่า 60 เท่า เมื่อเทียบกับปี พ.ศ. 2559 แต่ Cointelegraph พบว่าเงินทุนร้อยละ 37 กระจุกตัวอยู่กับโครงการใหญ่เพียง 20 โครงการ เช่น เทโซส์ (Tezos) 232 ล้านดอลลาร์สหรัฐ แบนคอร์ (Bancor) 153 ล้านดอลลาร์สหรัฐ สเตตัส (Status) 100 ล้านดอลลาร์สหรัฐ เป็นต้น อย่างไรก็ตาม Tokendata รายงานไว้ในเดือนกุมภาพันธ์ พ.ศ. 2561 ว่าจากทั้งหมด 902 โครงการที่ระดมทุนผ่าน ICO ในปี พ.ศ. 2560 มี 142 โครงการ ที่ระดมทุนไม่สำเร็จ และ 276 โครงการ ที่ล้มเหลว นั่นหมายความว่า มีโครงการล้มเหลวไปแล้วร้อยละ 46 นอกจากนี้ ยังมีอีก 113 โครงการ ที่ส่งสัญญาณว่ากำลังจะล้มเหลว ถึงแม้ว่าความเสี่ยงจะสูง แต่ ICO ยังคงเติบโตอย่างต่อเนื่อง ภายในสองเดือนแรกของปี พ.ศ. 2561 มี ICO จำนวน 271 โครงการ ระดมทุนได้มากกว่า 2,000 ล้านดอลลาร์สหรัฐ

การประเมินมูลค่าคริปโทเคอร์เรนซี

หากเงินตรามีค่า เพราะมีอยู่อย่างจำกัด และคนเชื่อว่าเป็นสิ่งมีค่า[20] ดังนั้น การที่คนกลุ่มหนึ่งเชื่อในกลไกคณิตศาสตร์ และการเข้ารหัสบนระบบเครือข่าย ก็น่าจะเป็นเหตุผลให้คริปโทเคอร์เรนซี ซึ่งถูกออกแบบให้มีจำนวนจำกัด มีค่าเช่นกัน ทั้งนี้ คริปโทเคอร์เรนซีถูกมองว่ามีลักษณะเหมือนสินค้าโภคภัณฑ์ (Commodity) เพราะคริปโทเคอร์เรนซีชนิดเดียวกันมีคุณสมบัติเหมือนกัน ไม่ขึ้นอยู่กับการขุด นอกจากนี้ คริปโทเคอร์เรนซีหลายชนิด ยังสามารถใช้ประโยชน์ในด้านอื่น ๆ เช่นเดียวกับสินค้าโภคภัณฑ์ ไม่ได้เป็นเพียงสื่อกลางในการแลกเปลี่ยน เมื่อเปรียบเทียบผู้ซื้อขายสินค้าโภคภัณฑ์ กับผู้ซื้อขายคริปโทเคอร์เรนซี ก็ประกอบด้วย 2 กลุ่มหลักเช่นเดียวกัน ได้แก่ กลุ่มผู้ผลิตและผู้ซื้อที่ต้องการใช้ประโยชน์จากสินค้าจริง และกลุ่มนักเก็งกำไรที่ต้องการทำกำไรจากการเปลี่ยนแปลงราคา เพราะฉะนั้น จำนวนนักลงทุนในตลาดคริปโทเคอร์เรนซีที่เพิ่มขึ้นในปัจจุบัน แต่กลับทำให้ราคาผันผวนสูงขึ้น[21] ลักษณะดังกล่าว จึงยืนยันข้อสังเกตของ Joseph Stiglitz ว่าคริปโทเคอร์เรนซีกำลังอยู่ในภาวะฟองสบู่[22] ที่ราคาเพิ่มขึ้นจากการเก็งกำไร ด้วยความคาดหวังว่าราคาจะขึ้นต่อไปเรื่อย ๆ

เมื่อไม่ถูกแทรกแซงโดยภาครัฐ อุปสงค์อุปทาน จึงถือเป็นปัจจัยสำคัญ ที่มีผลต่อการเปลี่ยนแปลงราคาสินค้าโภคภัณฑ์ และคริปโทเคอร์เรนซี ทั้งนี้ แม้ว่าอุปทานของคริปโทเคอร์เรนซีบางชนิดจะถูกควบคุมโดยผู้ดูแลระบบ แต่กลไกราคาของคริปโทเคอร์เรนซีส่วนใหญ่ยังคล้ายกับสินค้าโภคภัณฑ์ อย่างทองคำ คืออุปทานมีอยู่อย่างจำกัด และสัมพันธ์กับความสามารถในการผลิต โดยในกรณีของคริปโทเคอร์เรนซี คือ ระยะเวลาในการสร้างบล็อกใหม่ซึ่งระบบออกแบบไว้ให้เป็นไปอย่างสม่ำเสมอ ถึง

---

[20] ธนาคารกลางสหรัฐฯ (Federal Reserve Bank: Board of Governors of the Federal Reserve System) ระบุว่าในปัจจุบันการพิมพ์ธนบัตร 100 ดอลลาร์สหรัฐ มีต้นทุนเพียง 15.5 เซ็นต์ ด้วยระบบการออกใช้ธนบัตรในปัจจุบันของสหรัฐอเมริกา นั่นหมายความว่า มูลค่ามากกว่าร้อยละ 99 ของสกุลเงินดอลลาร์สหรัฐ มาจากความเชื่อว่าสกุลเงินดังกล่าวมีค่าตามที่รัฐบาลรับรอง

