BLOCKCHAIN TECHNOLOGY

BEYOND CRYPTOCURRENCIES

บล็อกเชน ... ที่มากกว่าเงินคริปโท

ETDA สพธอ www.etda.or.th
กระทรวงดิจิทัล เพื่อเศรษฐกิจและสังคม
GO DIGITAL with ETDA

Blockchain Technology: Beyond Cryptocurrencies
บล็อกเชน ... ที่มากกว่าเงินคริปโท

ดำเนินการภายใต้โครงการศึกษาวิจัยแนวทางการพัฒนาเทคโนโลยี
ที่เกี่ยวข้องกับ Blockchain เพื่อรองรับการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ

สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม

ISBN 978-616-438-593-1

ราคา 250 บาท

ลิขสิทธิ์ของ สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
พิมพ์ครั้งที่ 1 มิถุนายน พ.ศ. 2564 จำนวน 2,000 เล่ม
จัดพิมพ์โดย มหาวิทยาลัยขอนแก่น
อ.เมือง จ.ขอนแก่น 40002
พิมพ์ที่ โรงพิมพ์มหาวิทยาลัยขอนแก่น
มหาวิทยาลัยขอนแก่น อ.เมือง จ.ขอนแก่น 40002

สารบัญ

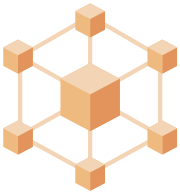
คำนำ

หนึ่งในโจทย์สำคัญของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ (สพธอ.) หรือ ETDA (เอ็ตด้า) กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม คือ การสร้างความเข้าใจเกี่ยวกับเทคโนโลยีใหม่ เช่น บล็อกเชน ซึ่งเป็นหนึ่งในเทคโนโลยีพื้นฐานสำคัญในการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ

หลายครั้งที่มักมีคำถามและความสับสน เช่น บล็อกเชนคืออะไร แล้วบล็อกเชนกับบิตคอยน์เป็นเรื่องเดียวกันไหม บล็อกเชนมีเฉพาะเรื่องการลงทุนในคริปโทเคอร์เรนซีหรือที่เรียกกันติดปากว่า **เงินคริปโท** เท่านั้นหรือไม่ การขุดเหรียญ การทำฟาร์ม ศัพท์เทคนิคต่าง ๆ เหล่านี้ ที่เมื่อได้ยินแล้ว ก็อาจเกิดคำถามว่า เทคโนโลยีเหล่านี้คืออะไร และจะส่งผลกระทบต่อชีวิตประจำวันของเรากันอย่างไร

เมื่อสำรวจในท้องตลาด หนังสือที่อธิบายเกี่ยวกับบล็อกเชนในมิตินอกเหนือจากการเงิน การลงทุน คริปโทเคอร์เรนซี ฉบับภาษาไทยยังมีจำนวนไม่มาก ดังนั้น ETDA และมหาวิทยาลัยขอนแก่นจึงได้ร่วมกันศึกษาและวิจัย พร้อมทั้งพัฒนาองค์ความรู้เกี่ยวกับเทคโนโลยีบล็อกเชนเพื่อการพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ของประเทศ โดยหวังให้เกิดชุมชนแห่งการแบ่งปันองค์ความรู้ กระตุ้นการประยุกต์ใช้เทคโนโลยีบล็อกเชน รวมทั้งพัฒนาต่อยอดให้เกิดประโยชน์ด้านธุรกรรมทางอิเล็กทรอนิกส์ต่อไป เราต้องการให้ผู้อ่านที่มีพื้นฐาน IT และผู้ที่สนใจด้านบล็อกเชน มีเพื่อนคู่คิดที่ช่วยแนะนำ ให้ข้อมูลเกี่ยวกับการประยุกต์ใช้เทคโนโลยีบล็อกเชนในเรื่องต่าง ๆ และหวังให้ผู้ประกอบการ หน่วยงานรัฐเอกชน และผู้ที่สนใจเกี่ยวกับเทคโนโลยีบล็อกเชนสามารถมองเห็นช่องทางหรือโอกาสในการพัฒนาต่อยอด ประยุกต์ใช้เทคโนโลยีบล็อกเชนได้อย่างสร้างสรรค์ รู้เท่าทัน นำไปสู่ความเชื่อมั่นในการใช้งานเทคโนโลยีดิจิทัลต่อไป

มาร่วม Go Digital With ETDA ในเส้นทางแห่งการเรียนรู้ และโลกของ **บล็อกเชน ...ที่มากกว่าเงินคริปโท**



> “Blockchain shifts trust in people and institutions to trust in technology”
>
> -- Bruce Schneier
> Cryptographer and Information Security Expert [1]

1 บิตคอยน์กับการกำเนิดบล็อกเชน

หลายคนได้ยินคำว่า **“บิตคอยน์”** มาพร้อมกับ **“บล็อกเชน”** และอาจนึกว่าสองสิ่งนี้เป็นเรื่องเดียวกัน เราจึงอยากเริ่มต้นทำความเข้าใจให้ชัดเจนก่อนว่าทั้งสองสิ่งเป็นเรื่องที่เกี่ยวข้องกัน แต่ไม่ใช่เรื่องเดียวกันเสียทีเดียว บล็อกเชนเป็นเทคโนโลยีที่นำมาประยุกต์ใช้สร้างระบบสารสนเทศได้มากมายดังที่จะกล่าวต่อไปในหนังสือเล่มนี้ หากแต่บล็อกเชนเป็นที่รู้จักเนื่องจากการถือกำเนิดและการเติบโตของบิตคอยน์ ซึ่งเป็นระบบที่สร้างมาเปลี่ยนแปลงธุรกรรมทางการเงิน

ปฏิเสธไม่ได้เลยว่าการดำเนินธุรกรรมทางการเงินเป็นส่วนหนึ่งของการใช้ชีวิตในสังคม เป็นกิจกรรมที่อยู่ใกล้ตัวทุกคนมากกว่าที่คิด และทุกครั้งที่เราทำธุรกรรมทางการเงินจะมีสถาบันการเงินเข้ามาเกี่ยวข้องเสมอ ตัวอย่างที่เห็นได้ชัดในปัจจุบัน คือการชำระเงิน

ผ่านระบบอิเล็กทรอนิกส์ต่าง ๆ ไม่ว่าจะเป็น บัตรเครดิต/เดบิต, การโอนเงินเข้าบัญชีธนาคาร, Mobile Banking Application, e-Money (เช่น LINE Pay, TrueMoney Wallet, WhatsApp), Bill Payments, PromptPay ล้วนแต่มีสถาบันการเงินทำหน้าที่เป็นตัวกลางในการดำเนินการชำระเงิน

แม้แต่การใช้จ่ายด้วยเงินสดก็ยังมีธนาคารกลางของประเทศทำหน้าที่เป็นตัวกลางในการสร้างมูลค่าให้กับ เหรียญ ธนบัตร ซึ่งเป็นเครื่องเก็บรักษามูลค่า (store of value) ในรูปแบบที่ชำระหนี้ได้ตามกฎหมาย

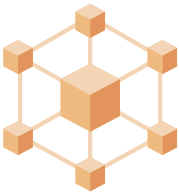
หลายคนไม่เคยรู้ตัวมาก่อนเลยว่า การชำระเงินทุกครั้ง เราในฐานะผู้ชำระเงินและผู้รับชำระเงินต่างต้องพึ่งพาและเชื่อถือการดำเนินธุรกรรมของสถาบันการเงินเสมอว่าสถาบันการเงินเหล่านี้จะทำงานได้อย่างถูกต้อง เป็นธรรม ตรวจสอบได้ เงินไม่สูญหาย หรือสูญค่า เรียกได้ว่า สถาบันการเงินทำหน้าที่เป็นบุคคลที่สามหรือหน่วยงานที่น่าเชื่อถือ (trusted third party) เป็นองค์กรกลางที่ผู้ชำระเงินและผู้รับชำระเงินต้องมอบความไว้ใจในการชำระเงิน

คำถามคือ “**เราไว้ใจหรือเชื่อถือสถาบันการเงินเหล่านี้ได้อย่างไร?**”

หากย้อนกลับมาพิจารณาแล้วจะพบว่า สถาบันการเงินทุกแห่งพยายามสร้างความเชื่อมั่นให้กับลูกค้าและประชาชนมาโดยตลอด โดยอาศัยกระบวนการกำกับดูแลตามกฎหมาย ระเบียบ มาตรฐาน และแนวปฏิบัติต่าง ๆ ในการควบคุมระบบการเงิน ระบบสารสนเทศทางการเงินและผู้เกี่ยวข้องในระบบการเงิน เพื่อให้การบริการและการประมวลผลธุรกรรมมีความมั่นคงปลอดภัย ข้อมูลธุรกรรมไม่สูญหายหรือถูกแก้ไขโดยไม่ได้รับอนุญาต ป้องกันการปลอมแปลง สามารถตรวจสอบการฉ้อโกงหรือการทุจริตอื่น ๆ ที่อาจจะเกิดขึ้น สถาบันการเงินจึงมีต้นทุนในการกำกับดูแลการประมวลผลธุรกรรมและบริหารความเสี่ยงทางการเงินและระบบสารสนเทศ ซึ่งต้นทุนเหล่านี้ ส่วนหนึ่งกลายเป็นค่าธรรมเนียมที่เรียกเก็บจากลูกค้าหรือภาษีที่เรียกเก็บจากประชาชน

ในมุมของลูกค้าและประชาชน เท่ากับว่าการดำเนินธุรกรรมทางการเงินไม่สามารถเลี่ยงสถาบันการเงินได้เลย ทั้งผู้ชำระเงินและผู้รับชำระเงิน จำต้องไว้ใจสถาบันการเงินเหล่านี้เป็นตัวกลางในการประมวลผลธุรกรรมโดยไม่มีทางเลือกอื่น

จนกระทั่งเกิด **“บิตคอยน์”**



“The Times 03/Jan/2009

Chancellor on brink of second bailout for banks”

-- Bitcoin Genesis Block [2]

1.1 บิตคอยน์ (Bitcoin)

ปัญหาและข้อจำกัดต่าง ๆ ของสถาบันการเงินในฐานะที่เป็น trusted third party ในระบบชำระเงินเป็นจุดที่ทำให้บุคคลหรือกลุ่มบุคคลที่ใช้นามแฝงว่า **ซาโตชิ นากาโมโตะ** (Satoshi Nakamoto) เสนอทางแก้ไขโดยใช้วิธีการทางอิเล็กทรอนิกส์สร้างระบบเครือข่ายสารสนเทศในการประมวลผลธุรกรรมทางการเงินบนเครือข่ายอินเทอร์เน็ตที่ทำให้ผู้ชำระเงินสามารถทำธุรกรรมกับผู้รับชำระเงินได้โดยตรงเสมือนการใช้เงินสดโดยไม่ต้องมีสถาบันการเงินเป็นตัวกลาง มีเพียงการประมวลผลโดยซอฟต์แวร์บนเครือข่ายคอมพิวเตอร์เท่านั้น

ซาโตชิ นากาโมโตะเผยแพร่แนวคิดนี้บนเว็บไซต์ bitcoin.org ในวันที่ 31 ตุลาคม ค.ศ. 2008 เป็นเอกสารชื่อ “Bitcoin: A Peer-to-Peer Electronic Cash System” [3]

ในระบบเงินสดเราใช้เหรียญหรือธนบัตรเป็นโทเคน (token) เพื่อแทนมูลค่าของเงิน แต่ในระบบเงินสดของบิตคอยน์ใช้ข้อมูลอิเล็กทรอนิกส์เป็นโทเคนแทนมูลค่าเงิน โดยเรียกโทเคนที่ว่านี้ตามชื่อระบบว่า บิตคอยน์ (ใช้อักษรย่อเป็น BTC หรือ XBT) แบบเดียวกับที่เราเรียกโทเคนในสกุลเงินบาทว่าเหรียญบาท โทเคนของบิตคอยน์สามารถใช้งานหมุนเวียนในระบบเครือข่ายของบิตคอยน์ซึ่งทำหน้าที่ในการบันทึกธุรกรรมของบิตคอยน์ที่เกิดขึ้นทั้งหมดระหว่างผู้ใช้งาน

ธุรกรรมของบิตคอยน์อาศัยความน่าเชื่อถือของเทคโนโลยีระบบรหัสแบบกุญแจสาธารณะ (Public-Key Cryptography) ในการระบุบัญชีผู้ชำระกับผู้รับชำระทำให้มั่นใจได้ว่าเป็นธุรกรรมเกิดขึ้นระหว่างบัญชีผู้ชำระกับผู้รับชำระที่ถูกต้องจริง ๆ ความแข็งแกร่งของการเข้ารหัสกุญแจสาธารณะทำให้การปลอมแปลงข้อมูลธุรกรรมแทบจะเป็นไปไม่ได้ ข้อมูลธุรกรรมที่ได้รับการยืนยันแล้วจะไม่สามารถเปลี่ยนแปลงได้ในภายหลัง และไม่สามารถปฏิเสธได้ว่าไม่ได้ทำธุรกรรมระหว่างกัน

ในอดีต การเข้ารหัสลับจะใช้กุญแจ (key) ชุดเดียวกันในการเข้ารหัสลับและถอดรหัสลับ ใช้กุญแจชุดใดเข้ารหัสก็ต้องใช้ชุดเดียวกันถอดรหัส ทำให้จัดการความลับของกุญแจได้ยากเพราะผู้ส่งสารและผู้รับสารต้องแชร์กุญแจใช้ด้วยกัน

ระบบรหัสกุญแจสาธารณะจึงถือกำเนิดขึ้นเพื่อแก้ปัญหาการแชร์กุญแจระหว่างกัน โดยใช้สมการทางคณิตศาสตร์สร้างคู่กุญแจ (keypair) ขึ้นมาใช้งานแทน ประกอบด้วยกุญแจสาธารณะ (public key) และกุญแจส่วนตัว (private key) ที่เข้าคู่กัน คุณสมบัติของระบบรหัสกุญแจสาธารณะที่สำคัญมีอยู่สองประการ คือ 1. กุญแจสาธารณะไม่สามารถนำมาคำนวณหากุญแจส่วนตัวได้ และ 2. ถ้าใช้กุญแจดอกหนึ่งเข้ารหัสข้อมูลจะมีเพียงกุญแจอีกดอกในคู่กุญแจเดียวกันเท่านั้นที่ถอดรหัสข้อมูลได้

ผู้ส่งสารสามารถใช้กุญแจสาธารณะของผู้รับสารในการเข้ารหัสลับ ซึ่งทำให้มีผู้รับสารผู้เดียวเท่านั้นที่ถอดรหัสได้ วิธีนี้เป็นหลักการที่บิตคอยน์ประยุกต์ใช้เพื่อแลกเปลี่ยนโทเคนระหว่างกัน

ระบบของบิตคอยน์ถูกออกแบบให้**กระจายศูนย์ (distributed)** โดยอาศัยคอมพิวเตอร์ที่เชื่อมต่ออินเทอร์เน็ตอาสาทำงานเป็นโหนด (node) ประมวลผลและจัดเก็บ ledger ของเครือข่ายบิตคอยน์

ซอฟต์แวร์ของบิตคอยน์จะประมวลผลตามโพรโทคอล (protocol) หรือเกณฑ์วิธีในการทำให้ข้อมูลธุรกรรมที่จัดเก็บลงใน ledger ของโหนดถูกต้องตรงกัน เรียกว่า consensus

ที่สำคัญกว่านั้น บิตคอยน์ออกแบบให้เกิดการ **กระจายอำนาจ (decentralized)** ไม่มีผู้ใดหรือองค์กรใดเป็นเจ้าของเทคโนโลยีหรือมีอำนาจควบคุมการประมวลผลธุรกรรมเบ็ดเสร็จ ซึ่งแตกต่างจากระบบการเงินของสถาบันการเงินที่เป็นระบบรวมศูนย์ (centralized) คงอำนาจควบคุมเบ็ดเสร็จไว้กับองค์กร เช่น อำนาจการผลิตเงินของธนาคารกลาง อำนาจในการแก้ไขเปลี่ยนแปลงข้อมูลบัญชีเงินฝากของลูกค้าที่เก็บในฐานข้อมูลของธนาคารพาณิชย์หรือสถาบันการเงิน

การประมวลผลที่กระจายศูนย์และการออกแบบให้กระจายอำนาจนี้ ทำให้เครือข่ายบิตคอยน์ไม่จำเป็นต้องมีตัวกลางเพื่อทำหน้าที่เป็น trusted third party ยิ่งมีจำนวนโหนดมาก การกระจายอำนาจยิ่งสูง การทุจริตหรือฉ้อโกงโดยการปลอมแปลงหรือแก้ไขธุรกรรมก็จะทำได้ยากขึ้นตามไปด้วยเพราะต้องแก้ไขข้อมูลใน ledger ของทุกโหนดในเครือข่ายให้ตรงกัน

เพื่อให้เครือข่ายของบิตคอยน์มีจำนวนโหนดมากพอที่จะรักษาการกระจายอำนาจและดำรงอยู่ได้ในระยะยาว บิตคอยน์ใช้วิธีผลิตโทเคนเป็นรางวัล (Rewards) ตอบแทนให้กับโหนดเป็นแรงจูงใจ ยิ่งโทเคนมีมูลค่าสูงขึ้น ก็ยิ่งดึงดูดให้มีผู้เข้าร่วมเป็นโหนดในเครือข่ายมากขึ้นไปด้วย

ในปี ค.ศ. 2015 มีการประมาณการว่าจำนวนโหนดในเครือข่ายบิตคอยน์มีอยู่ราว 5,000 โหนดและขยายเพิ่มขึ้นเป็น 10,000 โหนดในช่วงปลายปี ค.ศ. 2017 จำนวนโหนดของบิตคอยน์ยังคงอยู่ในระดับ 10,000 โหนดตั้งแต่นั้นมาจนถึงปัจจุบัน [4]

กลไกในการสร้างความน่าเชื่อถือที่สำคัญอีกประการของบิตคอยน์คือการใช้แนวทางของโอเพนซอร์ส (open source) ในการเปิดเผยการออกแบบ โครงสร้างข้อมูล ขั้นตอนวิธี (algorithm) ในการประมวลผล โพรโทคอล และรหัสต้นฉบับหรือซอร์สโค้ด

(source code) ของซอฟต์แวร์พื้นฐานทั้งหมด เป็นการเปิดโอกาสให้ทุกคนมีสิทธิตรวจสอบและมีส่วนร่วมในการแก้ไข ปรับปรุง พัฒนาบิตคอยน์ให้ดีขึ้น การที่บิตคอยน์ใช้แนวทางของโอเพนซอร์สทำให้บิตคอยน์ถูกขับเคลื่อนโดยชุมชนผู้ใช้งานและนักพัฒนา ไม่มีผู้ใดหรือองค์กรใดมีอำนาจควบคุมซอร์สโค้ดของบิตคอยน์ บิตคอยน์จึงมีความโปร่งใสและสร้างความเชื่อมั่นให้กับผู้ใช้งานได้สูง

โดยสรุป บิตคอยน์ทำให้เกิดระบบเงินสดอิเล็กทรอนิกส์ที่ไม่มีผู้มีอำนาจเบ็ดเสร็จในการควบคุมหรือกำกับดูแล ความเชื่อมั่นทั้งหมดฝากไว้กับเทคโนโลยีและการประมวลผลอัตโนมัติโดยซอฟต์แวร์ของบิตคอยน์ที่ชุมชนร่วมกันดูแลในรูปแบบโอเพนซอร์ส ซึ่งทำให้การทำธุรกรรมบนเครือข่ายบิตคอยน์ไม่จำเป็นต้องพึ่งพาคนหรือสถาบันการเงินเลย

ในปี ค.ศ. 2021 บิตคอยน์เป็นสินทรัพย์ในรูปแบบดิจิทัลที่มีมูลค่ามากกว่า 1 ล้านล้านเหรียญสหรัฐ [5] ซึ่งสูงยิ่งกว่าสินทรัพย์ภายใต้การกำกับดูแลของสถาบันการเงินหลายแห่งในโลก บิตคอยน์จึงเป็นเทคโนโลยีที่ส่งผลกระทบต่อสังคมโลกอย่างมาก เป็นเทคโนโลยีที่ท้าทายมนุษยชาติในการเปลี่ยนรากฐานความเชื่อมั่นที่อยู่กับมนุษย์หรือองค์กรมาอยู่ที่เทคโนโลยีเพียงอย่างเดียว

1.2 การทำงานของบิตคอยน์

หากจะทำความเข้าใจว่าบิตคอยน์สร้างความน่าเชื่อถือและกระจายอำนาจได้อย่างไร เราต้องเข้าใจธุรกรรม (transactions) ของบิตคอยน์เสียก่อน

ธุรกรรมของบิตคอยน์ใช้โมเดลที่เรียกว่า Unspent Transaction Output (UTXO) ทุกธุรกรรมของบิตคอยน์จะสร้างผลลัพธ์เป็นรายการ UTXO เสมอโดยที่แต่ละ UTXO ประกอบด้วย บิตคอยน์แอดเดรส (Bitcoin Address) ซึ่งเป็นหมายเลขประจำตัวของผู้รับกับจำนวนโทเคนของบิตคอยน์ที่จะส่งให้ผู้รับ

กุญแจส่วนตัวของบิตคอยน์เป็นเลขจำนวนเต็มขนาด 256 บิต

กุญแจสาธารณะสร้างให้เข้าคู่จากกุญแจส่วนตัวโดย Elliptic Curve Digital Signature Algorithm (ECDSA) โดยใช้ elliptic curve secp256k1

บิตคอยน์แอดเดรสคือค่าแฮชรหัสลับ (cryptographic hash) ของกุญแจสาธารณะ คำนวณโดยใช้อัลกอริทึม SHA-256 และ RIPEMD-160

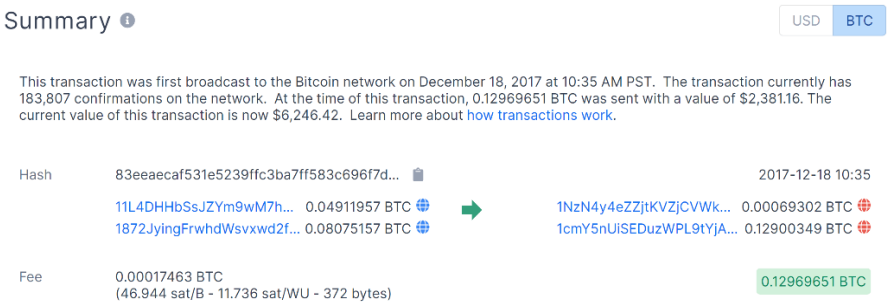
เมื่อต้องการใช้จ่ายบนบิตคอยน์ ผู้ชำระต้องสร้างธุรกรรมในการชำระเงินซึ่งประกอบด้วยข้อมูลสำคัญ 3 ส่วน ได้แก่

1. input เป็นรายการธุรกรรมที่ผู้ชำระได้รับ UTXO มาก่อนหน้าที่จะนำมาใช้จ่ายในธุรกรรมนี้
2. output เป็นรายการ UTXO ที่จะสร้างขึ้นใหม่ โดยผูกจำนวนโทเคนของบิตคอยน์ที่ต้องการชำระกับบิตคอยน์แอดเดรสของผู้รับชำระ
3. ลายมือชื่อดิจิทัล (Digital Signature) ที่ลงนามด้วยกุญแจส่วนตัวของผู้ชำระเงิน

โมเดล UXTO ของบิตคอยน์กำหนดให้รายการ UTXO ฝั่ง input และรายการ UTXO ฝั่ง output ของธุรกรรมต้องหักล้างเป็นศูนย์เสมอ และ input ต้องมีจำนวนโทเคนของบิตคอยน์รวมไม่น้อยกว่า output จึงจะถือว่าเป็นธุรกรรมที่สามารถดำเนินการได้ ผู้ชำระจึงมักต้องสร้าง UTXO ที่ output เพื่อโอนโทเคนของบิตคอยน์ที่เหลือ (เงินทอน) กลับเข้าบิตคอยน์แอดเดรสของตัวเองเพื่อให้ธุรกรรมหักล้างเป็นศูนย์พอดี

บิตคอยน์รองรับค่าธรรมเนียมในการทำธุรกรรมด้วย โดยระบุเป็นส่วนหนึ่งของ output ผู้สร้างธุรกรรมสามารถเลือกชำระค่าธรรมเนียมได้ตามความต้องการ หรือหากธุรกรรมไม่หักล้างเป็นศูนย์ เศษที่เหลือจะถูกใช้เป็นค่าธรรมเนียมอัตโนมัติ

ค่าธรรมเนียมของบิตคอยน์จ่ายโดยใช้โทเคนของบิตคอยน์ แต่มักระบุเป็นหน่วย satoshi (sat) ซึ่งเป็นหน่วยที่เล็กที่สุดของโทเคนของบิตคอยน์ โดย 1 satoshi มีค่าเท่ากับ 1/100,000,000 BTC



ภาพที่ 1
ธุรกรรมของบิตคอยน์

ตัวอย่างธุรกรรมของบิตคอยน์ ฝั่งซ้ายคือ input และฝั่งขวาคือ output

ธุรกรรมของบิตคอยน์ ประกอบด้วย input, output และ ลายมือชื่อดิจิทัล สามองค์ประกอบหลักนี้ทำให้มีการเรียกการบันทึกบัญชีของบิตคอยน์ว่าเป็น Triple-Entry Bookkeeping ล้อกับการบันทึกแบบ Double-Entry Bookkeeping ในการทำบัญชี

จะเห็นได้ว่า ธุรกรรมของบิตคอยน์คือการนำ UTXO ที่ฝั่ง input มาสร้างเป็น UTXO ใหม่ที่ฝั่ง output ทุกโทเคนของบิตคอยน์จึงมีที่มาเสมอ และสามารถตรวจสอบที่มาของโทเคนย้อนกลับไปได้จนถึงจุดโทเคนกำเนิดขึ้นมาหมุนเวียนในเครือข่าย โมเดล UTXO จึงทำให้ไม่สามารถสร้างโทเคนปลอมเข้ามาหมุนเวียนในระบบได้ และป้องกันการนำโทเคนมาใช้จ่ายซ้ำ (double spending) ได้

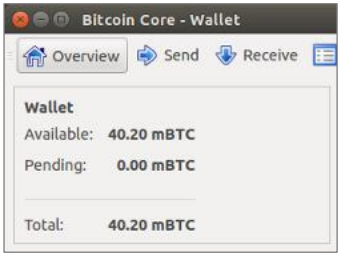
นอกจากนี้ วิธีการรหัสกุญแจสาธารณะ ยังทำให้สามารถตรวจสอบยืนยันได้ว่า:

1. UXTO ที่ input เป็นของผู้ชำระตัวจริง เพราะมีเพียงกุญแจส่วนตัวของผู้ชำระตัวจริงเท่านั้นที่สามารถปลด UXTO ที่ผูกกับบิตคอยน์แอดเดรสของผู้ชำระได้

2. ธุรกรรมนั้นสร้างโดยผู้ชำระตัวจริง เพราะมีเพียงกุญแจส่วนตัวของผู้ชำระตัวจริงเท่านั้นที่เข้าคู่กันกับลายมือชื่อดิจิทัลในธุรกรรม และ
3. ธุรกรรมนั้นจะโอนโทเคนบิตคอยน์ไปยังผู้รับชำระตัวจริงแน่นอน เพราะมีเพียงกุญแจส่วนตัวของผู้รับชำระตัวจริงเท่านั้นที่เข้าคู่กันกับบิตคอยน์แอดเดรสใน UTXO ที่ output

หากเปรียบเทียบ “ธุรกรรมของบิตคอยน์” กับ “ธุรกรรมการเงินทั่วไป” จะพบว่าธุรกรรมของบิตคอยน์มีความคล้ายกับการสั่งจ่ายโดยใช้เช็คเงินสด แต่เช็คเงินสดมีความเสี่ยงอยู่หลายอย่าง เช่น นำไปขึ้นเงินไม่ได้เพราะเงินในบัญชีไม่พอจ่าย ปลอมลายมือชื่อง่าย สั่งจ่ายซ้ำซ้อนได้ ทำสำเนาได้ หรือแก้ไขหน้าเช็คที่ลงลายมือชื่อไปแล้วได้ ซึ่งประเด็นเหล่านี้จะไม่สามารถเกิดกับธุรกรรมของบิตคอยน์ได้เลย

แม้ว่าการชำระด้วยบิตคอยน์ดูมีความซับซ้อนทางเทคนิค แต่การจัดการธุรกรรมของบิตคอยน์และการสร้างบิตคอยน์แอดเดรสในความเป็นจริงทำได้ง่ายมากโดยใช้ซอฟต์แวร์เฉพาะที่เรียกว่า **วอลเล็ต (Wallet)**



ภาพที่ 2 บิตคอยน์วอลเล็ต

ตัวอย่างโปรแกรมวอลเล็ต Bitcoin Core เป็นโปรแกรมที่พัฒนาเป็นซอฟต์แวร์พื้นฐานของบิตคอยน์ [6]

Bitcoin Core สามารถทำงานเป็นวอลเล็ต และเป็นโหนดของเครือข่ายบิตคอยน์ได้ด้วย

แม้ฟังดูจะให้ความรู้สึกว่าวอลเล็ตเป็นเหมือนกระเป๋าเก็บเงินสดที่บรรจุเหรียญหรือธนบัตร แต่ในความเป็นจริงแล้ววอลเล็ตของบิตคอยน์ไม่ได้เก็บโทเคนของบิตคอยน์ ต้องไม่ลืมว่าโทเคนของบิตคอยน์เป็นเพียงข้อมูลใน UTXO ที่ผูกกับบิตคอยน์แอดเดรส บันทึกเป็นธุรกรรมที่จัดเก็บรวมไว้ใน ledger ของเครือข่ายบิตคอยน์ เราสามารถเข้าถึง UTXO ที่เราถือครองเพื่อทำธุรกรรมต่าง ๆ ได้โดยใช้เพียงกุญแจส่วนตัวเท่านั้น อีกทั้ง

บิตคอยน์แอดเดรสประจำตัวของเราสามารถสร้างได้จากกุญแจส่วนตัวโดยตรง **กุญแจส่วนตัวจึงเป็นข้อมูลเดียวที่วอลเล็ตจำเป็นต้องเก็บรักษา**

การดูแลรักษาวอลเล็ตหรือกุญแจส่วนตัวให้ปลอดภัยจึงเป็นเรื่องที่สำคัญมาก หากกุญแจส่วนตัวสูญหายหรือลืมรหัสผ่านในการปลดล็อคกุญแจส่วนตัว เราจะไม่สามารถทำธุรกรรมกับ UTXO ของเราได้อีกเลย ปัจจุบันจึงมีทางเลือกในการเก็บรักษากุญแจส่วนตัวเพื่อป้องกันการสูญหายหรือถูกโจรกรรมข้อมูล เช่น วอลเล็ตที่เป็นฮาร์ดแวร์เก็บรักษากุญแจส่วนตัวในชิปคอมพิวเตอร์ วอลเล็ตที่เป็นกระดาษเก็บกุญแจส่วนตัวเป็นรหัส QR เป็นต้น

1.3 บล็อก (Block)

ธุรกรรมบนบิตคอยน์จะมีผลก็ต่อเมื่อได้รับการบันทึกในฐานข้อมูลที่จัดเก็บธุรกรรม เรียกว่า ledger โดยบิตคอยน์จะบันทึกธุรกรรมเป็นชุดเรียกว่า **“บล็อก”**

เมื่อวอลเล็ตสร้างธุรกรรมตามผู้ใช้สั่งแล้ว ธุรกรรมจะถูกส่งเข้าไปเครือข่ายบิตคอยน์ผ่านโหนดใดโหนดหนึ่ง โหนดที่นำเข้าธุรกรรมจะตรวจสอบโครงสร้างข้อมูลของธุรกรรมเบื้องต้น แล้วจึงกระจายธุรกรรมต่อไปยังโหนดใกล้เคียง โหนดที่ได้รับธุรกรรมก็จะกระจายต่อไปโหนดใกล้เคียงไปเรื่อย ๆ จนทั่วเครือข่ายบิตคอยน์ ทุกโหนดมีหน้าที่เก็บรวบรวมธุรกรรมเหล่านี้พักไว้เพื่อรอการบันทึก

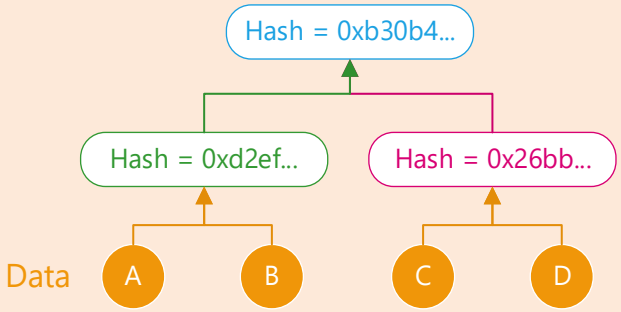
เมื่อถึงเวลาที่จะสร้างบล็อกใหม่ แต่ละโหนดจะเลือกธุรกรรมที่พักไว้มาประกอบเป็นบล็อก แต่ด้วยขนาดบล็อกที่จำกัด ทำให้พื้นที่ของบล็อกมีมูลค่า บิตคอยน์จึงเลือกธุรกรรมที่พักไว้โดยจัดลำดับก่อนหลังตามค่าธรรมเนียมธุรกรรมต่อขนาดของธุรกรรม (satoshi per byte: sat/B) ธุรกรรมที่มีค่า sat/B สูงจะได้บรรจุอยู่ในบล็อกก่อนธุรกรรมที่ sat/B ต่ำ วิธีนี้ทำให้โหนดส่วนใหญ่หรือทั้งหมดในเครือข่ายสร้างบล็อกใหม่ที่บรรจุธุรกรรมชุดเดียวกัน แม้ว่าจะประมวลผลเป็นอิสระต่อกันก็ตาม

หลังจากสร้างบล็อกใหม่เป็นของตัวเองได้แล้ว แต่ละโหนดจะเขียนข้อมูลของบล็อกไว้ในหัวบล็อก (block header) มีข้อมูลสำคัญ ๆ ได้แก่ แฮชเข้ารหัส (cryptographic

hash) ของหัวบล็อกก่อนหน้า แฮชเข้ารหัสของธุรกรรมทั้งหมดในบล็อก (Merkle Root) ประทับเวลา (timestamp) ค่าเป้าหมาย และค่าที่เติมเข้าในหัวบล็อกเพื่อคำนวณแฮชเข้ารหัสลับที่เรียกว่า nonce

ทุกบล็อกจึงมีข้อมูลเชื่อมกลับไปยังบล็อกก่อนหน้าเสมอ ledger ของบิตคอยน์จึงประกอบด้วยบล็อกที่บรรจุธุรกรรมร้อยกันเป็นสายย้อนกลับไปได้จนถึงบล็อกต้นกำเนิด (Genesis Block) ของบิตคอยน์ และเนื่องจากหัวบล็อกใช้ขั้นตอนวิธีตามวิทยาการเข้ารหัสลับ (cryptography) ในการหาค่า nonce ดังนั้น การเชื่อมโยงระหว่างบล็อกจึงแทบจะเปลี่ยนแปลงไม่ได้อีกเลย

Merkle Tree ถูกคิดค้นและเป็นสิทธิบัตรของ Ralph Merkle เป็น tree ที่แต่ละโหนดเก็บข้อมูลแฮชของโหนดที่เชื่อมในลำดับชั้นที่ต่ำกว่า



แฮชแต่ละโหนดจึงใช้ตรวจสอบข้อมูลของโหนดที่เชื่อมในลำดับชั้นที่ต่ำกว่าได้ ซึ่งเท่ากับว่าข้อมูลแฮชเข้ารหัสที่ root ของ Merkle Tree (เรียกว่า Merkle Root) จะสามารถใช้ในการตรวจสอบความถูกต้องสมบูรณ์ของข้อมูลทั้งหมดใน Merkle Tree นั้นได้

ด้วยโครงสร้างข้อมูลของ ledger ที่ประกอบด้วยบล็อกธุรกรรมร้อยต่อกันเป็นสายเชื่อมโยงกันด้วยวิธีการที่เปลี่ยนแปลงลำดับการร้อยบล็อก

จึงเป็นที่มาของการเรียกเทคโนโลยีรูปแบบนี้ว่า “บล็อกเชน” (blockchain)

1.4 Proof of Work

บล็อกที่สร้างขึ้นมาใหม่จะไม่ได้ร้อยเข้ากับ ledger ในทันที แต่ต้องได้รับการประทับเวลาซึ่งถือเป็นการประกาศให้ทุกโหนดในเครือข่ายบิตคอยน์รับรู้ตรงกันว่ามีบล็อกและธุรกรรมเกิดขึ้นในระบบแล้ว

บิตคอยน์ใช้การประทับเวลาแบบกระจายศูนย์โดยนำเทคนิคมาจาก Hashcash Proof of Work [7] โดยให้โหนดในเครือข่ายบิตคอยน์แข่งกันหาค่า nonce ที่ทำให้ค่าแฮชเข้ารหัสของหัวบล็อกมีค่าต่ำกว่าค่าเป้าหมายที่กำหนดเพื่อได้เป็นผู้ประทับเวลา

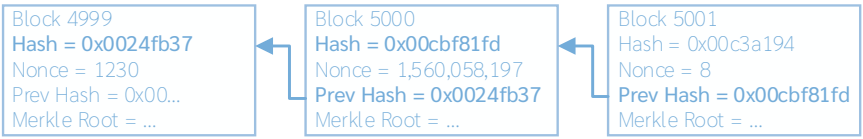
ระบบสารสนเทศทั่วไปที่ต้องการเวลาที่เที่ยงตรงจะใช้วิธีการเทียบเวลากับที่ใดที่หนึ่งเสมอ ตัวอย่างเช่น เวลามาตรฐานของประเทศไทยอ้างอิงเทียบกับเวลาที่กรมอุทกศาสตร์ กองทัพเรือ เวลามาตรฐานสากลอ้างอิงเทียบกับ Coordinated Universal Time (UTC)

การเทียบเวลากับหน่วยงานหรือองค์กรภายนอก เท่ากับว่าเวลาของระบบสารสนเทศนั้นถูกกำหนดโดย trusted third party

เนื่องจากแฮชเข้ารหัสที่บิตคอยน์เลือกใช้เป็นฟังก์ชันคณิตศาสตร์แบบทางเดียว (one-way function) จึงไม่สามารถนำค่าเป้าหมายมาคำนวณย้อนกลับไปหาค่า nonce ที่ถูกต้องได้ ทุกโหนดที่แข่งกันหาค่า nonce จึงต้องใช้วิธีลองผิดลองถูก (trial-and-error) ไปเรื่อย ๆ จนกว่าจะพบค่า nonce ที่ต่ำกว่าค่าเป้าหมาย โหนดที่พบค่า nonce ที่ถูกต้องก่อนจะได้เป็นผู้ประทับเวลา ร้อยบล็อกใหม่เข้า ledger ของโหนดพร้อมกับประกาศให้โหนดอื่นได้รับรู้ เมื่อโหนดอื่น ๆ พบว่ามีบล็อกใหม่เกิดขึ้น จะทำการตรวจสอบความถูกต้องของ nonce ถ้าค่า nonce เป็นไปตามเงื่อนไข จึงจะร้อยบล็อกใหม่เข้า ledger ของโหนดด้วยเช่นกัน โหนดที่ร้อยบล็อกใหม่เข้า ledger แล้ว ก็จะเริ่มกระบวนการสร้างบล็อกต่อไปทันที

ค่า nonce ของบิตคอยน์มีขนาด 32 บิต ซึ่งเท่ากับว่ามีค่าที่แตกต่างกัน 4,294,967,296 ค่า โหนดลองผิดลองถูกโดยเริ่มจากค่า nonce = 0 และเพิ่มค่าขึ้นเรื่อย ๆ จนกว่าจะพบ nonce ที่ทำให้ได้ผลต่ำกว่าค่าเป้าหมาย

หากลองผิดลองถูกจนครบทั้ง 4,294,967,296 ค่าแล้วยังไม่ได้ค่าต่ำกว่าเป้าหมาย โหนดจะเพิ่มข้อมูล extraNonce คำนวณ Merkel Root ใหม่ แล้วเริ่มหาค่า nonce จาก 0 อีกครั้ง



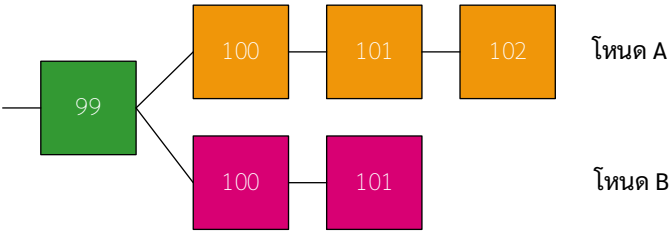
ภาพที่ 3
บล็อกของบิตคอยน์

บล็อกของบิตคอยน์ร้อยกันด้วยค่า Prev Hash ที่อ้างถึง Hash ของบล็อกก่อนหน้า การแก้ข้อมูลที่บล็อก 4999 จะทำให้ค่า hash ของบล็อก 4999 เปลี่ยนไป ซึ่งทำให้ต้องลองผิดลองถูกหา nonce เพื่อสร้างบล็อก 5000, 5001 และบล็อกถัดจากนั้นทุกบล็อกกันใหม่ทั้งหมด

ในกระบวนการ Proof of Work แต่ละโหนดทำงานเป็นอิสระต่อกัน แต่ละโหนดสร้างบล็อกใหม่ด้วยตัวเอง พยายามหาค่า nonce ด้วยตัวเอง และจะร้อยบล็อกใหม่เข้า ledger ของโหนดเองก็ต่อเมื่อโหนดหาค่า nonce ได้ก่อน หรือตรวจพบว่า nonce ที่โหนดอื่นคำนวณได้ก่อนเป็นค่าที่นำมาคำนวณกับบล็อกใหม่ของโหนดเองแล้วต่ำกว่าค่าเป้าหมายจริง การที่แต่ละโหนดทำงานเป็นอิสระต่อกัน ประมวลผล ledger ของโหนดเอง แต่ยังได้ผลลัพธ์ที่ถูกต้องตรงกันกับ ledger ของโหนดอื่น เท่ากับว่าข้อมูลที่บันทึกใน ledger แล้วเป็นข้อมูลที่ได้รับ consensus หรือเห็นพ้องตรงกันแล้วว่าเป็นข้อมูลที่ถูกต้อง

โครงสร้าง ledger เป็นการร้อยบล็อกของธุรกรรมต่อกัน ทำให้การแก้ไข ledger แทบเป็นไปไม่ได้เลย เพราะการแก้ไขข้อมูลทำให้ต้องลองผิดลองถูกหา nonce กันใหม่ตั้งแต่บล็อกที่มีการแก้ไขไปจนกว่าจะร้อยบล็อกได้ยาวที่สุด ธุรกรรมในบล็อกที่ร้อยเข้า ledger แล้วจึงเปลี่ยนแปลงแก้ไขได้ยาก ซึ่งถือเป็น**คุณลักษณะเฉพาะของข้อมูลธุรกรรมของบิตคอยน์และเทคโนโลยีบล็อกเชนอื่น ๆ ที่เกิดขึ้นในภายหลัง**

ในสภาพการทำงานจริง เสถียรภาพและประสิทธิภาพการเชื่อมต่ออินเทอร์เน็ตของโหนดอาจทำให้ข้อมูลธุรกรรมกระจายไม่ทั่วถึงทุกโหนด ส่งผลให้บล็อกธุรกรรมของแต่ละโหนดต่างกัน และมี ledger ที่ไม่ตรงกันได้ ในกรณีนี้บิตคอยน์จะถือว่า ledger ที่ร้อยบล็อกได้ยาวที่สุด (longest chain) เป็น ledger ที่ถูกต้อง โดยโพรโทคอลในการทำ consensus ของบิตคอยน์จะเลือก ledger ที่ร้อยบล็อกได้ยาวที่สุดอัตโนมัติ



ภาพที่ 4
Longest Chain

สมมติว่า หลังจากบล็อกที่ 99 โหนด B ถูกตัดขาดจากอินเทอร์เน็ต ทำให้โหนด B ได้รับธุรกรรมไม่เหมือนกับโหนด A และทำให้ข้อมูลบล็อกที่ 100 – 101 ไม่เหมือนกัน โพรโทคอลในการทำ consensus จะยังคงปล่อยให้โหนด A และ B ประมวลผลบน ledger ตัวเองอย่างอิสระ เมื่อโหนด B เชื่อมอินเทอร์เน็ตกลับมาได้ แล้วพบว่าโหนด A ประกาศบล็อกที่ 102 ซึ่งยาวกว่า ledger ที่โหนด B กำลังประมวลผลอยู่ ธุรกรรมในบล็อกที่ 100 – 101 ของโหนด B (สีชมพู) จะถูกแทนที่ด้วยธุรกรรมในบล็อกที่ 100 – 102 ของโหนด A (สีส้ม) ซึ่งเป็น longest chain ที่ได้รับการยืนยันแล้ว

1.5 Block Time

เพื่อให้โหนดทุกโหนดมีเวลามากพอในการแลกเปลี่ยนธุรกรรมที่ส่งเข้ามาในเครือข่ายได้ทั่วถึง บิตคอยน์จึงจำเป็นต้องถ่วงเวลาในการร้อยบล็อกใหม่เข้าใน ledger เรียกว่าค่า block time

บิตคอยน์กำหนด block time ไว้ *ประมาณ* 10 นาที โดยการกำหนดความยาก (difficulty) ของค่าเป้าหมาย ค่าความยากสูงจะทำให้ได้ค่าเป้าหมายต่ำ ส่งผลให้การหา nonce ที่ต่ำกว่าค่าเป้าหมายใช้เวลานาน แต่เนื่องจากเวลาที่ใช้ในการหา nonce ขึ้นกับความสามารถในการลองผิดลองถูกของโหนดทั้งหมดในเครือข่ายด้วย หากโหนดใน

เครือข่ายบิตคอยน์มีจำนวนมาก มีประสิทธิภาพในการประมวลผลสูง สามารถลองผิดลองถูกได้เร็ว ก็จะมีโอกาสหาค่า nonce ได้เร็ว โพรโทคอลของบิตคอยน์จึงกำหนดให้ทุกโหนดปรับค่าความยากและตั้งค่าเป้าหมายใหม่ทุก ๆ 2016 บล็อก (ประมาณ 14 วัน) ให้สอดคล้องกับจำนวนโหนดและความสามารถในการประมวลผลของทั้งเครือข่ายบิตคอยน์ ณ เวลานั้น เพื่อให้ block time มีค่าประมาณ 10 นาที

1.6 Rewards

ดังที่กล่าวมาก่อนหน้านี้ว่า บิตคอยน์อาศัยการให้รางวัลเพื่อจูงใจผู้ใช้เชื่อมต่อคอมพิวเตอร์เข้าเป็นโหนดของบิตคอยน์ ทำให้บิตคอยน์มีคอมพิวเตอร์ประมวลผล Proof of Work และเก็บสำเนาของ ledger อยู่ตลอดเวลา โดยโพรโทคอลในการทำ consensus ของบิตคอยน์จะให้รางวัลกับโหนดที่สามารถประทับเวลาบล็อกได้เป็นโหนดแรก รางวัลที่ตอบแทนโหนดนี้จะปรากฏเป็นธุรกรรมแรกของบล็อกเสมอ เรียกว่า Coinbase Transaction

ภาพที่ 5
Coinbase Transaction

ตัวอย่าง coinbase transaction เป็นรางวัล 50 BTCs และค่าธรรมเนียม 0.63517500 BTCs โอนเข้าวอลเล็ต 1MdYC22Gmjp2ejVPCxy...

