KKU RESEARCH JOURNAL (GRADUATE STUDY)
Vol. 18 NO. 1: January-March 2018

บิตคอยน์และเทคโนโลยีบล็อกเชน

Bitcoin & Blockchain Technology

ลักษนันท์ พลอยวัฒนาวงศ์ (Luxsanan Ploywattanawong)[1]* ดร.ศิรปัฐช์ บุญครอง (Dr.Sirapat Boonkrong)**

บทคัดย่อ

บทความนี้กล่าวถึงบิตคอยน์และเทคโนโลยีบล็อกเชนที่ทั่วโลกกำลังจับตามองถึงการเติบโตและการนำข้อดีของบิตคอยน์และบล็อกเชนมาใช้ประโยชน์ บล็อกเชนเป็นเทคโนโลยีที่อยู่เบื้องหลังความสำเร็จของบิตคอยน์ โดยมีโครงสร้างสถาปัตยกรรมแบบ peer-to-peer สามารถนำมาประยุกต์ใช้กับองค์กรได้หลากหลายรูปแบบ โครงสร้างและการขยายตัวของเทคโนโลยีทั้งสองจึงเป็นสิ่งที่ประเทศต่างๆให้ความสนใจที่จะนำมาประยุกต์ใช้ในด้านการเก็บข้อมูลสำคัญ การจ่ายสวัสดิการ การลดภาระการทำธุรกรรมและการจัดเก็บภาษีมูลค่าเพิ่ม เป็นต้น ผู้ใช้สามารถใช้งานบิตคอยน์ได้ด้วยการเปิดบัญชีใหม่ด้วยตนเอง โดยการสร้างกุญแจสาธารณะและกุญแจส่วนตัวเพื่อใช้ยืนยันข้อความ ความถูกต้องของการทำธุรกรรม ป้องกันปัญหาการคัดลอกไฟล์และความซ้ำซ้อนของการจ่ายเงิน (Double-spending) บิตคอยน์ได้นำวิธีการเข้ารหัสแบบกุญแจสาธารณะ (Public Key Cryptography) มาประยุกต์เพื่อพัฒนาบิตคอยน์ทำให้เกิดความปลอดภัยสูง มีความเป็นส่วนตัว ข้อมูลเป็นสาธารณะ และไม่สามารถปฏิเสธการกระทำใดที่เกิดขึ้นบนทรานเซกชันได้ นับเป็นการปฏิวัติครั้งใหญ่ด้านวงการไอที การเงิน และอีกหลายวงการที่มีความคิดที่จะนำบิตคอยน์และบล็อกเชนไปใช้ประโยชน์ต่างๆ

ABSTRACT

This article discusses Bitcoin and Blockchain technology. The world is paying attention to both technologies in terms of growth and features of Bitcoin and Blockchain. Blockchain is the technology behind Bitcoin success. It has a peer-to-peer architecture and can be applied to any organization. The structures and expansions of the both technologies is what all countries interested. And it needs to be applied in the information of collecting important, social welfare payments, to reduce transaction and tax collection. Users could be open a new account manually by creating a public key and private key to validate the message, accuracy of the transaction, prevent file copying and double-spending. Bitcoin has adopted a public key cryptography method to develop a Bitcoin for high security, privacy data is public and non-repudiation on the Bitcoin transposition. This is a big revolution in the IT industry and many other circles have the idea of bringing Bitcoin and Blockchain to use.