[21] Kim et al. (2016) เสนอวิธีคาดการณ์ความผันผวนของราคาคริปโทเคอร์เรนซี โดยวิเคราะห์จากปริมาณการแสดงความคิดเห็นภายในเครือข่ายผู้สนใจคริปโทเคอร์เรนซี และพบว่าความผันผวนราคาคริปโทเคอร์เรนซีสัมพันธ์กับจำนวนการสื่อสารที่เกี่ยวข้องกับคริปโทเคอร์เรนซีบนระบบอินเทอร์เน็ต อย่างไรก็ตาม Li and Wang (2017) พบว่าการเปลี่ยนแปลงอัตราแลกเปลี่ยนบิทคอยน์เมื่อเทียบกับดอลลาร์สหรัฐ อธิบายได้ด้วยปัจจัยพื้นฐานทางเศรษฐกิจ (Economics Fundamental Factors) และสภาพตลาด ณ ขณะนั้น มากกว่าการเปลี่ยนแปลงของปัจจัยทางเทคโนโลยี ในขณะที่ Katsiampa (2017) เสนอว่า AR-CGARCH เป็นแบบจำลองทางเศรษฐมิติที่อธิบายความผันผวนของราคาบิทคอยน์ได้แม่นยำที่สุด

[22] การศึกษาของ Fry and Cheah (2016) ยืนยันว่าตลาดคริปโทเคอร์เรนซีกำลังอยู่ในภาวะฟองสบู่ ทั้งยังพบว่าตลาดคริปโทเคอร์เรนซีแต่ละสกุลเปลี่ยนแปลงอย่างสัมพันธ์กัน โดยเฉพาะอย่างยิ่งบิทคอยน์ และริปเปิล โดยความผันผวนในตลาดริปเปิลสามารถกระจาย (Spillover) ไปยังตลาดบิทคอยน์

จะมีประเด็นความคุ้มค่าในการขุด จากค่าดำเนินการต่าง ๆ [23] เช่น ค่าเครื่องขุด ค่าไฟฟ้า ค่าดำเนินการ เป็นต้น แต่ด้วยโครงสร้างของระบบ ทำให้นักขุดมีอำนาจต่อรองต่ำ และอาจกล่าวได้ว่าอุปสงค์จากนักเก็งกำไรเป็นปัจจัยหลักที่กดดันราคาคริปโทเคอร์เรนซีในปัจจุบัน แต่ความผันผวนของราคาคริปโทเคอร์เรนซี ที่ดูเหมือนจะไม่อ้างอิงมูลค่าแท้จริง (Intrinsic Value) เป็นประเด็นปัญหา นำมาซึ่งคำถามว่าคริปโทเคอร์เรนซีมีมูลค่าแท้จริงหรือไม่ และเมื่อไม่มีสินทรัพย์อ้างอิง ไม่รายงานผลประกอบการ ผลตอบแทนไม่ชัดเจน และไม่จ่ายปันผล จะประเมินมูลค่าได้อย่างไร?

Tom Lee อดีตผู้บริหารของ JPMorgan Chase กล่าวว่าด้วยคุณสมบัติบางประการเป็นไปได้ที่คริปโทเคอร์เรนซีจะเข้ามาทำหน้าที่เก็บรักษามูลค่าแทนทองคำ ซึ่งการประเมินราคาอาจอ้างอิงจากสัดส่วนระหว่างมูลค่าปัจจุบันของทองคำในระบบที่จะถูกแทนที่ด้วยคริปโทเคอร์เรนซีกับอุปทานรวมของคริปโทเคอร์เรนซี นอกจากนี้ Wang (2014) พัฒนาแบบจำลองการประเมินมูลค่าของบิทคอยน์จากสมการของการแลกเปลี่ยน (Equation of Exchange) โดยเสนอว่า มูลค่าของบิทคอยน์ขึ้นกับความต้องการของผู้ถือที่จะเก็บบิทคอยน์ไว้ โดยไม่นำมาใช้ทำธุรกรรม เนื่องจากผู้ถือบิทคอยน์ (Hodler[24]) จำนวนหนึ่งมองว่าบิทคอยน์สามารถเก็บรักษามูลค่าได้ และราคาน่าจะเพิ่มขึ้นต่อไป ซึ่งมีมุมมองคล้ายกับผู้ถือทองคำ ดังนั้น นอกจากไม่ขายคริปโทเคอร์เรนซีแล้ว คนกลุ่มนี้ยังพร้อมจะซื้อเพิ่มเพื่อรอการใช้ประโยชน์ในอนาคต พวกเขาจึงมีแนวโน้มที่จะเป็นแหล่งอุปทาน และพฤติกรรมการซื้อขายยังสื่อถึงมูลค่าพื้นฐาน[25] ของคริปโทเคอร์เรนซีอีกด้วย อย่างไรก็ตาม เป็นการยากที่จะระบุตัวตนของพวกเขาในเครือข่ายเพื่อใช้กับทฤษฎีนี้

---

[23] Hayes (2017) ระดับการแข่งขันระหว่างนักขุดหรือความสามารถในการประมวลผล อัตราการผลตอบแทนเมื่อเทียบกับเวลาในการสร้างบล็อกใหม่ และความยากของปัญหาคณิตศาสตร์ ซึ่งถือเป็นต้นทุนของการขุดที่ทำให้คริปโทเคอร์เรนซีแต่ละชนิดแตกต่างกัน โดยปัจจัยทั้งสามมีความสัมพันธ์กับการเปลี่ยนแปลงราคาบิทคอยน์ ซึ่งต้นทุนที่เพิ่มขึ้นสามารถอธิบายการเพิ่มขึ้นของราคาบิทคอยน์ได้ ทั้งนี้ Balcilar et al. (2017) พบว่าปริมาณการซื้อขายก็มีความสัมพันธ์กับผลตอบแทนจากการลงทุนในตลาดบิทคอยน์เช่นเดียวกัน

[24] Hodler มีรากฐานมาจากคำว่า Hodl ซึ่งเกิดขึ้นในปี พ.ศ. 2556 โดยสื่อถึงพฤติกรรมของคนกลุ่มหนึ่งที่เชื่อในบิทคอยน์อย่างแน่วแน่ แม้ว่าในขณะนั้นราคาบิทคอยน์จะลดลง จากความกังวลต่อนโยบายของรัฐบาลจีน

[25] แบบจำลองการประเมินมูลค่าของบิทคอยน์ของ Joseph Wang

$$p_b = \frac{1}{l_t \alpha_t}$$

โดย p_b คือ ราคาต่อหน่วยของบิทคอยน์

l_t คือ แนวโน้มที่บิทคอยน์จะถูกใช้ทำธุรกรรม

α_t คือ ค่าคงที่ ซึ่งเกี่ยวข้องกับความเร็วของบิทคอยน์ที่ถูกใช้ทำธุรกรรม (ความถี่เฉลี่ยที่บิทคอยน์หนึ่งหน่วยจะถูกใช้)