Coinbase Transaction เป็นธุรกรรมเดียวในบล็อกที่จะไม่มี UTXO ที่ขา input แต่มี UTXO ผูกกับบิตคอยน์แอดเดรสที่กำหนดที่ขา output หากมองในทางการเงิน Coinbase Transaction เป็นกลไกผลิตโทเคนเข้าในระบบใช้จ่ายแบบเดียวกับที่มีการผลิตเหรียญและธนบัตรหมุนเวียนในประเทศ

เพื่อให้โทเคนสามารถเป็นเครื่องมือเก็บรักษามูลค่าได้เหมือนเงินตรา บิตคอยน์จึงได้รับการออกแบบให้จำกัดจำนวนโทเคนทั้งหมดที่ระบบจะผลิตขึ้น โดยบิตคอยน์เริ่มให้รางวัลใน Coinbase Transaction ตั้งแต่บล็อกแรกจำนวน 50 BTCs และลดรางวัลลงครึ่งหนึ่งทุก ๆ 210,000 บล็อก (ประมาณ 4 ปี) โทเคนที่ผลิตเป็นรางวัลนี้จะลดลงไปเรื่อย ๆ จนกลายเป็น 0 BTC ราวปี ค.ศ. 2140 ซึ่งจะทำให้เครือข่ายบิตคอยน์จะมีโทเคนหมุนเวียนในระบบทั้งหมดไม่เกิน 21,000,000 BTCs

กล่าวได้ว่า Proof of Work ทำให้โหนดแข่งขันกันหาค่า nonce เพื่อแลกกับรางวัลที่ลดลงและหมดไปในท้ายที่สุด เปรียบได้กับการทำเหมืองแร่ (mine) ที่ต้องออกแรงขุดโดยแร่ในเหมืองก็จะลดลงไปเรื่อย ๆ จึงเป็นที่มาของการเรียกโหนดของบิตคอยน์ ว่า Miner

ในทางการเงิน โทเคนของบิตคอยน์มีคุณสมบัติตรงกับเงินจริง ๆ ทุกประการ ทั้งความคงทน (durability) พกพาสะดวก (portability) หายาก (scarcity/limit supply) อยู่ในรูปแบบแบบเดียวกัน (uniformity/fungibility) แบ่งเป็นหน่วยย่อย ๆ ได้ (divisibility) และเป็นที่ยอมรับในการใช้ (acceptability) โทเคนของบิตคอยน์จึงมีคุณสมบัติที่นำมาใช้เป็นตัวกลางในการแลกเปลี่ยนเป็นสินค้าและบริการได้เช่นเดียวกับเงิน ตรงกับแนวคิดของบิตคอยน์ที่ตั้งใจพัฒนาเป็นระบบเงินสดอิเล็กทรอนิกส์ตั้งแต่แรก ประกอบกับที่บิตคอยน์อาศัยวิทยาการเข้ารหัสลับ (cryptography) เช่น เทคโนโลยีระบบรหัสแบบกุญแจสาธารณะเป็นพื้นฐานในการทำงาน จึงเกิดการประดิษฐ์คำเฉพาะขึ้นใหม่สำหรับเรียกสกุลเงินดิจิทัลที่มีลักษณะเดียวกันนี้โดยผสม cryptography กับ currency เป็นคำว่า **“คริปโทเคอร์เรนซี”** (Cryptocurrency)

1.7 ทำไมเราไม่ใช้บิตคอยน์แทนเงินสดไปเสียเลย?

บิตคอยน์ออกแบบโดยตั้งใจให้เป็นระบบเงินสดที่ไม่จำเป็นต้องมีตัวกลาง แต่ความเป็นจริงกลับมีการใช้บิตคอยน์ในการใช้จ่ายแทนเงินสดไม่มากเท่าไหร่นัก เหตุผลสำคัญคือ

block time 10 นาทีทำให้ต้องรอธุรกรรมมีผลอย่างน้อย 10 นาทีตามไปด้วย ซึ่งต่างจากการใช้เงินสดที่การใช้จ่ายมีผลได้แทบจะทันที

นอกจากนี้ อัตราแลกเปลี่ยนของบิตคอยน์เป็นไปตามอุปสงค์และอุปทาน จึงมีผู้นิยมลงทุนและเก็งกำไร **มูลค่าของบิตคอยน์ที่สูงขึ้น ส่งผลต่อค่าธรรมเนียมธุรกรรมที่สูงขึ้นตามไปด้วย** การใช้บิตคอยน์เพื่อใช้จ่ายจึงถูกจำกัดอยู่กับสินค้าหรือบริการที่มูลค่าสูงเพื่อให้คุ้มกับค่าธรรมเนียมที่ต้องเสียในการทำธุรกรรม

อีกด้านหนึ่ง ธุรกรรมที่บันทึกใน ledger มีเพียงบิตคอยน์แอดเดรสกับจำนวนโทเคนของบิตคอยน์ ไม่มีข้อมูลส่วนบุคคลที่สามารถระบุตัวบุคคลได้ (Personally Identifiable Information: PII) ธุรกรรมของบิตคอยน์จึงมีสภาวะนิรนาม (anonymity) เหมือนกับการใช้จ่ายเงินสดที่ไม่จำเป็นต้องรู้จักกัน **บิตคอยน์จึงเป็นตัวกลางที่นิยมใช้จ่ายในกลุ่มมิจฉาชีพ** เพราะติดตามถึงตัวผู้เกี่ยวข้องในธุรกรรมยาก โดยที่ผ่านมาบิตคอยน์จึงปรากฏในสื่อต่าง ๆ ในลักษณะที่พัวพันกับธุรกิจผิดกฎหมาย การฟอกเงิน เป็นส่วนหนึ่งในการหลอกลวง แชร์ลูกโซ่ ซึ่งให้ภาพลักษณ์ของบิตคอยน์ คริปโทเคอร์เรนซี และบล็อกเชนจึงไม่ดีเท่าไหร่นัก และกลายเป็นกระแสที่บดบังศักยภาพที่แท้จริงของเทคโนโลยี

ปัญหาทางเทคนิคที่สำคัญอีกประการคือ การเลือก longest chain ทำให้ ledger ที่ร้อยบล็อกได้ยาวที่สุดสามารถแทนที่ ledger ที่ร้อยบล็อกสั้นกว่าได้ ธุรกรรมที่เกิดขึ้นและได้รับการยืนยันไปแล้วจึงถูกยกเลิกได้ (เช่น ในภาพที่ 4 ที่ ledger ของโหนด B ถูกแทนที่ด้วย ledger ของโหนด A)

การยกเลิกธุรกรรมโดยใช้วิธีสร้าง ledger ที่ร้อยบล็อกได้ยาวที่สุดมีโอกาสสำเร็จได้ถ้าสามารถรวบรวมพลังในการประมวลผลได้เกินครึ่งหนึ่งของพลังการประมวลผลทั้งหมดในเครือข่ายรวมกัน จึงเรียกกันว่า **51% Attack**

ในทางปฏิบัติ 51% Attack เกิดได้ง่ายกับเครือข่ายบล็อกเชนที่ใช้ Proof of Work และมีจำนวนโหนดน้อย เพราะผู้โจมตีมีโอกาสที่จะหาพลังในการประมวลผลได้เกินครึ่งของ

เครือข่ายได้ เช่น เช่าบริการจากคลาวด์ แต่สำหรับเครือข่ายขนาดใหญ่เป็นหลักหมื่นโหนด อย่างบิตคอยน์ การเกิด 51% Attack เป็นไปได้ยากมาก

เดือนมิถุนายน ค.ศ. 2014 โหนดของบิตคอยน์ชื่อ GHash.io ซึ่งเป็น miner pool ที่ใหญ่ที่สุดในเวลานั้นมีพลังในการประมวลผลมากกว่า 51% [8] ทำให้บิตคอยน์ตกอยู่ในความเสี่ยงที่จะถูกโจมตีโดย 51% Attack

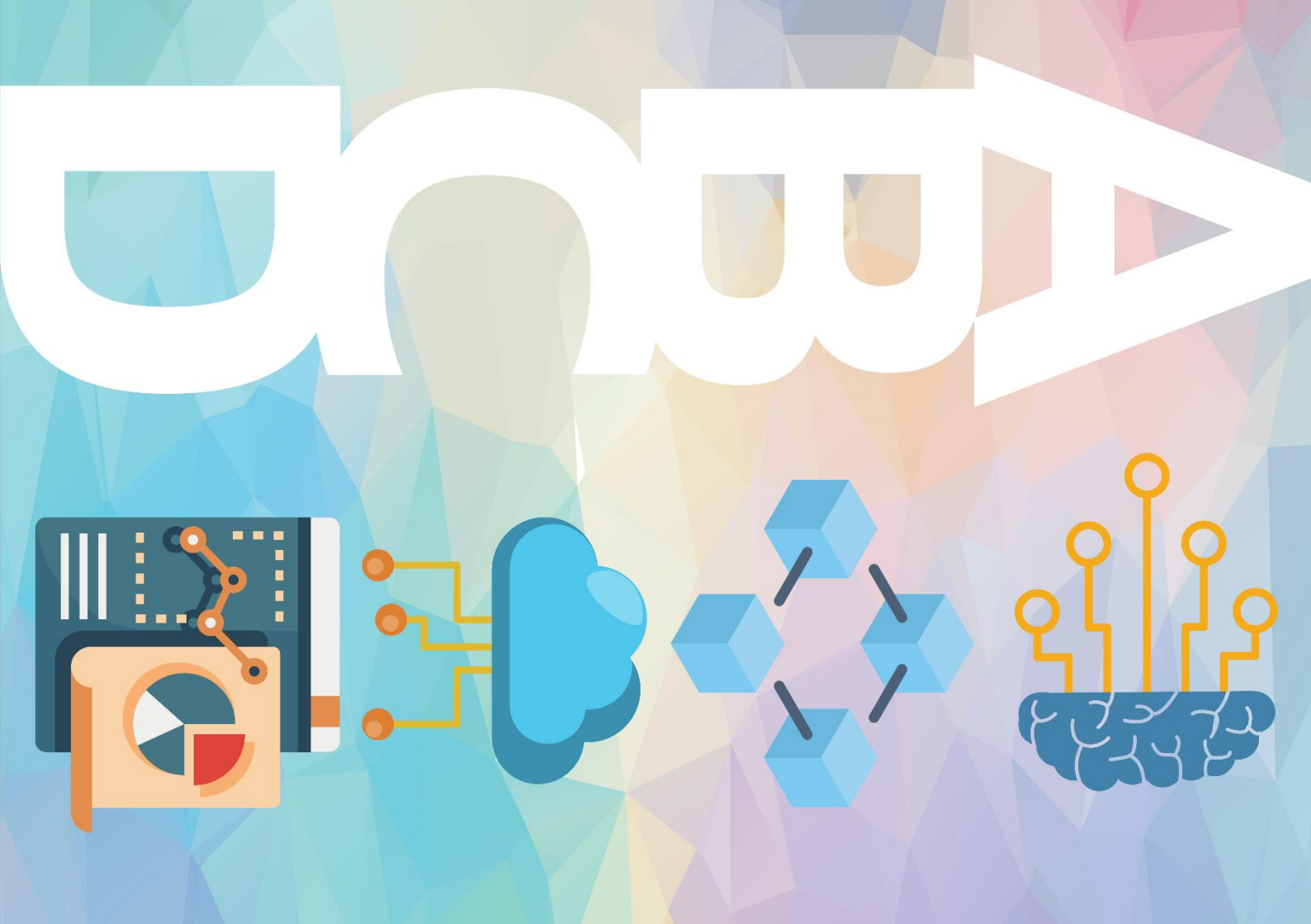
ชุมชน (community) ของบิตคอยน์ได้หารือกันอย่างกว้างขวาง แต่ไม่สามารถหาวิธีป้องกันหรือแก้ปัญหา 51% Attack ได้

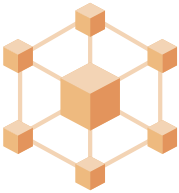
เหตุการณ์ครั้งนั้นจบลงที่ GHash.io ตกลงลดพลังในการประมวลผลลง และสัญญากับชุมชนว่าจะควบคุมพลังในการประมวลผลของ pool ไม่ให้เกิน 40%

ความเสี่ยงที่ธุรกรรมจะถูกเปลี่ยนแปลงได้ เป็นปัจจัยหนึ่งที่ทำให้ผู้รับชำระสินค้าที่มีมูลค่าสูง เช่น อสังหาริมทรัพย์ หรือ รถยนต์ จะรอให้ธุรกรรมยืนยันผ่านไปอย่างน้อย 6 บล็อก ซึ่งต้องใช้เวลาประมาณ 1 ชั่วโมง จึงจะมั่นใจได้ว่าธุรกรรมในบล็อกที่ร้อยเข้า ledger ไปแล้วจะไม่ถูกเปลี่ยนแปลง

แม้บิตคอยน์ไม่ได้ตอบโจทย์ในการชำระเงินอย่างที่ตั้งใจเท่าไรนัก แต่บิตคอยน์ยังคงเป็นคริปโทเคอร์เรนซีที่ได้รับความนิยมสูงในการลงทุน ทั้งการลงทุนโดยเข้าร่วมเป็น miner เพื่อมีโอกาสได้รางวัลตอบแทนที่สูง และการลงทุนซื้อขายเก็งกำไร

สำหรับมุมมองทางด้านเทคโนโลยี บิตคอยน์เป็นตัวอย่างแรกของระบบสารสนเทศแบบกระจายศูนย์และกระจายอำนาจที่รักษาความน่าเชื่อถือของข้อมูลได้โดยไม่จำเป็นต้องมีตัวกลางเป็น trusted third party บิตคอยน์จึงกลายเป็นต้นแบบที่ทำให้เกิดเทคโนโลยีบล็อกเชน และคริปโทเคอร์เรนซีอื่น ๆ อีกหลายสกุล เช่น Litecoin, Ethereum, Stellar, Dogecoin, และ Monero เป็นต้น





> “Everything will be tokenized and connected by a blockchain one day.”
>
> – Fred Ehrsam
> Coinbase Co-Founder

2 ทำความรู้จักกับบล็อกเชน

ศัพท์คำว่า บล็อกเชน เกิดขึ้นหลังจากมีบิตคอยน์แล้ว โดยเรียกจากลักษณะการบันทึกข้อมูลเป็นบล็อกร้อยต่อกัน อาจจะเรียกได้ว่า บิตคอยน์ถือเป็นบล็อกเชนแรกที่เกิดขึ้นบนโลก

ปัจจุบัน บล็อกเชน ยังไม่มีนิยามตามหลักวิชาการทางเทคโนโลยีสารสนเทศที่ชัดเจน แต่เป็นศัพท์ที่ยอมรับและใช้กันอย่างกว้างขวางในการอ้างถึงระบบสารสนเทศที่มีหลักการทำงานและลักษณะเฉพาะเหมือนกับบิตคอยน์

ลักษณะเฉพาะที่ปรากฏในบล็อกเชน ประกอบด้วย

Decentralized: บล็อกเชนเป็นเครือข่ายแบบ peer-to-peer ทำงานแบบกระจายศูนย์ การประมวลผลของโหนดในเครือข่ายเป็นอิสระต่อกัน มีจุดประสงค์ในการกระจายอำนาจการประมวลผลข้อมูลไม่ให้ตกอยู่ในการควบคุมของบุคคลหรือองค์กรใดองค์กรหนึ่ง

Distributed ledger: บล็อกเชนประมวลผลโครงสร้างข้อมูลที่เรียกว่า ledger โดยแต่ละโหนดมีสำเนา ledger เป็นของตัวเอง ประมวลผล ledger ด้วยตัวเอง โดยโพรโทคอลในการทำ consensus เดียวกัน ข้อมูลธุรกรรมใน ledger มักบันทึกเป็นชุดที่เรียกว่าบล็อก แต่ละบล็อกจะร้อยเชื่อมกับบล็อกก่อนหน้าโดยใช้วิทยาการรหัสลับ

Immutable: กลไกทางวิทยาการรหัสลับทำให้ธุรกรรมที่ได้รับการบันทึกใน ledger แล้ว จะย้อนคืน (revert) ลบทิ้ง หรือเปลี่ยนแปลงภายหลังแทบไม่ได้เลย บล็อกเชนจึงสามารถรักษาความถูกต้องสมบูรณ์และความโปร่งใสของข้อมูลได้

Consensus: การประมวลผลแบบ decentralized ทำให้โหนดในเครือข่ายบล็อกเชนต้องมีโพรโทคอลในการทำ consensus เพื่อประมวลผล ledger ที่จัดเก็บในแต่ละโหนดให้มีข้อมูลสอดคล้องตรงกัน

Openness: บล็อกเชนเผยแพร่การออกแบบระบบสารสนเทศ และใช้การพัฒนาซอฟต์แวร์โอเพนซอร์ส เพื่อความโปร่งใส สร้างความน่าเชื่อถือในระบบ และเปิดโอกาสให้ทุกคนประเมินความน่าเชื่อถือของระบบได้

Anonymity: ธุรกรรมบนบล็อกเชนมีเพียงแอดเดรส (เช่น บิตคอยน์แอดเดรส) ที่ใช้อ้างอิงระหว่างกันเท่านั้น ไม่จำเป็นต้องมีข้อมูลที่ระบุตัวผู้ทำธุรกรรมได้ จึงสามารถรักษาความเป็นส่วนตัวของผู้ทำธุรกรรมได้

บล็อกเชนมีการทำงานเป็นเครือข่าย แลกเปลี่ยนข้อมูลและประมวลผลตามโพรโทคอลในการทำ consensus ที่กำหนด เครือข่ายบล็อกเชนอาจแบ่งออกได้เป็นสองประเภทหลัก ๆ คือ permissionless และ permissioned

เครือข่ายบล็อกเชนแบบ permissionless เป็นเครือข่ายบล็อกเชนที่ **ไม่มีกลไกในการอนุญาตหรือกำหนดสิทธิในการเข้าถึง** ทุกคนสามารถเชื่อมต่อกับเครือข่ายได้ อ่าน/เขียน ledger ได้ และมีส่วนร่วมในการยืนยันธุรกรรมได้ โดยไม่มีข้อจำกัดหรือต้องขออนุญาตใคร เครือข่ายบล็อกเชนลักษณะนี้มักออกแบบให้มีการกระจายอำนาจมากที่สุดเท่าที่จะทำได้เพื่อลดความเสี่ยงที่จะมีผู้ใดผู้หนึ่งสามารถยึดครองเครือข่ายเป็นของตนเอง เครือข่ายบล็อกเชนสาธารณะ (public blockchain) เช่น บิตคอยน์ อีเธอเรียม เป็นตัวอย่างของเครือข่ายบล็อกเชนแบบ permissionless

ส่วนเครือข่ายบล็อกเชนแบบ permissioned ให้อำนาจผู้ดูแลเครือข่ายบล็อกเชนในการ**กำหนดสิทธิการเชื่อมต่อ การอ่าน/เขียน ledger และการมีส่วนร่วมในการยืนยันธุรกรรม** จึงเหมาะกับการใช้งานภายในองค์กร (private blockchain) หรือระหว่างองค์กรที่แลกเปลี่ยนข้อมูลระหว่างกัน (consortium blockchain) เครือข่ายบล็อกเชนแบบ permissioned มักมีจำนวนโหนดในการยืนยันธุรกรรมน้อย การกระจายข้อมูลธุรกรรมให้ทั่วถึงทำได้ง่ายและรวดเร็ว จึงมักกำหนด block time ได้ต่ำ เครือข่ายบล็อกเชนที่เป็น private หรือ consortium มักใช้ทรัพยากรขององค์กรเองในการประมวลผลจึงไม่จำเป็นต้องมีคริปโทเคอร์เรนซีสำหรับชำระค่าธรรมเนียมธุรกรรม ตัวอย่างเช่น Hyperledger, Corda, Quorum เป็นซอฟต์แวร์ที่ใช้สร้างบล็อกเชนแบบ permissioned ที่นิยมนำมาสร้างบล็อกเชนในองค์กร

2.1 โทเคน

ความหมายทั่วไปของโทเคนคือ**สิ่งที่ใช้แทนค่า หรือมีมูลค่าในตัว** เช่น เหรียญ ธนบัตร เป็นสิ่งแทนมูลค่าเงินตรา เหรียญหรือหน่วยนับของคริปโทเคอร์เรนซี จึงเรียกได้ว่าเป็นโทเคนเช่นเดียวกัน

สำหรับการใช้งานในบล็อกเชน โทเคนอาจแบ่งออกตามลักษณะการใช้ประโยชน์ได้ 3 ประเภท ได้แก่

Payment Token เป็นโทเคนที่ออกแบบเพื่อใช้ชำระแทนเงินเป็นหลัก ตัวอย่างเช่น โทเคนของบิตคอยน์ อีเธอเรียม และคริปโทเคอร์เรนซีอื่น ๆ โทเคนประเภทนี้มักจะกระทบกับกฎหมายเกี่ยวกับเงินและกฎหมายที่เกี่ยวกับการชำระเงิน มีผลต่อเสถียรภาพของเงิน มีความเสี่ยงในการใช้เป็นเครื่องมือในการฟอกเงิน หลายประเทศจึงมีการกำกับดูแลที่เข้มงวด

Security Token หมายถึง โทเคนที่ออกแบบเพื่อใช้แทนหน่วยลงทุน เช่น พันธบัตร ตราสารอนุพันธ์ ตราสารทุน หุ้น โทเคนประเภทนี้จึงมีความเฉพาะที่ มีจุดประสงค์ในการลงทุนเพื่อได้ผลตอบแทน และอาจมีการกำกับดูแลตามกฎหมายที่เกี่ยวข้องกับการแลกเปลี่ยนซื้อขายหลักทรัพย์

Utility Token หมายถึง โทเคนที่ใช้แทนสิทธิในการเข้าถึงบริการหรือแลกเปลี่ยนเป็นสิ่งของต่าง ๆ เช่น สิทธิในการโหวต สิทธิในการเข้าพักโรงแรม สิทธิในการเดินทาง ดูภาพยนตร์ หากเทียบแล้วโทเคนประเภทนี้คล้ายกับตั๋วหรือบัตรที่เราใช้งานกัน ลักษณะการใช้งานโทเคนประเภทนี้หากคาบเกี่ยวกับการเข้าถึงสินค้าหรือบริการ อาจจะมีผลกระทบกับการคุ้มครองผู้บริโภค

การกำหนดให้โทเคนแทนสิ่งหนึ่งสิ่งใด เรียกว่า tokenization ประกอบกับประโยชน์จากที่ข้อมูลในบล็อกเชนมีความน่าเชื่อถือมากกว่าบันทึกในฐานข้อมูลทั่วไป tokenization จึงเป็นหนึ่งในการประยุกต์ใช้บล็อกเชนที่ใช้งานจริงอย่างแพร่หลาย เช่น

การตรวจสอบแหล่งกำเนิดของสินค้า การซื้อขายพันธบัตร ระบบ settlement สำหรับสถาบันการเงิน การตรวจสอบความถูกต้องของเอกสารสำคัญ เป็นต้น

2.2 Consensus

โพรโทคอลในการทำ consensus แบบ Proof of Work มีข้อดีที่สามารถกระจายอำนาจได้สูงมาก แต่มีข้อเสียอย่างมากตรงที่สิ้นเปลืองพลังงานในการประมวลผล เนื่องจากทุกโหนดต่างแข่งขันกันหาค่า nonce แต่จะมีเพียงโหนดเดียวที่จะได้รางวัล เท่ากับว่าโหนดอื่น ๆ ประมวลผลทิ้งโดยไม่ได้ประโยชน์อะไรเลย นอกจากนี้ Proof of Work ยังมีความเสี่ยงที่จะเกิด 51% Attack ในเครือข่ายขนาดเล็ก บล็อกเชนที่เกิดขึ้นหลังบิตคอยน์จึงเริ่มคิดโพรโทคอลในการทำ consensus แบบอื่น ๆ อีกหลายแบบที่ไม่สิ้นเปลืองพลังงานและแก้ปัญหา 51% Attack ไปในตัว

ปัจจุบัน นอกจาก Proof of Work แล้ว โพรโทคอลในการทำ consensus ของบล็อกเชนจัดเป็นกลุ่มใหญ่ ๆ ได้อีก 3 กลุ่มได้แก่ Proof of Stake (PoS), Proof of Authority (PoA) และ Practical Byzantine Fault Tolerance (PBFT)

2.2.1 Proof of Stake

เนื่องจาก Proof of Work ทำให้สิ้นเปลืองพลังงานจากเหตุที่ทุกโหนดแข่งขันกันหาคำตอบทางคณิตศาสตร์ที่ซับซ้อน วิธีแก้ปัญหาที่ตรงไปตรงมาที่สุดคือเลี่ยงการแข่งขันหาคำตอบ โพรโทคอลในการทำ consensus แบบ Proof of Stake จึงเลี่ยงการแข่งขันโดยใช้วิธีสุ่มเลือกโหนดที่จะทำหน้าที่ยืนยันธุรกรรมในบล็อกตามสัดส่วนของการมีส่วนได้ส่วนเสียหรือ stake แทน

ใน Proof of Stake โหนดที่ทำหน้าที่ยืนยันธุรกรรมไม่ต้องประมวลผลแข่งขันเพื่อหาคำตอบให้ได้ก่อน แต่จะต้องวาง stake ในการเข้ามามีส่วนในการยืนยันธุรกรรม แต่ละรอบของการยืนยันธุรกรรม ระบบจะ**สุ่มเลือกโหนดมายืนยันธุรกรรมตามสัดส่วนของ**

stake ที่วางไว้ การทำงานของโหนดที่ได้รับเลือกจะมีเพียงการตรวจสอบยืนยันธุรกรรมเท่านั้น ไม่ต้องทำงานหนักเหมือน miner ของบิตคอยน์ โหนดที่ทำหน้าที่ยืนยันธุรกรรมของ Proof of Stake จึงเรียกเป็น **validator** แทน

Proof of Stake บางประเภท มีรางวัลตอบแทน validator โดยให้ตามสัดส่วนของ stake ที่วางไว้ ในขณะที่บางประเภทไม่มีรางวัลตอบแทนโดย validator จะได้รับเพียงค่าธรรมเนียมธุรกรรมในบล็อกที่ยืนยันเท่านั้นเพราะถือว่าการทำงานไม่ได้ใช้ทรัพยากรมากเหมือนกับ Proof of Work

การสุ่มเลือก validator ทำให้ Proof of Stake ปลอดภัยจาก 51% Attack แบบที่เกิดใน Proof of Work อย่างไรก็ตาม ในทางทฤษฎี Proof of Stake มีความเสี่ยงถูกโจมตีได้ หากโหนดใดโหนดหนึ่งมี stake มากกว่า 51% ของ stake ทั้งหมด การเลือกว่าจะใช้อะไรเป็น stake ในระบบจึงมีผลกระทบต่อความน่าเชื่อถือของระบบด้วย

Proof of Stake ที่มีการใช้งานปัจจุบัน นิยมใช้โทเคนของคริปโทเคอร์เรนซีเป็น stake มีผลทำให้การโจมตีด้วย 51% Attack แทบเป็นไปไม่ได้เลยเพราะผู้โจมตีต้องรวบรวมโทเคนเพื่อวาง stake ให้ได้มากกว่าครึ่งหนึ่งของโทเคนทั้งหมดที่หมุนเวียนในระบบ ณ ขณะนั้น ยิ่งมีความต้องการโทเคนมากขึ้น ค่าโทเคนก็จะยิ่งสูงขึ้น การรวบรวมโทเคนเพื่อโจมตีจะยิ่งต้องใช้เงินลงทุนมากขึ้น ในทางกลับกัน หากผู้โจมตีวาง stake ได้เกินครึ่งจริง ๆ ความเชื่อมั่นในคริปโทเคอร์เรนซีนั้นจะหายไปทันที มูลค่าโทเคนจะลดลง ซึ่งทำให้มูลค่าสินทรัพย์ในมือผู้โจมตีลดลงไปด้วย ดังนั้น **51% Attack ใน Proof of Stake จึงไม่มีความคุ้มค่าที่จะทำ**

นอกจากนี้ Proof of Stake บางประเภทมีกลไกป้องกันการโจมตีจาก validator ที่ไม่ซื่อสัตย์โดยถือว่า stake ที่วางไว้เป็นสินทรัพย์ค้ำประกันการทำงาน หากตรวจพบการโจมตีหรือการทำงานผิดปกติของ validator ระบบจะลงโทษ validator นั้นโดยสั่งยึด stake เป็นค่าปรับ หรือทำลาย stake ทิ้ง

Peercoin เป็นบล็อกเชนแรก ๆ ที่นำ Proof of Stake มาใช้งาน ปัจจุบันบล็อกเชนสาธารณะหลายตัวเริ่มหันมาใช้ Proof of Stake แทน Proof of Work มากขึ้น เช่น Polkadot, Tezos, Nxt, และ EOS เป็นต้น อีเธอเรียมซึ่งปัจจุบันใช้ Proof of Work ก็มีแผนจะเปลี่ยนมาใช้ Proof of Stake เพื่อลดการใช้พลังงานและรองรับธุรกรรมได้มากขึ้น

2.2.2 Proof of Authority

หากพิจารณาการทำงาน Proof of Work และ Proof of Stake จะเห็นได้ว่าการทำ consensus ทั้งสองแบบมีการกระจายอำนาจสูง ทุกโหนดใน Proof of Work สามารถเป็น miner ได้อย่างอิสระโดยไม่อยู่ใต้อำนาจควบคุมของใครเลย เช่นเดียวกับโหนดใน Proof of Stake ที่สามารถวาง stake เพื่อเป็น validator เมื่อใดก็ได้ กลไก consensus ทั้งสองแบบจึงเหมาะกับเครือข่ายแบบ public/permissionless

แต่กลไกเหล่านี้ไม่จำเป็นเลย หากใช้งานภายในองค์กรเดียวกันหรือระหว่างองค์กรที่เชื่อใจกันตั้งแต่แรก จึงเกิดแนวคิดในการทำ consensus ที่เรียกว่า Proof of Authority

สำหรับ Proof of Authority ผู้มีอำนาจของเครือข่ายบล็อกเชนนั้นจะเป็นผู้กำหนดโหนดในการตรวจสอบยืนยันธุรกรรมในเครือข่ายด้วยตัวเอง โหนดที่ทำหน้าที่นี้ เรียกว่า signer

signer ทุกตัวมีสิทธิในการตรวจสอบยืนยันธุรกรรมได้ทุกบล็อก หากเครือข่ายมี signer มากกว่า 1 โหนด signer สามารถเวียนกันยืนยันธุรกรรมได้เลย เมื่อ signer ตรวจสอบยืนยันและประกาศบล็อกใหม่ออกไปแล้ว ทุกโหนดจะถือว่าเป็นบล็อกธุรกรรมที่ถูกต้องและร้อยเข้า ledger ได้ทันที การทำงานของ Proof of Authority เรียบง่ายมาก และใช้พลังในการประมวลผลน้อยกว่า Proof of Work มาก

น้ำหนักความน่าเชื่อถือของ Proof of Authority จึงแทบไม่ได้อยู่ที่กลไก consensus แต่อยู่ที่การเลือก signer

signer ที่ดีต้องมีความน่าเชื่อถือ ไม่มีส่วนได้ส่วนเสียกับ signer อื่น มีการดูแลรักษาความมั่นคงปลอดภัยที่ดี มีความโปร่งใสตรวจสอบได้ และควรกระจายอำนาจการควบคุมไม่ให้ตกอยู่ภายใต้การดูแลของบุคคล กลุ่มบุคคล หรือองค์กรเดียวกัน ให้ได้มากที่สุด เพื่อป้องกันไม่เกิด 51% Attack

Proof of Authority มักใช้เป็น consensus สำหรับเครือข่ายบล็อกเชนแบบ permissioned ทั้งที่เป็น private และ consortium

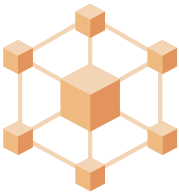
2.2.3 Practical Byzantine Fault Tolerance

Practical Byzantine Fault Tolerance (PBFT) [9] เป็นกลไก consensus โดยใช้วิธี **เสียงข้างมาก** นิยมใช้กับระบบสารสนเทศที่ต้องทำงานได้อย่างถูกต้องแม้จะอยู่ในสภาพแวดล้อมที่มีข้อบกพร่องในการประมวลผลข้อมูล เช่น ระบบควบคุมอากาศยาน วิธีเสียงข้างมากของ PBFT สามารถประยุกต์ใช้งานเป็นโพรโทคอลในการทำ consensus ของบล็อกเชนได้เช่นกัน

การทำงานตามหลักของ PBFT โหนดที่ทำหน้าที่ยืนยันธุรกรรมจะแลกเปลี่ยนผลการยืนยันกับโหนดอื่น ๆ ทุกโหนด ผลการยืนยันที่ตรงกันไม่น้อยกว่า ⅔ ของจำนวนโหนดทั้งหมดจะถือเป็นผลที่ถูกต้อง

PBFT มีข้อเสียสำคัญที่ต้องอาศัยการสื่อสารเพื่อแลกเปลี่ยนข้อมูลระหว่างโหนดสูง ยิ่งโหนดมีเยอะปริมาณการแลกเปลี่ยนยิ่งเพิ่มเป็นทวีคูณ PBFT จึงเหมาะจะใช้กับเครือข่ายบล็อกเชนแบบ private หรือ consortium ที่มีจำนวนโหนดน้อย และไม่เหมาะจะใช้กับบล็อกเชนสาธารณะที่มีโหนดจำนวนมาก

ตัวอย่างบล็อกเชนที่ประยุกต์ใช้ PBFT ในการทำ consensus เช่น Tendermint และ Hyperledger Fabric เป็นต้น



> “Has the Internet changed our lives?
> Have mobile phones changed our lives?
> The blockchain is something that is that transformative.”
>
> -- Brock Pierce
> Entrepreneur

3 บล็อกเชนในการทำธุรกรรมทางอิเล็กทรอนิกส์

สำหรับด้านไอทีแล้ว กลไกการทำงานและคุณสมบัติเฉพาะของเทคโนโลยีบล็อกเชนคือการเปลี่ยนแปลงครั้งยิ่งใหญ่ครั้งหนึ่งของอุตสาหกรรมไอที

กล่าวกันว่าคลื่นการเปลี่ยนแปลงของไอทีเกิดขึ้นครั้งแรกในสมัยที่ผู้ใช้ทั่วไปสามารถเข้าถึงคอมพิวเตอร์ จึงเกิดอุตสาหกรรมซอฟต์แวร์และบริษัทซอฟต์แวร์อย่าง

Microsoft, Apple, หรือ Adobe คลื่นการเปลี่ยนแปลงเกิดขึ้นอีกครั้งเมื่อผู้ใช้เข้าถึงอินเทอร์เน็ต ทำให้เกิดบริษัทที่ผลิตซอฟต์แวร์บริการบนเว็บ อย่าง Google และ Facebook

บล็อกเชน คือคลื่นการเปลี่ยนแปลงครั้งที่สาม

บล็อกเชนเป็นเทคโนโลยีที่สร้างศักยภาพการประมวลผลธุรกรรมอัตโนมัติและเป็นอิสระไม่ขึ้นกับบุคคลที่สาม พื้นฐานความน่าเชื่อถือฝากไว้กับโค้ดของบล็อกเชนและสัญญาอัจฉริยะ ใช้โมเดลการพัฒนาซอฟต์แวร์โอเพนซอร์สในการสร้างความโปร่งใสและเปิดโอกาสให้ผู้ใช้ทุกคนกำกับดูแลร่วมกัน อาจกล่าวได้ว่าลักษณะเฉพาะของบล็อกเชนทำให้อำนาจการควบคุมข้อมูลอยู่ในมือผู้ใช้

ปัจจุบันอุตสาหกรรมไอทีเริ่มใช้บล็อกเชนเพื่อกำจัดหรือลดความจำเป็นของ trusted third party กระจายการประมวลผลและการจัดเก็บข้อมูลให้อยู่บนเครือข่าย บล็อกเชนแทนการประมวลผลและเก็บข้อมูลรวมศูนย์แบบเดิม โดยเฉพาะกับระบบงานที่มีผู้มีส่วนได้ส่วนเสียใช้ร่วมกัน เช่น Supply Chain Management, เอกสารรับรอง, Digital Identity เป็นต้น

3.1 Supply Chain Management

ระบบ Supply Chain Management เป็นการจัดการข้อมูลของผลิตภัณฑ์ตลอดห่วงโซ่อุปทาน โดยมีวัตถุประสงค์หลักในการตรวจสอบแหล่งที่มา (Provenance) และการติดตามผู้เกี่ยวข้องกับการผลิตและจัดจำหน่ายตลอดห่วงโซ่อุปทาน (Traceability)