คำสำคัญ: บิตคอยน์ บล็อกเชน การเข้ารหัส

Keywords: Bitcoin, Blockchain, Cryptography

---

[1] *Correspondent author: luxsanun29@gmail.com, luxsanun.p@rmutsb.ac.th*

** นักศึกษา หลักสูตรปรัชญาดุษฎีบัณฑิต สาขาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*

*** รองศาสตราจารย์ ภาควิชาเทคโนโลยีสารสนเทศ คณะเทคโนโลยีสารสนเทศ มหาวิทยาลัยเทคโนโลยีพระจอมเกล้าพระนครเหนือ*

บทนำ

การพัฒนานวัตกรรมความเสมือนจริงในโลกดิจิตอลเกิดขึ้นมากมายในช่วงสิบปีที่ผ่านมา ก่อให้เกิดเทคโนโลยีใหม่ๆ ที่ส่งผลให้เกิดการเปลี่ยนแปลงต่อวงการวิชาการ การศึกษา ตลอดจนการเงินและเศรษฐกิจของโลกปัจจุบัน บิตคอยน์และเทคโนโลยีบล็อกเชน สร้างขึ้นโดย Satoshi Nakamoto ในปีคริสต์ศักราช 2008 บิตคอยน์เป็นสกุลเงินดิจิตอล เมื่อเกิดรายการทางการเงินขึ้นข้อมูลธุรกรรมดังกล่าวจะถูกส่งการกระจายไปยังโหนดต่างๆ บนอินเทอร์เน็ต โดยผู้ทำธุรกรรมทั้งสองฝ่ายสามารถส่งข้อมูลผ่านระบบที่เรียกว่า บล็อกเชน ซึ่งมีระบบรักษาความปลอดภัยด้วยวิธีฟังก์ชันแฮช (Hash Function) ระยะเวลาสามปีที่ผ่านมามีคนมากมายให้ความสนใจการใช้งานบิตคอยน์ และเริ่มมีการนำแนวคิดของเทคโนโลยีบล็อกเชนมาประยุกต์ใช้กับเทคโนโลยีดิจิตอลด้านอื่นๆ นักวิชาการได้คาดการณ์ว่าเทคโนโลยีดังกล่าวจะสามารถเปลี่ยนแปลงการดำเนินชีวิตของเราได้ในอนาคต

บทความนี้มีวัตถุประสงค์เพื่อถ่ายทอดความรู้ความเข้าใจของบิตคอยน์และเทคโนโลยีบล็อกเชน การรักษาความปลอดภัย การประยุกต์ใช้งานเทคโนโลยี ตลอดจนแนวคิดด้านการเงินเสมือนจริงบนเครือข่ายอินเทอร์เน็ตทางธุรกรรมในอนาคต และให้ผู้อ่านสามารถนำความรู้ไปเป็นแนวความคิดในการมองธุรกรรมบิตคอยน์และการประยุกต์ใช้ระบบบล็อกเชนให้ตอบรับกับองค์กรต่างๆ ในอนาคต

วิวัฒนาการของการเงิน: Evolution of Money

การแลกเปลี่ยนเกิดขึ้นเมื่อประมาณ 6,000–7,000 ปีก่อนคริสต์ศักราช [1] โดยการนำสิ่งของที่ตนมีอยู่ไปแลกกับสิ่งอื่นๆ ที่ตนต้องการและขาดแคลน ต่อมาความเจริญทางสังคมทำให้เกิดความต้องการปัจจัยในการดำรงชีวิตมากขึ้น จึงมีการนำวัตถุบางอย่างที่มีค่าในสังคมมาใช้เป็นตัวกลางในการแลกเปลี่ยนกับวัตถุสิ่งของหรือผลิตผลอื่นๆ ที่ตนต้องการ [2] ซึ่งตัวกลางในการแลกเปลี่ยนทำจากแร่ธาตุหรือโลหะที่มีค่าเรียกว่า เงิน เป็นตัวกลางที่ใช้ในการแลกเปลี่ยนสินค้าและบริการ ต่อมาได้มีการเปลี่ยนรูปร่างหน้าตาของตัวกลางให้มีลักษณะเป็นเหรียญและธนบัตร เพื่อใช้ในการแลกเปลี่ยนกันอย่างมีอัตราที่ชัดเจนจนถึงปัจจุบัน [3]