ในทางตรงกันข้าม Karl Marx กล่าวว่า จำนวนแรงงานที่ใช้ผลิตแสดงถึงคุณค่าของสินค้านั้น สอดคล้องกับ Metcalfe's Law ที่ระบุว่า คุณค่าของเครือข่ายโทรคมนาคมเป็นสัดส่วนกับจำนวนผู้ใช้งานบนเครือข่ายยกกำลังสอง ซึ่ง Gandal and Halaburda (2016) ยืนยันว่า ผลกระทบจากเครือข่าย (Network Effect) ทำให้บิทคอยน์ได้รับความนิยม และมีมูลค่ามากกว่าคริปโทเคอร์เรนซีชนิดอื่น ๆ แม้จะมีคุณสมบัติด้อยกว่าคริปโทเคอร์เรนซีเหล่านั้น ทั้งนี้ Van Vliet (2018) เสนอวิธีประเมินราคาบิทคอยน์ โดยอ้างอิงตาม Metcalfe's Law และพัฒนาต่อจาก Peterson (2017)

จุดยืนของประเทศต่าง ๆ ที่มีต่อคริปโทเคอร์เรนซี

ความผันผวนของคริปโทเคอร์เรนซี และข้อจำกัดในการควบคุมแทรกแซง สร้างความกังวลในหมู่ผู้กำหนดนโยบายในหลายประเทศ ถึงผลกระทบในด้านต่าง ๆ ที่อาจเกิดขึ้นจากการเติบโตของคริปโทเคอร์เรนซี โดยเฉพาะอย่างยิ่งการเป็นช่องทางการฟอกเงินของอาชญากร ความเสียหายที่อาจเกิดแก่นักลงทุนรายย่อย และผลกระทบต่อเสถียรภาพของระบบการเงิน อย่างไรก็ตาม ผู้กำหนดนโยบายทั่วโลกกำลังศึกษา เพื่อพัฒนากฎระเบียบ ที่สามารถป้องกันปัญหาเหล่านั้น โดยไม่ปิดกั้นการใช้ประโยชน์จากเทคโนโลยี ทั้งนี้ สถานการณ์ที่น่าสนใจของคริปโทเคอร์เรนซีในประเทศต่าง ๆ มีดังต่อไปนี้

- สหรัฐอเมริกา ในเดือนมีนาคม พ.ศ. 2556 Financial Crimes Enforcement Network (FinCEN) กำหนดให้กิจกรรมที่ถือเป็นธุรกิจบริการด้านเงิน (Money Services Businesses: MSBs) ซึ่งเกี่ยวข้องกับเงินตราเสมือนแบบกระจายศูนย์ (Decentralized Virtual Currency) ต้องถูกควบคุมด้วยกฎหมายต่อต้านการฟอกเงิน ทำให้ตลาดซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซี และนักขุดที่ทำกิจกรรมแลกเปลี่ยนด้วยสกุลเงินดอลลาร์สหรัฐต้องขึ้นทะเบียนกับรัฐบาล และกิจการจะต้องรับผิดชอบการเก็บข้อมูลลูกค้า ต่อมาในปี พ.ศ. 2557 Internal Revenue Service จัดว่าคริปโทเคอร์เรนซีเป็นทรัพย์สิน โดยกำไรจากส่วนเกินทุนระยะยาว (Long-Term Capital Gains) จะต้องเสียภาษี ทั้งนี้ ในปี พ.ศ. 2558 Commodities Futures Trading Commission (CFTC) ระบุว่า เงินตราเสมือนอาจถือเป็นสินค้าโภคภัณฑ์ หรือตราสารอนุพันธ์ (Derivatives Contracts) จึงอยู่ภายใต้การควบคุมของ CFTC ต่อมาในปี พ.ศ. 2560 U.S. Securities and Exchange Commission (SEC) พิจารณาว่าการขาย ICO อาจสามารถกำกับดูแลได้ด้วยกฎหมายหลักทรัพย์ (DAO Report of Investigation) ซึ่งการตีความดังกล่าวไม่เพียงมีผลกับ ICO ของบริษัทในสหรัฐอเมริกา แต่ยังส่งผลกระทบต่อ

กิจการในต่างประเทศ ที่ขาย ICO ให้กับนักลงทุนสหรัฐฯด้วย

- อังกฤษ ในปี พ.ศ. 2556 Her Majesty's Revenue and Customs จัดให้บิทคอยน์ และคริปโทเคอร์เรนซีชนิดอื่น ๆ เป็นบัตรกำนัล (Single Purpose Vouchers) ซึ่งจะต้องเสียภาษีมูลค่าเพิ่มระหว่างร้อยละ 10 ถึง 20 อย่างไรก็ตาม ในปี พ.ศ. 2559 ธนาคารแห่งประเทศอังกฤษโดย Barrdear and Kumhof (2016) ศึกษาความเป็นไปได้ในการออกคริปโทเคอร์เรนซีที่หนุนหลังโดยสหราชอาณาจักร โดยคาดว่าจะช่วยเพิ่มผลิตภัณฑ์มวลรวมภายในประเทศ (Gross Domestic Product - GDP) ได้ถึงร้อยละ 3 ทั้งนี้ อังกฤษ และสหภาพยุโรป เปิดโอกาสให้คริปโทเคอร์เรนซี และธุรกิจฟินเทคอื่น ๆ เติบโต ในปัจจุบันจึงยังไม่มีการควบคุมที่ชัดเจน โดยให้ความสำคัญกับการศึกษา และการให้คำแนะนำที่ไม่ทำลายการสร้างนวัตกรรม