ปัญหาใหญ่ของระบบ Supply Chain Management ที่มีอยู่ในปัจจุบันคือการแลกเปลี่ยนข้อมูลระหว่างผู้เกี่ยวข้องตลอดห่วงโซ่อุปทานทำให้เกิดสำเนาของข้อมูลธุรกรรมหลายชุด แต่ละชุดอยู่ภายใต้การควบคุมของผู้เกี่ยวข้องคนละคนกัน การควบคุมให้ข้อมูลครบถ้วนถูกต้องตรงกันตลอดเวลาทำได้ยาก และมีต้นทุนในการกำกับดูแลข้อมูลให้มีความโปร่งใสและเป็นประโยชน์ต่อผู้บริโภค ปัญหาเหล่านี้เป็นช่องว่างที่ทำให้เกิดการปลอมแปลงสินค้า วัตถุดิบ หรือปฏิเสธความรับผิดชอบข้อมูลธุรกรรมได้ง่าย

เทคโนโลยีบล็อกเชนเหมาะที่จะนำมาประยุกต์ใช้เพื่อแก้ปัญหาของระบบ Supply Chain Management โดยผู้มีส่วนได้ส่วนเสียตลอดห่วงโซ่อุปทานทำธุรกรรมบนบล็อกเชน ตรงไปยังสัญญาอัจฉริยะที่ทำงานอัตโนมัติและเป็นอิสระจากการควบคุมของผู้มีส่วนได้ส่วนเสียทุกราย ข้อมูลธุรกรรมที่ได้รับการยืนยันโดยบล็อกเชนแล้วจะถูกบันทึกใน ledger ถูกต้องตรงกันเสมอ การจงใจแก้ไขข้อมูลใน ledger เพื่อปลอมแปลง สินค้า วัตถุดิบ ระหว่างห่วงโซ่อุปทานทำได้ยากมาก สร้างความโปร่งใสและความเชื่อมั่นได้สูงกว่าระบบ Supply Chain Management ที่ไม่ใช่บล็อกเชน

ตัวอย่างเช่น Everledger [54] เป็นระบบงาน Supply Chain Management ที่ใช้บล็อกเชนในการบันทึกธุรกรรมเพื่อระบุแหล่งที่มาของเพชรและติดตามสถานะการครอบครองตลอดสายการผลิต โดยการ tokenize เพชรจากคุณสมบัติเฉพาะของเพชรแต่ละเม็ด (เช่น Cut, Color, Clarity, Carat - 4Cs และค่าอื่น ๆ กว่า 40 ค่า) รวมทั้งติดตามการครอบครองเมื่อมีการซื้อขาย ธุรกรรมเกิดขึ้นจากแอดเดรสผู้มีส่วนได้ส่วนเสียตรงไปยังสัญญาอัจฉริยะของ Everledger บนบล็อกเชน จึงสามารถตรวจสอบที่มาของเพชรทุกเม็ดที่บันทึกใน Everledger ตั้งแต่ผู้ที่เป็นเจ้าของคนล่าสุดย้อนกลับได้จนถึงเหมืองเพชรที่เป็นแหล่งกำเนิดของเพชรเม็ดนั้น ผู้ซื้อผู้ขายจึงมั่นใจได้ว่าเพชรทุกเม็ดที่บันทึกใน Everledger มีที่มาถูกต้องตามกฎหมาย บริษัทประกัน ตำรวจสากล สามารถใช้ประโยชน์จากข้อมูลของ Everledger ในการตรวจสอบเพชรที่ถูกโจรกรรม ลักลอบขุด ลักลอบนำเข้า ได้ตลอดเวลา

บริษัท De Beer ซึ่งเป็นผู้ผลิตเพชรรายใหญ่ของโลก ได้พัฒนา Supply Chain Management สำหรับเพชร ชื่อ Tracr ซึ่งทำงานบนบล็อกเชนเช่นกัน [55]

Everledger และ Tracr จึงเป็นตัวอย่างของการประยุกต์ใช้เทคโนโลยีบล็อกเชนเป็นแหล่งข้อมูลที่มีความน่าเชื่อถือ ในการป้องกันความสูญเสียจากการปนเปื้อน ปลอมแปลงเพชรที่ผิดกฎหมายเข้ามาในระบบได้

BLOCKCHAIN IN

SUPPLY CHAIN ~ PHARMACEUTICAL

บริษัทผลิตยา

บริษัทผลิตยา สร้าง QR code และโทเคน บันทึกข้อมูลการผลิตยา เช่น ชื่อผลิตภัณฑ์ ผู้ผลิต วันผลิต วันหมดอายุ Lot.No. ลงลายมือชื่อดิจิทัล บันทึกลงบล็อกเชน เพื่อส่งให้ตัวแทนจำหน่าย บล็อกเชนคืนค่าเป็นแฮชของธุรกรรมที่สามารถใช้ในการตรวจสอบได้ ข้อมูลที่บันทึกในโทเคนจะสามารถเปิดอ่านได้เฉพาะตัวแทนจำหน่ายที่จะได้รับยาไปจำหน่ายเท่านั้น

ตัวแทนจำหน่าย

ตัวแทนจำหน่ายตรวจสอบข้อมูลสินค้าและแหล่งผลิตได้จากแฮชธุรกรรม ลงรับสินค้าโดยลงลายมือชื่อดิจิทัลบันทึกในบล็อกเชน ยาที่ลงรับเรียบร้อยแล้ว สามารถจัดจำหน่ายต่อไปยังร้านค้าปลีก คลินิก หรือโรงพยาบาล โดยสัญญาอัจฉริยะเป็นตัวควบคุม หากใช้ CBDC ได้ในอนาคต ตัวแทนจำหน่ายสามารถตัดโอน CBDC ไปโรงงานผลิตได้ตามระบุในเงื่อนไขของสัญญาอัจฉริยะ

ร้านค้าปลีก

ร้านค้าปลีก คลินิก หรือโรงพยาบาล ตรวจสอบข้อมูลสินค้า แหล่งผลิต และตัวแทนจำหน่ายได้จากแฮชธุรกรรมเช่นกัน การขายหรือจ่ายยาให้กับผู้ป่วยจะได้รับการบันทึกในบล็อกเชนโดยลงลายมือชื่อดิจิทัลกำกับในธุรกรรมที่บันทึกในบล็อกเชน

ผู้บริโภค

ผู้ซื้อหรือผู้ป่วยสามารถสแกน QR code เพื่อตรวจสอบแหล่งผลิตและคุณภาพของยา ข้อมูลใน QR code สามารถเชื่อมโยงกลับไปยังธุรกรรมที่อยู่ในบล็อกเชนซึ่งช่วยให้มั่นใจได้ว่าเป็นยาที่มีการผลิตและจัดจำหน่ายใน supply chain ที่โปร่งใส การปลอมแปลงข้อมูลยา สำเนาใช้ซ้ำแทบเป็นไปไม่ได้เลยเนื่องจากบล็อกเชนป้องกันการปลอมโทเคนและ double spending ได้

การสำรวจโดยองค์การเพื่อความร่วมมือและการพัฒนาทางเศรษฐกิจ (OECD) พบว่าตลาดของอุตสาหกรรมยาทั่วโลกมีมูลค่าไม่ต่ำกว่า 1 ล้านล้านเหรียญสหรัฐต่อปี และมียาและเวชภัณฑ์ปลอมปนเปื้อนอยู่ใน supply chain ราว 3.3% บล็อกเชนสามารถป้องกันการปลอม ปนเปื้อน ข้อมูลแหล่งกำเนิด (provenance) และสามารถติดตามการเปลี่ยนมือ (traceable) ได้ตลอด supply chain จึงมีส่วนช่วยบรรเทาปัญหาที่เกิดขึ้นไม่เพียงเฉพาะในอุตสาหกรรมยา แต่รวมถึงผลิตภัณฑ์อื่น ๆ ที่มักมีการปลอมหรือปนเปื้อน เช่น ไวน์ กาแฟ ข้าว และผลิตภัณฑ์ที่มีข้อบ่งชี้ทางภูมิศาสตร์ เป็นต้น

นอกเหนือจากเพชรหรืออัญมณีแล้ว ยังมีสินค้าหลายอย่างที่เริ่มใช้บล็อกเชนเพื่อสร้างความมั่นใจให้กับลูกค้าโดยการบันทึกข้อมูลแหล่งกำเนิดและติดตามการเปลี่ยนมือตลอดวงจรชีวิตของสินค้า เช่น ยารักษาโรค วัคซีน กาแฟ ไวน์ งานฝีมือ ผลิตภัณฑ์ที่มีสิ่งบ่งชี้ทางภูมิศาสตร์ สินค้าฟุ่มเฟือย โดยผู้มีส่วนได้ส่วนเสีย มีแอดเดรสของตัวเองในการบันทึกข้อมูลผ่านสัญญาอัจฉริยะ

บริษัท PwC คาดการณ์ว่าในช่วงปี ค.ศ. 2020 – 2030 Supply Chain จะเป็นแอปพลิเคชันบนบล็อกเชนที่สร้างมูลค่าและสร้างงานได้สูงสุดเมื่อเทียบกับแอปพลิเคชันอื่น ๆ [56]

ภาพที่ 6 Supply Chain ของไวน์

ตัวอย่าง supply chain ของไวน์ในประเทศออสเตรเลียซึ่งมีแผนจะใช้บล็อกเชนในการบันทึกแหล่งกำเนิดตั้งแต่ไร่องุ่น โรงผลิตไวน์ โรงบรรจุ ร้านค้า ผู้บริโภค ไปจนถึงผู้ตรวจสอบของรัฐ การใช้บล็อกเชนช่วยให้แลกเปลี่ยนข้อมูลทำได้ง่าย มีความน่าเชื่อถือ ตรวจสอบแหล่งที่มาได้ตั้งแต่แหล่งกำเนิด ซึ่งช่วยลดความเสียหายจากการปลอมแปลงหรือปนเปื้อนสินค้าได้ [57]

ธุรกรรมในการค้าระหว่างประเทศเกี่ยวข้องกับการจัดการเอกสารจำนวนมาก ทั้งเอกสารที่เกี่ยวกับการซื้อขาย การเงิน การขนส่ง และระเบียบปฏิบัติในการนำเข้าและส่งออก เอกสารแต่ละฉบับมีขั้นตอนตรวจสอบหลายขั้นตอนในการขออนุญาต เกี่ยวข้องกับการประสานงานระหว่างกันจำนวนมาก ส่งผลถึงค่าใช้จ่ายในการดำเนินงาน และค่าธรรมเนียมต่าง ๆ ปริมาณเอกสารและความซับซ้อนในการทำธุรกรรมในการค้าระหว่างประเทศ ทำให้เกิดแนวคิดในการประยุกต์ใช้ระบบสารสนเทศสร้างแพลตฟอร์มสำหรับทำธุรกรรมการค้าระหว่างประเทศ และเกิดแนวคิดในการใช้บล็อกเชนเข้ามาแก้ปัญหาการจัดการเอกสาร ตัวอย่างเช่นระบบของ NTT DATA ที่ทดลองนำร่องใช้งานระหว่างประเทศญี่ปุ่นและประเทศไทย

Blockchain-based Trade Platform ของ NTT DATA อาศัยประโยชน์จากระบบบล็อกเชนที่เป็น decentralized ในการให้ความสำคัญผู้มีส่วนได้ส่วนเสียอย่างเสมอภาค และอาศัยคุณสมบัติของ distributed ledger ในการบันทึกข้อมูลในการตรวจสอบแต่ละขั้นตอนให้มีความถูกต้องตรงกันเสมอ มีความน่าเชื่อถือ ตรวจสอบได้ ป้องกันการปลอมแปลง

NTT DATA นำร่องทดสอบการใช้งาน Blockchain-based Trade Platform โดยเชื่อมโยงเอกสารต่าง ๆ ที่เกี่ยวข้องในการซื้อขาย การเงิน การส่งออกและนำเข้า การขนส่ง และกระบวนการศุลกากรระหว่าง Nippon Automated Cargo And Port Consolidated System (NACCS) ซึ่งเป็น National Single Window ของประเทศญี่ปุ่น กับ National Single Window ของประเทศไทย ซึ่งพบว่าระบบที่เป็นบล็อกเชนช่วยลดเวลาในการจัดทำและตรวจสอบยืนยันเอกสารในการขนส่ง การเงิน ประกันภัย ใบตราส่งสินค้า (Seaway bill, Bill of lading) ได้ไม่น้อยกว่า 30% และมีหลายธุรกรรมที่ลดเวลาได้มากกว่า 60% และมีแผนในการขยายผลสู่ประเทศอื่น ๆ ในอนาคต

3.2 เอกสารรับรอง

ทุกวันนี้ เรามีการใช้งานเอกสารรับรองอยู่เป็นจำนวนมากทั้งในรูปแบบที่เป็นกระดาษหรือบัตรพลาสติก เช่น บัตรประจำตัวประชาชน บัตรพนักงาน ใบขับขี่ ใบรับรองทางการศึกษา ใบอนุญาตสิทธิ หนังสือค้ำประกัน หนังสือมอบอำนาจ เอกสารรับรองโดยทนาย (notarized documents)

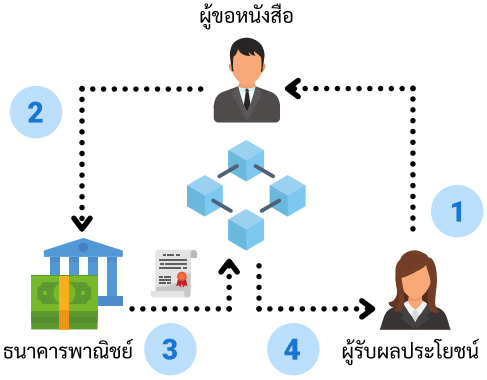
เอกสารรับรองเหล่านี้ มีข้อจำกัดในการตรวจสอบความถูกต้องสมบูรณ์อย่างมาก เพราะสิ่งที่ปรากฏบนเอกสารไม่สามารถนำมาใช้ยืนยันตัวเอกสารเองได้ ผู้รับเอกสารจำเป็นต้องตรวจสอบกลับไปที่ผู้ออกเอกสาร ซึ่งเป็นคอขวดในกระบวนการอัตโนมัติ

ตัวอย่างเช่น การขอหนังสือค้ำประกัน ผู้ขอหนังสือค้ำประกันจำเป็นต้องแสดงตนต่อสถาบันการเงินเพื่อพิสูจน์และยืนยันตัวตนก่อน สถาบันการเงินจึงจะสามารถออก

หนังสือค้ำประกันให้นำไปแสดงกับผู้รับผลประโยชน์ (beneficiary) ซึ่งมักจะต้องนำหนังสือค้ำประกันตรวจสอบกลับไปที่สถาบันการเงินที่เป็นผู้ออกเอกสารยืนยันอีกครั้งว่าเป็นเอกสารที่ถูกต้องสมบูรณ์

ปัญหาอุปสรรคนี้เป็นที่มาของโครงการ e-LG [58] โดยธนาคารพาณิชย์ในประเทศไทย 6 แห่งที่ร่วมมือกันพัฒนาระบบบริหารจัดการหนังสือค้ำประกันโดยใช้เทคโนโลยีบล็อกเชน ผู้ขอหนังสือค้ำประกันยืนยันตนโดยกุญแจส่วนตัวหรือรหัสผ่านโดยไม่ต้องแสดงตนที่สถาบันการเงิน สถาบันการเงินออกหนังสือค้ำประกันโดยระบุผู้รับผลประโยชน์บันทึกลงบล็อกเชนผู้รับผลประโยชน์สามารถตรวจสอบยืนยันความถูกต้องของหนังสือค้ำประกันได้อัตโนมัติจากข้อมูลที่บันทึกในบล็อกเชนได้โดยตรง

ภาพที่ 7 ภาพรวมการทำงานของ e-LG



ระบบการออกหนังสือค้ำประกัน e-LG เริ่มต้นเมื่อ ผู้รับผลประโยชน์เรียกหลักประกัน (1) ผู้ขอหนังสือสามารถขอให้ธนาคารพาณิชย์ในเครือข่าย e-LG ออกหนังสือค้ำประกันให้ (2) โดยบันทึกการออกหนังสือค้ำประกันในบล็อกเชน (3) เมื่อบันทึกในบล็อกเชนแล้วผู้รับผลประโยชน์สามารถตรวจสอบหลักประกันได้จากบล็อกเชน (4) [58]

e-LG บริหารจัดการองค์กรในรูปแบบบริษัทในชื่อ BCI (Thailand) ก่อตั้งโดยการร่วมทุนของ ธนาคารกรุงศรีอยุธยา, ธนาคารกรุงเทพ, ธนาคารกสิกรไทย, ธนาคารกรุงไทย, ธนาคารไทยพาณิชย์ และธนาคารทหารไทย โดยมีธนาคารแห่งประเทศไทยกำกับดูแลและมีกรมบัญชีกลางเป็นหนึ่งในผู้รับผลประโยชน์ของหนังสือค้ำประกัน

e-LG พัฒนาโดยบริษัท IBM โดยใช้ IBM Blockchain Platform ที่พัฒนาจาก Hyperledger Fabric เพื่อให้บริการเชิงพาณิชย์ บล็อกเชนของ e-LG จึงเป็น private และ permissioned ที่เข้าถึงได้เฉพาะสมาชิก แต่ละโหนดดูแลโดยธนาคารที่เป็นสมาชิกโดยโหนดทำงานได้ทั้ง on cloud หรือ on premise

e-LG เริ่มให้บริการมาตั้งแต่เดือนมิถุนายน ปี ค.ศ. 2019 จนถึงปัจจุบัน ระบบ e-LG มีสมาชิกเครือข่ายเป็นธนาคาร 22 แห่งและองค์กรธุรกิจที่เป็นผู้รับผลประโยชน์อีก 15 แห่ง ออกหนังสือค้ำประกันเป็นข้อมูลอิเล็กทรอนิกส์บนบล็อกเชนไปแล้วมูลค่ากว่า 9,500 ล้านบาท ลดเวลาในการออกและตรวจสอบหนังสือค้ำประกันจากเดิม 3 ถึง 7 วัน ลงเหลือไม่ถึง 1 วัน และไม่มีการผลิตเอกสารที่เป็นกระดาษเลย

ปัจจุบัน การประยุกต์ใช้บล็อกเชนในการจัดการเอกสารรับรองสามารถดำเนินการได้ตามมาตรฐาน Verifiable Credentials (VCs) [59] ของ W3C ซึ่งเป็นมาตรฐานที่สร้างขึ้นเพื่อออกเอกสารรับรองในรูปแบบข้อมูลอิเล็กทรอนิกส์ที่มีการลงลายมือชื่อดิจิทัล จึงตรวจสอบยืนยันความถูกต้องของข้อมูลโดยวิธีการดิจิทัลได้อย่างน่าเชื่อถือมากกว่าวิธีการตรวจสอบเอกสารรับรองที่เป็นกระดาษหรือบัตรพลาสติก

Verifiable Credentials ยังสามารถทำงานร่วมกับ Decentralized Identifiers (DID) [60] เพื่อสร้าง identifier สำหรับปกปิดหรือเปิดเผยข้อมูลเฉพาะที่จำเป็นในการตรวจสอบแต่ละครั้ง ผู้ใช้จึงเป็นศูนย์กลางการบริหารจัดการข้อมูลของตัวเอง (Self-

Sovereign Identity) ซึ่งเป็นข้อดีที่เหนือกว่าเอกสารรับรองที่เป็นกระดาษ หรือ digitally signed PDF ที่ผู้ใช้ไม่สามารถเลือกเปิดเผยหรือปกปิดข้อมูลที่ปรากฏในเอกสารได้

ตัวอย่างการประยุกต์ใช้ VC ปรากฏในโครงการ OpenCert [61] ภายใต้ Smart Nation Initiative [62] ของรัฐบาลสิงคโปร์ OpenCert เป็นแพลตฟอร์มในการออกและตรวจสอบใบรับรองทางการศึกษาเป็นข้อมูลดิจิทัลโดยเฉพาะ หน่วยงาน หรือองค์กรอื่น ๆ สามารถตรวจสอบยืนยันใบรับรองทางการศึกษาผ่านหน้าเว็บ OpenCert และมั่นใจได้ว่าเป็นข้อมูลที่ถูกต้องสมบูรณ์จริงโดยไม่ต้องส่งกลับมาตรวจสอบที่สถาบันการศึกษาที่ออกใบรับรอง

ปัจจุบันมหาวิทยาลัยในสิงคโปร์ 16 แห่งใช้งาน OpenCert ในการออกใบรับรองทางการศึกษาแล้ว ซอฟต์แวร์ที่โครงการ OpenCert ใช้เป็นฐานในการสร้างแพลตฟอร์มคือ OpenAttestation ซึ่งเป็นชุดซอฟต์แวร์โอเพนซอร์สและสัญญาอัจฉริยะในการทำ document notarization ด้วย Verifiable Credentials และ Decentralized Identity ที่ทำงานบนบล็อกเชนแบบอีเธอเรียม OpenAttestation สามารถประยุกต์ใช้กับเอกสารรับรองอื่น ๆ ได้ทุกประเภท เช่น หนังสือเดินทาง บัตรประชาชน ใบขับขี่ หนังสือรับรองคุณวุฒิ ใบอนุญาตประกอบวิชาชีพ ใบรับรองการรับวัคซีน ใบเสร็จรับเงิน ใบตราส่งสินค้า หรือแม้แต่ voucher ต่าง ๆ เช่น ตัวอย่างการใช้งานระบบ voucher ลดราคาเรียกว่า Stadjerspas ในเมือง Groningen ประเทศเนเธอร์แลนด์

Stadjerspas เป็น voucher แจกให้มีรายได้น้อยเพื่อนำไปใช้ลดค่าบริการต่าง ๆ ในเมือง เช่น โรงภาพยนตร์ สนามกีฬา สโมสรกีฬา Stadjerspas เริ่มให้บริการในปี ค.ศ. 1994 เป็นระบบกระดาษ จนถึงปี ค.ศ. 2013 ซึ่งพบปัญหาในการใช้งานผิดวัตถุประสงค์ ไม่ตรงตามเงื่อนไข ไม่ตรงกับกลุ่มเป้าหมายทั้งผู้รับผลประโยชน์ (beneficiaries) และผู้ให้บริการ ในปี ค.ศ. 2016 เมือง Groningen เปลี่ยนมาใช้บล็อกเชนในการควบคุมและสัญญาอัจฉริยะในการควบคุมการใช้ Stadjerspas แทน

ผู้รับผลประโยชน์สมัครใช้งาน Stadjerspas ได้ที่สำนักงานของเมือง Groningen ซึ่งจะตรวจสอบสิทธิจากข้อมูลที่เชื่อมกับเลขประจำตัวประชาชน (เช่นเขตที่อยู่อาศัย รายได้ จำนวนบุตร) และออก identifiers ในระบบ Stadjerspas เชื่อมกับข้อมูลส่วนบุคคลที่เก็บไว้นอกบล็อกเชน ผู้รับผลประโยชน์เก็บ identifier ใน mobile app แทนการใช้กระดาษ mobile app นี้ใช้แสดง QR code ที่สร้างจาก identifier เพื่อรับสิทธิส่วนลดต่าง ๆ จากผู้ให้บริการในเมือง ผู้ให้บริการสแกน QR code ที่ปรากฏ เพื่อตรวจสอบเงื่อนไขการได้รับสิทธิโดยสัญญาอัจฉริยะของ voucher ในบล็อกเชน และบันทึกการได้รับสิทธิจากผู้ให้บริการลงในบล็อกเชน

ระบบ Stadjerspas พัฒนาโดยบริษัท DutchChain ใช้ zCash ซึ่งเป็นบล็อกเชนที่ดัดแปลงจากซอร์สโค้ดของบิตคอยน์โดยเพิ่มความสามารถในการทำ selective disclosure ที่ผู้ใช้สามารถควบคุมการเปิดเผยข้อมูลธุรกรรมใน zCoin ซึ่งเป็นประโยชน์ต่อการตรวจสอบการเคลื่อนไหวของธุรกรรมตามเงื่อนไขของ AML/CTF หรือตามเงื่อนไขของการเก็บภาษี

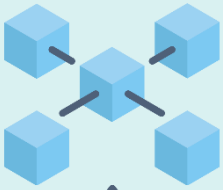
ระบบ Stadjerspas บนบล็อกเชนช่วยให้เมือง Groningen จัดสรรงบประมาณเพื่อช่วยเหลือผู้มีรายได้น้อยได้มีประสิทธิภาพมากขึ้นเนื่องจากสัญญาอัจฉริยะควบคุมให้การใช้ประโยชน์เป็นไปตามที่เมืองและผู้ให้บริการกำหนดไว้อย่างถูกต้องแม่นยำมากขึ้น ปลอดภัยจากการปลอมแปลง voucher และยังเป็นระบบอัตโนมัติที่ควบคุมโดยสัญญาอัจฉริยะ เมืองสามารถจ่ายคืนส่วนลดให้กับผู้ให้บริการอัตโนมัติ ทุกธุรกรรมสามารถตรวจสอบได้จากข้อมูลบนบล็อกเชน ธุรกรรมจึงมีความโปร่งใสมากกว่าระบบกระดาษ ซึ่งมีประโยชน์มากสำหรับการตรวจสอบการใช้จ่ายภาครัฐ

BLOCKCHAIN IN

CERTIFICATION ~ ACADEMIC RECORDS

2 ใบรับรองผลการศึกษาในแต่ละภาคการศึกษา รวมเป็นข้อมูลชุดเดียว บันทึกเป็นแฮช (e.g. Merkle root) ในบล็อกเชน

addc551d...011d7c95



1 สถาบันการศึกษาออกใบรับรองผลการศึกษาแบบดิจิทัล ลงลายมือชื่อดิจิทัลโดยสถาบันฯ ส่งให้กับนักศึกษาเก็บในวอลเล็ตส่วนตัว

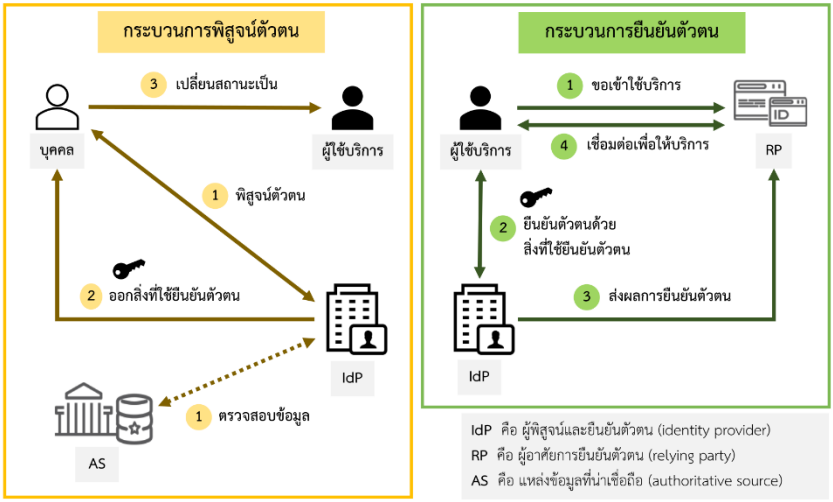
4 HR ของบริษัทยืนยันกับข้อมูลในบล็อกเชนว่าเป็นใบรับรองตัวจริงจากลายมือชื่อดิจิทัลของสถาบัน และผู้ถือใบรับรองเป็นนักศึกษาตัวจริงจากลายมือชื่อดิจิทัลของนักศึกษา

3 เมื่อต้องใช้ใบรับรองผลการศึกษา เช่น การสมัครงาน นักศึกษาใช้วอลเล็ตลงลายมือชื่อดิจิทัลกำกับบนใบรับรองฯ ส่งให้กับบริษัท

ใบรับรองทางการศึกษาที่เป็นกระดาษปลอมแปลงได้ง่ายแต่ตรวจสอบได้ยาก ทำให้ผู้ที่ได้รับจำเป็นต้องส่งตรวจสอบกับสถาบันการศึกษาที่เป็นผู้ออกใบรับรอง ใบรับรองดิจิทัลตรวจพบการแก้ไขปลอมแปลงได้ง่ายกว่ากระดาษมาก บล็อกเชนยังสนับสนุนให้การตรวจสอบใบรับรองดิจิทัลทำได้โดยตรงด้วยการโต้ตอบกับสัญญาอัจฉริยะบนบล็อกเชน มีความน่าเชื่อถือสูง และสามารถรองรับ Self-Sovereign Identity (SSI) ซึ่งทำให้เจ้าของข้อมูล เลือกเปิดเผยข้อมูลเฉพาะที่จำเป็นในการตรวจพิสูจน์เฉพาะรายเฉพาะคราวได้ จึงรักษาความเป็นส่วนตัวให้กับผู้ใช้งานได้ดีกว่า

3.3 ดิจิทัลไอดี

สภาพนิรนามของผู้ใช้เป็นคุณสมบัติอย่างหนึ่งที่เป็นจุดเด่นของบล็อกเชน โดยเฉพาะในบล็อกเชนสาธารณะที่การทำธุรกรรมไม่จำเป็นต้องรู้ตัวตนกัน แต่ธุรกรรมบางประเภทจำเป็นต้องรู้ตัวตนผู้ที่ทำธุรกรรมระหว่างกันเพื่อลดปัญหาอาชญากรรมที่อาจจะเกิดขึ้น การพิสูจน์ตัวตน (identity proofing, know your customer) และการยืนยันตัวตน (authentication) จึงเป็นเรื่องที่จำเป็นสำหรับธุรกรรมลักษณะนี้



ภาพที่ 8
ตัวอย่างระบบการจัดการดิจิทัลไอดี

ในโมเดลระบบการจัดการดิจิทัลไอดีตามข้อเสนอแนะมาตรฐานฯ ว่าด้วยการใช้ดิจิทัลไอดีสำหรับประเทศไทย [63] บุคคลสามารถสมัครใช้ดิจิทัลไอดีกับผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP) โดย IdP อาจตรวจสอบหลักฐานแสดงตนและข้อมูลเกี่ยวกับอัตลักษณ์ของบุคคลกับแหล่งข้อมูลที่น่าเชื่อถือ (Authoritative Source: AS) บุคคลที่ผ่านการพิสูจน์ตัวตนแล้วจะเปลี่ยนสถานะเป็นผู้ใช้บริการและสามารถใช้สิ่งยืนยันตัวตนในการยืนยันตัวตนเพื่อเข้าใช้บริการจากผู้อาศัยการยืนยันตัวตน (Relying Party: RP) ได้

สำหรับประเทศไทย แนวทางในการพิสูจน์และยืนยันตัวตนทางดิจิทัลกำหนดอยู่ในข้อเสนอแนะมาตรฐานฯ ว่าด้วยแนวทางการใช้ดิจิทัลไอดีสำหรับประเทศไทยของสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ [63] และมีตัวอย่างการนำข้อเสนอแนะฯ มาใช้

จัดการการพิสูจน์และยืนยันตัวตนทางดิจิทัลของ IdP ที่ให้บริการผ่านโครงการ National Digital ID (NDID) [64]

NDID เป็นแพลตฟอร์มในการเชื่อมโยง ผู้ใช้บริการ ผู้พิสูจน์และยืนยันตัวตน (Identity Provider: IdP) และผู้อาศัยการยืนยันตัวตน (Relying Party: RP) ช่วยให้ผู้ใช้บริการที่เคยพิสูจน์ตัวตนกับ IdP มาก่อนแล้ว สามารถยืนยันตัวตนเพื่อทำธุรกรรมกับ RP ต่าง ๆ ได้โดยไม่ต้องพิสูจน์ตัวตนใหม่ทุกครั้ง ผู้ใช้บริการจึงสามารถทำธุรกรรมออนไลน์ได้สะดวกขึ้น ผู้ให้บริการสามารถเชื่อมั่นได้ว่าผู้ใช้บริการมีตัวตนอยู่และเป็นตัวจริง มีความน่าเชื่อถือสูงพอจะทำธุรกรรมทางการเงินที่เดิมจำเป็นต้องทำ ณ ที่ทำการของสถาบันการเงินได้ เช่น การเปิดบัญชีธนาคารแห่งใหม่ผ่านระบบออนไลน์ โดยพิสูจน์และยืนยันตัวตนจากธนาคารที่เคยมีบัญชีเงินฝาก

บล็อกเชนของ NDID จะทำหน้าที่เชื่อมโยงและเก็บบันทึกธุรกรรมในการยืนยันตัวตนที่เกิดขึ้นระหว่าง RP และ IdP ใน ledger เป็นหลักฐานที่ใช้ในการพิสูจน์ว่าธุรกรรมในการยืนยันตัวตนระหว่าง RP และ IdP เกิดขึ้นจริง

NDID ใช้ Tendermint ในการสร้างเครือข่ายบล็อกเชน ใช้ consensus แบบ Proof of Stake สัญญาอัจฉริยะเขียนผ่าน Application BlockChain Interface (ABCI) ของ Tendermint

ข้อมูลที่บันทึกใน ledger ของ NDID เป็นเพียง log การยืนยันตัวตนระหว่าง RP กับ IdP ที่เกิดขึ้นเท่านั้น ไม่มีข้อมูลส่วนตัวของผู้ใช้งาน

ในต่างประเทศมีการนำร่องใช้งานดิจิทัลไอดีในเมือง Zug ประเทศสวิตเซอร์แลนด์ โดยใช้แพลตฟอร์มของ uPort เมื่อปลายปี 2017 ผู้ที่ลงทะเบียนและผ่านการพิสูจน์ตัวตนโดยรัฐแล้วจะสามารถใช้ uPort mobile app ในการยืนยันตนเพื่อทำธุรกรรมภาครัฐต่าง ๆ ได้ เช่น ยื่นภาษีออนไลน์ เลือกตั้งโดนวิธีอิเล็กทรอนิกส์ เช่าจักรยาน ชำระค่าจอดรถ

ยืมหนังสือห้องสมุด เป็นต้น ประชาชนจึงได้รับความสะดวกสบายมากขึ้นในการทำธุรกรรมต่าง ๆ และรักษาความเป็นส่วนตัวได้ดีกว่าการใช้บัตรประจำตัว

uPort ทำงานบนบล็อกเชนสาธารณะ ธุรกรรมทั้งหมดดำเนินการโดยวิธีการทางอิเล็กทรอนิกส์ บันทึกบนบล็อกเชนซึ่งแก้ไขเปลี่ยนแปลงภายหลังไม่ได้ ช่วยให้ลดค่าใช้จ่ายในการบริหารจัดการการจัดเก็บข้อมูลส่วนบุคคล และลดความเสี่ยงที่ฐานข้อมูลกลางจะถูกโจมตีได้

3.4 Central Bank Digital Currency

คริปโทเคอร์เรนซีได้แสดงให้เห็นศักยภาพของบล็อกเชนในการเป็นระบบชำระเงินที่อาจทดแทนการใช้เงินสดได้ ธนาคารกลางทั่วโลกกว่า 60 ประเทศจึงหันมาสนใจศึกษาการใช้บล็อกเชนเพื่อเพิ่มประสิทธิภาพและลดภาระในการกำกับดูแลระบบสารสนเทศที่เกี่ยวกับการชำระเงินทั้งภายในประเทศและระหว่างประเทศ การใช้โทเคนดิจิทัลเป็นสกุลเงินอาจช่วยลดต้นทุนในการบริหารจัดการการผลิต ทำลาย หมุนเวียนเหรียญและธนบัตรในระบบการชำระเงิน และลดความเสี่ยงการปลอมแปลงธนบัตร โทเคนดิจิทัลที่เป็นสกุลเงินบริหารจัดการโดยธนาคารกลางของประเทศ เรียกว่า Central Bank Digital Currency (CBDC)

การที่ CBDC บริหารจัดการโดยธนาคารกลางของประเทศ ทำให้ CBDC สามารถเป็นรูปแบบชำระหนี้ได้ตามกฎหมายเหมือนเหรียญหรือธนบัตร ทั้งนี้ CBDC อาจแบ่งได้เป็นสองประเภท ได้แก่ wholesale CBDC เป็นการรองรับธุรกรรมทางการเงินระหว่างสถาบันการเงิน และ retail CBCD สำหรับรองรับธุรกรรมรายย่อยของภาคธุรกิจและประชาชน

3.4.1 Project Inthanon

ประเทศไทยถือเป็นประเทศที่มีความก้าวหน้าในการพัฒนา wholesale CBDC มากที่สุดประเทศหนึ่งของโลกจากโครงการอินทนนท์ (Project Inthanon) [65]

โครงการอินทนนท์ดำเนินการโดยธนาคารแห่งประเทศไทย เป็นโครงการนำร่อง wholesale CBDC ใช้บล็อกเชนเป็นโครงสร้างพื้นฐานในการจัดการโทเคนดิจิทัลเพื่อทำ Real-Time Gross Settlement (RTGS) และ Atomic Delivery-versus-Payment ข้ามธนาคาร โดยร่วมมือกับธนาคารพาณิชย์ 8 แห่ง

ผลสำเร็จของโครงการอินทนนท์ทำให้ธนาคารแห่งประเทศไทยต่อยอดธุรกรรมชำระเงินระหว่างประเทศผ่านเทคโนโลยีบล็อกเชน โดยร่วมมือกับ Hong Kong Monetary Authority (HKMA) ใน Project Inthanon-LionRock [66] ซึ่งสามารถทำธุรกรรม real-time atomic Payment-versus-Payment (PvP) จากบัญชีเงินฝากระหว่างธนาคารพาณิชย์ในไทยกับฮ่องกงได้ทั้งสกุลเงินบาทหรือดอลลาร์ฮ่องกง ความก้าวหน้าของ Project Inthanon-LionRock ทำให้ PwC จัดอันดับให้ประเทศไทยและฮ่องกงเป็นสองประเทศที่มีความก้าวหน้าในการทำ wholesale CBDC มากที่สุดในโลก [67]

โครงการระยะที่ 2 ของ Project Inthanon-LionRock ขยายความร่วมมือกับธนาคารกลางของสหรัฐอาหรับเอมิเรตส์ (Central Bank of the United Arab Emirates: CBUAE) และธนาคารประชาชนจีน (People's Bank of China: PBC) และเปลี่ยนชื่อโครงการเป็น m-CBDC โดยยังคงวัตถุประสงค์ในการนำศักยภาพของ Distributed Ledger Technology มาใช้ในการทำธุรกรรมโอนเงินระหว่างประเทศที่ครอบคลุมหลายสกุลเงินและทำได้ตลอด 24 ชั่วโมง พร้อมทั้งช่วยลดต้นทุนการโอนเงินระหว่างประเทศ [68]

3.4.2 Project Stella

ธนาคารกลางยุโรป (European Central Bank: ECB) ได้ทำงานร่วมกับธนาคารแห่งประเทศญี่ปุ่น (Bank of Japan) ภายใต้ Project Stella โดยมีเป้าหมายในการศึกษาความเป็นไปได้ในการประยุกต์ใช้ Distributed Ledger Technology เป็นโครงสร้างพื้นฐานของตลาดเงิน โดยโครงการระยะที่ 1 เป็นการศึกษา Large-value Payments Processing [69], ในระยะที่ 2 เป็นการศึกษา Securities Delivery-versus-Payment [70], ในระยะที่ 3 เป็นการศึกษา Cross-border Payments [71] และปัจจุบัน Project Stella ดำเนินการอยู่ใน

ระยะที่ 4 ซึ่งเป็นการศึกษา Balancing Confidentiality and Auditability ใน Distributed Ledger Technology [72]

นอกจาก Project Stella แล้ว ธนาคารกลางยุโรปได้ทำการศึกษา retail CBDC หรือ Digital Euro และเผยแพร่ผลการศึกษาเมื่อตุลาคม 2020 [73] โดยเป้าหมายในการศึกษาอยู่ภายใต้แนวคิดในการออก Digital Euro โดยธนาคารกลาง มีสภาพเป็นสกุลเงินยูโรในรูปแบบดิจิทัลที่ชำระหนี้ได้ตามกฎหมาย ประชาชนและภาคธุรกิจสามารถนำไปใช้จ่ายได้ ทั้งในรูปแบบเดียวกับการใช้เงินสดและเงินฝากผ่านธนาคารกลาง (Wholesale Central Bank Deposits)

การศึกษาได้จำกัดขอบเขตการใช้ Digital Euro ในลักษณะที่เป็นทางเลือกเสริมการใช้จ่ายด้วยเงินสดที่มีอยู่ ไม่ได้เป็นการแทนที่ธนบัตรหรือเหรียญเงินยูโรที่มีอยู่แล้ว และไม่ใช่การผลิตเงินอีกสกุลหนึ่งเข้าสู่ระบบการชำระเงินขนานกับเงินยูโร ผลการศึกษาได้รายงานถึงศักยภาพของ Digital Euro ด้านประสิทธิภาพและความปลอดภัย เงื่อนไขที่จำเป็นต่อการออกแบบ สิ่งที่ควรคำนึงถึงในทางกฎหมาย ฟังก์ชั่นการใช้งานของ Digital Euro แนวทางทางด้านเทคนิคและองค์กรที่เกี่ยวข้องกับการให้บริการ Digital Euro และได้เสนอแนะ ให้หน่วยงานด้านการเงินในเขตยุโรป (Eurosystem) ซึ่งประกอบด้วยธนาคารกลางยุโรปและธนาคารกลางของประเทศสมาชิกสหภาพยุโรปเริ่มโครงการ Digital Euro ช่วงกลางปี 2021 โดยมีเป้าหมายหลักในการพัฒนาและตรวจสอบยืนยัน Minimum Viable Product (MVP) เพื่อเตรียมความพร้อมในการออก Digital Euro ในอนาคต

ธนาคารแห่งประเทศญี่ปุ่นให้ความสนใจในการพัฒนา retail CBDC เช่นเดียวกัน โดยมีแผนจะเริ่มต้นทำการทดสอบในช่วงต้นปี 2021 อย่างไรก็ตาม เงินสดหมุนเวียนในประเทศญี่ปุ่นยังมีอัตราค่อนข้างสูงเมื่อเทียบกับ GDP ของประเทศ และญี่ปุ่นมีเทคโนโลยีการชำระเงินที่ใช้งานกันอยู่ในปัจจุบันอีกหลายแบบ ธนาคารแห่งประเทศญี่ปุ่นจึงมีความเห็น retail CBDC อาจจะยังไม่ได้ใช้งานจริงในเร็ววันนี้