- รัสเซีย ในปี พ.ศ. 2559 รัฐบาลประกาศเตือนว่าการซื้อขายคริปโทเคอร์เรนซีในรัสเซียนั้นผิดกฎหมาย เนื่องจากขัดกับมาตรา 140 ของ Russian Civil Code ที่ระบุว่าต้องใช้เงินตราสกุลรูเบิลในการแสดงราคา และชำระสินค้าภายในประเทศรัสเซีย อย่างไรก็ตาม ในปี พ.ศ. 2560 Federal Tax Service เปลี่ยนแปลงนโยบาย โดยเตรียมออกกฎหมายรับรองการทำธุรกรรมด้วยคริปโทเคอร์เรนซี แต่ร่างกฎหมายฉบับแรกที่เตรียมนำเข้าสู่สภาดูมา (State Duma) ในปี พ.ศ. 2561 กลับระบุว่าคริปโทเคอร์เรนซีเป็นสินทรัพย์ทางการเงินดิจิทัล (Digital Financial Asset) แต่ยังไม่รับรองให้ใช้เป็นสื่อกลางของระบบชำระเงิน นอกจากนี้ ร่างกฎหมายฉบับดังกล่าวยังจำกัดการลงทุนใน ICO ของนักลงทุนที่ไม่ได้รับการรับรองไว้ไม่เกิน 900 ดอลลาร์สหรัฐ และมีเป้าหมายจะขึ้นทะเบียนนักขุด รวมถึงให้ทำการซื้อขายคริปโทเคอร์เรนซีในตลาดที่มีใบอนุญาตเท่านั้น

- ออสเตรเลีย ASIC (Australian Securities and Investments Commission) ตั้งศูนย์นวัตกรรมฟินเทค (FinTech Innovation Hub) ในปี พ.ศ. 2558 เพื่อสนับสนุนผู้ประกอบการที่ใช้เทคโนโลยีในการพัฒนาบริการทางการเงิน และตลาดทุน รวมทั้งใช้เป็นแหล่งศึกษา และพัฒนากฎระเบียบให้เหมาะสมกับธุรกิจฟินเทค นอกจากนี้ ในเดือนกันยายน พ.ศ. 2560 ASIC นำเสนอแนวทางในการออก ICO โดยรวบรวมประเด็นทางกฎหมายที่เกี่ยวข้อง พร้อมทั้งเตือนผู้ลงทุนถึงความเสี่ยงจากการเก็งกำไร และการฉ้อโกง

- จีน แม้ว่าจะเป็นหนึ่งในประเทศที่มีการลงทุนที่เกี่ยวข้องกับคริปโทเคอร์เรนซีมากที่สุดในโลก แต่ในปี พ.ศ. 2552 รัฐบาลจีนประกาศห้ามใช้เงินตราเสมือนในการซื้อขายสินค้าและบริการ เนื่องจากไม่มั่นใจถึงผลกระทบที่อาจเกิดกับระบบการเงิน ต่อมาในปี พ.ศ. 2556 ธนาคารแห่งประเทศจีน ห้ามสถาบันทางการเงินของจีนใช้บิทคอยน์ ส่งผลให้ BTCC ซึ่งเป็นตลาดซื้อขายแลกเปลี่ยนบิทคอยน์ที่ใหญ่

ที่สุดในโลก ณ ขณะนั้น ไม่สามารถรับเงินลงทุนในสกุลหยวน นอกจากนี้ เมื่อเดือนกันยายน พ.ศ. 2560 องค์กรที่เกี่ยวข้องกับการกำหนดนโยบายทางการเงินของจีน 7 แห่ง ห้ามทำกิจกรรมเกี่ยวกับ ICO โดยมีผลย้อนหลังถึง ICO ที่ขายไปแล้ว จะต้องยกเลิก และคืนเงินให้แก่นักลงทุน อย่างไรก็ตาม นับตั้งแต่ปี พ.ศ. 2557 ธนาคารแห่งประเทศจีนกำลังพัฒนาเงินตราดิจิทัลของตัวเอง ซึ่งในปี พ.ศ. 2560 ธนาคารแห่งประเทศจีนรายงานว่าการทดลองทำธุรกรรมระหว่างธนาคารกลาง และธนาคารพาณิชย์ประสบความสำเร็จเป็นอย่างดี โดยในปัจจุบันอยู่ระหว่างทดสอบ และแก้ปัญหาด้านความปลอดภัยของระบบ ก่อนนำเสนอสู่สาธารณะ

- ญี่ปุ่น ในเดือนมีนาคม พ.ศ. 2559 รัฐบาลญี่ปุ่นสนับสนุนการเติบโตของธุรกิจฟินเทคในประเทศ โดยประกาศรับรองสถานะของเงินตราเสมือน ว่ามีมูลค่าเหมือนสินทรัพย์ และสามารถใช้ชำระเงิน รวมถึงโอนให้กันได้ ทั้งนี้ กำหนดให้ตลาดซื้อขายแลกเปลี่ยนเงินตราเสมือนต้องขึ้นทะเบียนกับรัฐบาล โดยสถานะทางกฎหมายของคริปโทเคอร์เรนซี ได้รับการรับรองอย่างเป็นทางการจากรัฐบาลญี่ปุ่น เมื่อเดือนมีนาคม พ.ศ. 2560 ซึ่งระบุว่าคริปโทเคอร์เรนซีถือเป็นหนึ่งในระบบชำระเงินของญี่ปุ่น นอกจากนี้ ในปี พ.ศ. 2561 National Tax Agency ระบุว่ากำไรจากการซื้อขายคริปโทเคอร์เรนซีถือเป็นรายได้เบ็ดเตล็ด (Miscellaneous Income) ซึ่งจะต้องเสียภาษีระหว่างร้อยละ 15 ถึง 55

- เกาหลีใต้ ในเดือนกันยายน พ.ศ. 2560 Financial Services Commission ห้ามการระดมทุนด้วย ICO และคริปโทเคอร์เรนซีทุกชนิด โดยจะควบคุมการซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซีอย่างเข้มงวด ซึ่งในปีเดียวกันนี้ Financial Services Commission ยังห้ามสมาชิกของ Korea Financial Investment Association ขายสัญญาซื้อขายล่วงหน้าที่อ้างอิงราคาบิทคอยน์ ทั้งนี้ ในเดือนมกราคม พ.ศ. 2561 เพื่อจัดการกับปัญหาอาชญากรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซี Financial Service Commission จึงกำหนดให้ต้องแสดงชื่อจริงในการซื้อขายบิทคอยน์ โดยชื่อเจ้าของบัญชีในตลาดซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซี จะต้องเป็นชื่อเดียวกับเจ้าของบัญชีธนาคารที่เชื่อมโยงกัน

- สิงคโปร์ ในปี พ.ศ. 2556 Monetary Authority of Singapore (MAS) ออกรายงานเตือนถึงความเสี่ยงจากการใช้บิทคอยน์ แต่ระบุว่าการซื้อขายแลกเปลี่ยนด้วยบิทคอยน์เป็นการตัดสินใจทางธุรกิจ ซึ่ง MAS จะยังไม่แทรกแซง ต่อมาในปี พ.ศ. 2557 Inland Revenue Authority of Singapore เสนอแนวทางการจัดเก็บภาษี ที่ระบุว่าธุรกรรมที่เกี่ยวกับบิทคอยน์ถือเป็นการแลกเปลี่ยนสินค้าระหว่างกันโดยตรง (Barter Exchange) ซึ่งกำไรที่เกิดขึ้นจะต้องเสียภาษี นอกจากนี้ ในปี พ.ศ. 2560 MAS ยังระบุแนวทางการควบคุม ICO ว่าดิจิทัลโทเคนที่มี

ลักษณะเป็นผลิตภัณฑ์ในตลาดทุน (Capital Market Product) จะต้องถูกควบคุมโดย Securities and Futures Act (SFA) และ Financial Advisers Act

สถานการณ์ของคริปโทเคอร์เรนซีในประเทศไทย

ผู้กำหนดนโยบายภายในประเทศไทย มีความตื่นตัว และใช้แนวทางการดำเนินงานที่เปิดกว้างต่อคริปโทเคอร์เรนซี และเทคโนโลยีทางการเงินอื่น ๆ โดยทำความเข้าใจ และร่วมมือกับทุกส่วนที่เกี่ยวข้อง เพื่อสร้างระบบนิเวศทางธุรกิจ (Ecosystem) ที่เหมาะสมทัดเทียมประเทศชั้นนำอื่น ๆ เนื่องจากมองถึงโอกาสที่ประชาชนภายในประเทศจะได้รับจากการใช้ประโยชน์เทคโนโลยีทางการเงิน ซึ่งสอดคล้องกับผลการศึกษาเกี่ยวกับการสร้างระบบนิเวศทางธุรกิจเทคโนโลยีทางการเงินในประเทศไทย ของ Chunhachinda (2017) ทั้งนี้ มีการกำหนดบทบาทหน้าที่ของหน่วยงานหลัก ในการกำกับดูแลคริปโทเคอร์เรนซี เช่น กระทรวงการคลัง ป้องกันการหลอกลวงประชาชน และกำหนดมาตรการทางภาษี สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ดูแลเพื่อให้เกิดความโปร่งใสในการลงทุน สำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) ป้องกันการฟอกเงิน และใช้เป็นช่องทางก่อการร้าย ธนาคารแห่งประเทศไทย (ธปท.) ป้องกันผลกระทบที่อาจเกิดกับเสถียรภาพของระบบการเงิน และระบบการชำระเงิน เป็นต้น นอกจากนี้ ในปี พ.ศ. 2559 ธปท. ได้ปรับโครงสร้างองค์กรเพื่อรองรับเทคโนโลยีทางการเงิน โดยตั้งฝ่ายเทคโนโลยีทางการเงิน ซึ่งอยู่ภายใต้สายงานนโยบายระบบการชำระเงินและเทคโนโลยีทางการเงิน เช่นเดียวกับ ก.ล.ต. ที่ตั้งฝ่ายส่งเสริมเทคโนโลยีทางการเงิน อย่างไรก็ตาม ธปท.คำนึงถึงผลกระทบของคริปโทเคอร์เรนซีที่อาจมีต่อระบบการเงินเป็นสำคัญ โดยในปี พ.ศ. 2556 ธปท. ไม่อนุญาตให้ทำธุรกรรมด้วยบิทคอยน์ แต่ระเบียบดังกล่าวได้รับการผ่อนผันในปี พ.ศ. 2560 เพื่อเปิดโอกาสให้นวัตกรรมทางการเงินเติบโตภายในประเทศ โดยยังคงจับตาดูอย่างใกล้ชิด

ตลาดซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซีในประเทศไทยจะต้องได้รับใบอนุญาตพาณิชย์อิเล็กทรอนิกส์ จากกระทรวงพาณิชย์ ในปัจจุบันมีตลาดที่สำคัญ 3 ตลาด ได้แก่ bx.in.th tdax.com และ coins.co.th โดยทุกตลาดจะต้องมีระบบทำความรู้จักกับลูกค้า (KYC) และการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Client Due Diligence: CDD) ซึ่งเป็นไปตามกฎกระทรวงที่บัญญัติไว้ในปี พ.ศ. 2555 ทั้งนี้ ในปี พ.ศ. 2560 ก.ล.ต. ได้ให้แนวทางการกำกับดูแล ICO โดยระบุว่าการขายดิจิทัลโทเคนที่มีการให้ผลตอบแทนและสิทธิคล้ายกับหลักทรัพย์จะต้องดำเนินการตามกฎหมายที่เกี่ยวข้อง ในขณะที่ ธปท. ออกหนังสือห้ามสถาบันการเงินทำธุรกรรมที่เกี่ยวข้องกับคริปโทเคอร์เรนซี ใน