3.4.3 Digital RMB/e-CNY

ธนาคารประชาชนจีน (The People's Bank of China) ในฐานะธนาคารกลางของประเทศจีนเริ่มศึกษาสกุลเงินดิจิทัลมาตั้งแต่ปี ค.ศ. 2014 มีการจัดตั้ง Digital Currency Research Institute เป็นหน่วยงานภายใต้ธนาคารกลางของจีนในปี ค.ศ. 2017

สกุลเงินดิจิทัลของจีนเริ่มเป็นที่รู้จักในปี ค.ศ. 2019 ในชื่อโครงการ Digital Currency/Electronic Payment (DC/EP) เป็นโครงการที่มีเป้าหมายในการนำสกุลเงินดิจิทัลมาใช้หมุนเวียนเสริมและทดแทนเงินสด โดยประชาชนไม่จำเป็นต้องมีบัญชีธนาคารในการใช้จ่าย และไม่ต้องพึ่งพาแพลตฟอร์มการชำระเงินของเอกชนอย่าง AliPay หรือ WeChat Pay ทั้งนี้เชื่อว่าสกุลเงินดิจิทัลในโครงการ DC/EP จะช่วยลดปัญหาธนบัตรปลอม การฟอกเงิน และลดค่าใช้จ่ายในการบริหารจัดการธนบัตรและเหรียญได้

DC/EP ออกโทเคนที่รู้จักในชื่อ digital RMB หรือ e-CNY บนบล็อกเชนและสัญญาอัจฉริยะของธนาคารกลาง ใช้สินทรัพย์ของธนาคารกลางเป็นทุนสำรองในการตรึงมูลค่าโทเคนให้เท่ากับเงินสกุล RMB การกระจายโทเคน digital RMB สู่ประชาชนทำผ่านธนาคารพาณิชย์ของจีนเช่นเดียวกับการกระจายธนบัตรและเหรียญ ประชาชนจีนสามารถถือครอง digital RMB และใช้จ่ายผ่านเป็นโมบายแอปพลิเคชันที่เป็นวอลเล็ต digital RMB ซึ่งทำงานได้ทั้ง online และ offline

เดือนตุลาคม ค.ศ. 2020 รัฐบาลจีนเริ่มทดสอบใช้จ่าย digital RMB ในเมืองเซินเจิ้นโดยสุ่มแจกโทเคน 10 ล้าน RMB ให้กับผู้ลงทะเบียนร่วมทดสอบ 50,000 คน เพื่อเป็นการพัฒนาฟังก์ชันการทำงาน ประเมินเสถียรภาพและประสิทธิภาพของระบบ และความสามารถในการป้องกันการฟอกเงิน [74]

ธนาคารกลางมีแผนจะขยายไปถึง 28 เมืองใหญ่ และเตรียมทดสอบกับคนต่างชาติในช่วงการแข่งขันกีฬาโอลิมปิกฤดูหนาวที่จีนจะเป็นเจ้าภาพในปี ค.ศ. 2022

จนถึงเดือนเมษายน 2021 รัฐบาลจีนขยายการทดสอบ 10 เมืองใหญ่ มีผู้ทดสอบ 1.2 ล้านคนโดยแจกโทเคนไปแล้ว 160 ล้าน RMB [75]

3.4.4 Sand Dollar

โครงการ Sand Dollar [76] เป็นโครงการ CBDC ของธนาคารกลางของประเทศบาฮามาส (Central Bank of the Bahamas) เป็นโครงการที่มีจุดประสงค์หลักในการเพิ่มประสิทธิภาพในการบริหารจัดการระบบการเงินที่กระจายอยู่ตามหมู่เกาะต่าง ๆ ของประเทศ ลดค่าใช้จ่ายในการจัดการเงินสดและเช็คเงินสด

ภูมิประเทศที่เป็นหมู่เกาะกระจัดกระจายกว่า 700 เกาะของบาฮามาส ทำให้ค่าธรรมเนียมในการโอนเงินข้ามบัญชีของบาฮามาสค่อนข้างสูง ประกอบกับจำนวนสาขาของธนาคารลดลง ประชาชนไม่เห็นความจำเป็นในการมีบัญชีธนาคาร ทำให้ประชากรของบาฮามาสจำนวนมากไม่มีบัญชีธนาคาร การใช้จ่ายในประเทศบาฮามาสจึงพึ่งพาเงินสดและเช็คเงินสดเป็นส่วนใหญ่ เพราะสามารถทำธุรกรรมได้ทันที

ภูมิประเทศที่เป็นหมู่เกาะทำให้ธนาคารพาณิชย์และธนาคารกลางมีภาระในการขนส่งเงินสดและเช็คเงินสดสูง ส่งผลถึงต้นทุนในการบริหารจัดการเงินสดของประเทศสูงขึ้นไปด้วย การทำ retail CBDC จึงเป็นทางออกที่เหมาะสมในสภาพแวดล้อมของบาฮามาส

ธนาคารกลางของบาฮามาส ประกาศใช้ Sand Dollar เป็นสกุลเงินตั้งแต่วันที่ 31 ธันวาคม ค.ศ. 2020 [77] และมีการใช้งานเป็นเงินสดใช้จ่ายได้ทั่วประเทศ โครงการ Sand Dollar จึงนับเป็น retail CBDC ที่มีความก้าวหน้ามากที่สุดในปัจจุบัน [67]

Sand Dollar ในความหมายที่เป็นคำสามัญ หมายถึงสัตว์ทะเลไม่มีกระดูกสันหลัง จัดอยู่ในคลาสเดียวกับ เม่นทะเล ดาวทะเล และปลิงทะเล ลักษณะกลมแบนเหมือนเหรียญ ฝังตัวอยู่ใต้ทราย ภาษาไทยเรียกว่า เหรียญทะเล หรืออีแปะทะเล

3.5 เครือข่ายบล็อกเชนสาธารณะของประเทศ

เครือข่ายบล็อกเชนแบบ public มีข้อดีที่การทำงานเป็นการกระจายศูนย์กลางและกระจายอำนาจการประมวลผลโดยสมบูรณ์ ไม่มีผู้ใดควบคุมหรือมีอำนาจในการเปลี่ยนแปลงข้อมูลที่ได้รับการยืนยัน จึงสร้างความโปร่งใสให้กับข้อมูลได้ดี แต่ไม่สามารถควบคุมการเข้าถึงข้อมูลที่เป็นสาธารณะบนเครือข่ายได้ และค่าธรรมเนียมธุรกรรมผันผวนมาก

ข้อจำกัดนี้ทำให้หลายประเทศมีแนวคิดในการมีโครงสร้างพื้นฐานของตัวเองเพื่อส่งเสริมให้เกิดการพัฒนาเทคโนโลยีบล็อกเชนในประเทศ และใช้งานเป็นโครงสร้างพื้นฐานทั้งเพื่อเป็น regulatory sandbox และใช้งานจริงในระยะยาวทั้งภาครัฐและเอกชน โดยไม่จำเป็นต้องพึ่งพาเครือข่ายบล็อกเชนแบบ public กำหนดค่าธรรมเนียมได้ถูกและไม่ผันผวนตามราคาคริปโทเคอร์เรนซีในตลาด นักพัฒนาและผู้ใช้งานสามารถควบคุมค่าใช้จ่าย ยังคงความน่าเชื่อถือของข้อมูลและการประมวลผล และเป็นที่ยอมรับ

ตัวอย่างเครือข่ายบล็อกเชนของประเทศ เช่น

- Australian National Blockchain, DLT. co ของประเทศออสเตรเลีย [78]
- Regulatory Sandbox ของประเทศญี่ปุ่น [79]
- European Blockchain Services Infrastructure ของสหภาพยุโรป [80]
- Blockchain-based Service Network ของประเทศจีน [81]
- FabricSharp ของประเทศสิงคโปร์ [82]

3.5.1 European Blockchain Services Infrastructure เครือข่ายบล็อกเชนของสหภาพยุโรป

สหภาพยุโรปเป็นหนึ่งในตัวอย่างของกลุ่มประเทศที่ให้การสนับสนุนเทคโนโลยีบล็อกเชนอย่างเป็นรูปธรรมและมีการพัฒนาอย่างก้าวกระโดดภายในระยะเวลาเพียงไม่กี่ปีภายใต้ยุทธศาสตร์ด้านบล็อกเชนของสหภาพยุโรป

คณะกรรมาธิการยุโรปกำหนดยุทธศาสตร์ทางด้านบล็อกเชนของสหภาพยุโรปโดยมีองค์ประกอบสำคัญในการร่วมพัฒนาวิสัยทัศน์และกรอบความร่วมมือของประเทศสมาชิกผ่าน European Blockchain Partnership (EBP) ซึ่งประกอบด้วยประเทศสมาชิกทั้งหมดในสหภาพยุโรป 27 ประเทศ ประเทศนอร์เวย์ และประเทศลิกเตนสไตน์

ยุทธศาสตร์ด้านบล็อกเชนของสหภาพยุโรปมีการวางโครงสร้างพื้นฐานบล็อกเชนสำหรับการบริการภาครัฐ (European Blockchain Service Infrastructure: EBSI) ที่เข้าถึงได้ทั่วทั้งยุโรป EBSI ออกแบบด้วยสถาปัตยกรรมแบบเปิดโดยใช้ซอฟต์แวร์โอเพนซอร์สสนับสนุนความสามารถในการทำงานร่วมกัน (Interoperability) รวมถึงสนับสนุนให้ทำงานภายใต้มาตรฐานระดับนานาชาติต่าง ๆ เช่น ISO/TC 307, IEEE, ITU-T จึงมีความยืดหยุ่นในการนำไปใช้งานสูง

นอกเหนือจากสร้างโครงสร้างพื้นฐานแล้ว โครงการ EBSI รุ่นแรก (EBSI v1) ในช่วงปี ค.ศ. 2020 ได้พัฒนาต้นแบบของ self-sovereign Identity, document notarization, และ diploma management โดยใช้ verifiable credentials และ decentralized identifiers เป็นบริการที่ประชาชนสามารถเข้าถึงได้ และปี ค.ศ. 2021 EBSI v2 มีบริการเพิ่มเติมอีก 3 ระบบ ได้แก่ระบบบริหารจัดการการสนับสนุนการเงินให้โครงการ SME ในยุโรป, ระบบ European Social Security Identification Number (ESSIN) แบบดิจิทัลเพื่อป้องกันข้อผิดพลาดและการฉ้อโกง และระบบบริหารจัดการกระบวนการลี้ภัยซึ่งจำเป็นต้องมีความมั่นคงปลอดภัยในการแลกเปลี่ยนข้อมูลข้ามองค์กรและข้ามประเทศ

นอกจากนี้ คณะกรรมาธิการยุโรป ยังลงทุนให้การสนับสนุนการพัฒนาทักษะทางด้านบล็อกเชนและทักษะดิจิทัลอื่น ๆ ซึ่งถือเป็นหัวใจสำคัญที่จะทำให้ประชาชนในยุโรปมีทักษะดิจิทัลที่เพียงพอต่อการเข้าถึงเทคโนโลยีต่าง ๆ ไม่ว่าจะเป็นด้านเทคนิค ด้านธุรกิจ กฎหมาย และทักษะที่จำเป็นสำหรับการทำงานในองค์กร คณะกรรมาธิการยุโรปยังได้ทำงานและสร้างความร่วมมือกับภาคการศึกษา และภาคเอกชน ผ่านทาง 2 องค์กรหลัก ได้แก่ International Association for Trusted Blockchain Applications (INATBA) และ

European Union Blockchain Observatory and Forum แสดงถึงหลักคิดที่มีประชาชนเป็นศูนย์กลาง

โหนดของ EBSI ทำงานบนลินุกซ์ โดยภาพรวมประกอบด้วย layer ของ on-chain public ledgers และ off-chain distributed storage

on-chain public ledgers ใช้ Hyperledger Fabric และ Besu โดยมี consensus เป็น Proof of Authority (RAFT และ iBFT)

off-chain distributed storage ใช้ Cassandra เป็น distributed key-value database, MongoDB เป็น local key-value database, และ GlusterFS เป็น distributed file system

3.5.2 Blockchain-based Service Network ของประเทศจีน

Blockchain-based Service Network (BSN) เป็นโครงการที่ริเริ่มโดยรัฐบาลจีน มีจุดประสงค์หลักในการลดภาระค่าใช้จ่ายและการดูแลรักษาเครือข่ายบล็อกเชนขององค์กร โดยสร้างแพลตฟอร์มบล็อกเชนกลางที่นักพัฒนาสามารถใช้งานร่วมกัน ทำให้ค่าใช้จ่ายบน BSN ต่ำกว่าการบริหารจัดการโครงสร้างพื้นฐานโดยองค์กรเอง 30-80%

BSN บริหารจัดการโดย BSN Development Association ซึ่งประกอบด้วยองค์กรทั้งภาครัฐและเอกชน ได้แก่ State Information Center, China Mobile, China UnionPay, Red Date Technology

ปัจจุบัน BSN ให้บริการบล็อกเชนแบบ permissioned อาทิ Hyperledger Fabric, R3 Corda, ConsenSys Quorum, FISCO BCOS, Baidu XUPER, Rivtower, JD Digit และรองรับบล็อกเชนแบบ public/permissionless เช่น อีเธอเรียม, EOS, Tezos, Polkadot, NEAR และบล็อกเชนสาธารณะอื่น ๆ อีกมากกว่า 10 เครือข่าย มี Public City Node (PCN)

เป็นโครงสร้างพื้นฐานสำหรับบริการบล็อกเชนอยู่ทั่วประเทศจีนกว่า 120 เมือง และให้บริการผู้ใช้ทั้งภายในและนอกประเทศจีน

3.6 มาตรฐานและการแลกเปลี่ยนข้อมูล

การประยุกต์ใช้เทคโนโลยีบล็อกเชนสำหรับแต่ละภาคส่วนอาจมีความเฉพาะที่ทำให้ข้อมูลที่ต้องแลกเปลี่ยนกันระหว่าง DApp มาตรฐานและการแลกเปลี่ยนข้อมูลมีความจำเป็นโดยเฉพาะการประยุกต์ใช้กับภาคส่วนที่มีผลกระทบในวงกว้างในการแลกเปลี่ยนข้อมูล เช่น identity ของประชากร ข้อมูลสุขภาพ อินเทอร์เน็ตของสรรพสิ่ง ห่วงโซ่อุปทาน ซึ่งปัจจุบันยังไม่มีการกำหนดมาตรฐานและวิธีการแลกเปลี่ยนข้อมูลบนบล็อกเชน แต่เริ่มมีการศึกษาแล้ว ดังจะเห็นได้จากกลุ่มทำงานของ ISO, W3C และ IEEE เช่น

- ISO/TC 307 Blockchain and Distributed Ledger Technologies [83] เป็นกลุ่มทำงานของมาตรฐานที่เกี่ยวข้องกับบล็อกเชนและ Distributed Ledger Technologies ของ ISO กลุ่มทำงานนี้เผยแพร่มาตรฐานแล้ว 4 รายการ ประกอบด้วยศัพท์บัญญัติ ข้อพึงระวังเกี่ยวกับข้อมูลส่วนบุคคล สัญญาอัจฉริยะ และ ความมั่นคงปลอดภัยของระบบรับฝากสินทรัพย์ปัจจุบัน กลุ่มทำงาน TC 307 อยู่ระหว่างการพัฒนามาตรฐานอีก 11 รายการ
- W3C มีกลุ่มทำงานในการออกแบบโครงสร้างและการประมวลผลข้อมูลของ Verifiable Credentials ซึ่งเผยแพร่มาตรฐานแล้ว [59] และกลุ่ม Decentralized Identifiers [60] ที่เผยแพร่ร่างมาตรฐานของข้อมูลและกระบวนการในการทำ decentralized identifiers ที่ไม่จำเป็นต้องผูกกับระบบข้อมูลกลาง
- IEEE มีกลุ่มทำงานในการออกมาตรฐานในการนำบล็อกเชนไปประยุกต์ใช้กับระบบสารสนเทศต่าง ๆ เช่น อินเทอร์เน็ตของสรรพสิ่ง [84], การเกษตร [85], Connected and Autonomous Vehicles (CAVs) [86], พลังงาน [87], บริการสุขภาพ [88] และการเงินในห่วงโซ่อุปทาน [89]

การศึกษาเหล่านี้มีความก้าวหน้าเป็นลำดับ และคาดว่าจะเผยแพร่เป็นมาตรฐานได้ในอนาคตอันใกล้ ซึ่งจะส่งผลให้การประยุกต์ใช้บล็อกเชนกับเทคโนโลยีอื่นมีแบบแผนที่ชัดเจนขึ้น และมีโอกาสทำให้การแลกเปลี่ยนข้อมูลทำได้ง่ายขึ้น


{ }
HTML
</>

4 ใช้บล็อกเชนกันเลยดีไหม?

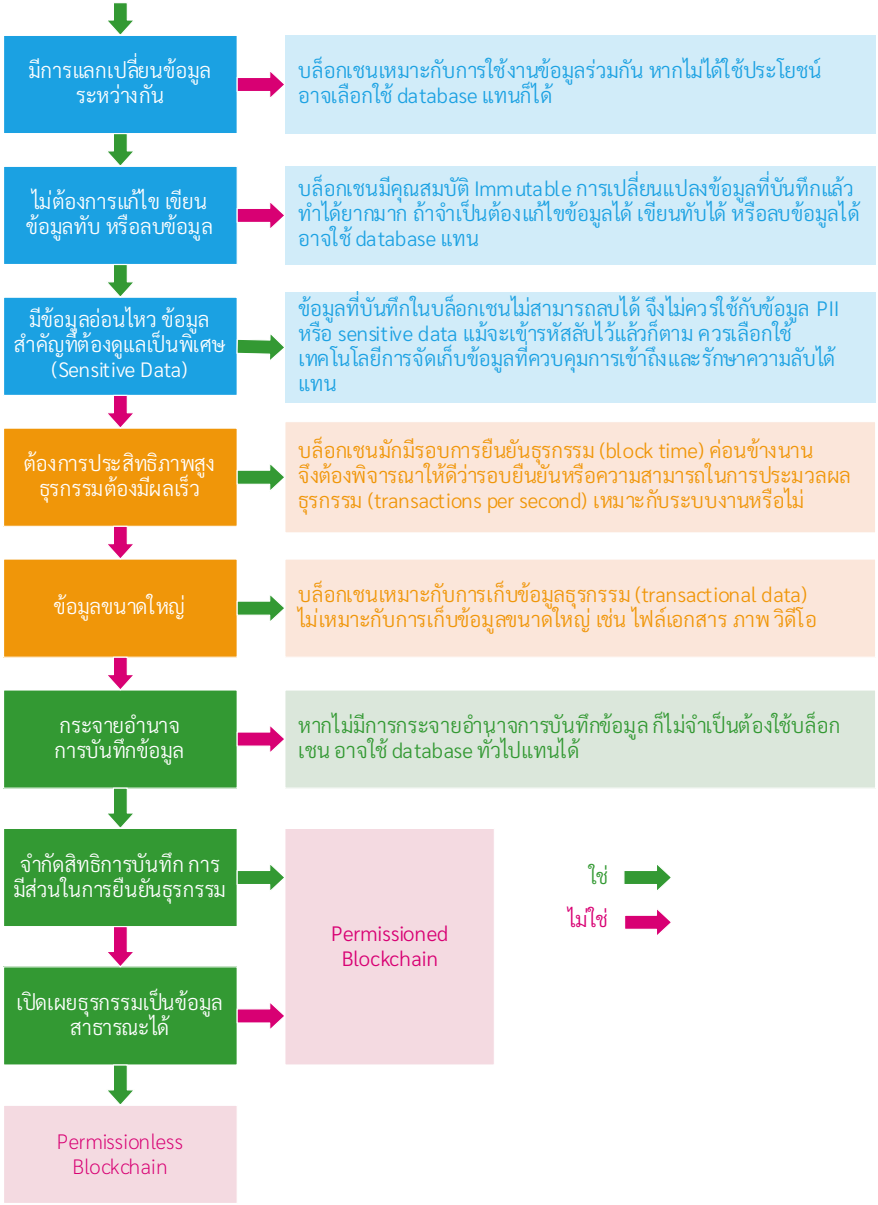
บล็อกเชนแสดงให้เห็นแล้วว่ามีคุณค่าในตัวเองที่ต่างไปจากระบบงานไอทีปกติทั่วไป อาทิ การป้องกันการปลอมแปลงสินค้า เอกสาร ผลงาน ที่ช่วยให้เราสามารถลดค่าใช้จ่ายในการบริหารจัดการความเสียหายที่เกิดขึ้นจากการปลอมแปลง ความสามารถในการติดตามการเปลี่ยนมือของโทเคนช่วยให้มั่นใจในแหล่งที่มาของสิ่งที่โทเคนแทนค่า การแลกเปลี่ยนข้อมูลกับองค์กรธุรกิจอื่นทำได้อย่างน่าเชื่อถือและช่วยลดขั้นตอนการตรวจสอบข้อมูลที่เกิดซ้ำซ้อน หรือจะเป็นสัญญาอัจฉริยะเองที่สามารถสร้างธุรกิจใหม่บนแพลตฟอร์มใหม่อย่าง DeFi หรือ DAO ดังที่จะได้แนะนำในบทที่ 6

บล็อกเชนอาจมอบคุณค่าเหล่านี้ให้กับระบบงานและธุรกิจของเราได้เช่นกัน

อย่างไรก็ตาม **บล็อกเชนไม่ได้เหมาะกับทุกระบบงานหรือทุกธุรกิจ ดังนั้นจึงต้องพิจารณาก่อนที่จะเลือกใช้บล็อกเชน** เช่นในภาพที่ 9 เป็นตัวอย่าง diagram ในการตัดสินใจเลือกใช้บล็อกเชน [90] [91] [92] [93]

กรณีที่ระบบงานต้องการกระจายอำนาจมาก ไม่จำกัดสิทธิในการเข้าถึง ไม่จำกัดสิทธิอ่าน-เขียน-โต้ตอบ กับสัญญาอัจฉริยะ ไม่จำกัดจำนวนโหนดในเครือข่าย และสามารถเปิดเผยข้อมูลเป็นสาธารณะได้ ก็เหมาะที่จะใช้บล็อกเชนแบบ permissionless ซึ่งอาจจะใช้บล็อกเชนสาธารณะที่สามารถเขียนสัญญาอัจฉริยะอย่างอีเธอเรียม หรือ BSC ได้ ทั้งนี้การจะเลือกใช้บล็อกเชนสาธารณะ ควรพิจารณาถึงค่าธรรมเนียมในการบันทึกสัญญาอัจฉริยะบนบล็อกเชน และค่าธรรมเนียมในการทำงานโต้ตอบกับสัญญาอัจฉริยะประกอบด้วย

ภาพที่ 9 ตัวอย่างการพิจารณาเลือกใช้บล็อกเชน



แต่ธุรกิจและระบบงานส่วนใหญ่ในปัจจุบัน มักมีเงื่อนไขในการเข้าถึง เช่น การจำกัดการทำธุรกรรมเฉพาะลูกค้า การแลกเปลี่ยนข้อมูลเฉพาะคู่ค้าหรือผู้มีส่วนได้ส่วนเสียด้วยกัน หรือกฎระเบียบที่จำเป็นต้องรักษาอำนาจในการทำธุรกรรมหรือบริหารจัดการ ระบบงานลักษณะนี้จะเหมาะกับบล็อกเชนแบบ permissioned เป็น private หรือ consortium ซึ่งมีทางเลือกของโพรโทคอลในการทำ consensus ที่หลากหลาย ขึ้นกับความไว้ใจ ความต้องการในการกระจายอำนาจ และความสามารถในการประมวลผลธุรกรรมที่ระบบงานต้องรองรับ

เมื่อได้โครงสร้างพื้นฐานบล็อกเชนที่เหมาะกับธุรกรรมแล้ว ก็จะสามารถเข้าสู่วงจรการพัฒนาซอฟต์แวร์ เป็นสัญญาอัจฉริยะที่ทำงานบนบล็อกเชน และอาจมีการตรวจสอบคุณภาพและความมั่นคงปลอดภัยของระบบงาน (audit) เช่นเดียวกับวงจรการพัฒนาซอฟต์แวร์ทั่วไป

4.1 ความโปร่งใส ธรรมาภิบาล การกำกับดูแลที่ดี

เช่นเดียวกับวงจรการพัฒนาระบบงานและซอฟต์แวร์ทั่วไป การจัดการเรื่องการกำกับดูแล ความโปร่งใส ธรรมาภิบาลสำหรับบล็อกเชนและสัญญาอัจฉริยะมีความจำเป็นเช่นกัน

บล็อกเชนแบบ permissionless เช่น อีเธอเรียมออกแบบให้มีความโปร่งใสในการทำงานและกระจายอำนาจโดยตัวเอง อยู่นอกเหนือการควบคุมของบุคคลหรือองค์กรใด การกำกับดูแลบล็อกเชนอย่างอีเธอเรียมจึงอยู่ที่มาตรฐานในการควบคุมการประมวลผลอย่างที่ได้กล่าวต่อไปในหัวข้อ Governance ในบทที่ 5

บล็อกเชนแบบ permissioned เช่น consortium หรือ private มักเป็นขององค์กร การกำกับดูแลจึงอยู่ที่การตกลงในองค์กรหรือระหว่างองค์กรที่แลกเปลี่ยนข้อมูลด้วยกัน แต่หากความโปร่งใส ธรรมาภิบาล การกำกับดูแลที่ดี เป็นสิ่งที่จำเป็นต้องส่งมอบให้กับลูกค้าหรือผู้มีส่วนได้ส่วนเสีย สามารถใช้วิธีการเดียวกับบล็อกเชน ICO, DeFi, หรือ DAO หลาย ๆ

แห่งใช้กัน คือ ใช้วิธีการของโอเพนซอร์สเพื่อให้ผู้มีส่วนได้ส่วนเสียมีโอกาสตรวจสอบได้อย่างกว้างขวาง และใช้ governance token หากต้องการให้มีผู้มีส่วนได้ส่วนเสียร่วมในการกำกับดูแล

4.1.1 ซอร์สโค้ดของบล็อกเชน

เครือข่ายบล็อกเชนที่มีอยู่ในเวลานี้รวมทั้งที่พัฒนาเชิงพาณิชย์เช่น R3 Corda ConsenSys Quorum เลือกแนวทางการพัฒนาซอฟต์แวร์แบบโอเพนซอร์ส เปิดโอกาสให้ทุกคนสามารถมีส่วนตรวจสอบ และร่วมพัฒนาปรับปรุงโพรโทคอลในการทำงานและซอร์สโค้ดของซอฟต์แวร์พื้นฐานให้มีคุณภาพที่ดีขึ้นได้ นอกจากนี้บางบล็อกเชนยังได้รับการตรวจสอบ (audit) ความมั่นคงปลอดภัยของโพรโทคอลและซอร์สโค้ดโดยหน่วยงานภายนอก และเผยแพร่ผลการตรวจสอบสู่สาธารณะด้วย เช่น อีเธอเรียม [94] [95] [96] [97] [98] และ Hyperledger [99] ซึ่งเท่ากับว่าเครือข่ายบล็อกเชนอื่น ๆ ที่ใช้ซอร์สโค้ดชุดเดียวกันกับบล็อกเชนเหล่านี้ (เช่น ThaiChain ซึ่งสร้างเครือข่ายบล็อกเชนโดยใช้ซอร์สโค้ดเดียวกันกับอีเธอเรียม [100]) ก็เสมือนได้รับการตรวจสอบตามไปด้วย ดังนั้น หากจำเป็นต้องสร้างเครือข่ายบล็อกเชนสำหรับระบบงาน การเลือกใช้ซอร์สโค้ดเดียวกับบล็อกเชนที่มีอยู่แล้วจึงถือเป็นทางเลือกและเป็นแนวปฏิบัติที่ดี

แบบแผนการสร้างความโปร่งใสโดยโอเพนซอร์ส กลายเป็นแนวปฏิบัติที่โครงการ ICO DAO และ DeFi ยึดถือและนำมาปฏิบัติด้วย ชุมชนและผู้ใช้งานจึงสามารถตรวจสอบสัญญาอัจฉริยะที่โครงการต่าง ๆ บันทึกในบล็อกเชนไว้แล้วได้เสมอ

4.1.2 ซอร์สโค้ดสัญญาอัจฉริยะ

ซอร์สโค้ดของสัญญาอัจฉริยะนอกจากจะใช้วิธีการโอเพนซอร์สแล้ว โครงการที่ต้องการสร้างความเชื่อมั่นให้กับผู้ใช้ เช่น DeFi ที่ถือมีธุรกรรมสินทรัพย์จำนวนมาก ๆ มักจะมีการตรวจสอบความมั่นคงปลอดภัยของสมการทางการเงิน โพรโทคอล และซอร์สโค้ดด้วยเช่นกัน เช่น Compound [101], Uniswap [102], Kulap [103] และเช่นเดียวกับซอร์สโค้ด

ของบล็อกเชน การเลือกใช้ซอร์สโค้ดสัญญาอัจฉริยะเดียวกันกับโครงการที่มีอยู่ เป็นทางเลือกและเป็นแนวปฏิบัติที่ดีที่สามารถทำได้

ส่วนสัญญาอัจฉริยะที่พัฒนาขึ้นมาใหม่สามารถตรวจสอบการประมวลผลและความมั่นคงปลอดภัยได้เช่นเดียวกับซอร์สโค้ดของซอฟต์แวร์คอมพิวเตอร์ทั่วไป ซึ่งประกอบด้วย

1. Model checking เพื่อตรวจสอบความถูกต้องของการออกแบบระบบงานตามทฤษฎีการคำนวณ (Theory of computation) โดยใช้เทคนิค Formal Methods เช่น Finite-State Verification, Simulation หรือ Stress Test
2. Code audit เพื่อตรวจสอบความเข้ากันได้ของข้อมูล จุดอ่อน ข้อบกพร่อง ที่อาจพบได้ในตัวซอร์สโค้ด โดยใช้เทคนิคในการตรวจสอบซอร์สโค้ดโปรแกรม เช่น static analysis

ทั้งนี้ปัจจุบัน มีธุรกิจที่รับตรวจสอบสัญญาอัจฉริยะ ทั้ง model checking และ code audit อยู่ทั้งในประเทศไทยและต่างประเทศ เช่น ThaiChain Foundation, Atato, Certik, ConsenSys เป็นต้น

4.1.3 การดูแลเครือข่ายบล็อกเชน

การสร้างเครือข่ายบล็อกเชนขึ้นมาใช้งานด้วยตัวเอง ควรให้ความสำคัญเพิ่มเติมจากการดูแลโครงสร้างพื้นฐานระบบสารสนเทศทั่วไป เพื่อให้กับธุรกรรมที่บันทึกใน ledger มีความน่าเชื่อถือ ซึ่งโดยหลักจะอยู่ที่การเลือกใช้โพรโทคอลในการทำ consensus ที่เหมาะสมกับการประยุกต์ใช้งาน

เครือข่ายบล็อกเชนแบบ permissionless มีวัตถุประสงค์หลักในการทำให้เครือข่ายอยู่ได้ด้วยตัวเองอย่างอิสระ จึงพึ่งพาโพรโทคอลในการทำ consensus ที่กระจายอำนาจเต็มรูปแบบอย่าง Proof of Work หรือ Proof of Stake เพื่อไม่ให้มีใครสามารถยึด

ครองหรือเข้าไปเปลี่ยนแปลงเครือข่ายได้โดยง่าย การกำกับดูแลจึงอยู่ที่การตกลงของชุมชน ดังเช่นที่เกิดกับการทำ hard fork ของอีเธอเรียม

ส่วนเครือข่ายบล็อกเชนแบบ permissioned อนุญาตให้กำหนดอำนาจในการควบคุมและกำหนดสิทธิในการเข้าถึงได้หลายระดับ จะมีประเด็นหลักในการควบคุมโหนดที่ทำหน้าที่ยืนยันข้อมูลใน ledger ให้อยู่ภายใต้เงื่อนไขการทำงานที่น่าเชื่อถือของโพรโทคอลในการทำ consensus

ในทางปฏิบัติเครือข่ายบล็อกเชนแบบ permissioned ไม่ควรใช้ Proof of Work เนื่องจากเครือข่ายมีแนวโน้มที่จะมีจำนวนโหนดในการยืนยันธุรกรรมน้อย ซึ่งทำให้การโจมตีด้วย 51% Attack เกิดขึ้นได้ง่าย Proof of Stake จึงเป็นทางเลือกที่ดีกว่าสำหรับเครือข่ายบล็อกเชนแบบ permissioned

การจัดการ validator และ stake จะเป็นประเด็นในการกำกับดูแลที่ควรตกลงกันภายในองค์กร หรือระหว่างองค์กรใน consortium ที่จะใช้เครือข่ายร่วมกัน

Validator ควรมีการกระจายตัวภายในองค์กรหรือในสมาชิกของ consortium อย่างยุติธรรม เพื่อป้องกันการยึดครองเครือข่าย และเพื่อให้มีสำเนา ledger มากพอที่จะรักษา consensus ได้

Stake ที่จะเลือกใช้ควรกระจายอำนาจการถือครอง และสามารถป้องกันไม่ให้มีผู้ใดยึดเครือข่ายโดยถือครอง stake มากกว่าโหนดอื่น จึงนิยมใช้ โทเคนของคริปโทเคอร์เรนซีประกอบกับ aging นอกจากนี้อาจมีการตกลงเกณฑ์ในการควบคุมเพิ่มเติม เช่น กำหนดบทลงโทษกรณีเกิดเหตุไม่พึงประสงค์ เพื่อลดความเสี่ยงที่จะเกิดการทำ double sign เพื่อ double spending

แต่หากเครือข่ายที่สร้างไม่จำเป็นต้องกระจายอำนาจการยืนยันธุรกรรม เช่น ใช้งานในองค์กรเป็น private หรือเป็น consortium ที่เชื่อใจกันได้ตั้งแต่แรก Proof of Authority หรือ PBFT อาจเป็นทางเลือกที่เหมาะสมที่สุด เพราะใช้ทรัพยากรในการประมวลผลน้อย

การใช้ Proof of Authority และ PBFT ควรมีโหนดกระจายตัว เพื่อให้มีสำเนา ledger มากพอที่จะรักษา consensus เช่นกัน กรณี Proof of Authority นิยมมีโหนดเป็นจำนวนคี่ ไม่น้อยกว่า 3 โหนด ส่วนจำนวนโหนดของ PBFT จะต้องไม่น้อยกว่า 3f + 1 เมื่อ f เป็นจำนวนโหนดที่ทำงานบกพร่องทำให้มีผลไม่สอดคล้องกับโหนดอื่น แต่ละโหนดไม่ควรมีผู้ดูแลโหนดเป็นคนเดียวกันหรือมีส่วนได้เสียระหว่างกัน

จะเห็นได้ว่ากลไกการกำกับดูแลในบล็อกเชนแบบ permissioned มีคนเข้ามาเกี่ยวข้องในกระบวนงาน จึงอาจต้องมีการตรวจสอบกระบวนงานเพื่อสร้างความโปร่งใสและความเชื่อมั่นให้กับผู้ใช้งาน

4.2 การแลกเปลี่ยนข้อมูลและทำงานร่วมกัน

การประยุกต์ใช้บล็อกเชนอาจต้องนำเข้าข้อมูลจากภายนอกเครือข่ายบล็อกเชนเพื่อให้สัญญาอัจฉริยะทำงานได้ และอาจจำเป็นต้องแลกเปลี่ยนข้อมูลระหว่างเครือข่ายบล็อกเชนอื่นที่มีการทำงานที่เหมือนหรือต่างกัน จึงควรรู้จักหลักการพื้นฐานของการนำเข้าและแลกเปลี่ยนข้อมูลระหว่างบล็อกเชน เพื่อจะได้นำไปใช้งานได้อย่างเหมาะสม

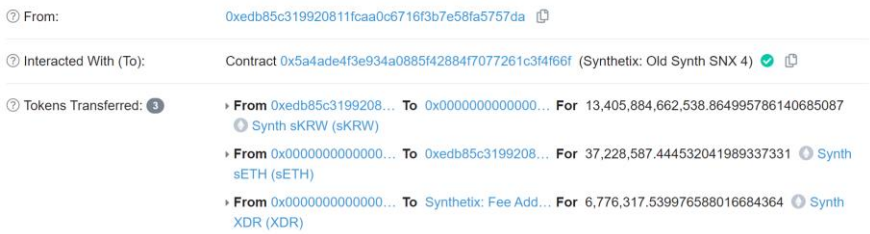
4.2.1 Oracle - ข้อมูลจากโลกจริงสู่บล็อกเชน

ในบริบทของบล็อกเชน Oracle คือระบบสารสนเทศที่ส่งข้อมูลจากด้านนอกเครือข่ายบล็อกเชนให้กับสัญญาอัจฉริยะที่อยู่บนบล็อกเชน เช่น ข้อมูลราคาสินค้า อัตราแลกเปลี่ยนสกุลเงินตรา อัตราดอกเบี้ย ตารางบิน ข้อมูลจากเซ็นเซอร์ หรือค่าอื่น ๆ ที่สัญญาอัจฉริยะจำเป็นต้องใช้เป็นข้อมูลในการประมวลผลอัตโนมัติ

ตัวอย่าง Oracle ที่นิยมใช้กันในปัจจุบัน ได้แก่ Band protocol [104] และ Chainlink [105] ข้อมูลที่ได้จาก Oracle ส่งผลกระทบต่อธุรกรรมของสัญญาอัจฉริยะ จึงจำเป็นต้องมีความน่าเชื่อถือสูง และเป็นส่วนสำคัญที่ทำให้ระบบเหล่านี้ควรได้รับการตรวจสอบด้านความมั่นคงปลอดภัย และสัญญาอัจฉริยะที่ต้องการใช้ข้อมูลจาก Oracle

ควรจะต้องเตรียมความพร้อมรับมือหากเกิดอุบัติการณ์ไม่พึงประสงค์ล่วงหน้า สัญญาอัจฉริยะหลายแห่งเลือกใช้ข้อมูลจาก Oracle หลายแหล่งเพื่อลดความเสี่ยงที่จะถูกโจมตีจาก Oracle ตัวอย่างเช่น กรณีที่เกิดกับ Synthetix ในภาพที่ 10

ภาพที่ 10 ผลกระทบของ Oracle ที่เกิดกับ Synthetix



Synthetix [107] เป็นสัญญาอัจฉริยะในการสร้างโทเคนแทนสินทรัพย์อัตโนมัติ เช่น สกุลเงิน คริปโทเคอร์เรนซี หุ้น ทองคำ เงิน น้ำมัน โดยอาศัย Oracle หลายแห่งในการส่งข้อมูลอัตราแลกเปลี่ยน ราคาหุ้นรายตัว ราคาดัชนี ราคาทอง เพื่อกำหนดมูลค่าของโทเคนแทนสินทรัพย์ ณ ขณะมีการประมวลผล

วันที่ 24 มิถุนายน ค.ศ. 2019 Oracle ที่ Synthetix ใช้บริการอยู่รายงานข้อมูลอัตราแลกเปลี่ยนสกุลเงินวอนสูงกว่าปรกติ 1,000 เท่า ส่งผลให้ผู้ถือ sKRW (โทเคนแทนสกุลเงินวอนของ Synthetix) รายหนึ่งแลก sKRW เป็นโทเคน sETH (โทเคนแทน ETH ของ Synthetix) ที่อยู่ใน pool ได้มากกว่าปกติ 1000 เท่า ทำกำไรได้หลายพันล้านเหรียญสหรัฐ ในธุรกรรม 0x93819f6bbea390d7709fa033f5733d16418674e99c43b9ed2 3adb41 0d657f0c [108]

ผู้ดูแลระบบสั่งสัญญาอัจฉริยะ Synthetix ให้หยุดรับข้อมูลจาก Oracle ทันทีที่ทราบและยืนยันปัญหาได้ ส่งผลให้ Synthetix หยุดให้บริการธุรกรรมในการแลกเปลี่ยนโทเคนทั้งหมดของ Synthetix และหาทางแก้ไขก่อนจะกลับมาเปิดบริการอีกครั้ง ผู้ใช้ที่ถือโทเคน sKRW ที่ทำกำไรได้ในครั้งนั้นตกลงกับ Synthetic ที่จะคืนผลกำไรทั้งหมดและคืนสภาพสถานะของสินทรัพย์ใน pool sKRW และ sETH กลับมาเป็นเหมือนเดิม [109]

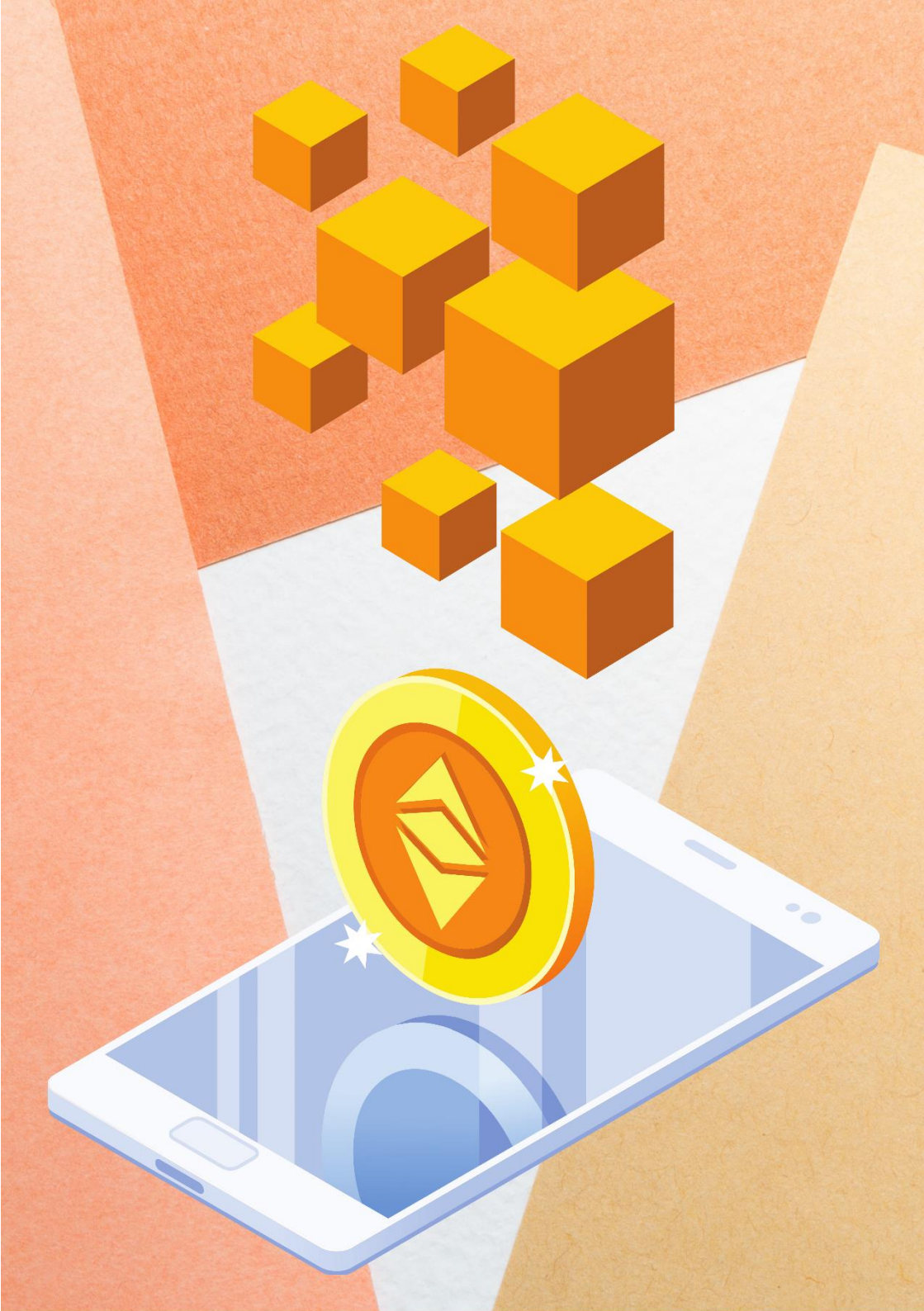
4.2.2 การทำงานข้ามเครือข่ายบล็อกเชน

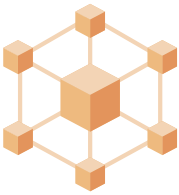
เช่นเดียวกับระบบงานที่มีอยู่ในปัจจุบันอยู่มากมาย ความท้าทายในการพัฒนาระบบงานบนบล็อกเชนมีมากขึ้นไปอีกเมื่อจำเป็นต้องเชื่อมการทำงานร่วมกับระบบงานบนบล็อกเชนอื่น

Oracle เป็นวิธีหนึ่งที่ช่วยให้บล็อกเชนที่ต่างกันใช้โทเคนคนละแบบกันทำงานร่วมกันได้ โดยแต่ละบล็อกเชนถือว่าข้อมูลจากบล็อกเชนอื่นเป็นข้อมูลภายนอกที่รับเข้ามาประมวลผลได้ผ่าน Oracle

แต่นอกเหนือจากการใช้ Oracle แล้ว ยังมีอีก 2 เทคนิคที่เลือกใช้ได้ตามความเหมาะสม ได้แก่การใช้บริการ Sidechain/Relay เช่น Polkadot ที่ได้ยกตัวอย่างไปแล้วในบทก่อนหน้านี้ และการทำ Hashed Time-Lock Contract [106]

Hashed Time-lock Contract (HTLC) เป็นเทคนิคของสัญญาอัจฉริยะที่ตั้งเงื่อนไขในการแลกเปลี่ยนให้มีการยืนยันโดยผู้รับภายในระยะเวลาที่กำหนด หากผู้รับยืนยันการแลกเปลี่ยนครบถ้วนทุกคนในเวลาที่กำหนดไว้ การแลกเปลี่ยนจึงจะเกิดขึ้นและได้รับการยืนยันโดยเครือข่าย แต่ถ้าหากเงื่อนไขไม่ครบถ้วน หรือพ้นเวลาที่กำหนดไว้การแลกเปลี่ยนจะไม่เกิดขึ้น เทคนิคนี้มีข้อดีที่ไม่ต้องมีตัวกลางที่ทำหน้าที่เป็น trusted third party เป็นเทคนิคที่นิยมใช้ทำการแลกโทเคนข้ามเครือข่ายบล็อกเชน (cross-chain atomic swaps)





“Bitcoin is great as a form of digital money,

but its scripting language is too weak

for any kind of serious advanced applications to be built on top.”