เดือนกุมภาพันธ์ปี พ.ศ. 2561 ซึ่งครอบคลุมการเข้าไปลงทุนหรือซื้อขายในคริปโทเคอร์เรนซี การให้บริการรับแลกเปลี่ยนคริปโทเคอร์เรนซี การสร้างแพลตฟอร์มเพื่อเป็นสื่อกลางให้ลูกค้าเข้าไปทำธุรกรรมเกี่ยวกับคริปโทเคอร์เรนซี การให้ลูกค้าใช้บัตรเครดิตในการซื้อคริปโทเคอร์เรนซี การสนับสนุนหรือให้คำปรึกษากับลูกค้าเกี่ยวกับการลงทุนหรือการแลกเปลี่ยนคริปโทเคอร์เรนซี นอกจากนี้ ในเดือนมีนาคมปี พ.ศ. 2561 ที่ประชุมคณะรัฐมนตรี ได้พิจารณาเห็นชอบร่างพระราชกำหนด (พ.ร.ก.) การประกอบสินทรัพย์ดิจิทัล โดยกำหนดอัตราภาษีเงินได้บุคคลธรรมดาหัก ณ ที่จ่ายในอัตราร้อยละ 15 สำหรับกำไรจากทรัพย์สินดิจิทัล

ผลการสำรวจพฤติกรรมการใช้งานดิจิทัลโทเคนของคนไทยกว่า 2,000 คน จากเว็บไซต์ SiamBlockchain ในปี พ.ศ. 2560 พบว่าคนไทยใช้บิทคอยน์ร้อยละ 41.8 อีเธอร์ร้อยละ 25.4 และไลท์คอยน์ร้อยละ 11 ตามลำดับ ซึ่งเน้นการขุดมากกว่าซื้อขาย นอกจากนี้ ยังพบว่ามีเพียงร้อยละ 6.2 ที่ลงทุนใน ICO ทั้งนี้ เริ่มมีนักพัฒนาชาวไทยออกดิจิทัลโทเคนที่ได้รับการยอมรับและถูกใช้เป็นคริปโทเคอร์เรนซี เช่น OmiseGo (ไม่ต้องผูกกับบัญชีธนาคาร) Zcoin (เพิ่มความเป็นส่วนตัวให้กับผู้ใช้งาน) Hommalicoin (ตัดพ่อค้าคนกลาง โดยราคาอ้างอิงข้าวหอมมะลิอำนาจเจริญ) เป็นต้น และยิ่งไปกว่านั้น มีกิจการในประเทศไทยที่ระดมทุนผ่าน ICO เช่น OmiseGo (ระดมทุน 20 ล้านดอลลาร์สหรัฐ ผ่าน Bitcoin Suisse AG) JFIN Coin (ระดมทุน 660 ล้านบาท ผ่านตลาด TDAX เพื่อพัฒนา Decentralized Digital Lending Platform) Tuk Tuk Pass (ระดมทุน 700 ล้านดอลลาร์สหรัฐ เพื่อสร้างแพลตฟอร์มเชื่อมโยงบริการด้านการท่องเที่ยว) เป็นต้น ในปี พ.ศ. 2561 ยังมีการเปิดตัว ICORA ซึ่งเป็นบริษัทที่ปรึกษาด้านการออก ICO แห่งแรก ๆ ของโลกอีกด้วย

อนาคตของคริปโทเคอร์เรนซี

กิจกรรมผิดกฎหมาย และราคาที่ผันผวน ทำให้คริปโทเคอร์เรนซีถูกเพ่งเล็งจากฝ่ายกำกับนโยบาย ซึ่งชัดเจนว่าการแทรกแซงยังสามารถทำได้ เนื่องจากคริปโทเคอร์เรนซีที่ไม่สามารถแยกตัวจากระบบการเงินได้อย่างสมบูรณ์ เช่น ในปี พ.ศ. 2556 สำนักงานสอบสวนกลาง (Federal Bureau of Investigation: FBI) ใช้กฎหมายต่อต้านการฟอกเงินปิดตลาดซิลค์โรด และอายัดบัญชีที่เชื่อมโยงกับตลาดฯ เมาท์ก๊อก ธนาคารแห่งประเทศไทยขอความร่วมมือให้ธนาคารพาณิชย์หยุดทำธุรกรรมที่เกี่ยวกับคริปโทเคอร์เรนซี ในปี พ.ศ. 2561 เป็นต้น นอกจากนี้ Raymaekers (2015) และ Harwick (2016) ยังได้สรุปปัจจัยอื่น ๆ ที่มีผลต่ออนาคตของคริปโทเคอร์เรนซี เช่น การพัฒนาวิธีการเก็บรักษาคริปโทเคอร์เรนซีที่ปลอดภัยจากการสูญหายและการจารกรรม จำนวนร้านขายสินค้าและบริการที่รับชำระด้วยค

ริปโทเคอร์เรนซี ความเข้าใจและการยอมรับเงินตราดิจิทัลของประชาชน การใช้ประโยชน์ในด้านอื่น ๆ ของคริปโทเคอร์เรนซี แนวทางจัดการเกี่ยวกับการไม่ระบุตัวตนและประเด็นภาษี การพัฒนาและการแพร่กระจายของระบบโทรคมนาคมและเทคโนโลยีอื่น ๆ เป็นต้น

ประเด็นเหล่านั้นยังเป็นคำถามที่ต้องใช้เวลาพิสูจน์ อย่างไรก็ตาม ไม่ว่าคริปโทเคอร์เรนซีจะเติบโตจนแทนที่เงินตราสกุลหลัก หรือเป็นเพียงกระแสการเก็งกำไรระยะสั้น แต่เชื่อว่าเทคโนโลยีบล็อกเชน มีศักยภาพมากพอที่จะถูกใช้ประโยชน์ต่อไปในอนาคต อย่างไรก็ตาม การพัฒนาอย่างไม่หยุดนิ่งของเทคโนโลยี นอกจากทำให้มีสิ่งใหม่ ๆ เก็บขึ้นในวงการคริปโทเคอร์เรนซี เทคโนโลยีบล็อกเชนก็มีความก้าวหน้าเช่นกัน เริ่มต้นจาก บล็อกเชน 1.0 ซึ่งถูกนำมาใช้ในแง่การเป็นสื่อการในการแลกเปลี่ยนเพียงอย่างเดียว บล็อกเชน 2.0 ใช้บล็อกเชนในการทำธุรกรรม โดยเฉพาะการสร้างสัญญาอัจฉริยะ ซึ่งนำโดยอีเธอร์เรียม ในปี พ.ศ. 2557 บล็อกเชน 3.0 เริ่มต้นในปี พ.ศ. 2560 โดยพัฒนาต่อจากสัญญาอัจฉริยะไปสู่การเป็นแอพพลิเคชันแบบกระจายศูนย์ (Decentralized Application: Dapp) เพื่อลดการพึ่งพาโครงสร้างพื้นฐาน (Infrastructure) ของบุคคลใดบุคคลหนึ่ง โดยจะถูกสร้างและพัฒนา เก็บข้อมูล สื่อสาร รวมทั้งทำงานบนเครือข่าย และบล็อกเชน 4.0 ซึ่งคาดว่าบล็อกเชนจะถูกบูรณาการกับการดำเนินงานต่าง ๆ ของธุรกิจในอนาคต

ยิ่งไปกว่านั้น ในปัจจุบันคาดว่าแฮชกราฟ (HashGraph) อาจเป็นแพลตฟอร์มที่มาแทนที่บล็อกเชน ทั้งนี้ แฮชกราฟ ซึ่งได้รับการรับรองสิทธิบัตรในปี พ.ศ. 2559 เป็นระบบสมุดบัญชีแยกประเภทแบบกระจายศูนย์ ซึ่งใช้การสื่อสารภายในเครือข่ายแบบซุบซิบ (Gossip about Gossip Protocol) และการลงคะแนนแบบเสมือน (Virtual Voting Algorithm) เพื่อรับรองธุรกรรม (แทน Proof-of-Work และ Proof-of-Stake) โดยทุกจุดบนเครือข่ายจะส่งความเห็นของตัวเอง และข้อมูลความเห็นที่ได้รับจากจุดอื่นก่อนหน้า ให้กับจุดที่กำลังสื่อสารกัน (เฉพาะข้อมูลที่อีกจุดไม่มี) ซึ่งทำให้ทุกจุดมีข้อมูลความเห็นของทั้งเครือข่าย โดยไม่ต้องสื่อสารกันโดยตรง วิธีการนี้เพิ่มความยุติธรรม เพราะลดอำนาจนักขุด ซึ่งเคยเป็นผู้เลือกธุรกรรมที่จะรวบรวมไว้ในบล็อก นอกจากนี้แต่ละบล็อกยังไม่จำเป็นต้องเชื่อมต่อกันเป็นเส้นเดียวอย่างบล็อกเชน ซึ่งโครงสร้างแบบนี้ช่วยลดการสูญเสียจากการที่นักขุดสร้างบล็อกพร้อม ๆ กัน และความล่าช้าจากการที่ทั้งเครือข่ายต้องตัดสินใจเลือกบล็อกใหม่ ด้วยกลไกดังกล่าว แฮชกราฟจึงรับรองธุรกรรมได้ประมาณ 250,000 ธุรกรรมต่อวินาที

บทสรุป

เทคโนโลยีทางการเงินเป็นกลุ่มนวัตกรรมที่มีผลต่อความอยู่รอดของสถาบันการเงินเป็นอย่างมาก ซึ่งคาดการณ์กันว่าเทคโนโลยีดังกล่าวไม่เพียงพลิกโฉมหน้าของวงการการเงิน แต่ยังรวมถึงทุกกิจกรรมทางเศรษฐกิจ และชีวิตประจำวัน โดยคริปโทเคอร์เรนซี และบล็อกเชน ถือเป็นแกนกลาง หรือรากฐานที่สำคัญของเทคโนโลยีเหล่านั้น ด้วยความสำคัญของคริปโทเคอร์เรนซี และเทคโนโลยีเบื้องหลัง บทความชิ้นนี้ จึงมุ่งนำเสนอข้อมูลที่เกี่ยวข้องกับคริปโทเคอร์เรนซีอย่างรอบด้าน โดยเฉพาะอย่างยิ่งในแง่ที่เชื่อมโยงกับเศรษฐกิจการเงิน อันจะเห็นได้ว่า เทคโนโลยีนี้มีความซับซ้อนในระดับสูง ทำให้ไม่มีความชัดเจนในหลายประเด็น เพราะฉะนั้น ทุกฝ่ายจึงควรให้ความสนใจ ทำการศึกษา และพัฒนา ทั้งในทางวิชาการ และในทางปฏิบัติ เพื่อสร้างความเข้าใจในวงกว้าง ให้มีการนำเทคโนโลยีนี้ไปใช้ให้เกิดประโยชน์สูงสุด ยิ่งไปกว่านั้น สิ่งที่สำคัญไม่แพ้การใช้ประโยชน์ คือ การเรียนรู้ถึงโทษที่อาจเกิดจากเทคโนโลยี ทั้งนี้ เพื่อวางแนวทางป้องกันปัญหา ซึ่งสามารถสร้างความเสียหายมหาศาล โดยแนวทางเหล่านั้นไม่ควรปิดกั้นโอกาสเติบโตของระบบนิเวศทางธุรกิจเทคโนโลยีทางการเงิน

กิตติกรรมประกาศ

ผู้เขียนขอขอบคุณ คุณ พศิน วณิชย์วรนันต์ ที่ช่วยจัดทำบทความฉบับนี้

บรรณานุกรม

ธนาคารแห่งประเทศไทย ฝ่ายนโยบายการกำกับสถาบันการเงิน. (23) ว. 276/2561. (2018). ขอความร่วมมือสถาบันการเงินไม่ให้ทำธุรกรรมที่เกี่ยวข้องกับคริปโตเคอเรนซี (Cryptocurrency). *ธนาคารแห่งประเทศไทย*

Australian Securities and Investments Commission. (2017). Information Sheet 225 (Info 225). *Australian Securities and Investments Commission*.

Balcilar M., Bouri E., Gupta R., and Roubaud D. (2017). Can Volume Predict Bitcoin Returns and Volatility? A Quantiles-Based Approach. *Economic Modelling*. 64. pp. 74 - 81.

Barrdear J. and Kumhof M. (2016). The Macroeconomics of Central Bank Issued Digital Currencies. *Bank of England*. Working Paper. bitcoin.org. (2009). About bitcoin.org. Web site: https://bitcoin.org/en/about-us

Board of Governors of the Federal Reserve System. (2018). How much does It Cost to Produce Currency and Coin?. *Federal Reserve Bank*.