-- Vitalik Buterin
Ethereum Co-Founder

5 อีเธอเรียม

ย้อนกลับมาเรื่องบิตคอยน์อีกครั้ง เราอาจเข้าใจว่าธุรกรรมของบิตคอยน์เป็นบันทึกการแลกเปลี่ยนโทเคน แต่แท้จริงแล้วธุรกรรมของบิตคอยน์คือ **สคริปต์ (script) ประมวลผลข้อมูล**

เมื่อผู้ใช้สร้างธุรกรรมด้วยวอลเล็ต สิ่งที่เกิดขึ้นเบื้องหลังจริง ๆ คือวอลเล็ตจะสร้างสคริปต์กำหนดขั้นตอนประมวลผลข้อมูลไว้เมื่อธุรกรรมได้รับการยืนยัน ตัวอย่างเช่น การชำระเงินจะนิยมใช้สคริปต์ที่เรียกกันว่า Pay-to-PubKey-Hash (P2PKH)

สคริปต์ Pay-to-PubKey-Hash (P2PKH) เทียบได้กับการปลดล็อกกระเป๋าเพื่อนำเงินทั้งหมดมาแบ่งใส่อีกกระเป๋าผู้รับเงินแล้วใส่กุญแจล็อกไว้

ในทางเทคนิค P2PKH ประกอบด้วยคำสั่งประมวลผล UTXO ฝั่ง input โดยทดสอบว่าเจ้าของธุรกรรมเป็นผู้ถือกุญแจส่วนตัวที่เข้าคู่กับบิตคอยน์แอดเดรสใน UTXO จริง ๆ ถ้าทดสอบผ่าน จึงจะสร้าง UTXO ฝั่ง output โดยผูกเหรียญไว้กับบิตคอยน์แอดเดรสของผู้รับเงิน

หมายความว่าบิตคอยน์ไม่ได้ทำได้แค่ทำธุรกรรมชำระเงินหรือโอนเงินระหว่างกันเท่านั้น เรายังสามารถเขียนสคริปต์สร้างเงื่อนไขในการทำธุรกรรมอัตโนมัติอื่น ๆ ได้อีกมากมาย เช่น ระบบตัดยอดใช้จ่ายทุกนาที ระบบคืนเงินใช้จ่ายตามเงื่อนไข สลากออมทรัพย์ หรือสร้างกลไกควบคุมบัญชีดูแลผลประโยชน์คู่สัญญา (escrow)

การเขียนสคริปต์กำหนดเงื่อนไขทำธุรกรรมอัตโนมัติ พ้องกับการกำหนดเงื่อนไขของสัญญาและปฏิบัติตามเงื่อนไขธุรกรรมสัญญา ยิ่งไปกว่านั้นการทำงานจะถูกบังคับให้เป็นไปตามสคริปต์ที่เขียนขึ้นและเมื่อสคริปต์ทำงานแล้วจะแก้ไขเปลี่ยนแปลงยาก ซึ่งเท่ากับว่าสัญญาสามารถประมวลผลอัตโนมัติได้โดยไม่ต้องกังวลว่าฝ่ายใดฝ่ายหนึ่งจะผิดสัญญา คุณสมบัติของสคริปต์บนบิตคอยน์ทำให้มีผู้กล่าวถึงสัญญาอัจฉริยะ (smart contract) ในเวลาต่อมา

5.1 สัญญาอัจฉริยะ

สัญญาอัจฉริยะ เป็นคำที่ประดิษฐ์ขึ้นโดย Nick Szabo ในปี 1994 [10] โดยนิยามว่า เป็นสัญญา (promises) ในรูปแบบดิจิทัลที่แต่ละฝ่ายที่เกี่ยวของในสัญญานั้นถือปฏิบัติรูปแบบดิจิทัลที่กล่าวถึงในที่นี้ไม่ใช่เป็นเพียงไฟล์เอกสาร แต่เป็นรูปแบบที่สามารถประมวลผลได้ตามเงื่อนไขสัญญาอัตโนมัติ เพื่อลดผู้ทำหน้าที่เป็นตัวกลาง ลดค่าใช้จ่ายทั้งเงิน เวลา และความเสียหายอื่น ๆ ที่เกิดจากการฉ้อโกง ผิดสัญญา ทั้งที่ตั้งใจและไม่ตั้งใจ

> "A Set of promises, specified in digital form, including protocols within which the parties perform on these promises."

-- Nick Szabo
Cryptographer and Legal Scholar

Nick Szabo จบการศึกษาด้านคอมพิวเตอร์และกฎหมาย แนวคิดดั้งเดิมของสัญญาอัจฉริยะคือการแก้ปัญหาที่เกิดขึ้นในการทำสัญญาที่มีผลผูกพันตามกฎหมายโดยใช้เทคโนโลยีสารสนเทศ แต่ภายหลังที่มีเทคโนโลยีบล็อกเชนเกิดขึ้น คำว่าสัญญาอัจฉริยะถูกใช้อย่างกว้างขวางกับการประมวลผลธุรกรรมอัตโนมัติในบล็อกเชนซึ่งไม่ได้มีผลผูกพันตามกฎหมายไปเสียทั้งหมด สัญญาอัจฉริยะที่มีผลผูกพันตามกฎหมายจริง ๆ จึงเลี่ยงไปใช้คำที่ชัดเจนชี้นว่า legally-binding smart contract

อย่างไรก็ตามสคริปต์ของบิตคอยน์ไม่สามารถใช้เขียนโปรแกรมได้เหมือนกับภาษาคอมพิวเตอร์อื่น ๆ ทำให้ศักยภาพในการพัฒนาสัญญาอัจฉริยะบนเครือข่ายบิตคอยน์มีข้อจำกัดอยู่มาก

สคริปต์ของบิตคอยน์ มี syntax แบบ Reverse Polish Notation (RPN) ทำงานด้วย stack คล้ายกับภาษา Forth มี instructions จัดการ stack, arithematic operations, bitwise logic operations, cryptographic operations, มีโครงสร้าง if-else แต่ไม่มี iteration และไม่รองรับ recursion ทั้งนี้เพื่อเลี่ยง halting problem จึงอาจกล่าวได้ว่า สคริปต์ของบิตคอยน์ไม่ใช่ภาษา Turing Complete

ในปี ค.ศ. 2013 Vitalik Buterin ได้เสนอทางออกในการแก้ไขข้อจำกัดสคริปต์ของบิตคอยน์เป็นโครงการบล็อกเชนใหม่ที่ไม่เพียงมีสคริปต์ทำธุรกรรมทางการเงินดิจิทัลอัตโนมัติได้ แต่สามารถพัฒนาเป็นซอฟต์แวร์ที่ซับซ้อนได้เหมือนกับภาษาคอมพิวเตอร์อื่น ๆ

บล็อกเชนที่ Vitalik เสนอจึงเหนือกว่าบิตคอยน์ที่สามารถเป็นแพลตฟอร์มในการพัฒนาแอปพลิเคชันที่กระจายอำนาจการประมวลผลได้ โดยไม่ต้องมีบุคคลที่สามทำหน้าที่เป็น trusted third party แอปพลิเคชันที่ทำงานบนบล็อกเชนนี้ เรียกว่า Decentralized Application หรือ DApp

โครงการบล็อกเชนนี้มีชื่อว่า **“อีเธอเรียม”**

5.2 โครงการอีเธอเรียม (Ethereum)

โครงการอีเธอเรียมมีเป้าหมายในการพัฒนาเครือข่ายบล็อกเชนขึ้นมาใหม่ปรับปรุงการประมวลผลโดยพยายามแก้จุดอ่อนที่มีอยู่ในบิตคอยน์ เพื่อให้อีเธอเรียมเป็นแพลตฟอร์มในการพัฒนา DApp

กล่าวได้ว่า ศักยภาพของอีเธอเรียมที่แท้จริง ไม่ได้อยู่ที่การทำธุรกรรมของคริปโทเคอร์เรนซี แต่อยู่ที่การเป็นแพลตฟอร์มสำหรับพัฒนา DApp หรือสัญญาอัจฉริยะ

ในเครือข่ายอีเธอเรียมที่จะพัฒนาขึ้น ผู้ใช้สามารถทำธุรกรรมตรงไปยัง DApp และได้ผลลัพธ์การทำงานกลับมาตามที่ซอร์สโค้ดของ DApp เขียนไว้ หากเทียบว่าซอร์สโค้ดของ DApp คือเงื่อนไขของสัญญา อีเธอเรียมจะทำให้การทำงานของ DApp เป็นไปตามสัญญาที่เขียนไว้ ไม่มีใครผิดสัญญาได้ ไม่มีใครแก้สัญญาทีหลัง หรือแก้ผลที่เกิดขึ้นจากสัญญาได้

ภายใต้บริบทของบล็อกเชน DApp และสัญญาอัจฉริยะจึงมักเป็นคำที่ใช้แทนกันอยู่บ่อยครั้ง

ความน่าสนใจอีกประการของโครงการอีเธอเรียมคือวิธีระดมทุน (crowdfunding) เพื่อเป็นค่าใช้จ่ายของโครงการในการพัฒนาซอฟต์แวร์พื้นฐานของระบบบล็อกเชนและเพื่อที่จะสร้างเครือข่ายบล็อกเชนตามที่ระบุใน white paper [11]

โครงการอีเธอเรียมใช้การระดมทุนที่เรียกว่า Initial Coin Offering (ICO) มีลักษณะคล้ายกับการเสนอขายหุ้นแก่ประชาชนทั่วไปเป็นครั้งแรก (Initial Public Offering: IPO) แต่ใน ICO ผู้ร่วมสนับสนุนจะได้รับสิทธิถือโทเคนแทนที่จะเป็นสิทธิในหุ้น ผู้สนใจสามารถร่วมสนับสนุนโครงการอีเธอเรียมโดยใช้โทเคนของบิตคอยน์ซื้อโทเคนของอีเธอเรียม (Ether: ETH) หากโครงการพัฒนาอีเธอเรียมประสบความสำเร็จ ผู้ลงทุนจะได้ ETH เป็นการตอบแทนหลังกำเนิด genesis block

อีเธอเรียมเสนอขาย ETH เป็นระยะเวลา 42 วัน เริ่มต้นขายในวันที่ 22 กรกฎาคม ค.ศ. 2014 โดย 14 วันแรกมีอัตราแลกเปลี่ยนคงที่ 2,000 ETH ต่อ 1 BTC จากนั้นอัตราจะลดลงเรื่อย ๆ จนถึงวันที่ 2 กันยายน ค.ศ. 2014 จะมีอัตราที่ 1,337 ETH ต่อ 1 BTC [12]

42 เป็น jargon ในชุมชนแฮ็กเกอร์ (in a spirit of playful cleverness) มาจากคำตอบของของชีวิต เอกภพ และทุกสรรพสิ่ง ตามหนังสือนิยายเรื่อง The Hitchhiker's Guide to the Galaxy ของ Douglas Adams

1337 เป็น jargon ในชุมชนแฮ็กเกอร์เช่นกัน มาจากการแทนตัวอักษร leet ในภาษาอังกฤษด้วยตัวเลข คำว่า leet กร่อนมาจากคำว่า elite

เบื้องหลังการขายเหรียญ ETH คือการทำธุรกรรมตรงไปยังบิตคอยน์แอดเดรส 36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2 ซึ่งเป็นแอดเดรสสัญญาอัจฉริยะที่โครงการอีเธอเรียมเขียนขึ้นเพื่อบันทึกธุรกรรมการร่วมสนับสนุน ตลอดระยะเวลาระดมทุนมีการทำธุรกรรมผ่านแอดเดรสนี้เกือบ 9,000 รายการ เป็นจำนวนมากกว่า 30,000 BTCs มูลค่าในเวลานั้นคือประมาณ 18.5 ล้านเหรียญสหรัฐ [13]

ในวันที่ 30 กรกฎาคม ค.ศ. 2015 เวลา 03:26:13 PM +UTC เครือข่ายอีเธอเรียมถือกำเนิดจาก genesis block ภายในบล็อกหมายเลข 0 ของอีเธอเรียมประกอบด้วยธุรกรรม 8,893 รายการที่โอน ETH ให้กับผู้สนับสนุนทุกคน [14]

5.3 จากบิตคอยน์มาสู่อีเธอเรียม

อีเธอเรียมสร้างระบบประมวลผลที่ต่างไปจากบิตคอยน์หลายอย่าง ในระดับซอฟต์แวร์ เราสามารถพัฒนา DApp ได้โดยภาษาสคริปต์ที่สร้างขึ้นมาใหม่ชื่อ Solidity

Solidity เป็นภาษาคอมพิวเตอร์ที่เข้าใจได้ง่ายกว่าสคริปต์ของบิตคอยน์มาก และยังเป็นภาษาคอมพิวเตอร์ที่มีความสามารถครบถ้วนในการพัฒนาแอปพลิเคชันที่ซับซ้อนได้เหมือนภาษาคอมพิวเตอร์ทั่วไป ไม่จำกัดอยู่เฉพาะการประมวลผลธุรกรรมของคริปโทเคอร์เรนซีเหมือนบิตคอยน์

Solidity ยังมีโครงสร้างและคำสั่งคล้ายกับภาษาที่นักพัฒนาซอฟต์แวร์บนเว็บคุ้นเคย ทำให้นักพัฒนาซอฟต์แวร์ที่มีพื้นฐานอยู่แล้วสามารถปรับมาเขียน DApp ได้โดยไม่ต้องศึกษาภาษาใหม่ทั้งหมด

Solidity เป็น statically-typed object-oriented programming language ที่ออกแบบโดยใช้ syntax และ structure เหมือน ECMAScript (JavaScript) เป็นภาษาที่เรียกได้ว่า Turing Complete

DApp ที่พัฒนาด้วย Solidity จะ compile เป็น bytecode ที่ทำงานบน Ethereum Virtual Machine (EVM) และได้ Application Binary Interface (ABI) สำหรับ call DApp นั้น

Solidity ในภาษาอังกฤษมีความหมายว่า ความน่าเชื่อถือ ความมั่นคง ความแน่นอน

DApp หรือสัญญาอัจฉริยะที่พัฒนาเสร็จแล้วจะถูกส่งไปบันทึก (deploy) เก็บในบล็อกเชนของอีเธอเรียม เมื่อ DApp ได้รับการยืนยันแล้วจะได้แอดเดรสของสัญญาอัจฉริยะกลับมา แอดเดรสนี้มีไว้เพื่อเรียก DApp ขึ้นมาทำงาน อีเธอเรียมเปิดกว้างให้ผู้ใช้งานอีเธอเรียมทุกคนสามารถพัฒนา DApp และ deploy ได้โดยอิสระ และผู้ใช้ทุกคนสามารถเรียก DApp ใดก็ได้ขึ้นมาใช้งาน ถ้ารู้แอดเดรสของ DApp นั้น

เมื่อผู้ใช้สร้างธุรกรรมไปยังแอดเดรสของ DApp จะเป็นการเรียก DApp นั้นขึ้นมาประมวลผลให้กับผู้ใช้ โดยการประมวลผลจะเกิดบนเครือข่ายอีเธอเรียม หากมีผลลัพธ์จากการประมวลผล ก็จะได้รับการบันทึกและยืนยันในเครือข่ายอีเธอเรียมด้วยเช่นกัน

ในระดับการประมวลผล อาจมองได้ว่าอีเธอเรียมเสมือนเครื่องคอมพิวเตอร์ที่มี DApp ติดตั้งพร้อมให้ใช้งาน การเรียกใช้งาน DApp เหมือนการเรียกใช้โปรแกรมขึ้นมาทำงาน ซึ่งต้องใช้ทรัพยากรของฮาร์ดแวร์ในการประมวลผลและจัดเก็บผลลัพธ์ อีเธอเรียมเก็บค่าทำธุรกรรมที่มีการบันทึกหรือประมวลผลทุกรายการให้กับโหนดที่ยืนยันบล็อก ค่าธรรมเนียมในอีเธอเรียม เรียกกันว่าค่า gas ชำระโดยใช้ ETH

อีเธอเรียม ใช้คำว่า gas เพราะการประมวลผลของ DApp บนอีเธอเรียมคล้ายการใช้พาหนะเดินทางที่ต้องเติมเชื้อเพลิงล่วงหน้าก่อนออกเดินทาง

ในอีเธอเรียมทุกคำสั่งของ DApp จะคิดเป็นหน่วยของ gas แต่เนื่องจาก DApp อาจจะมีคำสั่ง loop ซึ่งไม่สามารถบอกล่วงหน้าได้จะวนกี่รอบ จึงไม่สามารถระบุได้ว่าการประมวลผล DApp แต่ละครั้งจะใช้ gas เท่าไหร่ อีเธอเรียมจึงให้ผู้ใช้เป็นผู้กำหนดเองว่าจะยอมใช้ gas ในการประมวลผลสูงสุดกี่หน่วย (gas limit) และจะยอมจ่ายค่า gas (gas price) ในราคาเท่าไหร่ต่อ gas 1 หน่วย

ค่าธุรกรรมในการประมวลผล DApp แต่ละครั้งจะใช้ไม่เกิน gas limit คูณ gas price หากการประมวลผล DApp ใช้ gas น้อยกว่า gas limit ก็จะจ่ายค่าธรรมเนียมเฉพาะที่ใช้ไป

gas price ที่สูงกว่าทำให้โหนดของอีเธอเรียมได้รับผลตอบแทนที่สูงกว่า จึงใช้เป็นหน่วยในการเลือกธุรกรรมในการสร้างบล็อก

ในระดับเครือข่ายบล็อกเชน อีเธอเรียมเป็นบล็อกเชนสาธารณะเหมือนกับบิตคอยน์ ใช้ consensus แบบ Proof of Work ออกแบบให้มี block time 12 วินาที โดยปรับค่า difficulty ทุกบล็อก และมีระบบการให้รางวัลเป็นแรงจูงใจ โดยปรับค่ารางวัลตามสภาพความเฟ้อของคริปโทเคอร์เรนซีด้วยการอัปเกรดโพรโทคอลการทำงานของอีเธอเรียมเป็นระยะ

consensus ของ อีเธอเรียม ใช้ Greedy Heaviest Observed Sub Tree (GHOST) นับ chain ที่มีน้ำหนักมากที่สุด ซึ่งคิดบล็อกที่ได้รับการยืนยันแต่ไม่ได้อยู่ใน longest chain (uncle block) รวมเข้าไปด้วย ทำให้ปลอดภัยจากการโจมตีด้วย 51% Attack มากกว่าการเลือก longest chain

อีเธอเรียมจึงให้รางวัลทั้งโหนดที่ยืนยันบล็อกที่อยู่ใน longest chain และโหนดที่ยืนยัน uncle block เพราะถือว่ามีส่วนต่อน้ำหนัก consensus การยืนยัน uncle block จึงไม่ได้สูญเปล่าเหมือนกับบิตคอยน์ และทำให้ไม่จำเป็นต้องมี miner pool ขนาดใหญ่เพื่อให้มีโอกาสได้รางวัล

อีเธอเรียมไม่ได้จำกัดจำนวนเหรียญที่จะผลิตเหมือนบิตคอยน์ จำนวนเหรียญหมุนเวียนในเครือข่ายจึงเพิ่มขึ้นตลอดเวลาตามจำนวนรางวัลที่ได้ในแต่ละบล็อก

นอกจาก ETH แล้ว ในอีเธอเรียมมีหน่วยที่กำหนดไว้อีก 3 หน่วยคือ

- Wei = 1/1,000,000,000,000,000,000 ETH
- szabo = 1/1,000,000 ETH
- finney = 1/1,000 ETH

หน่วย wei ตั้งตามชื่อ Wei Dai วิศวกรคอมพิวเตอร์ที่คิด b-money ในปี ค.ศ. 1998 ซึ่งเป็นรากฐานของคริปโทเคอร์เรนซีบนบล็อกเชนในภายหลัง หน่วย szabo ตั้งตามชื่อของ Nick Szabo และหน่วย finney ตั้งตามชื่อของ Harold Finney นักพัฒนาซอฟต์แวร์ที่สร้าง reusable proof of work ในปี ค.ศ. 2004 ซึ่งเป็นรากฐานการทำงานของบล็อกเชน

5.4 โทเคนบนอีเธอเรียม

นอกจากภาษา Solidity แล้ว อีเธอเรียมยังมีกลไกสนับสนุนให้เป็นแพลตฟอร์มสำหรับสร้าง DApp ที่สำคัญอีกประการคือการสร้างโทเคน

เราสามารถเขียนสัญญาอัจฉริยะเพื่อสร้างโทเคนเป็นของตัวเองบนเครือข่ายอีเธอเรียมได้ โดยไม่จำเป็นต้องใช้โทเคน ETH โดยตรง โทเคนที่สร้างขึ้นมาใหม่จะเป็นหน่วยดิจิทัลที่สามารถแทนของสิ่งหนึ่งสิ่งใด ทั้งที่จับต้องได้ เช่น ข้าว น้ำมัน เพชร ที่ดิน หรือที่จับต้องไม่ได้ เช่น หุ้น สัญญาอนุญาต หมายเลขบัตรประจำตัว

อีเธอเรียมมีประเภทของโทเคนให้นักพัฒนา DApp เลือกใช้งานได้ 3 แบบ ดังนี้

1. Fungible Token ตามมาตรฐาน ERC-20 [15] เหมาะในการเป็นสิ่งแทนของที่แทนกันได้ หรือวัดเชิงปริมาณ เช่น คริปโทเคอร์เรนซีนับตามจำนวน เหรียญ ข้าวนับตามน้ำหนัก น้ำมันนับตามปริมาตร

2. Non-Fungible Token ตามมาตรฐาน ERC-721 [16] เหมาะเป็นสิ่งแทนของที่ทดแทนกันไม่ได้ หรือวัดเชิงคุณภาพ เช่น อัญมณีที่แม้จะมีน้ำหนักเท่ากัน แต่มูลค่าเป็นไปตามคุณภาพ งานศิลปะที่แต่ละชิ้นมีมูลค่าต่างกัน ที่ดินแต่ละผืนแม้จะมีขนาดเท่ากันแต่มีมูลค่าไม่เท่ากัน
3. Multi Token มาตรฐาน ERC-1155 [17] เหมาะเป็นสิ่งแทนของที่เป็นได้ทั้ง ERC-20 และ ERC-721 เช่น สินทรัพย์ในเกมเศรษฐี (Monopoly) มีธนบัตรซึ่งเป็น ERC-20 และโฉนดที่ดินซึ่งเป็น ERC-721

การที่นักพัฒนาสามารถเขียนสัญญาอัจฉริยะในการประมวลผลโทเคนได้บนเครือข่ายอีเธอเรียม ทำให้ไม่มีความจำเป็นต้องสร้างเครือข่ายบล็อกเชนขึ้นมาใหม่เพื่อรองรับ DApp ช่วยลดภาระค่าใช้จ่ายและการบริหารจัดการโครงสร้างพื้นฐานในการประมวลผลไปได้ทั้งหมด

5.5 Governance

อีเธอเรียมใช้เอกสารมาตรฐานที่เรียกว่า Ethereum Improvement Proposal (EIP) เป็นกลไกในการกำกับการทำงานของเครือข่ายและซอฟต์แวร์หลักของอีเธอเรียมให้มีคุณภาพ ทำงานร่วมกันได้ และมีความสามารถใหม่ ๆ ตลอดเวลา โดย EIP แบ่งออกเป็น 3 ประเภท ได้แก่ Standard Track EIP, Meta EIP, และ Informational EIP [18]

อีเธอเรียมเปิดโอกาสให้ทุกคนสามารถส่งข้อเสนอได้โดยอิสระ ข้อเสนอที่ริเริ่มใหม่เป็นเหตุเป็นผล มีความเป็นไปได้ทางเทคนิค จะได้รับการผลักดันให้เป็น draft EIP ซึ่งจะมีกลไกติดตามความเคลื่อนไหวอย่างเปิดเผย โดยมีกลุ่ม core developers และ EIP editors ร่วมตรวจสอบ ทบทวนทางเทคนิค พัฒนาซอฟต์แวร์ขึ้นมาทดลองใช้ ขั้นตอนนี้เป็นภาระที่สูงมาก เพราะทุกคนที่มีส่วนร่วมจะต้องสละเวลามาร่วมพัฒนา draft EIP ข้อเสนอจึงต้องแข็งแรงมากพอที่จะดึงดูดให้มีคนมีส่วนร่วมมากพอที่จะได้ผลสะท้อนที่ครบถ้วน

draft EIP ที่มีความสมบูรณ์ทางเทคนิคเพียงพอแล้วจะได้รับการเผยแพร่เพื่อรับการสะท้อนผลจากชุมชนอีเธอเรียมเป็นครั้งสุดท้าย (last call) หากชุมชนเห็นชอบ จึงจะเปลี่ยนสถานะเป็น final EIP ซึ่งจะเป็นมาตรฐานที่ใช้กำกับซอฟต์แวร์หลักของอีเธอเรียมต่อไป

การปรับปรุงซอฟต์แวร์หลักแต่ละครั้งจะมีการเลือก EIP ที่จะรวมในการปรับปรุงซอฟต์แวร์รุ่นนั้น ซึ่งอาจทำให้โหนดในเครือข่ายที่ใช้ซอฟต์แวร์ต่างรุ่นกันทำงานด้วยกันไม่ได้เลย อีเธอเรียมจึงถือว่าเป็นการทำ hard fork

การทำ hard fork ทุกครั้งของอีเธอเรียมจะได้รับการเผยแพร่เป็น EIP ด้วยเช่นกัน

ในบริบทของบล็อกเชน fork เป็นกลไกในการอัปเกรดบล็อกเชนโดยการอัปเกรดซอฟต์แวร์ที่แต่ละโหนดใช้ประมวลผลให้กับบล็อกเชนนั้น

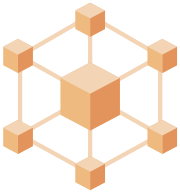
การอัปเกรดบางครั้งไม่ทำให้เกิดผลกระทบกับข้อมูลหรือการประมวลผลของเครือข่ายบล็อกเชน เรียกว่า soft fork ในขณะที่การอัปเกรดบางครั้งทำให้ ข้อมูล หรือการประมวลผลของโหนดที่อัปเกรดแล้วขัดแย้งกับโหนดที่ยังไม่ได้อัปเกรดจนไม่สามารถทำงานด้วยกันได้ และอาจทำให้ ledger ที่กระจายอยู่แต่ละโหนดแยกออกเป็นหลายชุด เรียกว่า hard fork

โดยทางเทคนิค การจัดการ hard fork ให้ราบรื่นเป็นเรื่องค่อนข้างยาก สำหรับเครือข่ายขนาดใหญ่เพราะโหนดส่วนใหญ่จะต้องอัปเกรดซอฟต์แวร์และเปลี่ยนการประมวลผลแทบจะในเวลาเดียวกันเพื่อให้เครือข่ายยังคง consensus ได้ บล็อกเชนจึงใช้วิธีกำหนดหมายเลขบล็อกที่จะอัปเกรดล่วงหน้า เพื่อให้โหนดเปลี่ยนการประมวลผลไปพร้อม ๆ กัน

แม้ว่า EIP จะเป็นกระบวนการที่ทำให้อีเธอเรียมได้รับการปรับปรุงให้ดีขึ้นหรือแก้ปัญหาที่อาจจะเกิดขึ้นในอนาคตได้ แต่ในทางกลับกัน อาจกล่าวได้ว่า อีเธอเรียมอยู่ภายใต้การควบคุมของ EIP และผู้ที่เกี่ยวข้องในการเสนอ พิจารณา ตรวจสอบ ทบทวน และ

ตัดสินใจเลือก EIP ที่จะรวมการทำ hard fork แต่ละครั้ง อีเธอเรียมจึงเลือกใช้โมเดลและเครื่องมือโอเพนซอร์สในการพัฒนา EIP เพื่อให้ชุมชนเข้าถึงและตรวจสอบได้ เช่นเดียวกับซอร์สโค้ดของซอฟต์แวร์หลักของอีเธอเรียม


CONTRACT



> “The industrial revolution allowed us, for the first time,
> to start replacing human labour with machines.”
>
> -- Vitalik Buterin
> Ethereum Co-Founder

6 Decentralized Applications

อีเธอเรียมเป็นแพลตฟอร์มที่ได้รับความนิยมสูงมากในการพัฒนา DApp และเริ่มมีผู้พัฒนา DApp มากขึ้นเรื่อย ๆ รวมถึงเป็นที่สนใจของบริษัทซอฟต์แวร์ขนาดใหญ่ที่พัฒนา DApp ให้กับลูกค้าองค์กร

ยกตัวอย่างเช่น Supply Chain Management สามารถเขียน DApp กำหนดให้โทเคนเป็นสิ่งแทนสินค้า ติดตามการโอนถ่ายสินค้าจากแอดเดรสที่ถือครองโทเคน ข้อมูลเหล่านี้เมื่อบันทึกในบล็อกเชนแล้ว จะแก้ไขเปลี่ยนแปลงไม่ได้ ข้อมูลจึงมีความน่าเชื่อถือ

การปลอมแปลงหรือนำสินค้านอกระบบปนเข้ามาในระบบจะทำได้ยากกว่าระบบที่ใช้ฐานข้อมูลทั่ว ๆ ไป หรือระบบที่ต้องอาศัยคนในการทำงาน

จะเห็นได้ว่าระบบ Supply Chain Management ได้ประโยชน์จากบล็อกเชนตรงคุณสมบัติที่เป็น distributed และ immutable ledger ทำให้ข้อมูลแลกเปลี่ยนกันได้และมีความน่าเชื่อถือ ซึ่งเป็นข้อพิจารณาสำคัญข้อหนึ่ง หากจะย้ายระบบงานที่เป็นสารสนเทศแบบเดิมมาใช้บล็อกเชน

แต่บล็อกเชน ไม่ได้เป็นเพียงแค่ระบบสารสนเทศหรือระบบฐานข้อมูลแบบกระจายศูนย์ที่มีความน่าเชื่อถือเท่านั้น ศักยภาพของบล็อกเชนและ DApp ที่แท้จริง ปรากฏชัดเจนยิ่งขึ้นใน โครงการ The DAO

6.1 Decentralized Autonomous Organization

เดือนพฤษภาคม ค.ศ. 2016 ชุมชนอีเธอเรียมได้รับทราบข่าวของโครงการ The DAO เป็นสัญญาอัจฉริยะที่เขียนเพื่อดำเนินธุรกิจเงินร่วมลงทุน (Venture Capital) สร้างกองทุนสำหรับร่วมลงทุนในโครงการต่าง ๆ ด้วยวิธี crowdfunding ผู้สนใจสามารถร่วมลงสินทรัพย์ในกองทุนด้วยการโอนเหรียญ ETH ไปยังสัญญาอัจฉริยะ The DAO และจะได้โทเคน DAO กลับคืนมาในสัดส่วน 100 DAO ต่อ 1 ETH โทเคน DAO ใช้เป็นสิทธิในการโหวตโครงการต่าง ๆ ที่ต้องการขอทุนจาก The DAO

โครงการที่ต้องการขอทุนเสนอเอกสารของโครงการให้กลุ่มนักลงทุนโหวต หากโครงการได้รับการโหวตว่าสมควรได้รับทุนสนับสนุนไม่น้อยกว่า 20% ของผู้ร่วมโหวต The DAO จะโอน ETH ในกองทุนให้กับโครงการอัตโนมัติ และหากโครงการมีผลกำไรจากการประกอบการ The DAO ก็จะแบ่งสัดส่วนผลกำไรคืนให้กับผู้ลงทุนอัตโนมัติ

The DAO เปิดระดมทุนเป็นระยะเวลา 28 วัน มีผู้ร่วมลงทุนกับ The DAO มากถึง 18,000 ราย มีเหรียญ ETH อยู่ในกองทุนราว 12 ล้าน ETH มีมูลค่ากว่า 150 ล้านเหรียญสหรัฐในเวลานั้น

เอกสารขอทุน The DAO จะผ่านการคัดกรองโดยอาสาสมัครที่ทำงานเป็น curator ว่าเป็นโครงการที่ชอบด้วยกฎหมายและมีตัวตนอยู่จริง curator จะเพิ่มแอดเดรสในการรับเงินของโครงการเข้า whitelist ของ The DAO โครงการจะสามารถส่งขอทุนได้เมื่ออยู่ใน whitelist แล้วเท่านั้น

ในเดือนเดียวกันกับที่มีการเปิดตัว มีผู้ตรวจสอบสัญญาอัจฉริยะของ The DAO และพบช่องโหว่ในฟังก์ชันการถอนตัวจากการลงทุน ต้นเดือนมิถุนายนมีความพยายามเสนอให้แก้ไขฟังก์ชันการถอนตัวจากการลงทุนและเปลี่ยนสัญญาอัจฉริยะของ The DAO ใหม่

แต่ไม่ทันจะได้ลงมือเปลี่ยนสัญญาอัจฉริยะใหม่ วันที่ 16 มิถุนายน ค.ศ. 2016 มีผู้อาศัยช่องโหว่ดังกล่าวโจมตีสัญญาอัจฉริยะของ The DAO ได้สำเร็จ สามารถถอนโทเคนออกจากกองทุนไปได้ 3.6 ล้าน ETH ไปพักไว้ที่แอดเดรสหนึ่งของผู้ลงทุน

เงื่อนไขการถอนตัวจากการลงทุนของ The DAO กำหนดไว้ว่าโทเคน ETH ที่ถอนจากกองทุนจะถูกพักไม่ให้มีการเคลื่อนไหวใด ๆ เป็นเวลา 28 วันนับจากถอนออกจากกองทุน โทเคนจำนวน 3.6 ล้าน ETH คิดเป็นประมาณ 14% ของ ETH ทั้งหมดที่มีหมุนเวียนอยู่ ณ เวลานั้น มีมูลค่าราว 50 ล้านเหรียญสหรัฐ ทำให้ชุมชนอีเธอเรียมยกประเด็นนี้มาหารือกันเพื่อหาทางออกให้ทันเวลาพักการเคลื่อนไหว ในขณะเดียวกัน อาสาสมัครกลุ่มหนึ่งในชุมชนอีเธอเรียม (Robin Hood Group: RHG) โจมตีจุดอ่อนเดียวกันของ The DAO เพื่อถอนทุนทั้งหมดมาพักไว้ในแอดเดรสที่ปลอดภัย เพื่อป้องกันไม่ให้มีความสูญเสียมากไปกว่าที่เป็นอยู่

ทางเลือกเดียวที่จะล้างความเสียหายที่เกิดจาก The DAO ได้ในเวลานั้น คือการทำ hard fork เพื่อย้อน ledger ของเครือข่ายกลับไปยังจุดที่ยังไม่ถูกโจมตี แล้วย้ายกองทุนทั้งหมดไปพักในแอดเดรสเพื่อจ่ายคืนผู้ลงทุนทั้งหมด

hard fork นี้เป็นประเด็นที่ถกกันในชุมชนอย่างมาก มีผู้ที่เห็นด้วยและไม่เห็นด้วย เนื่องจากเป็นการลบประวัติของธุรกรรมที่เกิดขึ้นและได้รับการยืนยันไปแล้ว และต้นตอปัญหาก็ไม่ได้เกิดกับตัวเครือข่ายอีเธอเรียม ชุมชนไม่มีทางเลือกอื่นนอกจากลงมติว่าจะ hard fork หรือไม่

ผลการลงมติ 87% ของผู้ออกเสียง เห็นด้วยกับการทำ hard fork

อีเธอเรียมจึงออก EIP-779 DAO Fork โดยตั้งให้ hard fork ที่บล็อก 1,920,000 และ deploy สัญญาอัจฉริยะให้ผู้ลงทุนส่งโทเคน DAO เพื่อถอน ETH คืนในอัตราเดิม [20] [21]

กรณี The DAO มีโหนดที่ไม่เห็นด้วยจำนวนหนึ่งตัดสินใจไม่ hard fork ตามไปด้วยและยังคงรักษา ledger ที่มีประวัติความเสียหายของ The DAO ไว้ หลังบล็อก 1,920,000 เครือข่ายอีเธอเรียมจึงแยกออกเป็นสองเครือข่าย คือเครือข่ายที่ hard fork ตาม EIP-779 ใช้ชื่ออีเธอเรียมเหมือนเดิม และเครือข่ายที่ไม่ hard fork ตาม EIP-779 เปลี่ยนชื่อเป็น อีเธอเรียมคลาสสิค (Ethereum Classic: ETC)

โครงการ The DAO จึงปิดตัวลงก่อนที่จะเริ่มได้ใช้งาน เหตุการณ์ของ The DAO เป็นบทเรียนราคาแพงที่ให้ชุมชนตระหนักถึงเรื่องความมั่นคงปลอดภัยของสัญญาอัจฉริยะ และมีส่วนอย่างมากในการกระตุ้นให้มีความรอบคอบในการลงทุนในโครงการลักษณะนี้มากขึ้น

แต่หากสัญญาอัจฉริยะของ The DAO ไม่มีข้อบกพร่องและทำงานได้สมบูรณ์แบบ The DAO จะกลายเป็น **องค์กรธุรกิจเงินร่วมลงทุนที่ไม่มีพนักงานบัญชี ไม่มีผู้จัดการกองทุน ไม่มีสถาบันรับฝากสินทรัพย์ ไม่มีการจดทะเบียน และใคร ๆ ก็สามารถสร้างองค์กรธุรกิจแบบนี้ขึ้นใหม่อีกกี่องค์กรก็ได้** ธุรกรรมและกิจการของ The DAO ดำเนินการผ่านสัญญาอัจฉริยะ ทำงานอัตโนมัติ และเป็นอิสระจากการควบคุมของบุคคลที่สามโดย