Brenig C., Accorsi R., and Müller G. (2015). Economic Analysis of Cryptocurrency Backed Money Laundering. *Twenty-Third European Conference on Information Systems*. ECIS 2015 Completed Research Papers.

Chunhachinda P. (2017). FinTech: Towards Thailand 4.0. *Electronic Journal of Open and Distance Innovative Learning (e-JODIL)*. 7 (1). pp. 1 – 23.

Cocco L., Concas G., and Marchesi M. (2017). Using an Artificial Financial Market for studying a Cryptocurrency Market. *Journal of Economic Interaction and Coordination*. 12 (2). pp 345 – 365.

CoinDesk. (2018). Bitcoin (USD) Price. Web site: https://www.coindesk.com/price/

CoinMarketCap. (2018). Cryptocurrency Market Capitalizations.Web site: https://coinmarketcap.com/

CoinMarketCap. (2018). 24 Hour Volume Rankings (Exchange). Website: https://coinmarket cap.com/exchanges/volume/24-hour/all/

Cointelegraph. (2018). Post-ICO Review: What Happens to the Tokens of the Largest ICOs?. Website: https://cointelegraph.com/news/post-ico-review-what-happens-to-the-tokens-of-the-largest-icos

Forbes. (2018). The Richest People in Cryptocurrency.Web site:https://www.forbes.com/ richest-in-cryptocurrency/#508342f71d49

Fry J. and Cheah E. (2016). Negative Bubbles and Shocks in Cryptocurrency Markets. *International Review of Financial Analysis*. 47. pp. 343 - 352.

Gandal N. and Halaburda H. (2016). Can We Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market. *Games*. 7 (3). pp. 1 - 21.

Gjermundrød H. and Dionysiou I. (2014). Recirculating Lost Coins in Cryptocurrency Systems. *International Conference on Business Information Systems*. Conference Paper. pp 229 - 240.

Harwick C. (2016). Cryptocurrency and the Problem of Intermediation. *The Independent Review*. 20 (4). pp. 569 - 588.

Hayes A.S. (2017). Cryptocurrency Value Formation: An Empirical Study Leading to a Cost of Production Model for Valuing Bitcoin. *Telematics and Informatics*. 34 (7). pp. 1308 -1321.

ICOdata. (2018). Funds raised in 2018. Web site: https://www.icodata.io/stats/2018

Katsiampa P. (2017). Volatility Estimation for Bitcoin: A Comparison of GARCH Models. *Economics Letters*. 158. pp. 3 - 6.

Kim Y.B., Kim J.G., Kim W., Im J.H., Kim T.H., Kang S.J., and Kim C.H. (2016). Predicting Fluctuations in Cryptocurrency Transactions Based on User Comments and Replies. *PLoS ONE*. 11 (8). pp. 1 - 17.

Lee T. (2018). As Bitcoin's Price Plunges, Skeptics Say the Cryptocurrency has No Value. Here's One Argument for Why They're Wrong. *CNBC*. Website: https://www.cnbc.com/2018/01/16/skeptics-say-bitcoin-has-no-value-heres-why-theyre-wrong.html

Li X. and Wang C.A. (2017). The Technology and Economic Determinants of Cryptocurrency Exchange Rates: The Case of Bitcoin. *Decision Support Systems*. 95. pp. 49 - 60.

Nadarajah S. and Chu J. (2017). On the Inefficiency of Bitcoin. *Economics Letters*. 150. pp. 6 - 9.Nakamoto S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Web site: https://bitcoin.org/bitcoin.pdf

Nakamoto S. (2008). Bitcoin P2P e-Cash Paper.Web site: https://www.mail-archive.com/search?l=cryptography@metzdowd.com&q=from:%22Satoshi+Nakamoto%22

Panigirtzoglou N. (2017). JPMorgan Strategist: Bitcoin Futures can 'Add Legitimacy' to Potential Emerging Asset Class. *CNBC*. Web site: https://www.cnbc.com/2017/12/01/jpmorgan-strategist-bitcoin-futures-can-add-legitimacy.html

Peterson T. (2017). Metcalfe's Law as a Model for Bitcoin's Value. Working Paper.

Pieters G. and Vivanco S. (2017). Financial Regulations and Price Inconsistencies across Bitcoin Markets. *Information Economics and Policy*. 39. pp. 1 - 14.

Powell J. (2018). Cryptocurrency Market will hit $1 Trillion Valuation This Year. *CNBC*. Website: https://www.cnbc.com/2018/02/13/cryptocurrency-market-to-hit-1-trillion-valuation-in-2018 rakenceo.html

Raymaekers W. (2015). Cryptocurrency Bitcoin: Disruption, Challenges and Opportunities. *Journal of Payments Strategy & Systems*. 9 (1). pp. 30 - 46.

Saito K. and Iwamura M. (2018). How to Make a Digital Currency on a Blockchain Stable. Working Paper.

Scott B. (2016). How Can Cryptocurrency and Blockchain Technology Play a Role in Building Social and Solidarity Finance?. *United Nations Research Institute for Social Development (UNRISD)*. Working Paper.

Securities and Exchange Commission. (2017). Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO. *Securities and Exchange Commission*.

Stiglitz J. (2017). Bitcoin 'Ought to Be Outlawed,' Nobel Prize Winner Stiglitz Says. *Bloomberg*. Web site: https://www.bloomberg.com/news/articles/2017-11-29/ bitcoin-ought-to-be-outlawed-nobel-prize-inner- stiglitz-says-jal10hxd

Urquhart A. (2016). The Inefficiency of Bitcoin. *Economics Letters*. 148. pp. 80 - 82.

Van Vliet B. (2018). An Alternative Model of Metcalfe's Law for Valuing Bitcoin. *Economics Letters*. 165. pp. 70 - 72.

Wang J.C. (2014). A Simple Macroeconomic Model of Bitcoin. Working Paper.

World Economic Forum. (2017). In 2020 Bitcoin will Consume more Power than the World does Today. *World Economic Forum*. Website: https://www.weforum.org/ agenda/2017/12/bitcoin-consume-more-power-than-world-2020/