สมบูรณ์ จึงเป็นที่มาของคำว่า Decentralized Autonomous Organization (DAO) ซึ่งเป็นคำเต็มของ The DAO

ศักยภาพของเทคโนโลยีบล็อกเชนจึงไม่ใช่เพียงเรื่องการเป็นแพลตฟอร์มของคริปโทเคอร์เรนซี แต่เป็นการสร้างสัญญาอัจฉริยะที่ทำให้ไม่มีความจำเป็นที่จะต้องพึ่งองค์กรที่เป็น trusted third party ในการทำธุรกรรมใด ๆ อีกต่อไป

องค์กร งานหรืออาชีพ ที่ทำหน้าที่เป็นตัวกลาง เป็นศูนย์กลางของการทำธุรกรรม มีโอกาสถูกบล็อกเชน disrupt ได้โดยสัญญาอัจฉริยะเพียงไม่กี่บรรทัด

สัญญาอัจฉริยะและบล็อกเชนจึงเป็น Disruptive Technology ที่รุนแรงมาก

และองค์กรที่ได้รับผลกระทบรุนแรงที่สุดในเวลานี้ คือ สถาบันการเงิน ซึ่งกำลังถูกท้าทายด้วยสัญญาอัจฉริยะทางการเงินที่ไม่ต้องมีตัวกลาง ที่เรียกว่า Decentralized Finance หรือ DeFi

6.2 Decentralized Finances

Decentralized Finance หรือ DeFi เป็นการประยุกต์ใช้บล็อกเชนเพื่อให้บริการทางการเงินในรูปแบบดิจิทัล โดยไม่ต้องพึ่งพาสถาบันการเงินที่เป็นตัวกลางอย่าง โบรคเกอร์ ตลาดแลกเปลี่ยนสินทรัพย์ ธนาคารพาณิชย์ หรือแม้แต่ธนาคารกลางของประเทศ ปัจจุบันมี DeFi ที่ให้บริการทางการเงินบนบล็อกเชนจำนวนมาก

ในส่วนนี้ เราจะมาทำความรู้จักตัวอย่างสัญญาอัจฉริยะในการให้บริการทางการเงิน ที่ได้รับความนิยมเป็นอันดับต้น ๆ ได้แก่ Compound, MakerDAO และ Uniswap

6.2.1 Compound

Compound [22] เป็นธุรกิจรับฝากและปล่อยกู้สินทรัพย์ดิจิทัล อธิบายหลักการอย่างง่ายคือ Compound รวบรวมสินทรัพย์ดิจิทัลที่มีผู้ฝากไว้กับ Compound ไปปล่อยกู้

ให้กับผู้ที่สนใจกู้ ผลกำไรจากดอกเบี้ยเงินกู้นำมาตอบแทนคืนผู้ฝาก Compound จึงมีการทำงานคล้ายกับ **ธนาคารพาณิชย์**

เบื้องหลังการทำงานของ Compound ประกอบด้วยสัญญาอัจฉริยะในการคำนวณดอกเบี้ยฝากและดอกเบี้ยกู้โดยคำนวณจากความต้องการในตลาดเวลานั้น ด้วยการใช้สัญญาอัจฉริยะจึงทำให้ ผู้ใช้สามารถสั่งทำธุรกรรม ฝาก ถอน กู้ ชำระหนี้ ได้ตลอดเวลา โดย Compound จะคำนวณดอกเบี้ย กำไร และปรับอัตราดอกเบี้ยอัตโนมัติทุกครั้งที่ทำธุรกรรมและมีผลทันทีที่อีเธอเรียมยืนยันธุรกรรม

เท่ากับว่า Compound คำนวณดอกเบี้ยทบต้น (compound interest) ทุก ๆ block time ของอีเธอเรียม

ความรวดเร็วและเห็นผลลัพธ์ได้ทันที เป็นจุดดึงดูดที่ทำให้ผู้ใช้สนใจฝากโทเคนของคริปโทเคอร์เรนซีสกุลต่าง ๆ กับ Compound เพราะสามารถเห็นรายได้จากดอกเบี้ยเพิ่มขึ้นในเวลาไม่กี่วินาที ไม่เสียเวลาเปิดบัญชี สามารถถอนโทเคนของคริปโทเคอร์เรนซีที่ฝากไว้พร้อมกับดอกเบี้ยได้ตลอดเวลา

เมื่อผู้ใช้ฝากโทเคนของคริปโทเคอร์เรนซีกับ Compound จะได้โทเคน cToken เป็นสิ่งแทนโทเคนคริปโทเคอร์เรนซีที่ฝากไว้ โดย cToken จะมีมูลค่าเท่ากับโทเคนของคริปโทเคอร์เรนซี ณ เวลาที่ฝาก มูลค่าของ cToken ของผู้ฝากจะเพิ่มขึ้นตามอัตราดอกเบี้ยเรื่อย ๆ เมื่อใช้ cToken ถอนสินทรัพย์คืน compound จะแลกเปลี่ยน cToken กลับไปเป็นโทเคนของคริปโทเคอร์เรนซีผู้ใช้ก็จะได้ดอกเบี้ยทบต้นเป็นผลตอบแทน

การกู้คริปโทเคอร์เรนซีใน Compound ใช้วิธีค้ำประกันด้วย cToken โดย Compound จะคำนวณวงเงิน (borrowing capacity) อัตโนมัติจาก cToken ที่นำมาค้ำประกัน แต่ด้วยมูลค่าโทเคนของคริปโทเคอร์เรนซีเปลี่ยนแปลงได้ตลอดเวลา ทำให้มูลค่า cToken ที่นำไปค้ำประกันกับโทเคนของคริปโทเคอร์เรนซีที่กู้เปลี่ยนแปลงได้ตลอดเวลาเช่นกัน หากโทเคนของคริปโทเคอร์เรนซีที่กู้มีมูลค่าเกินวงเงินค้ำประกัน จะเกิดความเสี่ยงที่หนี้จะสูญ Compound จะเริ่มกระบวนการบังคับชำระหนี้ (liquidate) โดยอนุญาตให้ผู้ใช้

รายอื่นจะสามารถชำระหนี้แทนได้และได้รับส่วนลดในการชำระหนี้ เสมือนซื้อโทเคนของคริปโทเคอร์เรนซีได้ในราคาถูกกว่าปกติ การได้รับส่วนลดเป็นแรงจูงใจให้หนี้ได้รับการชำระแทนอย่างรวดเร็ว กลไกบังคับชำระหนี้จะดำเนินไปจนกว่ามูลค่าสินทรัพย์ที่กู้ไม่เกินวงเงิน

Stablecoin เป็นประเภทของโทเคนหรือคริปโทเคอร์เรนซีที่มีการตรึงมูลค่าให้คงที่เมื่อเทียบกับสกุลเงิน คริปโทเคอร์เรนซีอื่น หรือโภคภัณฑ์ที่มีการซื้อขายในตลาด เช่น โลหะมีค่า ทำให้การปั่นราคา (Market Manipulation) ทำได้ยาก จึงมีเสถียรภาพทางการเงินที่ดีกว่าโทเคนหรือคริปโทเคอร์เรนซีที่มักมีมูลค่าลอยตัวตามตลาดซื้อขายแลกเปลี่ยน

ในทางปฏิบัติ มูลค่าของ Stablecoin อาจมีความผันผวนได้ในระยะสั้น ๆ ตามอุปสงค์/อุปทานในตลาด จึงควรเข้าใจว่า Stablecoin มีความผันผวนของมูลค่าต่ำ แต่ไม่ได้มีมูลค่าคงที่ตลอดเวลา

Compound รองรับคริปโทเคอร์เรนซีที่เป็น Stablecoin ด้วย เช่น Dai, USDC, USDT เป็นต้น ผู้กู้ Stablecoin จะสามารถแลกเปลี่ยนคริปโทเคอร์เรนซีเป็นเงินตราในอัตราแลกเปลี่ยน 1:1 ได้ ความเสี่ยงจากความผันผวนของอัตราแลกเปลี่ยนมีน้อยมาก ผู้กู้ใช้เงินตราแลกเป็น Stablecoin ใช้หนี้ Compound ได้โดยไม่ต้องกังวลกับความผันผวนของอัตราแลกเปลี่ยนเหมือนคริปโทเคอร์เรนซีอื่น ๆ การกู้ Stablecoin จึงเป็นทางเลือกหนึ่งในการบริหารสภาพคล่อง สำหรับผู้ที่ถือคริปโทเคอร์เรนซีไว้อยู่แล้ว

ขณะเดียวกัน คริปโทเคอร์เรนซีที่มีอัตราแลกเปลี่ยนผันผวนสูงก็ได้รับความนิยมในการลงทุนด้วย Compound จึงมักเป็นจุดเริ่มต้นสำหรับนักลงทุนคริปโทเคอร์เรนซีที่หาผลกำไรจากส่วนต่างทั้ง ฝากเข้า Compound เพื่อ long และ กู้ Compound เพื่อ short

การลงทุนหน่วยลงทุนซื้อขายล่วงหน้า โดยทั่วไปมักคาดหวังผลกำไรจากมูลค่าที่เพิ่มขึ้นในอนาคต (ซื้อถูก ขายแพง) เรียกว่า long position

มีการลงทุนอีกประเภทที่ทำกำไรจากมูลค่าที่ลดลง โดยการยืมหน่วยลงทุนมาถือไว้ในระยะสั้น หากมูลค่าหน่วยลงทุนลดลง ผู้ลงทุนจะสามารถซื้อหน่วยลงทุนเพื่อใช้คืนในราคาที่ถูกกว่าและได้กำไรจากผลต่าง เรียกว่า short position

Compound มีกลไกการควบคุมการทำงานของสัญญาอัจฉริยะโดยชุมชนด้วยโทเคน COMP ผู้ที่ถือโทเคน COMP มีสิทธิเสนอและโหวตให้เปลี่ยนแปลงการทำงานของสัญญาอัจฉริยะของ Compound ได้ หรือโอนสิทธิให้ผู้อื่นโหวตแทนก็ได้ วิธีนี้ทำให้สัญญาอัจฉริยะของ Compound มีความยืดหยุ่นการรองรับคริปโทเคอร์เรนซีสกุลใหม่ เพิ่มความสามารถใหม่ เปลี่ยนอัตราในการคำนวณ หรือสูตรคำนวณทางการเงินต่าง ๆ ได้

โทเคนที่ให้สิทธิในการกำกับควบคุมสัญญาอัจฉริยะ จัดว่าเป็น utility token แบบหนึ่ง มีชื่อเฉพาะเรียกว่า governance token โทเคนประเภทนี้อาจมีการซื้อขายแลกเปลี่ยนในตลาดคริปโคเคอร์เรนซีด้วย บางครั้งจึงเรียกกันว่าเป็น governance coin

การใช้ประโยชน์จาก governance token อาจมีความแตกต่างไปในแต่ละสัญญาอัจฉริยะ บางระบบใช้ซ้ำได้ไม่จำกัดครั้ง บางระบบจะทำลายโทเคนทิ้งเมื่อมีการใช้สิทธิไปแล้ว

การกระจายผู้ถือเหรียญ COMP การส่งข้อเสนอ และการโหวต จึงเป็นกลไกที่ Compound ใช้กระจายอำนาจ และสร้างความโปร่งใส การเสนอและโหวตทุกครั้งจะเปิดเผยต่อสาธารณะ มีเวลาโหวต 3 วัน หากโหวตชนะ จะใช้เวลาปรับการทำงานตามข้อเสนอ (Time Lock) อย่างน้อย 2 วัน

การกระจายอำนาจสู่ชุมชน กับสัญญาอัจฉริยะที่ทำงานอัตโนมัติ และธุรกรรมบล็อกเชนที่มีความน่าเชื่อถือ ทำให้ Compound เป็นบริษัทที่มีพนักงานเพียงสิบกว่าคน แต่มีคริปโทเคอร์เรนซีฝากอยู่กับสัญญาอัจฉริยะของ Compound มูลค่ามากกว่า 8,000 ล้านเหรียญสหรัฐ และเป็นหนึ่งในไม่กี่ DeFi ที่เคยถือครองโทเคนของคริปโทเคอร์เรนซีเกิน 10,000 ล้านเหรียญสหรัฐ

เนื่องจาก DeFi เป็นเพียงสัญญาอัจฉริยะ ไม่มีมูลค่าในตัวเอง ในบริบทของ DeFi จึงนิยมใช้ Total Value Locked (TVL) เป็นตัววัดมูลค่าแทน โดย TVL คำนวณได้จากผลรวมของมูลค่าคริปโทเคอร์เรนซีที่ถือครองโดยสัญญาอัจฉริยะหรือ DeFi นั้น

6.2.2 MakerDAO

การตรึงราคา Stablecoin หลาย ๆ สกุลเลือกใช้ทุนสำรองค้ำประกัน เช่น USDT ของ Tether [23] และ USDC ของ Circle [24] ซึ่งใช้เงินดอลลาร์สหรัฐค้ำประกัน คล้ายกับทุนสำรองค้ำประกันในการผลิตเหรียญหรือธนบัตรที่ใช้ทองคำ พันธบัตรหรือเงินตราสกุลอื่นที่มีความมั่นคงสูง

การใช้ทุนสำรองที่บริหารจัดการอยู่นอกบล็อกเชน ทำให้จำเป็นต้องมีกลไกกำกับดูแลทางการเงินที่เข้มงวด ต้องพึ่งพาผู้ตรวจสอบบัญชีภายนอกที่มีความน่าเชื่อถือสูง ซึ่งเป็นภาระค่าใช้จ่ายในการดำเนินกิจการ

MakerDAO [25] เสนอวิธีการใหม่ในการผลิตโทเคนที่เป็น Stablecoin โดยใช้โทเคนของคริปโทเคอร์เรนซีเป็นทุนสำรองค้ำประกัน โทเคนที่ MakerDAO ผลิตมีชื่อว่า Dai เป็น Stablecoin ที่ตรึงมูลค่าเท่ากับ 1 ดอลลาร์สหรัฐ MakerDAO เรียกสัญญาอัจฉริยะสำหรับผลิต Dai ว่า Collateralized Debt Position (CDP)

Tether เป็นบริษัทแรก ๆ ที่เริ่มทำธุรกิจในการผลิตโทเคนเป็น Stablecoin เข้าสู่บล็อกเชน โดยใช้วิธีค้ำประกันด้วยเงินตราโดยฝากเข้าทุนสำรองของบริษัทโดยรักษาทุนสำรองให้ไม่น้อยกว่าจำนวนโทเคนที่หมุนเวียน ณ เวลานั้น

ตัวอย่างเช่น โทเคน USDT เป็นโทเคนของ Tether ที่ตรึงกับเงินสกุลดอลลาร์สหรัฐ โดยหลักการแล้ว 1 USDT จะมีมูลค่าคงที่เท่ากับ 1 USD การผลิต USDT เพิ่มเข้าในเครือข่ายบล็อกเชนจะต้องมีเงินฝากเข้าทุนสำรองที่เท่ากัน และการถอนเงินจากทุนสำรองจะต้องทำลาย USDT จำนวนเท่ากันด้วย

Tether ทำกำไรจากค่าธรรมเนียมฝาก-ถอนเงินตราในการแลกเปลี่ยนเป็นโทเคน ปัจจุบันมีการใช้งานในเครือข่ายบิตคอยน์ อีเธอเรียม EOS, Tron, Algorand, SLP และ OMG โดยตรึงค่าโทเคน USDT, EURT, และ CNHT กับสกุลเงิน USD, EUR และ CNH ในอัตรา 1:1 ตามลำดับ

ในปี ค.ศ. 2021 สินทรัพย์รวมของ Tether มีมูลค่ามากกว่า 40,000 ล้านเหรียญสหรัฐ

Tether ถูกตั้งคำถามบ่อยครั้งถึงความโปร่งใสของการจัดการทุนสำรอง และยังไม่สามารถแสดงหลักฐานการตรวจสอบที่เชื่อถือได้ว่ามีทรัพย์สินในกองทุนมากกว่าโทเคนที่หมุนเวียนจริง

การทำงานของ CDP เริ่มต้นที่ผู้ใช้ฝาก ETH เข้าใน CDP เป็นสินทรัพย์ค้ำประกัน CDP จะคำนวณมูลค่าของ ETH ที่รับฝากเป็นเงินเหรียญสหรัฐ และกำหนดวงเงินที่สามารถสร้างเหรียญ Dai ออกมาตาม liquidation ratio ผู้ใช้สามารถผลิต Dai เท่าไหร่ก็ได้ แต่ไม่เกินวงเงินที่กำหนดไว้ Dai ที่ผลิตขึ้นมาจะถูกโอนให้กับผู้ใช้ตามจำนวนที่สั่งผลิต เมื่อผู้ใช้

ชำระคืน Dai พร้อมกับดอกเบี้ย CDP จะทำลาย Dai ทิ้งแล้วจึงปลดล็อกให้ผู้ใช้ถอนสินทรัพย์ค้ำประกันคืน

การผลิตและทำลาย Dai และการมีสินทรัพย์ค้ำประกัน จึงมักเปรียบเทียบ MakerDAO ว่าทำงานลักษณะเดียวกับ**ธนาคารกลางของประเทศ**ที่มีอำนาจผลิตและทำลายธนบัตรของสกุลเงินตราภายใต้อำนาจควบคุม (Monetary Sovereignty)

เนื่องจากสินทรัพย์ค้ำประกันมีมูลค่าเปลี่ยนแปลงได้ CDP จึงต้องคำนวณมูลค่าสินทรัพย์ค้ำประกันตลอดเวลา หากสินทรัพย์ค้ำประกันมีมูลค่าต่ำกว่า Dai ที่ผลิตจากสินทรัพย์ค้ำประกันนั้น CDP จะเริ่มกระบวนการบังคับชำระหนี้อัตโนมัติโดยนำสินทรัพย์ค้ำประกันมาขายทอดตลาดด้วยการประมูลในจำนวนที่หักล้างหนี้และค่าปรับได้หมด

สูตรคำนวณทางการเงินของ MakerDAO ประกอบกับการกำหนดอัตราต่าง ๆ และการประมูลเพื่อล้างหนี้เสียทำให้ MakerDAO แทบไม่มีโอกาสจะขาดทุนเพราะหนี้เสียเลย

MakerDAO มีการกำกับดูแลโดยชุมชนในลักษณะคล้ายกับ Compound โดยใช้ governance token ชื่อ MKR

MKR ผลิตเริ่มต้นทั้งหมด 1,000,000 โทเคน ใช้สำหรับโหวตเปลี่ยนแปลงอัตราต่าง ๆ เช่น liquidation ratio, liquidation penalty, stability fee หรือควบคุมการทำงานของ CDP เช่น สั่งหยุดทำงานกรณีฉุกเฉิน MKR ยังใช้ในกระบวนการอื่น ๆ ที่เกี่ยวข้องกับการกำกับดูแลด้วย เช่น ใช้เพิ่มทุนในระบบ กรณีที่ไม่สามารถตรึงราคาได้ตามกระบวนการปกติ

ปี ค.ศ. 2021 MakerDAO ถือสินทรัพย์ดิจิทัลมูลค่ารวมมากกว่า 10,000 ล้านเหรียญสหรัฐ เป็นหนึ่งใน DeFi ที่ถือครองสินทรัพย์ดิจิทัลมูลค่าสูงสุดในบรรดา DeFi ด้วยกัน

โดยหลักการแล้ว การนำสินทรัพย์ค้ำประกันขายทอดตลาดโดยการประมูลอัตโนมัติ จะไม่มีทางทำให้ MakerDAO ขาดทุนได้ จนกระทั่งมีผู้พบจุดอ่อนของ CDP ในการขายทอดตลาด เหตุการณ์นี้เป็นที่รู้จักในชื่อ Black Thursday เกิดขึ้นในวันที่ 12-13 มีนาคม ค.ศ. 2020

Black Thursday เกิดจากปัจจัยหลักคือความคับคั่งของธุรกรรมบนเครือข่ายอีเธอเรียม ทำให้มีการแข่งขันจ่ายค่า gas ที่สูงขึ้น อัตราแลกเปลี่ยน ETH จึงสูงขึ้นตามไปด้วย ความคับคั่งของธุรกรรมบนอีเธอเรียมยังทำให้ CDP ไม่ได้รับข้อมูลอัตราแลกเปลี่ยนของ ETH เป็นระยะเวลานาน ข้อมูลที่ใช้คำนวณตามสูตรบังคับชำระหนี้จึงไม่เป็นปัจจุบัน

จนเมื่อปัญหาความคับคั่งของธุรกรรมคลี่คลายแล้ว CDP จึงสามารถปรับอัตราแลกเปลี่ยนของ ETH ได้ แล้วพบว่าอัตราแลกเปลี่ยน ETH สูงขึ้นมาก จนทำให้เกิดการบังคับชำระหนี้อัตโนมัติโดยมี Dai ที่ถูกบังคับชำระหนี้คราวเดียวกันเป็นจำนวนราว 5 ล้าน Dai

เวลานั้น CDP จึงนำ ETH มาขายทอดตลาดด้วยการประมูลเป็นจำนวนมาก แต่กลับไม่มีคนเข้าประมูลมากนัก สาเหตุมาจากสคริปต์ประมูลอัตโนมัติของ MakerDAO ที่ผู้ใช้ส่วนใหญ่ใช้งานอยู่ไม่ยอมทำงานเพราะ gas สูงเกินไป

ปรากฏว่ามีผู้เห็นโอกาสที่ไม่มีผู้ยื่นประมูล จึงยื่นประมูล ETH ที่ขายทอดตลาดในเวลานั้นด้วย 0 Dai และชนะการประมูลได้จริง ๆ ผลคือสินทรัพย์ค้ำประกันใน CDP มากกว่า 60,000 ETH มูลค่ามากกว่า 8 ล้านเหรียญสหรัฐ ถูกประมูลออกไปด้วย 0 Dai

Black Thursday ทำให้ MakerDAO ขาดทุนจากการขายสินทรัพย์ในราคาต่ำกว่าทุนเป็นครั้งแรก และไม่สามารถตรึงราคา Dai ให้คงที่ได้

ผู้ถือโทเคน MKR ถือว่าเป็นผู้มีส่วนได้ส่วนเสียในธุรกิจของ MakerDAO ยอมขายโทเคน MKR แลกเป็นโทเคน Dai จำนวน 4.5 ล้าน Dai เพื่อชดเชยที่ขาดทุน Dai จึงกลับมาตรึงราคาได้อีกครั้ง

6.2.3 Uniswap

บิตคอยน์ อีเธอเรียม และคริปโทเคอร์เรนซีอื่น ๆ ทำให้เกิดธุรกิจซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซีโดยใช้วิธีการรับฝากสินทรัพย์ (custodian) รับคำสั่งซื้อขายและจับคู่ราคา และสามารถซื้อขายแลกเปลี่ยนสินทรัพย์ดิจิทัลเป็นเงินตราได้ คล้ายกับการซื้อขายหลักทรัพย์

ธุรกิจซื้อขายแลกเปลี่ยนสินทรัพย์ดิจิทัลลักษณะนี้ อำนาจการจัดการสินทรัพย์ทั้งหมดอยู่ที่เจ้าของธุรกิจ จึงเรียกว่าเป็น Centralized Exchange (CEX) ผู้ใช้ไม่ได้ทำธุรกรรมกับสินทรัพย์ดิจิทัลโดยตรง แต่ผ่านคำสั่งซื้อขายแลกเปลี่ยนบนระบบสารสนเทศของ CEX อีกที กรณีนี้ CEX จึงเป็น trusted third party ที่ผู้ซื้อขายแลกเปลี่ยนจำเป็นต้องมอบความไว้ใจ และเนื่องจาก CEX เป็นที่รับฝากคริปโทเคอร์เรนซี จึงเป็นเป้าหมายของมิจฉาชีพในการโจมตีเพื่อโจรกรรมคริปโทเคอร์เรนซี CEX แทบทุกแห่งจึงมีต้นทุนในการบริหารจัดการให้ระบบมีความมั่นคงปลอดภัยและกลไกมีความโปร่งใส ตรวจสอบได้ทั้งด้านเทคโนโลยีสารสนเทศและบัญชีการเงิน

หลังจากมีสัญญาอัจฉริยะบนเครือข่ายอีเธอเรียมและคริปโทเคอร์เรนซีที่ใช้โทเคน ERC-20 จึงเริ่มมีความพยายามพัฒนาสัญญาอัจฉริยะที่ทำให้สามารถซื้อขายแลกเปลี่ยนได้โดยไม่ต้องอาศัยตัวกลาง เรียกว่าเป็น Decentralized Exchange (DEX)

Uniswap [26] [27] [28] เป็น DEX รายแรก ๆ ที่พัฒนาสัญญาอัจฉริยะเป็น Automated Market Maker (AMM) ผู้ใช้งานสามารถโต้ตอบกับสัญญาอัจฉริยะได้โดยตรงแลกเปลี่ยนสินทรัพย์ดิจิทัล (swap) ได้ทันทีโดยไม่ต้องรอจับคู่ราคา

กลไกการทำงานของ Uniswap ใช้วิธีสร้าง pool ของคู่สินทรัพย์ที่รับฝากจาก liquidity providers ผู้ฝากจะได้รับ liquidity token คืนเป็นสิ่งแทนการรับฝาก อัตราแลกเปลี่ยนของสินทรัพย์จะเป็นไปตามจำนวนโทเคนของคู่ของสินทรัพย์นั้น โดยคำนวนได้จากสมการ Constant Product Market Maker Model

$$x \times y = k$$

Uniswap เก็บค่าธรรมเนียมธุรกรรมโดยหักจากสินทรัพย์ที่นำมาแลกเปลี่ยนในอัตราร้อยละ 0.3 โดย Uniswap นำค่าธรรมเนียมทั้งหมดจ่ายเป็นค่าตอบแทนให้กับ liquidity pool ที่เกิดธุรกรรมนั้น เพื่อเป็นการสร้างแรงจูงใจให้กับ liquidity providers

Uniswap อาศัยการทำกำไรจากผลต่างอัตราแลกเปลี่ยน (arbitrage) เป็นเครื่องมือในการปรับอัตราแลกเปลี่ยนให้ใกล้เคียงกับตลาดในเวลานั้น ตัวอย่างเช่น CEX หรือ DEX แห่งหนึ่งที่มีอัตราแลกเปลี่ยน 1 ETH ต่อ 200 Dai ในขณะที่ Uniswap มีอัตราแลกเปลี่ยน 1 ETH ต่อ 100 Dai จะเป็นโอกาสให้มีผู้ทำกำไรจากผลต่างอัตราแลกเปลี่ยน โดยนำ 1 ETH ไปแลก 200 Dai ที่ CEX แล้วนำ 200 Dai ที่ได้มาแลกที่ Uniswap ได้ 2 ETH ซึ่งเท่ากับว่า ETH pool จะเล็กลงและ Dai pool จะใหญ่ขึ้นการทำกำไรนี้จะเกิดขึ้นไปจนกว่าไม่สามารถทำกำไรจากผลต่างอัตราแลกเปลี่ยน ซึ่งเท่ากับว่าอัตราแลกเปลี่ยนของ Uniswap ใกล้เคียงกับตลาดแล้วนั่นเอง

Uniswap มี governance coin ชื่อ UNI แจกจ่ายให้กับผู้ใช้ไปเมื่อเดือนกันยายน ค.ศ. 2020 ผู้ถือ UNI มีสิทธิโหวตข้อเสนอต่าง ๆ ในการควบคุมการทำงานสัญญาอัจฉริยะของ Uniswap

ปี ค.ศ. 2021 Uniswap เป็น DEX ที่มีการแลกเปลี่ยนสินทรัพย์มากที่สุดใน DeFi มี TLV มากกว่า 5,000 ล้านเหรียญสหรัฐ ธุรกรรมแลกเปลี่ยนสินทรัพย์ไปแล้วมากกว่า 10,000 ล้านเหรียญสหรัฐ และมีหลายครั้งที่เกิดการแลกเปลี่ยนมากกว่า 1,000 ล้านเหรียญสหรัฐในวันเดียว

ตัวอย่างการคำนวณอัตราแลกเปลี่ยน สมมติว่า ETH-Dai pool มีการฝาก 10 ETH และ 1000 Dai จะได้ว่า

$k = 10 \times 1{,}000 = 10{,}000$

หากมีผู้ต้องการแลก 1 ETH เป็น Dai เมื่อหักค่าธรรมเนียม 0.3% แล้วจะทำให้ ETH pool เพิ่มขึ้น

ETH pool = 10 + 1 - (0.003) = 10.997

และ Dai pool จะต้องลดลง

Dai pool = 10,000/10.997 = 909.338911

1 ETH จึงแลกได้

1,000 - 909.338911 = 90.661089 Dai

หลังจากสั่งแลกเปลี่ยนแล้ว Uniswap จะบวกค่าธรรมเนียม 0.3% กลับเข้า ETH pool และคำนวณค่า k ใหม่

$k = (10.997 + 0.003) \times 909.338911 = 10{,}002.728021$

6.2.4 Aave

Aave [29] เป็น DeFi บริการสินเชื่อและ DEX คล้าย ๆ กับ Compound, MakerDAO และ Uniswap แต่เพิ่มบริการที่ DeFi อื่นไม่เคยมีมาก่อนคือ Flash loan

Flash loan เป็นการยืมสินทรัพย์ดิจิทัลโดยไม่ต้องใช้สินทรัพย์ค้ำประกัน แต่จะต้องคืนสินทรัพย์ที่ยืมพร้อมกับค่าธรรมเนียมภายใน 1 บล็อกธุรกรรม หากไม่สามารถคืนสินทรัพย์พร้อมค่าธรรมเนียมได้ตามกำหนด ธุรกรรมทั้งหมดจะย้อนค่ากลับ เสมือนกับไม่เกิดอะไรขึ้น

Flash loan ของ Aave มีค่าธรรมเนียมที่ 0.09% ค่าธรรมเนียมที่ค่อนข้างต่ำ ทำให้มีการนำ flash loan ไปใช้ในหลายรูปแบบ เช่น ทำกำไรจาก arbitrage สลับสินทรัพย์ค้ำประกันใน Compound หรือ MakerDAO และทำ self-liquidation เพื่อไม่ให้ถูกปรับ

ภาพที่ 11 ตัวอย่างการทำ arbitrage คริปโทเคอร์เรนซีบนบล็อกเชน

ตัวอย่าง arbitrage ด้วย flash loan ในธุรกรรม 0x01afae47b0c98731b5d20c776e58bd8ce5c2c89ed4bd3f8727fad3ebf32e9481 [30]

ธุรกรรมนี้เป็นสัญญาอัจฉริยะ arbitrage มีลำดับการทำงานดังนี้

- flash loan 405,067.106448 USDC จาก dYdX
- swap 450,000 USDC เป็น 1,071.715628795502233433 Ether บน Uniswap
- swap 1,071.715628795502233433 Ether เป็น 492,798.99809 USDT บน Uniswap
- swap 492,798.99809 USDT เป็น 492,730.278141 USDC บน Curve.fi
- repay 405,067.10645 USDC ให้ dYdX

ผลต่างที่ได้ในธุรกรรมนี้คือ 492,730.278141 - 405,067.10645 = 87,663.171691 USDC

เมื่อหักต้นทุนที่เติมเข้า swap 450,000 - 405,067.106448 = 44,932.893552 USDC

เท่ากับได้กำไร 87,663.171691- 44,932.893552 = 42,730.278139 USDC

จุดที่สามารถทำ arbitrage สำหรับธุรกรรมนี้คืออัตราแลกเปลี่ยน USDC-ETH กับ ETH-USDT บน Uniswap ซึ่งปกติ 1 USDC ควรจะเท่ากับ 1 USDT เพราะเป็น Stablecoin ตรึงกับเหรียญสหรัฐทั้งคู่ แต่ Uniswap ใช้สถานะ pool ในการคำนวณอัตราแลกเปลี่ยน ไม่ได้ใช้ราคาตลาด จึงทำ arbitrage ได้

นอกจาก Aave แล้ว dYdX เป็น DeFi อีกแห่งที่สามารถเรียกใช้ฟังก์ชันการยืมสินทรัพย์ดิจิทัลทำธุรกรรมเลียนแบบ flash loan ของ Aave ได้ ความสามารถนี้ไม่ได้ระบุอยู่ในการให้บริการของ dYdX และไม่มีเอกสารเผยแพร่วิธีการใช้งาน แต่ได้รับความนิยมในการทำ flash loan พอสมควรเนื่องจากไม่มีค่าธรรมเนียมธุรกรรม มีเพียงเงื่อนไขที่ต้องคืนสินทรัพย์มากกว่าที่ยืมไป 2 wei เท่านั้น

7 การกำกับดูแลสินทรัพย์ดิจิทัล

คริปโทเคอร์เรนซีมีอัตราแลกเปลี่ยนให้เป็นไปตามอุปสงค์และอุปทานในตลาด ทำให้มุมมองที่มีต่อคริปโทเคอร์เรนซีกลายเป็นเรื่องการลงทุนมากกว่าจะเป็นสื่อในการชำระค่าสินค้าหรือบริการ นอกจากนี้การลงทุนกับคริปโทเคอร์เรนซียังทำให้เกิดการแข่งขันกำหนดอัตราค่าธรรมเนียมเพื่อให้ธุรกรรมได้รับการยืนยันก่อน ค่าธรรมเนียมธุรกรรมจึงสูงขึ้นจนไม่คุ้มกับการใช้คริปโทเคอร์เรนซีในการทำธุรกรรมทางการเงินทั่วไป การใช้จ่ายด้วยคริปโทเคอร์เรนซีในปัจจุบัน จึงเกิดขึ้นกับสินค้าที่มีมูลค่าสูง มีเวลารอยืนยันธุรกรรม เช่น รถยนต์ หรืออสังหาริมทรัพย์ การทำธุรกรรมที่ต้องการเลี่ยงการตรวจสอบหรือติดตามเส้นทางทางการเงิน เช่น เป็นช่องทางการโอนเงินของมิจฉาชีพ หรือเป็นช่องทางชำระค่าไถ่ของมัลแวร์เรียกค่าไถ่ (ransomware)

มัลแวร์เรียกค่าไถ่ (ransomware) เป็นซอฟต์แวร์ไม่พึงประสงค์ (malicious software หรือ malware) ประเภทหนึ่ง

มัลแวร์เรียกค่าไถ่ทำงานโดยเข้ารหัสลับไฟล์ข้อมูลในคอมพิวเตอร์ เช่น ไฟล์ภาพ เอกสาร วิดีโอ ทำให้ผู้ใช้ไม่สามารถเปิดไฟล์ได้ตามปกติ หากผู้ใช้พยายามจะเปิดไฟล์ มัลแวร์เรียกค่าไถ่จะแสดงข้อความบังคับให้ผู้ใช้จ่ายค่ากุญแจในการถอดรหัสลับไฟล์นั้น ซึ่งส่วนมากให้จ่ายเป็นคริปโทเคอร์เรนซี

คริปโทเคอร์เรนซีจึงมีสถานะเป็นเสมือนเงินตราหรือสื่อในการชำระค่าสินค้าหรือบริการ และเป็นสินทรัพย์ในการลงทุน สถานะทั้งสองอย่างนี้เป็นหลักที่หลายประเทศยกมาพิจารณาในการกำกับดูแลคริปโทเคอร์เรนซีเพื่อคุ้มครองประชาชน ซึ่งอาจส่งผลกระทบต่อการประยุกต์ใช้บล็อกเชนและสัญญาอัจฉริยะ

ในส่วนนี้เราจะยกตัวอย่างการกำกับดูแลคริปโทเคอร์เรนซีและสินทรัพย์ดิจิทัลในประเทศสหรัฐอเมริกา สหภาพยุโรป ออสเตรเลีย ญี่ปุ่น สิงคโปร์ เปรียบเทียบกับประเทศไทย

7.1 คริปโทเคอร์เรนซีคือเงินตรา?

กฎหมายของหลาย ๆ ประเทศไม่ได้มีการกำหนดนิยามของคำว่าคริปโทเคอร์เรนซีโดยตรง แต่มักถือว่าคริปโทเคอร์เรนซีเป็นส่วนหนึ่งของสื่อในการชำระเงินในรูปแบบอิเล็กทรอนิกส์หรือดิจิทัล

ประเทศออสเตรเลีย เป็นประเทศแรก ๆ ที่มีการกำหนดนิยามในลักษณะนี้ โดยให้กำหนดในนิยามของคำว่า สกุลเงินดิจิทัล (Digital Currency) ในกฎหมาย Anti-Money Laundering and Counter-Terrorism Financing Act:

> “digital currency means:
>
> (a) a digital representation of value that:
>
> (i) functions as a medium of exchange, a store of economic value, or a unit of account; and
>
> (ii) is not issued by or under the authority of a government body; and
>
> (iii) is interchangeable with money (including through the crediting of an account) and may be used as consideration for the supply of goods or services; and

(iv) is generally available to members of the public without any restriction on its use as consideration; or

(b) a means of exchange or digital process or crediting declared to be digital currency by the AML/CTF Rules;

but does not include any right or thing that, under the AML/CTF Rules, is taken not to be digital currency for the purposes of this Act." [31] [32]

ประเทศญี่ปุ่น การกำหนดนิยามนี้ในกฎหมาย Payment Service Act ปี ค.ศ. 2009 โดยใช้คำว่า สกุลเงินเสมือน (Virtual Currency)

The term "Virtual Currency" as used in this Act means any of the following:

(i) property value (limited to that which is recorded on an electronic device or any other object by electronic means, and excluding the Japanese currency, foreign currencies, and Currency-Denominated Assets; the same applies in the following item) which can be used in relation to unspecified persons for the purpose of paying consideration for the purchase or leasing of goods or the receipt of provision of services and can also be purchased from and sold to unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system; and

(ii) property value which can be mutually exchanged with what is set forth in the preceding item with unspecified persons acting as counterparties, and which can be transferred by means of an electronic data processing system [33]

ประเทศสหรัฐอเมริกา ได้กำหนดนิยามเงินเสมือนในลักษณะเดียวกัน โดย Financial Crimes Enforcement Network (FinCEN) ของกระทรวงการคลัง (U.S. Department of the Treasury) ได้กำหนดนิยามเงินเสมือนไว้ในปี ค.ศ. 2013 ว่า

"a medium of exchange that operates like a currency in some environments, but does not have all the attributes of real currency. In particular, virtual currency does not have legal tender status in any jurisdiction" [34]

ในปี ค.ศ. 2014 Internal Revenue Service (IRS) ซึ่งมีหน้าที่ในการจัดเก็บภาษีภายในสหรัฐอเมริกากำหนดนิยามว่าคริปโทเคอร์เรนซี (Cryptocurrency) ว่าเป็นรูปแบบหนึ่งของเงินเสมือน ซึ่งมีความหมายว่า

> "a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value that does not have legal tender status in any jurisdiction" [35]

ประเทศสิงคโปร์ นิยามคริปโทเคอร์เรนซีโดยถือเป็นส่วนหนึ่งของ Digital Payment Token (DPT) ซึ่งนิยามไว้ใน Payment Services Act ปี ค.ศ. 2019 [36]

> "digital payment token" means any digital representation of value (other than an excluded digital representation of value) that --
>
> (a) is expressed as a unit;
>
> (b) is not denominated in any currency, and is not pegged by its issuer to any currency;
>
> (c) is, or is intended to be, a medium of exchange accepted by the public, or a section of the public, as payment for goods or services or for the discharge of a debt;
>
> (d) can be transferred, stored or traded electronically; and
>
> (e) satisfies such other characteristics as the Authority may prescribe

สหภาพยุโรป โดย European Securities and Markets Authority (ESMA) ไม่ได้กำหนดนิยามคริปโทเคอร์เรนซี แต่ใช้คำใกล้เคียงกันมากคือคำว่า crypto-asset

> "A type of private asset that depends primarily on cryptography and Distributed Ledger Technology (DLT) or similar technology as part of their perceived or inherent value. Unless otherwise stated, ESMA uses the term to refer to both so-called 'virtual currencies' and 'digital tokens'. Crypto-asset additionally means an asset that is not issued by a central bank." [37]

จะเห็นได้ว่าประเทศและกลุ่มประเทศที่ยกตัวอย่างนี้ แม้จะใช้คำทางกฎหมายที่ต่างกันไปบ้าง แต่มีนิยามที่ใกล้เคียงกันมาก กล่าวโดยสรุป คริปโทเคอร์เรนซีคือ:

- สิ่งแทนค่าในรูปแบบอิเล็กทรอกนิกส์หรือดิจิทัล
- นำมาใช้จ่ายหรือชำระสินค้าหรือบริการได้
- อยู่ภายใต้การกำกับดูแลเพื่อต่อต้านการฟอกเงินหรือสนับสนุนการเงินในการก่อการร้าย (AML/CTF) ของ Financial Action Task Force (FATF)
- ไม่ถือเป็นสกุลเงินตราที่ออกโดยธนาคารกลางของประเทศ **ไม่มีสภาพที่ใช้ชำระหนี้ได้ตามกฎหมาย (legal tender)** เหมือนกับเหรียญหรือธนบัตรที่เงินตราสกุลต่าง ๆ กำหนดไว้

ประเทศเอลซัลวาดอร์เป็นประเทศแรกที่ออกกฎหมายรับรองว่าบิตคอยน์เป็นสกุลเงินตราที่มีสภาพที่ใช้ชำระหนี้ได้ตามกฎหมายเมื่อเดือนมิถุนายน ค.ศ. 2021 [38] นอกจากประเทศเอลซัลวาดอร์แล้วไม่มีประเทศใดเลยที่ถือว่าบิตคอยน์หรือคริปโทเคอร์เรนซีอื่น ๆ เป็นสกุลเงินตรา

สำหรับ **ประเทศไทย** การกำกับดูแลเงินและการชำระเงินอยู่ภายใต้อำนาจของธนาคารแห่งประเทศไทยซึ่งเคยให้ข้อมูลเกี่ยวกับบิตคอยน์และหน่วยข้อมูลทางอิเล็กทรอนิกส์ที่ลักษณะใกล้เคียงกัน (รวมถึงคริปโทเคอร์เรนซี) เมื่อวันที่ 18 มีนาคม พ.ศ. 2557 ว่าไม่ถือเป็นเงินที่ชำระหนี้ได้ตามกฎหมาย ไม่มีมูลค่าในตัวเอง และไม่ได้เป็นสื่อในการชำระเงินตามกฎหมาย จึงมีความเสี่ยงที่ไม่ได้รับการคุ้มครองจากกฎหมายทางการเงิน [39] [40]

7.2 คริปโทเคอร์เรนซีคือสินทรัพย์?

การที่คริปโทเคอร์เรนซีมีมูลค่าจากอุปสงค์/อุปทาน ทำให้มุมมองของผู้ใช้งานที่ผ่านมาตั้งแต่อดีตจนถึงปัจจุบัน เห็นคริปโทเคอร์เรนซี เป็นสินทรัพย์ในการลงทุน มากกว่าเป็นสกุลเงินตราเพื่อใช้จ่าย หลายประเทศจึงมีกฎหมายในการกำกับดูแลการลงทุนในคริปโทเคอร์เรนซีโดยหน่วยงานรัฐที่เกี่ยวข้องกับการลงทุนในสินทรัพย์

ประเทศสหรัฐอเมริกา กำหนดให้ธุรกิจซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซี (Exchange) จะต้องปฏิบัติตามกฎหมายความลับทางธนาคาร (Bank Secrecy Act: BSA) และต้องขึ้นทะเบียนเป็นธุรกิจที่ให้บริการทางการเงิน (Money Service Business: MSB) ซึ่งมีหน้าที่ปฏิบัติตามกฎหมายต่อต้านการฟอกเงิน มีกระบวนการพิสูจน์ตัวตนลูกค้า (Know Your Customer: KYC) และการตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้า (Customer Due Diligence: CDD) รวมถึงรายงานการเคลื่อนไหวทางการเงินที่ผิดปกติ

ในปี ค.ศ. 2014 Commodity Futures Trading Commission (CFTC) ซึ่งกำกับดูแลการซื้อขายในตลาดอนุพันธ์ของสหรัฐอเมริกาประกาศว่าเงินเสมือนตามนิยามของ IRS ถือเป็นโภคภัณฑ์ตามกฎหมายซื้อขายแลกเปลี่ยนโภคภัณฑ์ (Commodities Exchange Act) [41] ซึ่งทำให้สินทรัพย์ดิจิทัลสามารถซื้อขายแลกเปลี่ยนในตลาดอนุพันธ์ เช่น การทำสัญญาซื้อขายล่วงหน้า และทำให้มีการบังคับใช้ระเบียบที่เกี่ยวข้องได้ตามกฎหมายเช่น สั่งปรับ หรือ สั่งระงับการซื้อขาย เช่นเดียวกับโภคภัณฑ์อื่น ๆ

นอกเหนือจากการกำกับดูแลธุรกิจซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซีและการกำกับในลักษณะเป็นโภคภัณฑ์แล้ว การกำกับดูแลกิจการที่เกี่ยวข้องกับสินทรัพย์ดิจิทัลอื่น ๆ โดยเฉพาะการลงทุนด้วยการเสนอขายโทเคนดิจิทัล (Initial Coin Offering: ICO) ในสหรัฐอเมริกายังไม่มีการออกกฎระเบียบหรือนิยามในการกำกับดูแลที่ชัดเจน

คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ของสหรัฐอเมริกา (U.S. Securities and Exchange Commission: SEC) ให้ความเห็นว่าธุรกรรมที่เกี่ยวข้องกับสินทรัพย์ดิจิทัลและ ICOs อาจเป็นสัญญาการลงทุน (investment contracts) [42] [43] ซึ่ง

ถือเป็นหลักทรัพย์ (Securities) ที่อยู่ภายใต้การกำกับดูแลโดยกฎหมายหลักทรัพย์ (Securities Act) และกฎหมายตลาดหลักทรัพย์ (Securities Exchange Act)

ในสหรัฐอเมริกา การพิจารณาว่าธุรกรรมเป็นสัญญาการลงทุนหรือไม่ อ้างอิงจากข้อพิจารณาลักษณะของสัญญาการลงทุนที่รู้จักในชื่อ Howey Test ซึ่งเกิดขึ้นในการพิจารณาคดีระหว่าง SEC กับ W. J. Howey Co. ในปี 1946 โดยศาลสูงสุดของสหรัฐอเมริกา (U.S. Supreme Court)

ข้อพิจารณาดังกล่าวกำหนดว่าธุรกรรมใด ๆ จะถือเป็นสัญญาการลงทุน ถ้า

1. เป็นการลงทุน (Investment of Money)
2. ในวิสาหกิจที่มีเป้าหมายร่วมกัน (Common Enterprise) และ
3. เพื่อแสวงหาผลกำไรในการลงทุน จากความพยายามของผู้อื่น (Reasonable Expectation of Profits Derived from Efforts of Others) [44]

แต่เนื่องจากปัจจุบันยังไม่มีการออกกฎระเบียบในการกำกับดูแล และยังไม่มีกรณีที่เป็นบรรทัดฐานตามกฎหมาย การกำกับดูแลธุรกรรมที่เกี่ยวกับสินทรัพย์ดิจิทัลจึงยังคงไม่มีความชัดเจน

สหภาพยุโรป ใช้การกำหนดนิยามคริปโทเคอร์เรนซีให้เข้ากับกฎหมายต่อต้านการฟอกเงินที่มีอยู่แล้ว (EU AML directive 2018/843) และกำหนดให้สมาชิกทุกประเทศต้องออกกฎหมายของประเทศตนเอง ให้สอดคล้องกับ 5AMLD ภายในวันที่ 10 มกราคม 2020 ปัจจุบันประเทศสมาชิกของสหภาพยุโรปทุกประเทศจึงมีกฎหมายในการกำกับสินค้าดิจิทัลที่เป็นแบบแผนเดียวกัน และมีแผนในการปรับเปลี่ยนสู่ยุทธศาสตร์การเงินดิจิทัลแบบใหม่ (Markets in Crypto-Assets Regulation: MiCA) [45] ในอนาคต

ประเทศออสเตรเลีย แบ่งการกำกับดูแลตามลักษณะของผลิตภัณฑ์ หากสินทรัพย์ดิจิทัลเป็นผลิตภัณฑ์ทางการเงิน (Financial Products) ได้แก่

- การบริหารจัดการการลงทุน (Managed Investment Scheme: MIS)
- การเสนอขายหุ้น (shares)
- การเสนอขายตราสารอนุพันธ์ (derivative)
- Non-Cash Payment (NCP) facility

การประกอบกิจการสินทรัพย์ดิจิทัล เช่น ICOs ที่เข้าข่ายเป็นผลิตภัณฑ์ทางการเงิน จะต้องได้รับใบอนุญาตประกอบธุรกิจ Australian Financial Services License (AFSL) และถูกกำกับดูแลภายใต้กฎหมายว่าด้วยบริษัท (Corporations Act) และกฎหมายการกำกับหลักทรัพย์และการลงทุน (Australian Securities and Investments Commission Act) โดยมีคณะกรรมการกำกับหลักทรัพย์และการลงทุน (Australian Securities and Investments Commission: ASIC) เป็นหน่วยงานหลักในการกำกับดูแล [46]

กิจการสินทรัพย์ดิจิทัลที่ไม่ใช่ผลิตภัณฑ์ทางการเงิน (Non-Financial Products) เช่น การซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซี จะอยู่ภายใต้การกำกับดูแลของกฎหมายคุ้มครองผู้บริโภค (Australian Consumer Laws) ควบคู่กับ AML/CFT โดยมี Australian Transaction Reports and Analysis Center (AUSTRAC) เป็นหน่วยงานหลักในการกำกับดูแล

ประเทศญี่ปุ่น มีการควบคุมบริษัทที่ทำธุรกิจเกี่ยวกับคริปโทเคอร์เรนซี โดย Financial Services Agency โดยกฎหมายของประเทศญี่ปุ่นกำหนดให้บริษัทที่ทำธุรกิจประเภทนี้ต้องได้รับใบอนุญาต มีกระบวนการ KYC/CDD รวมถึงรายงานการเคลื่อนไหวทางการเงินตามกฎหมายต่อต้านการฟอกเงินและการสนับสนุนการเงินในการก่อการร้าย ตามกฎหมายของประเทศญี่ปุ่น ICO ที่มีลักษณะเป็นกองทุนรวม (Collective Investment Schemes) ถือเป็นหลักทรัพย์ ซึ่งจะต้องได้รับการกำกับดูแลภายใต้กฎหมายเครื่องมือทางการเงินและตลาดหลักทรัพย์ (Financial Instrument and Exchange Act)

ในอดีต ประเทศญี่ปุ่น มักเป็นประเทศเป้าหมายของธุรกิจที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล เนื่องจากมีโครงสร้างพื้นฐานที่พร้อม และมีการกำกับดูแลไม่เข้มงวดเหมือนประเทศอื่น ๆ

ปี 2010 Mt.Gox เริ่มธุรกิจซื้อขายแลกเปลี่ยนบิตคอยน์ในประเทศญี่ปุ่น และกลายเป็นบริษัทที่มีปริมาณการซื้อขายสูงที่สุดในโลกในช่วงปี 2013 กว่า 70% ของธุรกรรมทั้งหมดบนเครือข่ายบิตคอยน์เกิดขึ้นที่ Mt.Gox

ต้นปี 2014 Mt.Gox ถูกโจรกรรมข้อมูล สูญบิตคอยน์ ไปราว 650,000 BTC ส่งผลให้บริษัทล้มละลายในเดือนเมษายนปี 2014

การล้มละลายของ Mt.Gox สร้างความเสียหายมูลค่ามหาศาล รัฐบาลญี่ปุ่นได้รับเสียงวิพากษ์วิจารณ์เป็นอย่างมากที่ละเลยการกำกับดูแลจนทำให้เกิดความเสียหาย รัฐบาลญี่ปุ่นจึงออกระเบียบในการกำกับดูแลธุรกิจที่เกี่ยวกับสินทรัพย์ดิจิทัลที่เข้มงวดขึ้น โดยแก้ไข Payment Service Act และประกาศใช้ในปี 2017

ในปี 2021 Financial Services Agency ของประเทศญี่ปุ่นประกาศว่าจะเริ่มแก้ไขกฎระเบียบเกี่ยวกับสินทรัพย์ดิจิทัลให้เป็นไปตามกฎของ FATF

ใน **ประเทศสิงคโปร์** องค์การเงินตราแห่งประเทศสิงคโปร์ (Monetary Authority of Singapore: MAS) กำหนดให้ธุรกิจที่อำนวยความสะดวกในการถ่ายโอน แลกเปลี่ยน จัดเก็บ DPT จะต้องขอใบอนุญาตในการประกอบธุรกิจ และต้องปฏิบัติตามเงื่อนไขของ AML/CFT ตั้งแต่มกราคม ค.ศ. 2020 เป็นต้นไป ส่วนโทเคนดิจิทัล (ICOs) จะถือว่าเป็นหลักทรัพย์ ซึ่งการซื้อขายแลกเปลี่ยนจะต้องเป็นไปตาม Security and Futures Act (FSA) และ Financial Advisors Act (FAA)

ในปี พ.ศ. 2561 **ประเทศไทย** ออกพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ. 2561 โดยกำหนดนิยาม คริปโทเคอร์เรนซี โทเคนดิจิทัล และสินทรัพย์ดิจิทัลไว้ดังนี้

> “คริปโทเคอร์เรนซี” หมายความว่า หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้า บริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และให้หมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นใดตามที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด
>
> “โทเคนดิจิทัล” หมายความว่า หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีวัตถุประสงค์เพื่อ (๑) กำหนดสิทธิของบุคคลในการเข้าร่วมลงทุนในโครงการหรือกิจการใด ๆ (๒) กำหนดสิทธิในการได้มาซึ่งสินค้าหรือบริการหรือสิทธิอื่นใดที่เฉพาะเจาะจง ทั้งนี้ ตามที่กำหนด ในข้อตกลงระหว่างผู้ออกและผู้ถือ และให้หมายความรวมถึงหน่วยแสดงสิทธิอื่นตามที่คณะกรรมการ ก.ล.ต. ประกาศกำหนด
>
> “สินทรัพย์ดิจิทัล” หมายความว่า คริปโทเคอร์เรนซีและโทเคนดิจิทัล [47]

พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัลฯ มีสาระสำคัญในการนิยามและกำหนดแบบแผนในการประกอบธุรกิจที่เกี่ยวข้องกับสินทรัพย์ดิจิทัล โดยกำหนดให้ศูนย์ซื้อขายสินทรัพย์ดิจิทัล (Exchange) นายหน้าซื้อขายสินทรัพย์ดิจิทัล (Broker) ผู้ค้าสินทรัพย์ดิจิทัล (Dealer) จะต้องขอใบอนุญาตในการประกอบธุรกิจสินทรัพย์ดิจิทัลจากคณะกรรมการคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) และมีหน้าที่ในการทำ KYC/CDD และถือเป็นสถาบันการเงินตามกฎหมายว่าด้วยการป้องกันและปราบปรามการฟอกเงิน ซึ่งมีสำนักงานป้องกันและปราบปรามการฟอกเงิน (ปปง.) เป็นหน่วยงานหลักในการกำกับดูแล

นอกจากนี้ ในพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัลฯ ยังกำหนดระเบียบในการเสนอขายโทเคนดิจิทัล (ICO) ต่อประชาชน ผู้ออกโทเคนดิจิทัลที่ประสงค์จะเสนอขายโทเคนดิจิทัลต้องได้รับอนุญาตจากสำนักงาน ก.ล.ต. และให้กระทำได้เฉพาะนิติบุคคลประเภทบริษัทจำกัดหรือบริษัทมหาชนจำกัด โดยการเสนอขายต้องทำผ่านผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล (ICO portals) ที่ได้รับความเห็นชอบจากคณะกรรมการ ก.ล.ต. เท่านั้น

จนถึงปี พ.ศ. 2564 มีบริษัทที่ได้รับใบอนุญาตในการประกอบธุรกิจสินทรัพย์ดิจิทัลจากคณะกรรมการ ก.ล.ต. แล้ว 11 บริษัท และมีผู้ให้บริการระบบเสนอขายโทเคนดิจิทัล 4 บริษัท

และไม่ว่าแต่ละประเทศจะพิจารณาว่า สินทรัพย์ดิจิทัลเป็นสื่อในการชำระเงินหรือเป็นการลงทุน ทั้งสองอย่างนำมาซึ่งสิ่งที่หลีกเลี่ยงไม่ได้นั่นคือ **“ภาษี”**

7.3 คริปโทเคอร์เรนซีเสียภาษีหรือไม่ อย่างไร?

โดยภาพรวม รูปแบบการเก็บภาษีในส่วนของผู้บริโภค อาจแบ่งได้เป็นสองส่วนคือ ภาษีผลได้จากทุน (Capital Gains Tax: CGT) และภาษีที่เกิดจากการซื้อสินค้าหรือรับบริการ/ภาษีมูลค่าเพิ่ม (Good and Service Tax/Value-Added Tax)

การลงทุนในสินทรัพย์ดิจิทัลสามารถก่อให้เกิดรายได้ หลายประเทศจึงมีมาตรการจัดเก็บภาษีจากรายได้ที่เกิดจากการลงทุนในสินทรัพย์ดิจิทัล โดยอยู่ในรูปแบบภาษีผลได้จากทุนที่ต้องยื่นในการเสียภาษีเงินได้ (Income Tax) ประจำปี

ประเทศที่มีกฎหมายอนุญาตให้ใช้คริปโทเคอร์เรนซีในการชำระค่าสินค้าหรือบริการได้ อาจมีการเก็บภาษีที่เกิดจากการซื้อสินค้าหรือรับบริการหรือภาษีมูลค่าเพิ่มได้ด้วย

ใน **ประเทศสหรัฐอเมริกา** เงินเสมือนตามคำนิยามของ IRS ถือว่าเป็นทรัพย์สิน (Property) ซึ่งอยู่ภายใต้หลักการพื้นฐานในการเก็บภาษีที่เกี่ยวข้องกับธุรกรรมของ

ทรัพย์สิน รายได้จากการซื้อขายแลกเปลี่ยนเงินเสมือนจึงมีภาระในการเสียภาษีผลได้จากทุน

สำหรับประเทศที่เป็นสมาชิก **สหภาพยุโรป** กลไกด้านภาษีของแต่ละประเทศยังคงขึ้นกับกฎหมายของประเทศนั้น ๆ ซึ่งมีความแตกต่างกันทั้งรูปแบบและอัตรา

ความชัดเจนในการเก็บภาษีมูลค่าเพิ่มจากการซื้อขายแลกเปลี่ยนสินทรัพย์ดิจิทัลภายในสหภาพยุโรป เกิดขึ้นในปี 2015 จากการตัดสินคดีของศาลยุติธรรมแห่งยุโรป (European Court of Justice) ซึ่งถือเป็นศาลสูงสุด (Supreme Court) ของสหภาพยุโรปในคดีระหว่าง Skatteverket ซึ่งเป็นหน่วยงานจัดเก็บภาษีของประเทศสวีเดน กับ นาย David Hedqvist ซึ่งเป็นเจ้าของธุรกิจแลกเปลี่ยนบิตคอยน์ในสวีเดน โดยคำพิพากษาตัดสินให้การแลกเปลี่ยนซื้อขายสินทรัพย์ดิจิทัลได้รับการยกเว้นภาษีมูลค่าเพิ่ม [48] ซึ่งกลายเป็นบรรทัดฐานในการจัดเก็บภาษีมูลค่าเพิ่มที่ใช้ทั่วสหภาพยุโรป บรรทัดฐานจากคำตัดสินนี้ นำไปสู่การกำหนดระเบียบการจัดเก็บภาษีมูลค่าเพิ่มหรือภาษีที่เกิดจากการซื้อสินค้าหรือรับบริการของประเทศที่ไม่ได้เป็นสมาชิกสหภาพยุโรปอีกหลายประเทศ [49]

ในส่วนการจัดเก็บภาษีเงินได้ ประเทศในสหภาพยุโรปได้กำหนดคำจำกัดความของสินทรัพย์ดิจิทัลให้เข้ากับนิยามของทรัพย์สินที่สามารถจัดเก็บภาษีได้ตามกฎหมายของประเทศนั้น ๆ เช่นนิยามเป็นสินทรัพย์ไม่มีตัวตน (Intangible Assets) เป็นเครื่องมือทางการเงินหรือสินทรัพย์ (Financial Instruments or Assets) หรือเป็นโภคภัณฑ์ (Commodities) ระเบียบกฎเกณฑ์ในการเก็บภาษีเงินได้ของประเทศในสหภาพยุโรปจึงมีเงื่อนไขในการจัดเก็บที่แตกต่างกันไปด้วย

ตัวอย่างเช่น ประเทศมอลตา ไม่มีการเก็บภาษีผลได้จากทุนที่เกิดจากสินทรัพย์ดิจิทัลและการลงทุนในสินทรัพย์ดิจิทัลระยะยาว ประเทศเยอรมนี ถือว่ารางวัลที่ได้จากการ mining ไม่เข้าข่ายนิยามตามกฎหมายที่เกี่ยวข้องกับการเงินจึงได้รับการยกเว้นภาษี ผลได้จากทุนที่เกิดจากสินทรัพย์ดิจิทัล หากไม่เกิน 600 ยูโร หรือถือสินทรัพย์ดิจิทัลนั้นไว้นานกว่า 1 ปี ก็จะได้รับการยกเว้นภาษีเช่นกัน ข้อยกเว้นทางภาษีบุคคลธรรมดาที่เอื้อประโยชน์ต่อการลงทุนในสินทรัพย์ดิจิทัลทำให้บางประเทศเป็นประเทศที่เป้าหมายของนักลงทุน

ใน **ประเทศออสเตรเลีย** Australian Tax Office (ATO) มีระเบียบในการจัดเก็บภาษีสินทรัพย์ดิจิทัลอยู่สองส่วน ได้แก่ ภาษีที่เกิดจากการซื้อสินค้าหรือรับบริการ (GST) และภาษีผลได้จากทุน (CGT) [50] [51]

ในอดีตรัฐบาลออสเตรเลียเรียกเก็บ GST ทุกครั้งที่มีการซื้อขายสกุลเงินดิจิทัล แต่เนื่องจากสกุลเงินดิจิทัลสามารถใช้แลกเปลี่ยนเป็นสินค้าหรือบริการในออสเตรเลียได้อย่างถูกกฎหมาย จึงทำให้เกิดการเก็บ GST ซ้ำซ้อนทุกครั้งที่มีการใช้สกุลเงินดิจิทัลแลกเปลี่ยนเป็นสินค้าหรือบริการ รัฐบาลออสเตรเลียจึงได้ยกเลิกการจัดเก็บ GST จากธุรกรรมที่เป็นการซื้อขายสกุลเงินดิจิทัล ตั้งแต่วันที่ 1 กรกฎาคม 2017 เป็นต้นมา

ในส่วนของ CGT จะคิดภาษีเมื่อสินทรัพย์ดิจิทัลพ้นจากการครอบครอง (เช่น ขายให้ แลกเปลี่ยนเป็นคริปโทเคอร์เรนซีอื่น แลกเป็นเงิน แลกเปลี่ยนเป็นสินค้าหรือบริการ) การถือสินทรัพย์ดิจิทัลนานกว่า 12 เดือนสามารถขอลดหย่อน CGT ได้ในลักษณะเดียวกับทุนอื่น ๆ

สำหรับ **ประเทศญี่ปุ่น** กฎหมายภาษีการบริโภค (Consumption Tax Act) ของญี่ปุ่น ยกเว้นการเก็บภาษีการบริโภคที่เกิดจากธุรกรรมของเงินเสมือน ตั้งแต่วันที่ 1 กรกฎาคม ค.ศ. 2017 แต่ต้องแสดงรายได้ที่เกิดจากธุรกรรมสินทรัพย์ดิจิทัลในการยื่นภาษีเงินได้ประจำปี

การจัดเก็บภาษีใน **ประเทศสิงคโปร์** ขึ้นกับ Inland Revenue Authority of Singapore (IRAS) ที่ DPT ซึ่งหมายรวมถึงคริปโทเคอร์เรนซีได้รับการยกเว้นการจัดเก็บ GST แต่ต้องแสดงรายได้ที่เกิดจากธุรกรรมสินทรัพย์ดิจิทัลในการยื่นภาษีเงินได้ประจำปี [52]

ปัจจุบัน การซื้อขายสินทรัพย์ดิจิทัลใน **ประเทศไทย** เทียบได้กับการซื้อสินค้าหรือบริการ ผู้ประกอบธุรกิจที่เป็นนิติบุคคลจึงต้องเสียภาษีมูลค่าเพิ่มตามอัตราร้อยละ 7 นอกจากนี้ตามพระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19) กำหนดให้รัฐจัดเก็บภาษีเงินได้บุคคลธรรมดาจากเงินได้พึงประเมินที่ได้จากการถือหรือครอบครอง

โทเคนดิจิทัลหรือการโอนคริปโทเคอร์เรนซีหรือโทเคนดิจิทัล โดยเพิ่มนิยามเงินได้พึงประเมินตามมาตรา 40 แห่งประมวลรัษฎากร ไว้ดังนี้

"(ซ) เงินส่วนแบ่งของกำไร หรือผลประโยชน์อื่นใดในลักษณะเดียวกันที่ได้จากการถือหรือครอบครองโทเคนดิจิทัล

(ฌ) ผลประโยชน์ที่ได้รับจากการโอนคริปโทเคอร์เรนซีหรือโทเคนดิจิทัล ทั้งนี้ เฉพาะซึ่งตีราคาเป็นเงินได้เกินกว่าที่ลงทุน"

เงินได้พึงประเมินตามมาตรา 40 ประเภท (4) (ซ) และ (ฌ) ต้องคำนวณหักภาษี ณ ที่จ่ายในอัตราร้อยละ 15 ของเงินได้ [53]

ตัวอย่างการคำนวณภาษี สมมติได้กำไรจากการซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซีเป็นจำนวน 100,000 บาท เมื่อถอนเงินก้อนนี้ออกจากศูนย์ซื้อขายสินทรัพย์ดิจิทัลเป็นเงินสดหรือเข้าบัญชีธนาคาร ศูนย์ฯ จะมีหน้าที่หักภาษี ณ ที่จ่ายส่งสรรพากรในอัตราร้อยละ 15 เป็นเงิน 15,000 บาท

การหักภาษีอัตราร้อยละ 15 นี้ ไม่ใช่ภาษีสุดท้าย (final tax) จึงต้องนำรายได้ 100,000 บาท และภาษีหัก ณ ที่จ่าย 15,000 บาท ตามมาตรา 40 (4) (ฌ) ยื่นพร้อมกับรายได้ตามมาตรา 40 (1) – (8) ในการเสียภาษีเงินได้บุคคลธรรมดาประจำปี

ภาษีที่ต้องจ่ายจริงจึงเป็นไปตามเงินได้สุทธิในปีภาษีนั้น เช่น รายได้สุทธิในปีภาษีไม่ถึง 150,000 บาท ไม่ต้องเสียภาษี ก็จะสามารถขอคืนภาษีหัก ณ ที่จ่าย 15,000 บาทได้ทั้งหมด แต่หากเงินได้สุทธิเป็น 500,000 บาท จะต้องเสียภาษี

$(150{,}000 \times 5\%) + (200{,}000 \times 10\%) = 27{,}500$ บาท

เท่ากับต้องจ่ายเพิ่มอีก $27{,}500 - 15{,}000 = 12{,}500$ บาท


Login
****
GO!

8 ภาคผนวก

8.1 Blockchain อื่น ๆ

นอกเหนือจากอีเธอเรียมที่เราสามารถพัฒนาสัญญาอัจฉริยะใช้งานบนเครือข่ายสาธารณะแล้ว ยังมีเทคโนโลยีบล็อกเชนอื่น ๆ อีกหลายตัวที่เราสามารถเลือกใช้งานได้ เนื้อหาส่วนนี้จะยกตัวอย่างเครือข่ายบล็อกเชนที่มีความเฉพาะที่น่าสนใจและควรศึกษาเพื่อเป็นทางเลือก

8.1.1 Ripple & Stellar

ริปเพิล [113] กำเนิดในช่วงปี ค.ศ. 2012 เป็นเครือข่ายสารสนเทศทางการเงินที่ออกแบบมาเพื่อรองรับธุรกรรมของสถาบันการเงินโดยเฉพาะ มีฟังก์ชันหลักประกอบด้วยการทำ Real-Time Gross Settlement การแลกเปลี่ยนสกุลเงินตรา และการโอนเงินข้ามประเทศ ริปเพิลจึงมักได้รับการเปรียบว่าเป็นคู่แข่งโดยตรงกับ SWIFT (Society for Worldwide Interbank Financial Telecommunication) ที่ธนาคารพาณิชย์นิยมใช้ในการทำธุรกรรมข้ามประเทศ ริปเพิลจึงเป็นทางเลือกหนึ่งในการพัฒนาระบบงานที่ต้องการใช้บล็อกเชนเป็นสะพานเชื่อมกับระบบเงิน โดยเฉพาะกับสถาบันทางการเงิน

การยืนยันธุรกรรมของริปเพิลทำเป็นรอบทุก ๆ 3 - 5 วินาที ทุกธุรกรรมจะต้องส่งตรวจสอบยืนยันโดย validators ด้วยโพรโทคอลในการทำ consensus ของริปเพิลเอง ธุรกรรมที่ได้รับการยืนยันแล้วจะเก็บอยู่ใน ledger แต่ละโหนดโดยร้อยกับ ledger index ที่เกิดขึ้นก่อนหน้า ริปเพิลไม่มีการสร้างบล็อกธุรกรรม จึงมักไม่ได้เรียกว่าเป็นบล็อกเชน แต่เรียกว่าเป็น Distributed Ledger Technology (DLT) แทน

Consensus ของ ริปเพิลมีชื่อเฉพาะว่า Ripple Protocol Consensus Algorithm [114] มีพื้นฐานจาก Federated Byzantine Agreement (FBA)

FBA ทำงานคล้ายกับ PBFT โดยมีความแตกต่างตรงที่แต่ละโหนดไม่จำเป็นต้องให้ ทุก validator ยืนยันธุรกรรม แต่เลือกได้ว่าจะเชื่อถือ validator ใดบ้างเรียกว่า quorum slices ธุรกรรมจะถูกส่งไปโหวตเฉพาะ validators ใน quorum slices ที่ intersect กันตั้งแต่ quorum slice ที่ต้นทางของธุรกรรมเชื่อถือ ไปจนถึง quorum slice ที่ปลายทางของธุรกรรมเชื่อถือ โดยธุรกรรมจะต้องได้รับการโหวตผ่านทุก quorum slice ไม่น้อยกว่าค่าที่กำหนดจึงจะได้รับการยืนยันและร้อยเข้า ledger

การทำ quorum slices ทำให้ FBA แลกเปลี่ยนข้อมูลน้อยกว่าและกระจายอำนาจได้ดีกว่า PBFT

คริปโทเคอร์เรนซีของริปเพิล ชื่อ XRP โดยริปเพิลผลิตโทเคน XRP ทั้งหมด 100,000 ล้าน XRP ตั้งแต่เริ่มแรกเพื่อใช้หมุนเวียนในเครือข่ายและใช้ชำระค่าธรรมเนียมในการทำธุรกรรม โดย Ripple Lab ที่เป็นผู้พัฒนาซอฟต์แวร์ของริปเพิลถือครองไว้ 55,000 ล้าน XRP และปล่อยให้มีการหมุนเวียนอิสระ 45,000 ล้าน XRP การที่ Ripple Lab ถือครองสินทรัพย์จำนวนมาก ทำให้เกิดความกังวลในการปั่นราคา XRP ในปี ค.ศ. 2017 Ripple Lab จึงพัฒนาสัญญาอัจฉริยะ escrow ในการปล่อย XRP ออกมาหมุนเวียนทุกเดือน

ค่าธรรมเนียมการทำธุรกรรมของริปเพิลเริ่มต้นที่ 0.00001 XRP (อัตราแลกเปลี่ยนปี ค.ศ. 2021 1 XRP = ประมาณ 1.3 - 1.4 เหรียญสหรัฐ) ซึ่งถือว่าต่ำมากเมื่อเทียบกับค่าธรรมเนียมของเครือข่ายบล็อกเชนอื่น ๆ ธนาคารพาณิชย์หลายแห่งจึงเริ่มใช้ริปเพิลในการทำธุรกรรมทางการเงินข้ามประเทศ ในปี ค.ศ. 2021 ริปเพิลมีสมาชิกเป็นธนาคารพาณิชย์และสถาบันการเงินทั่วโลกมากกว่า 300 แห่ง

สัญญาอัจฉริยะ escrow ของ Ripple Lab มีทั้งหมด 55 สัญญา แต่ละสัญญาถือครองโทเคน 1,000 ล้าน XRP โดยแต่ละสัญญาจะหมดอายุในวันที่ 1 ของทุกเดือน

เมื่อสัญญาอัจฉริยะหมดอายุจะปล่อยโทเคน 1,000 ล้าน XRP ที่ถือครองอยู่ออกขายในตลาด หากสิ้นเดือนแล้วยังขายไม่หมด โทเคนที่เหลือจะถูกเก็บคืนและตั้งเป็นสัญญาอัจฉริยะใหม่เป็นสัญญาที่ 56, 57, .. ไปเรื่อย ๆ จนกว่าจะขายได้หมดทั้ง 55,000 ล้าน XRP

สเตลลาร์ [115] เป็น DLT เช่นเดียวกับริปเพิล ใช้ซอร์สโค้ดของริปเพิลมาพัฒนาเพื่อให้เหมาะกับการรองรับผู้ใช้ทั่วไป และองค์กรที่ไม่ใช่สถาบันการเงิน มีโพรโทคอลในการทำ consensus ของตัวเองเช่นกัน แต่มีหลักการทำงานเหมือนกับริปเพิล

สเตลลาร์มีคริปโทเคอร์เรนซีของตัวเองชื่อ Lumen (XLM) ในการทำธุรกรรมและชำระค่าธรรมเนียม มีจำนวนโทเคนเริ่มต้นที่ 100,000 ล้าน XLM และเพิ่มขึ้น 1% ทุก ๆ ปี

จนในเดือนตุลาคม ค.ศ. 2019 ชุมชนของสเตลลาร์ลงมติให้คงจำนวน XLM หมุนเวียนไว้ราว 50,000 ล้าน XLM และไม่มีการผลิตเพิ่ม ปัจจุบันมี XLM หมุนเวียนในตลาดราว 20,000 ล้าน XLM และอีกราว 30,000 ล้าน XLM ถือครองโดย Stellar Development Foundation เพื่อใช้ในการพัฒนาซอฟต์แวร์ โปรโมตการใช้งานสเตลลาร์ และถือครองโดยสัญญาอัจฉริยะ escrow เพื่อปล่อยโทเคนออกสู่ตลาดในวันที่ 1 มกราคม ค.ศ. 2021 - 2023 ปีละ 3,000 ล้าน XLM

ค่าธรรมเนียมธุรกรรมของสเตลลาร์เริ่มต้นที่ 0.00001 XLM (อัตราแลกเปลี่ยนปี ค.ศ. 2021 1 XLM = ประมาณ 0.6 – 0.7 เหรียญสหรัฐ)

จะเห็นได้ว่า ริปเพิล และ สเตลลาร์ คล้ายกันมาก ๆ ส่วนหนึ่งเป็นเพราะทั้งริปเพิลและ สเตลลาร์มี Chief Technology Officer คนเดียวกันคือ Jed McCaleb

McCaleb เป็นผู้สร้าง eDonkey peer-to-peer file sharing ที่ได้รับความนิยมสูงมากในช่วงปี ค.ศ.2000 และเป็นผู้ก่อตั้งบริษัทซื้อขายแลกเปลี่ยนบิตคอยน์ Mt.Gox ในประเทศญี่ปุ่น

Mt.Gox ย่อมาจาก Magic: the Gathering Online eXchange ซึ่งเป็นชื่อเว็บที่ McCaleb ตั้งใจจะสร้างเป็น portal แลกเปลี่ยน card ในเกม Magic: the Gathering แต่พอมารู้จักบิตคอยน์จึงพบว่าทำเว็บแลกเปลี่ยนบิตคอยน์น่าจะดีกว่า

8.1.2 Binance Smart Chain

Binance เป็นบริษัทที่ทำธุรกิจซื้อขายแลกเปลี่ยนคริปโทเคอร์เรนซีที่มีปริมาณการซื้อขายสูงที่สุดในโลก และมีเครือข่ายบล็อกเชนให้บริการในการพัฒนา DApp เป็นของตัวเองชื่อ Binance Smart Chain

Binance Smart Chain [116] เป็นเครือข่ายบล็อกเชนสาธารณะเพื่อใช้ในการพัฒนา DApp ของ Binance เครือข่าย BSC เป็น Ethereum Virtual Machine (EVM) compatible จึงสามารถนำสัญญาอัจฉริยะที่พัฒนาสำหรับอีเธอเรียมมาทำงานบน BSC ได้

BSC ใช้ Binance Coin (BNB) ซึ่งเป็นคริปโทเคอร์เรนซีของ Binance สำหรับชำระค่าธรรมเนียมธุรกรรมและการประมวลผลสัญญาอัจฉริยะ

เครือข่าย BSC ใช้โพรโทคอลในการทำ consensus ที่ Binance พัฒนาขึ้นมาเองเรียกว่า Proof of Staked Authority (PoSA) [117] เป็นการใช้ Proof of Authority ในการเลือกโหนดที่จะทำหน้าที่เป็น validators และใช้ Proof of Stake ในการเลือก validator

ที่จะยืนยันบล็อกธุรกรรม วิธีนี้ทำให้ BSC สามารถควบคุมจำนวน validators ที่อยู่ในเครือข่ายและลดปริมาณการกระจายธุรกรรมระหว่าง validator ได้ BSC จึงสามารถกำหนด block time ได้ที่ 3 วินาที ธุรกรรมบน BSC จึงมีผลเร็วกว่าบนอีเธอเรียมหรือบิตคอยน์มาก

Validators ของ BSC มีอยู่ทั้งหมดราว ๆ 40 โหนดประกอบด้วยโหนดของ Binance เองและขององค์กรภายนอกเพื่อกระจายอำนาจ โดย Binance มีอำนาจในการกำหนด validator ที่จะเข้าร่วมในการยืนยันบล็อกธุรกรรม และจาก validators ทั้งหมดที่มีอยู่ BSC จะเลือกโหนดที่วาง stake สูงสุด 21 อันดับแรกให้ทำงานเป็น validators ในแต่ละวัน โหนดที่เป็น validator จะได้รางวัลและค่าธรรมเนียมจากบล็อกที่โหนดเป็นผู้ยืนยันโดยจะโอนเข้าเป็นรายวัน

BSC มีกลไกปรับ validator ที่มีพฤติกรรมไม่พึงประสงค์ด้วย เช่น validator ที่ยืนยันข้อมูลบล็อกเดียวซ้ำหลายครั้ง (double sign) จะถูกยึด stake ที่วางไว้ 10,000 BNB และถูกขับออกจากการเป็น validator

การที่ BSC มี block time ต่ำ ทำให้ BSC รองรับธุรกรรมได้มากกว่าอีเธอเรียม อีกทั้งค่า gas ของ BSC เฉลี่ยไม่ถึง 10 Gwei ของ BNB ในขณะที่ค่า gas ของอีเธอเรียมเฉลี่ยมากกว่า 40 Gwei ของ ETH ค่าธรรมเนียมธุรกรรมของ BSC จึงต่ำกว่าอีเธอเรียมมาก ประกอบกับสัญญาอัจฉริยะบนอีเธอเรียมสามารถย้ายมาทำงานบน BSC ได้ง่าย ส่งผลให้ BSC ได้รับความนิยมในการทำธุรกรรมมากขึ้นเรื่อย ๆ โดยในเดือนเมษายน ค.ศ. 2021 จำนวนธุรกรรมเฉลี่ยของอีเธอเรียมอยู่ที่ 1.4 ล้านธุรกรรมต่อวัน ในขณะที่ BSC มีจำนวนธุรกรรมเฉลี่ยในช่วงเวลาเดียวกันราว 5.4 ล้านธุรกรรมต่อวัน

8.1.3 Polkadot

นอกจากบิตคอยน์ อีเธอเรียม แล้ว ปัจจุบันยังมีเครือข่ายบล็อกเชนสาธารณะอื่น ๆ อีกหลายเครือข่าย เช่น Cardano, Ripple, Stellar, EOS, Litecoin, NEM, Solana เครือข่ายบล็อกเชนเหล่านี้ได้รับการพัฒนาภายใต้แนวคิดที่ต่างกัน โทเคน ข้อมูล โพรโทคอล จึงมี

ความแตกต่างกัน ซึ่งทำให้เครือข่ายบล็อกเชนที่มีอยู่ในปัจจุบันไม่สามารถเชื่อมข้อมูลหากันได้ หรือทำงานร่วมกัน (interoperable) ได้อัตโนมัติ

Polkadot [118] แก้ปัญหานี้ โดยสร้างเครือข่ายบล็อกเชนกลางเชื่อมโยงเครือข่ายบล็อกเชนที่ต่างกันเข้าด้วยกัน เพื่อให้สามารถทำงานข้ามกันได้ เครือข่ายบล็อกเชนกลางที่ Polkadot สร้างขึ้นมา เรียกว่า Relay Chain เป็นทางผ่านของธุรกรรม ทำให้สามารถโอนถ่ายข้อมูล โทเคน จากเครือข่ายบล็อกเชนหนึ่งไปอีกเครือข่ายหนึ่งได้ รวมถึงพัฒนาแอปพลิเคชันที่ทำงานข้ามเครือข่ายบล็อกเชนได้

ความสามารถที่เชื่อมโยงเครือข่ายบล็อกเชนเข้าด้วยกันเหมือนกับอินเทอร์เน็ตที่เชื่อมโยงเครือข่ายคอมพิวเตอร์ทั่วโลกเข้าด้วยกัน จึงมักมีการกล่าวถึง Polkadot ว่าเป็น Internet of blockchains

Polkadot มีโทเคนชื่อ DOT เป็นคริปโทเคอร์เรนซีในการชำระค่าธุรกรรมในการประมวลผลและโอนถ่ายข้อมูล Relay Chain ทำงานโดยใช้โพรโทคอลในการทำ consensus แบบ Proof of Stake

8.1.4 Diem

โครงการ Diem [119] เดิมชื่อ Libra เป็นโครงการที่ริเริ่มโดยบริษัท Facebook ในช่วงกลางปี ค.ศ. 2019 มีเป้าหมายในการสร้างระบบชำระเงินสำหรับ Facebook โดยใช้บล็อกเชนจัดการธุรกรรม

Diem บริหารจัดการโครงการในรูปแบบสมาคม โดยก่อตั้งเป็นนิติบุคคลในประเทศสวิตเซอร์แลนด์ มีสมาชิกเป็นบริษัทเอกชนที่ทำธุรกิจด้านการชำระเงิน เทคโนโลยี สื่อสาร บล็อกเชน และการเงินรวม 27 ราย

Diem ใช้กลไกการสร้าง Stablecoin โดยใช้ทุนสำรองคล้าย ๆ กับ USDT ของ Tether คริปโทเคอร์เรนซีของ Diem จะมีหลายสกุล โทเคนของแต่ละสกุล ใช้ทุนสำรองเป็นเงินสดหรือสินทรัพย์แทนเงินสดของสกุลนั้นและบริหารโดยองค์กรหรือบริษัทที่ดำเนินธุรกิจ

ในประเทศที่มีอำนาจในการควบคุมเงินสกุลนั้น เช่น ≋USD เป็นโทเคนที่สำหรับสกุลเงินดอลลาร์สหรัฐ ใช้ทุนสำรองเป็นเงินดอลลาร์สหรัฐ อัตรา 1:1 กับโทเคน และจะออกโทเคนใหม่โดยองค์กรหรือบริษัทที่ดำเนินธุรกิจในประเทศสหรัฐอเมริกา องค์กรหรือบริษัทที่ดำเนินธุรกิจที่สามารถดำเนินการได้ Diem เรียกว่าเป็น Virtual Asset Service Provider (VASP) จะต้องได้รับการกำกับดูแลทางการเงินตามกฎหมายของประเทศที่ตั้งและได้รับการรับรองโดยสมาคม

Diem มีแผนจะสร้างโทเคน ≋LBR เป็นโทเคนที่รองรับเงินตราหลายสกุล (multi-currency coin) สำหรับประเทศไม่ได้ใช้เงินสกุลเดียว และอาจใช้ในการทำ settlement ธุรกรรมระหว่างประเทศ โดยมีเงินสดหรือสินทรัพย์แทนเงินสดเป็นทุนสำรองเช่นกัน

เครือข่ายบล็อกเชนของ Diem ได้รับการออกแบบเป็น permissioned ใช้โพรโทคอล ในการทำ consensus แบบ Byzantine Fault Tolerance พัฒนาเป็นซอฟต์แวร์โอเพนซอร์ส มีภาษา Move เป็นภาษาสำหรับสร้างธุรกรรมและเขียนสัญญาอัจฉริยะ [120]

ด้วยบทบาทของโครงการที่คล้ายกับธนาคารกลางของประเทศ โครงการ Diem จึงได้รับเสียงวิพากษ์วิจารณ์ค่อนข้างมาก ธนาคารกลางของหลายประเทศมีความเห็นไปในทางเดียวกันว่า Diem เป็นภัยคุกคามต่อการควบคุมเสถียรภาพทางการเงินของประเทศ และเช่นเดียวกับคริปโทเคอร์เรนซีอื่น ๆ Diem อาจถูกใช้เป็นช่องทางในการฟอกเงิน หรือสนับสนุนทางการเงินในการกระทำผิดกฎหมายหรือการก่อการร้าย และอาจสร้างปัญหาในการการคุ้มครองผู้บริโภค

โครงการ Diem ยังอยู่ระหว่างการพัฒนาซอฟต์แวร์พื้นฐาน และมีแผนที่จะนำร่องทำ Stablecoin ที่ตรึงกับเหรียญสหรัฐในประเทศสหรัฐอเมริกาในปี 2021 [121]

8.1.5 Hyperledger

การประยุกต์ใช้บล็อกเชน โดยเฉพาะระบบงานภายในองค์กรหรือระหว่างองค์กรอาจไม่เหมาะที่จะใช้งานเครือข่ายบล็อกเชนสาธารณะอย่างอีเธอเรียม ริปเพิล หรือ BSC

ที่การทำงานเป็นอิสระจากการควบคุมขององค์กร ระบบงานภายในองค์กรจึงมักจะเลือกสร้างเครือข่ายภายในเป็น permissioned private หรือ consortium

เราอาจเลือกใช้ซอฟต์แวร์เดียวกับ อีเธอเรียม เช่น Geth ในการสร้างโหนดทำงานภายในองค์กรก็ได้ หรืออีกทางเลือกหนึ่งคือใช้ซอฟต์แวร์สำหรับสร้างเครือข่ายบล็อกเชนภายในองค์กรโดยเฉพาะ เช่น Hyperledger

Hyperledger [122] เป็นโครงการพัฒนาซอฟต์แวร์สำหรับสร้างเครือข่ายบล็อกเชนใช้งานในองค์กร (Enterprise grade) ประกอบด้วยโครงการย่อย ๆ (เช่น Fabric, Besu, Iroha) ที่พัฒนาซอฟต์แวร์เครือข่ายสำหรับจุดประสงค์ในการนำไปใช้งานที่ต่างกัน และใช้โพรโทคอลในการทำ consensus ที่ต่างกัน เพื่อให้องค์กรสามารถเลือกใช้ที่เหมาะกับระบบงานภายในองค์กรได้

ตารางที่ 1 โครงการของ Hyperledger

Ledgers	Focus	Consensus
Hyperledger Fabric	Enterprise, Generic, Scalable	Kafka, Solo, RAFT
Hyperledger Sawtooth	High modularity	PBFT, PoET
Hyperledger Burrow	Lightweight, Speed	BFT
Hyperledger Besu	Permissioned, EVM compatible	PoW, PoA
Hyperledger Indy	Digital Identity, Verifiable Credentials	RBFT
Hyperledger Iroha	IoT, Mobile	YAC

การที่ Hyperledger ตั้งใจให้เป็นบล็อกเชนสำหรับองค์กร อยู่ภายใต้การควบคุมขององค์กรและใช้ทรัพยากรขององค์กรเอง จึงได้รับการออกแบบให้เน้นเรื่องประสิทธิภาพในการประมวลผลที่สูง มี block time ต่ำ โพรโทคอลในการทำ consensus ไม่จำเป็นต้องกระจายอำนาจโดยสมบูรณ์เหมือน permissionless blockchain

และเนื่องจากเป็นการใช้งานในองค์กร ไม่จำเป็นต้องมีค่าธรรมเนียม Hyperledger จึงไม่มีโทเคนเป็นคริปโทเคอร์เรนซีเหมือนกับบิตคอยน์หรืออีเธอเรียม แต่ยังคงความสามารถในการพัฒนา DApp และสร้างโทเคนอื่น ๆ ได้

ซอฟต์แวร์ทั้งหมดของ Hyperledger พัฒนาเป็นซอฟต์แวร์โอเพนซอร์ส ภายใต้การสนับสนุนของ Linux Foundations โครงการย่อยของ Hyperledger หลายโครงการ เช่น Fabric และ Besu ผ่านการ audit จากองค์กรภายนอกแล้ว

8.2 ศัพท์น่ารู้เกี่ยวกับบล็อกเชน

Anti-Money Laundering and Combating the Financing of Terrorism/Counter-Terrorism Financing (AML/CFT, AML/CTF): การต่อต้านการฟอกเงินและการสนับสนุนการเงินในการก่อการร้าย เป็นข้อเสนอแนะมาตรฐานระดับนานาชาติ โดย Financial Action Task Force ซึ่งเป็นองค์กรสากลที่ก่อตั้งเพื่อต่อต้านการฟอกเงินโดยกลุ่ม G7 ในปี ค.ศ. 1987

Blockchain (บล็อกเชน): วิธีการเก็บข้อมูลรายการเปลี่ยนแปลงตามหลักการทางบัญชี โดยการเข้ารหัสและจัดเรียงข้อมูลเหล่านี้ต่อกันตามลำดับเวลาที่ข้อมูลเข้ามา กลุ่มข้อมูลดังกล่าวจะเผยแพร่ไปให้ผู้ใช้ในเครือข่ายที่กำหนดได้ทราบทั่วกัน ทั้งนี้ ผู้ใช้ทุกคนจะทราบการแก้ไขเพิ่มเติมรายการเปลี่ยนแปลงในบล็อกเชนทุกรายการตลอดเวลา

Bitcoin (บิตคอยน์): ระบบเงินสดอิเล็กทรอนิกส์ประเภทหนึ่งซึ่งใช้เทคโนโลยีบล็อกเชนและเป็นต้นแบบของเทคโนโลยีบล็อกเชนในปัจจุบัน บิตคอยน์ยังเป็นชื่อที่ใช้เรียกโทเคนที่เป็นหน่วยเงิน และเครือข่ายของระบบเงินสดอิเล็กทรอนิกส์นี้ด้วย

Bitcoin address (บิตคอยน์แอดเดรส): หมายเลขประจำผู้ใช้ของบิตคอยน์ ใช้ในการระบุตัวผู้ทำธุรกรรมในเครือข่ายบิตคอยน์

Block time: เวลาที่หน่วงไว้โดยโพรโทคอลในการทำ consensus เพื่อให้ข้อมูลธุรกรรมสามารถกระจายได้อย่างทั่วถึงทั้งเครือข่าย block time สูง ทำให้มั่นใจได้ว่าข้อมูลธุรกรรมกระจายได้ทั่วถึงทั้งเครือข่ายแต่ทำให้ธุรกรรมใช้เวลาในการยืนยันนาน ในทางกลับกัน block time ต่ำการยืนยันธุรกรรมเกิดได้เร็วกว่า แต่ข้อมูลธุรกรรมกระจายไม่ทั่วถึง ซึ่งมีผลทำให้ไม่สามารถหา consensus ได้ แต่ละเครือข่ายจึงต้องพิจารณา block time อย่างรอบคอบ เพราะมีผลต่อความน่าเชื่อถือของธุรกรรม

Capital Gains Tax (CGT): ภาษีผลได้จากทุน ได้แก่ ภาษีที่เก็บจากผลได้ที่เกิดจากการเพิ่มขึ้นในมูลค่าของสินทรัพย์หรือหลักทรัพย์

Central Bank Digital Currency (CDBC): ระบบเงินดิจิทัลที่บริหารจัดการและกำกับดูแลโดยธนาคารกลางของประเทศ

Centralized Exchange (CEX): ศูนย์ซื้อขายแลกเปลี่ยนสินทรัพย์แบบรวมศูนย์

Consensus: กลไกการทำให้ข้อมูลสอดคล้องตรงกันกันในบล็อกเชน

Consortium blockchain: เครือข่ายบล็อกเชนแบบ permissioned ที่ใช้งานระหว่างองค์กรที่มีความร่วมมือในการแลกเปลี่ยนข้อมูลหรือทำธุรกรรมระหว่างกัน

Cryptocurrency (คริปโทเคอร์เรนซี): ตามนิยามในพระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล พ.ศ.2561 หมายความว่า หน่วยข้อมูลอิเล็กทรอนิกส์ซึ่งถูกสร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์โดยมีความประสงค์ที่จะใช้เป็นสื่อกลางในการแลกเปลี่ยนเพื่อให้ได้มาซึ่งสินค้าบริการ หรือสิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล และให้หมายความรวมถึงหน่วยข้อมูลอิเล็กทรอนิกส์อื่นใดตามที่คณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์ประกาศกำหนด

Cryptographic Hash: แฮชรหัสลับ เป็นแฮชที่เกิดจากการคำนวณโดยวิธีวิทยาการเข้ารหัสลับ มาตรฐานที่นิยมใช้ในระบบสารสนเทศได้แก่ MD5, SHA, RIPEMD มีขนาดตั้งแต่ 128 ถึง 512 บิต (16 ถึง 64 ไบต์)

Customer Due Diligence (CDD): การตรวจสอบเพื่อทราบข้อเท็จจริงเกี่ยวกับลูกค้าเป็นกระบวนการเฝ้าระวัง ตรวจสอบ ตรวจทาน การเคลื่อนไหวทางการเงินหรือการทำธุรกรรมของลูกค้า เพื่อตรวจจับความผิดปกติหรือไม่สอดคล้องกับสถานภาพทางเศรษฐกิจของลูกค้า

Decentralized Exchange (DEX): ศูนย์ซื้อขายแลกเปลี่ยนสินทรัพย์แบบกระจายอำนาจ ศูนย์ซื้อขายฯ ลักษณะนี้ทำหน้าที่อำนวยความสะดวกในการซื้อขายแลกเปลี่ยนตามที่สัญญาอัจฉริยะกำหนดไว้ อำนาจการจัดการสินทรัพย์ดิจิทัลจะอยู่กับเจ้าของสินทรัพย์ ลูกค้าไม่ต้องฝากสินทรัพย์ไว้กับศูนย์ฯ หรือต้องให้อำนาจกระทำการแทนเหมือนกับ Centralized Exchange

Decentralized Application (DApp): แอปพลิเคชันที่สร้างจากสัญญาอัจฉริยะ ทำงานบนบล็อกเชน จึงมีคุณสมบัติในการกระจายศูนย์และกระจายอำนาจในการประมวลผล DApp และสัญญาอัจฉริยะเป็นคำที่ใช้แทนกันได้

Decentralized Finance (DeFi): สัญญาอัจฉริยะในการบริการทางการเงินแบบกระจายอำนาจ

Decentralized Identifier (DID): identifier แบบกระจายศูนย์/กระจายอำนาจ บริหารจัดการได้โดยผู้ใช้เอง ใช้งานในสารรับรองที่ตรวจสอบได้ (Verifiable Credential)

Delivery-versus-Payment (DvP): การชำระเงินและส่งมอบหลักทรัพย์ในคราวเดียว ธุรกรรมในการชำระเงินและส่งมอบหลักทรัพย์จะแยกออกจากกันไม่ได้ (atomic)

Distributed Ledger Technology (DLT): เทคโนโลยีในการประมวลผล ledger แบบกระจายศูนย์ หลักการทำงานคล้ายกับบล็อกเชน มีความแตกต่างจากบล็อกเชนที่ DLT ไม่มีการรวมธุรกรรมเป็น block และไม่มี block time

Double spending: การทำธุรกรรมซ้ำซ้อนโดยใช้โทเคนเดียว ตัวอย่างการทำธุรกรรมซ้ำซ้อน เช่น การปลอมแปลงธนบัตร หรือปลอมเช็คโดยการทำสำเนา เพื่อนำไปใช้จ่ายหรือขึ้นเงินได้หลาย ๆ ครั้ง

Ethereum Virtual Machine (EVM): ส่วนประมวลผลธุรกรรมและสัญญาอัจฉริยะติดตั้งอยู่ภายในโหนดของเครือข่ายอีเธอเรียม

Fork: ในบริบทของบล็อกเชน fork เป็นกลไกในการอัปเกรดบล็อกเชนโดยการอัปเกรดซอฟต์แวร์ของโหนดในบล็อกเชน

Gas: ค่าธรรมเนียมในการทำธุรกรรมในเครือข่ายอีเธอเรียม และ EVM-compatible

Good and Service Tax (GST): ภาษีที่เกิดจากการซื้อสินค้าหรือรับบริการ

Governance Token: เป็น utility token ที่ให้สิทธิผู้ถือในการกำกับควบคุมสัญญาอัจฉริยะ

Hash: ศาสตร์ทางวิทยาการคอมพิวเตอร์ แฮชเป็นข้อมูลขนาดเล็กที่เป็นเอกลักษณ์ของข้อมูลอื่น ในอุดมคติ ข้อมูลที่เหมือนกันทุกประการต้องคำนวณได้แฮชเป็นค่าเดียวกัน และข้อมูลที่ต่างกันต้องคำนวณได้แฮชที่ไม่เหมือนกัน

Initial Coin Offering (ICO): การลงทุนด้วยการเสนอขายโทเคนดิจิทัล เป็นรูปแบบในการระดมทุนโดยให้สิทธิถือโทเคนดิจิทัลเป็นการตอบแทน

Keypair (คู่กุญแจ): ข้อมูลที่เป็นกุญแจในการเข้าและถอดรหัสลับในระบบรหัสกุญแจสาธารณะ (public key cryptography) คู่กุญแจประกอบด้วยกุญแจสองดอกที่สร้างขึ้นให้เข้าคู่กันโดยเฉพาะ ได้แก่กุญแจส่วนตัว (private key) ที่ต้องเก็บเป็นความลับ และกุญแจสาธารณะ (public key) ที่สามารถเปิดเผยได้โดยไม่ต้องกังวลว่าจะทำให้ผู้อื่นล่วงรู้กุญแจส่วนตัวที่เข้าคู่กัน

Know Your Customer (KYC): กระบวนการพิสูจน์ตัวตนลูกค้า เพื่อให้ทราบตัวตนที่แท้จริง มักพิสูจน์โดยเอกสารที่ออกโดยรัฐที่มีภาพถ่าย (เช่น บัตรประชาชน หนังสือเดินทาง) การพิสูจน์ตัวตนลูกค้าเป็นส่วนหนึ่งในการป้องกันและปราบปรามการฟอกเงิน

Ledger: ฐานข้อมูลสำหรับเก็บบันทึกข้อมูลธุรกรรมในบล็อกเชน

Minimum Viable Product (MVP): สินค้าหรือบริการที่มีคุณสมบัติหรือฟังก์ชันน้อยที่สุดเท่าที่จะใช้งานหรือให้บริการได้จริง มักใช้ในการประเมินหรือทดสอบความต้องการของตลาด

Miner: โหนดในการยืนยันธุรกรรมในเครือข่ายที่ใช้ consensus แบบ Proof of Work

Mining: การหารายได้จากรางวัลที่เครือข่ายคริปโทเคอร์เรนซีผลิตให้ในกระบวนการ Proof of Work

Node (โหนด): คอมพิวเตอร์ที่เชื่อมต่อเป็นสมาชิกของเครือข่ายคอมพิวเตอร์ หากใช้ในบริบทของบล็อกเชน โหนดคือคอมพิวเตอร์ที่เป็นสมาชิกเครือข่ายบล็อกเชน

Nonce: ข้อมูลที่มีการใช้งานเพียงครั้งเดียวตลอดอายุการประมวลผลข้อมูล สำหรับบิตคอยน์ nonce เป็นค่าที่เติมในหัวบล็อกเพื่อให้ได้ hash ของหัวบล็อกต่ำกว่าค่าเป้าหมาย ซึ่งต้องลองผิดลองถูกจนกว่าจะพบ

Oracle: ระบบสารสนเทศที่ส่งข้อมูลจากด้านนอกเครือข่ายบล็อกเชนให้กับสัญญาอัจฉริยะที่อยู่บนบล็อกเชน

Permissioned blockchain: เครือข่ายบล็อกเชนที่มีการกำหนดสิทธิการเชื่อมต่อ การอ่าน-เขียน ledger และการมีส่วนร่วมในการยืนยันธุรกรรม

Permissionless blockchain: เครือข่ายบล็อกเชนที่ไม่มีกลไกในการอนุญาตหรือกำหนดสิทธิในการเข้าถึง ทุกคนสามารถเชื่อมต่อกับเครือข่าย อ่าน/เขียน ledger และมีส่วนร่วมในการยืนยันธุรกรรมได้โดยไม่มีข้อจำกัดหรือต้องขออนุญาตใคร

Practical Byzantine Fault Tolerance (PBFT): อัลกอริทึมในการยืนยันข้อมูลที่ถูกต้องโดยใช้เสียงข้างมาก หลักการทำงานของ PBFT สามารถประยุกต์ใช้ในการยืนยันธุรกรรมบนเครือข่ายบล็อกเชนได้

Private blockchain: เครือข่ายบล็อกเชนแบบ permissioned ที่ใช้งานภายในองค์กรเดียว

Proof of Authority (PoA): โพรโทคอลในการทำ consensus ที่กำหนดอำนาจในการยืนยันธุรกรรมให้กับโหนดโดยผู้ดูแลเครือข่ายบล็อกเชน

Proof of Stake (PoS): โพรโทคอลในการทำ consensus โดยสุ่มโหนดในการยืนยันธุรกรรมตามสัดส่วนของ stake ที่วางไว้

Proof of Work (PoW): โพรโทคอลในการทำ consensus ที่แข่งขันกันประมวลผลข้อมูลเพื่อแก้โจทย์หรือหาค่าตามเงื่อนไขที่กำหนด จะได้เป็นผู้ยืนยันธุรกรรมและประทับเวลา

Protocol (โพรโทคอล): เกณฑ์วิธี เป็นข้อตกลงที่กำหนดขึ้นเพื่อให้การสื่อสารเป็นไปตามวัตถุประสงค์ ตัวอย่างเช่น consensus protocol ของบล็อกเชน

Public blockchain: เครือข่ายบล็อกเชนสาธารณะ มักเป็นเครือข่ายแบบ permissionless เช่น บิตคอยน์ อีเธอเรียม

Signer: โหนดในการยืนยันธุรกรรมในเครือข่ายที่ใช้ consensus แบบ Proof of Authority

Smart Contract (สัญญาอัจฉริยะ): ซอฟต์แวร์ที่เขียนขึ้นเพื่อประมวลผลบนบล็อกเชนโดยเฉพาะ โดยตัวซอฟต์แวร์จะต้องได้รับการติดตั้ง (deploy) ในบล็อกเชน สัญญาอัจฉริยะประมวลผลบนบล็อกเชนและเก็บบันทึกผลลัพธ์บนบล็อกเชน

Stablecoin: คริปโทเคอร์เรนซีที่มีการตรึงมูลค่ากับสินทรัพย์จริง ส่วนมากจะตรึงมูลค่ากับสกุลเงิน

Tree: โครงสร้างข้อมูลประเภทหนึ่งในศาสตร์ทางวิทยาการคอมพิวเตอร์ ใช้แสดงความสัมพันธ์ของข้อมูลที่ขยายหรือแตกกิ่งเหมือนต้นไม้

Token (โทเคน) : สิ่งที่ใช้แทนค่า เช่น เหรียญ ธนบัตร คือสิ่งแทนค่าของเงิน ตั๋วชมภาพยนตร์คือสิ่งแทนสิทธิในการชมภาพยนตร์ของผู้ถือ

Validator: โหนดในการยืนยันธุรกรรมในเครือข่ายที่ใช้ consensus แบบ Proof of Stake

Value-Added Tax (VAT): ภาษีมูลค่าเพิ่ม

Verifiable Credential (VC): เอกสารรับรอง ตาม ขมธอ. 24-2563 โดยสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์ หมายถึง ชุดของข้อความยืนยันอย่างน้อยหนึ่งรายการที่ถูกรับรองโดยผู้ออกเอกสาร (issuer) ทั้งนี้ VC มีคุณสมบัติที่สามารถตรวจพบการเปลี่ยนแปลงใด ๆ ที่เกิดกับความถูกต้องครบถ้วนของข้อมูล และตรวจสอบลายมือชื่ออิเล็กทรอนิกส์ของผู้ออกเอกสารได้ด้วยกระบวนการเข้ารหัสลับ

Wallet (วอลเล็ต): ซอฟต์แวร์ในการเก็บกุญแจส่วนตัวในการทำธุรกรรมบนบล็อกเชน

อ้างอิง

[1] E. Shein, "How Blockchain Changes the Nature of Trust," January 2019. https://www.linuxfoundation.org/en/blog/how-blockchain-changes-the-nature-of-trust/.

[2] Bitcoin, "Bitcoin Block 1," 2009. https://www.blockchain.com/btc/block/1.

[3] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 31 October 2008. https://bitcoin.org/bitcoin.pdf.

[4] Bitnodes, "Global Bitcoin Node Distribution," 2021. https://bitnodes.io/.

[5] CNBC, "Bitcoin hits $1 trillion in market value as cryptocurrency surge continues," February 2021. https://www.cnbc.com/2021/02/19/bitcoin-hits-1-trillion-in-market-value-as-cryptocurrency-surge-continues.html.

[6] Bitcoin Core Developer, "Bitcoin Core," 2009. https://bitcoin.org/en/wallets/desktop/windows/bitcoincore/.

[7] A. Back, "Hashcash - A Denial of Service Counter-Measure," 1 April 2002. http://www.hashcash.org/papers/hashcash.pdf.

[8] A. Hern, "Bitcoin currency could have been destroyed by '51%' attack," June 2014. https://www.theguardian.com/technology/2014/jun/16/bitcoin-currency-destroyed-51-attack-ghash-io.

[9] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance," *ACM Transactions on Computer Systems,* pp. 398-461, 2002.

[10] N. Szabo, "Smart Contracts," 1994. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html.

[11] V. Buterin, "Ethererum Whitepaper," 2013. https://ethereum.org/en/whitepaper/.

[12] V. Buterin, "Launching the Ether Sale," 2014. https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/.

[13] Bitcoin, "Address 36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2," 2014. https://www.blockchain.com/btc/address/36PrZ1KHYMpqSyAQXSG8VwbUiq2EogxLo2.

[14] Ethereum, "Block 0," 2015. https://etherscan.io/block/0.

[15] Ethereum, "EIP-20: ERC-20 Token Standard," 2015. https://eips.ethereum.org/EIPS/eip-20.

[16] Ethereum, "EIP-721: ERC-721 Non-Fungible Token Standard," 2018. https://eips.ethereum.org/EIPS/eip-721.

[17] Ethereum, "EIP-1155: ERC-1155 Multi Token Standard," 2018. https://eips.ethereum.org/EIPS/eip-1155.

[18] Ethereum, "EIP-1: EIP Purpose and Guidelines," 2015. https://eips.ethereum.org/EIPS/eip-1.

[19] The DAO, "The DAO," 2016. https://github.com/TheDAO/DAO-1.0.

[20] J. Wilcke, "To fork or not to fork," 2016. https://blog.ethereum.org/2016/07/15/to-fork-or-not-to-fork/.

[21] V. Buterin, "Hard Fork Completed," 20 July 2016. https://blog.ethereum.org/2016/07/20/hard-fork-completed/.

[22] Compound Labs, Inc., "Compound: The Money Market Protocol," 2019. https://compound.finance/documents/Compound.Whitepaper.pdf.

[23] Tether, "Tether: Digital money for a digital age," 2012. https://tether.to/.

[24] Circle, "USDC: the world's leading digital dollar stablecoin," 2018. https://www.circle.com/en/usdc.

[25] MakerDAO, "The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System," 2017. https://makerdao.com/en/whitepaper.

[26] H. Adams, "Uniswap Whitepaper," 2018. https://hackmd.io/@HaydenAdams/HJ9jLsfTz.

[27] H. Adams, N. Zinsmeister and D. Robinson, "Uniswap V2 Core," 2020. https://uniswap.org/whitepaper.pdf.

[28] A. Hayden, N. Zinsmeister and M. Salem, "Uniswap v3 Core," 2021. https://uniswap.org/whitepaper-v3.pdf.

[29] Aave, "AAVE Protocol," 2020. https://github.com/aave/aave-protocol.

[30] Ethereum, "Transaction Hash 0x01afae47b0c98731b5d20c776e58bd8ce5c2c89ed4bd3f8727fad3ebf32e9481," 2020. https://etherscan.io/tx/0x01afae47b0c98731b5d20c776e58bd8ce5c2c89ed4bd3f8727fad3ebf32e9481.

[31] Australian Government, "Anti-Money Laundering and Counter-Terrorism Financing Act 2006," 2006. https://www.legislation.gov.au/Details/C2019C00011.

[32] Australian Government, "Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2017," 2017. https://www.legislation.gov.au/Details/C2017A00130.

[33] Government of Japan, "Payment Services Act," 2009. http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02.

[34] Financial Crimes Enforcement Network, "Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies," 2013. https://www.fincen.gov/sites/default/files/guidance/FIN-2013-G001.pdf.

[35] Internal Revenue Service, "Internal Revenue Bulletin: 2014-16," 2014. https://www.irs.gov/irb/2014-16_IRB#NOT-2014-21.

[36] Government of Singapore, "Payment Services Act 2019," 11 February 2019. https://sso.agc.gov.sg/Acts-Supp/2-2019/Published/20190220?DocDate=20190220&ViewType=Pdf&_=20210521183338.

[37] European Securities and Markets Authority, "Advice on Initial Coin Offerings and Crypto-Assets," 9 January 2019. https://www.esma.europa.eu/document/advice-initial-coin-offerings-and-crypto-assets.

[38] Reuters, "In a world first, El Salvador makes bitcoin legal tender," 2021. https://www.reuters.com/world/americas/el-salvador-approves-first-law-bitcoin-legal-tender-2021-06-09/.

[39] ธนาคารแห่งประเทศไทย, "ข้อมูลเกี่ยวกับ Bitcoin และหน่วยข้อมูลทางอิเล็กทรอนิกส์อื่น ๆ ที่ลักษณะใกล้เคียง," 18 มีนาคม 2557. https://www.bot.or.th/Thai/PressAndSpeeches/Press/News2557/n0857t.pdf.

[40] ธนาคารแห่งประเทศไทย, "ขอความร่วมมือสถาบันการเงินไม่ให้ทำธุรกรรมที่เกี่ยวข้องกับคริปโทเคอเรนซี," 12 กุมภาพันธ์ 2561. https://www.bot.or.th/Thai/FIPCS/Documents/FPG/2561/ThaiPDF/25610039.pdf.

[41] Commodity Futures Trading Commission, "A CFTC Primer on Virtual Currencies.," 2017. https://www.cftc.gov/LabCFTC/Primers/index.htm.

[42] U.S. Securities and Exchange Commission, "Spotlight on Initial Coin Offerings (ICOs)," 7 January 2020. https://www.sec.gov/ICO.

[43] U.S. Securities and Exchange Commission, "Framework for “Investment Contract” Analysis of Digital Assets," 3 April 2019. https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[44] U.S. Supreme Court, "SEC v. Howey Co., 328 U.S. 293 (1946)," 1946. https://supreme.justia.com/cases/federal/us/328/293/.

[45] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on Markets in Crypto-assets, and amending Directive (EU) 2019/1937," 2020. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593.

[46] Australia Securities and Investments Commission, "Information Sheet 225 (INFO 225)," May 2019. https://asic.gov.au/regulatory-resources/digital-transformation/initial-coin-offerings-and-crypto-currency/.

[47] พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล, พ.ศ.2561.

[48] European Court of Justice, "Judgment of the Court (Fifth Chamber) of 22 October 2015," 22 October 2015. http://curia.europa.eu/juris/document/document.jsf?text=&docid=170305&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1636630.

[49] OECD, "Taxing Virtual Currencies An Overview of Tax Treatments and Emerging Tax Policy Issues," 2020. https://www.oecd.org/tax/tax-policy/taxing-virtual-currencies-an-overview-of-tax-treatments-and-emerging-tax-policy-issues.pdf.

[50] Australian Taxation Office, "GST and digital currency," 16 March 2018. https://www.ato.gov.au/business/gst/in-detail/your-industry/financial-services-and-insurance/gst-and-digital-currency/.

[51] Australian Taxation Office, "Tax Treatment of Cryptocurrencies," 30 March 2020. https://www.ato.gov.au/general/gen/tax-treatment-of-crypto-currencies-in-australia---specifically-bitcoin/.

[52] Inland Revenue Authority of Singapore, "Digital Payment Tokens," 25 March 2020. https://www.iras.gov.sg/irashome/GST/GST-registered-businesses/Specific-business-sectors/Digital-Payment-Tokens/.

[53] พระราชกำหนดแก้ไขเพิ่มเติมประมวลรัษฎากร (ฉบับที่ 19), พ.ศ.2561.

[54] Foreverhold, "Everledger," 2015. https://www.everledger.io/.

[55] Tracr, "Tracr," 2019. https://www.tracr.com/.

[56] PwC, "Time for Trust: How Blockchain Will Transform Business and the Economy," October 2020. https://www.pwc.com/gx/en/industries/technology/publications/blockchain-report-transform-business-economy.html.

[57] Department of Industry, Science, Energy and Resources, "National Blockchain Roadmap," 1 February 2020. https://www.industry.gov.au/data-and-publications/national-blockchain-roadmap.

[58] BCI (Thailand), "e-LG (Electronic Letter of Guarantee) on Blockchain," https://en.bci.network/products.

[59] M. Sporny, D. Longley and D. Chadwick, "Verifiable Credentials Data Model 1.0," 2019. https://www.w3.org/TR/vc-data-model/.

[60] D. Reed, M. Sporny and M. Sabadello, "Decentralized Identifiers (DIDs) v1.0," 2021. https://www.w3.org/TR/did-core/.

[61] OpenCerts, "OpenCerts," 2017. https://www.opencerts.io/.

[62] Governmennt of Singapore, "Smart Nation Initiatives," 2014. https://www.smartnation.gov.sg/what-is-smart-nation/initiatives.

[63] สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์, "Digital Identity Guideline for Thailand - Overview and Glossary," พ.ศ. 2561. https://standard.etda.or.th/wp-content/uploads/2019/02/20171204-ER-DigitalID-Overview-V08-30F.pdf.

[64] NDID, "National Digital ID," 2018. https://www.ndid.co.th/.

[65] ธนาคารแห่งประเทศไทย, "Inthanon Phase I," พ.ศ. 2561. https://www.bot.or.th/Thai/PaymentSystems/Documents/Inthanon_Phase1_Report.pdf.

[66] ธนาคารแห่งประเทศไทย & Hong Kong Monetary Authority, "Inthanon-LionRock," 2020. https://www.bot.or.th/English/FinancialMarkets/ProjectInthanon/Documents/Inthanon-LionRock.pdf.

[67] PwC, "PwC CBDC Global Index 2021," 2021. https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-cbdc-global-index-1st-edition-april-2021.pdf.

[68] ธนาคารแห่งประเทศไทย, "ข่าว ธปท. ฉบับที่ 11/2564," 2021. https://www.bot.or.th/Thai/PressandSpeeches/Press/2021/Pages/n1164.aspx.

[69] Project Stella, "Payment systems: liquidity saving mechanisms in a distributed ledger environment," September 2017. https://www.ecb.europa.eu/pub/pdf/other/ecb.stella_project_report_september_2017.pdf.

[70] Project Stella, "Securities settlement systems: delivery-versus-payment in a distributed ledger environment," March 2018. https://www.ecb.europa.eu/pub/pdf/other/stella_project_report_march_2018.pdf.

[71] Project Stella, "Synchronised Cross-Border Payments," June 2019. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604.en.pdf.

[72] Project Stella, "Balancing confidentiality and auditability in a distributed ledger environment," February 2020. https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical200212.en.pdf.

[73] European Central Bank, "Report on a Digital Euro," October 2020. https://www.ecb.europa.eu/pub/pdf/other/Report_on_a_digital_euro~4d7268b458.en.pdf.

[74] Ledger Insights, "Results of China's central bank digital currency giveaway worth $1.3 million," 2020. https://www.ledgerinsights.com/china-central-bank-digital-currency-cbdc-ecny-giveaway-results/.

[75] Ledger Insights, "Latest digital yuan trial is 10x the first. Hong Kong cross border tests start," 2021. https://www.ledgerinsights.com/latest-digital-yuan-trial-is-10x-the-first-hong-kong-cross-border-tests-start/.

[76] Central Bank of The Bahamas, "Digital Bahamas Dollar," 2019. https://www.sanddollar.bs/.

[77] Central Bank of The Bahamas, "Public Update on The Bahamas Digital Currency Rollout," 2020. https://www.centralbankbahamas.com/news/public-notices/public-update-on-the-bahamas-digital-currency-rollout.

[78] Australian National Blockchain, 2018. https://www.australiannationalblockchain.com/.

[79] Government of Japan, "New Regulatory Sandbox Framework in Japan," 2018. https://www.jetro.go.jp/ext_images/en/invest/incentive_programs/pdf/Detailed_overview.pdf .

[80] CEF Digital, "European Blockchain Services Infrastructure," 2019. https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/EBSI.

[81] BSN Development Association, "Blockchain-based Service Network," 2020. https://bsnbase.io/g/main/index.

[82] Singapore Blockchain Innovation Programme, "Singapore Blockchain Innovation Programme," 2020. https://sbip.sg/.

[83] ISO, "ISO/TC 307 Blockchain and distributed ledger technologies," 2016. https://www.iso.org/committee/6266604.html.

[84] IEEE, "P2418.1 - Standard for the Framework of Blockchain Use in Internet of Things (IoT)," 2020. https://standards.ieee.org/project/2418_1.html.

[85] IEEE, "P2418.3 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Agriculture," 2019. https://standards.ieee.org/project/2418_3.html.

[86] IEEE, "P2418.4 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Connected and Autonomous Vehicles (CAVs)," 2018. https://standards.ieee.org/project/2418_4.html.

[87] IEEE, "P2418.5 - Standard for Blockchain in Energy," 2020. https://standards.ieee.org/project/2418_5.html.

[88] IEEE, "P2418.6 - Standard for the Framework of Distributed Ledger Technology (DLT) Use in Healthcare and the Life and Social Sciences," 2018. https://standards.ieee.org/project/2418_6.html.

[89] IEEE, "P2418.7 - IEEE Draft Standard for the Use of Blockchain in Supply Chain Finance," 2018. https://standards.ieee.org/project/2418_7.html.

[90] National Institute of Standards and Technology, "Blockchain Technology Overview," 2018. https://doi.org/10.6028/NIST.IR.8202.

[91] CompTIA, "Blockchain Decision Tree," 2019. https://connect.comptia.org/content/infographic/blockchain-decision-tree.

[92] World Economic Forum, "These 11 questions will help you decide if blockchain is right for your business," 2018. https://www.weforum.org/agenda/2018/04/questions-blockchain-toolkit-right-for-business.

[93] C. Wust and A. Gervais, "Do you need a Blockchain?," 2017. https://eprint.iacr.org/2017/375.pdf.

[94] TrueSec, "Go Ethereum Security Review," 2017. https://github.com/ethereum/go-ethereum/blob/master/docs/audits/2017-04-25_Geth-audit_Truesec.pdf.

[95] NCC Group, "Ethereum Clef Review," 2018. https://github.com/ethereum/go-ethereum/blob/master/docs/audits/2018-09-14_Clef-audit_NCC.pdf.

[96] Least Authority, "Node Discovery Protocol Review Report," 2019. https://github.com/ethereum/go-ethereum/blob/master/docs/audits/2019-10-15_Discv5_audit_LeastAuthority.pdf.

[97] Cure53, "Consulting-Report Ethereum Discv5," 2020. https://github.com/ethereum/go-ethereum/blob/master/docs/audits/2020-01-24_DiscV5_audit_Cure53.pdf.

[98] Agiletech, "Go Ethereum Code Analysis," 2018. https://github.com/agiletechvn/go-ethereum-code-analysis.

[99] Hyperledger, "Hyperledger Security Code Audit," 2018. https://wiki.hyperledger.org/display/SEC/Security+Code+Audits.

[100] ThaiChain Foundation, "ThaiChain," 2019. https://github.com/thaichain.

[101] Compound, "Compound - Security," 2019. https://compound.finance/docs/security.

[102] Uniswap, "Uniswap V2 Audit Report," 2020. https://uniswap.org/audit.html.

[103] Atato, "KULAP Decentralized Exchange Smart Contract Security Review," 2020. https://www.atato.com/wp-content/uploads/2020/11/Kulap-Security-Review.pdf.

[104] Band Protocol, "Secure, Scalable Blockchain-Agnostic Decentralized Oracle," 2020. https://bandprotocol.com/.

[105] Chainlink, "Chainlink," 2017. https://chain.link/.

[106] V. Buterin, "Chain Interoperability," 2016. https://static1.squarespace.com/static/55f73743e4b051cfcc0b02cf/t/5886800ecd0f68de303349b1/1485209617040/Chain+Interoperability.pdf.

[107] Synthetix, "Synthetix," 2018. https://synthetix.io/.

[108] Ethereum, "Ethereum Transaction 0x93819f6bbea390d7709fa033f5733d16418674e99c43b9ed23adb4110d657f0c," 2019. https://etherscan.io/tx/0x93819f6bbea390d7709fa033f5733d16418674e99c43b9ed23adb4110d657f0c.

[109] K. Warwick, "Synthetix Response to Oracle Incident," June 2019. https://blog.synthetix.io/response-to-oracle-incident/.

[110] S. Akter, K. Micheal, M. R. Uddin and G. McCarthy, "Transforming business using digital innovations: the application of AI, blockchain, cloud and data analytics," *Annals of Operations Research,* 2020.

[111] Gartner, "Gartner Top Strategic Technology Trends for 2021," 2020. https://www.gartner.com/smarterwithgartner/gartner-top-strategic-technology-trends-for-2021/.

[112] TEDSummit, "How the blockchain will radically transform the economy," 2016. https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy.

[113] Ripple, "Ripple," 2013. https://ripple.com/.

[114] D. Schwartz, N. Youngs and A. Britto, "The Ripple Protocol Consensus Algorithm," 2014. https://ripple.com/files/ripple_consensus_whitepaper.pdf.

[115] Stellar Development Foundation, "Stellar - an open network for money," 2014. https://www.stellar.org/.

[116] Binance, "Binance Smart Chain," 2020. https://www.binance.org/en/smartChain.

[117] Binance, "Binance Smart Chain," 2020. https://github.com/binance-chain/whitepaper/blob/master/WHITEPAPER.md.

[118] Polkadot, "Polkadot," 2021. https://polkadot.network/.

[119] Diem Association, "Diem Project," 2020. https://www.diem.com/.

[120] Diem Association, "Diem White Paper 2.0," 2020. https://www.diem.com/en-us/white-paper/.

[121] Diem Association, "Diem Announces Partnership with Silvergate and Strategic Shift to the United States," May 2021. https://www.diem.com/en-us/updates/diem-silvergate-partnership/.

[122] Linux Foundation, "Hyperledger," 2016. https://www.hyperledger.org/about.

ที่ปรึกษาและคณะทำงาน

ที่ปรึกษา สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ดร.ชัยชนะ มิตรพันธ์	ผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
ดร.ศักดิ์ เสกขุนทด	รองผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์
มีธรรม ณ ระนอง	รองผู้อำนวยการสำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ที่ปรึกษา มหาวิทยาลัยขอนแก่น

ดร.กิตติ์ เธียรธโนปจัย	หัวหน้าโครงการ
รศ.ดร.วนิดา แก่นอากาศ	นักวิจัยด้านเทคโนโลยีสารสนเทศ
ผศ.ดร.ภัทรวิทย์ พลพินิจ	นักวิจัยด้านเทคโนโลยีสารสนเทศ
ผศ.ดร.เด่นพงษ์ สุดภักดี	นักวิจัยด้านวิศวกรรมศาสตร์
ดร.ปาริฉัตร ศิลปะเทศ	นักวิจัยด้านเศรษฐศาสตร์
ดร.ปิ่นประภา แสงจันทร์	นักวิจัยด้านเศรษฐศาสตร์
รศ.ดร.กฤตพา แสนชัยธร	นักวิจัยด้านนิติศาสตร์ สังคมศาสตร์ บริหารธุรกิจ

คณะทำงาน สำนักงานพัฒนาธุรกรรมทางอิเล็กทรอนิกส์

ขนิษฐ์ ผาทอง	**ธิติกร ตระกูลศิริศักดิ์**
อุษณิษา คุณเอกอนันต์	**กัญญาณัฐ เปรมแสง**
นิธินุช โศภารักษ์	**ชนิดาภา เจริญการณ์**
อัจฉรา จิรเสถียรพร	**จิตติ กุลพฤกษ์**
จิรายุทธ์ กุลพฤกษ์	**พงษ์พันธ์ ศรีปาน**
วีรศักดิ์ ดีอ่ำ	**ทศพร โขมพัตร**