ระบบเงินตราที่ใช้กันอยู่ทั่วโลกคือ ระบบไฟแอทเคอเรินซี่ (Fiat Currency System) เป็นระบบที่รัฐบาลเป็นผู้กำหนดค่าของเงินในการแลกเปลี่ยน แต่ไม่ได้มีสินทรัพย์หนุนหลัง [4-5] ดังนั้นเพื่อให้เกิดความเชื่อมั่น รัฐบาลจึงจำเป็นต้องกำหนดมูลค่าของเงินตราออกมา ระบบไฟแอทเคอเรินซี่นั้นมีข้อดีอยู่ประการหนึ่งคือ รัฐบาลสามารถมีความยืดหยุ่นในการกำหนดค่าเงินให้เป็นไปตามสภาวะเศรษฐกิจในระยะสั้นได้ แต่มีข้อเสียคือ เมื่อเศรษฐกิจล้มหรือรัฐบาลล้มละลายค่าเงินต่างๆ จะหมดความน่าเชื่อถือและค่าเงินจะน้อยลงไปเรื่อยๆ นักธุรกิจบางคนจะเก็บรักษาเงินของตนเองในรูปของทองคำ ซึ่งสามารถรักษามูลค่าได้เมื่อเทียบกับค่าของเงินตรา สิ่งที่สำคัญถัดมาในเรื่องของการเงินและการแลกเปลี่ยนบนโลกปัจจุบันคือ ระบบการชำระเงินดิจิตอล (Digital Payment System) มีการใช้อย่างแพร่หลายบนอินเทอร์เน็ต อย่างเช่น PayPal, Alipay, M-pay, Truemoney, Paysbuy, PromptPay ระบบต่างๆ ที่กล่าวล้วนดำเนินการบนอินเทอร์เน็ต มีทุนจดทะเบียนสูง ภายใต้การรองรับของกฎหมาย และต้องการระบบรักษาความปลอดภัยในการส่งข้อมูลธุรกรรมต่างๆ จึงเป็นที่มาของการคิดหาวิธีการต่างๆ เพื่อนำมาใช้ในการรักษาความปลอดภัยของข้อมูล ระบบรักษาความปลอดภัยของข้อมูลที่ดีต้องสามารถปกป้องรักษาคุณสมบัติของข้อมูล 3 ด้านอย่างครบถ้วนโดยประกอบด้วย ความลับ ความคงสภาพ และความพร้อมใช้งาน

จากการพัฒนาของ Satoshi Nakamoto ทำให้เกิดบิตคอยน์และเทคโนโลยีบล็อกเชนขึ้น บิตคอยน์เป็นสกุลเงินดิจิตอล (Crypto Currency) หรือสินทรัพย์ดิจิตอลที่ออกแบบมาเพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยน ลักษณะของสกุล

เงินบิตคอยน์จะตรงกันข้ามกับเงินกระดาษ (Fiat Currency) มูลค่าของมันจะขึ้นอยู่กับความต้องการอย่างแท้จริง (Demand and Supply) ซึ่งมีอยู่อย่างจำกัด โดยถูกกำหนดตั้งแต่ตอนเริ่มต้นและการเพิ่มค่าความยากในการหาสกุลเงินดิจิตอลนั้นๆ ยิ่งจำนวนสกุลเงินดิจิตอลมีมากขึ้นในระบบ ค่าความยากในการหาบิตคอยน์จะมากขึ้นตามไปด้วย นอกจากแนวคิดเรื่องสกุลเงินดิจิตอลแล้ว Satoshi Nakamoto ได้คิดทฤษฎีทางคณิตศาสตร์ โดยใช้วิธีการเข้ารหัสเพื่อสร้างความปลอดภัยบนบิตคอยน์ [6] และเทคโนโลยีบล็อกเชนที่มีทรานเซกชันที่ดีในการสร้างความน่าเชื่อถือ สำหรับเป็นเครือข่ายในการเชื่อมโยงข้อมูลด้านการแลกเปลี่ยนธุรกรรม ประเทศมหาอำนาจทั่วโลกต่างเฝ้าจับตามองการเติบโตของจำนวนผู้ใช้งานและการเพิ่มขึ้นของจำนวนเงินบิตคอยน์บนระบบ

บิตคอยน์: Bitcoin

บิตคอยน์ หรือ เงินเสมือนจริงในโลกดิจิตอล [7] เป็นระบบการแลกเปลี่ยนที่นักเศรษฐศาสตร์และนักเทคโนโลยีสารสนเทศต่างให้ความสนใจ การจัดการระบบของบิตคอยน์และบล็อกเชน เกิดจากการนำสถาปัตยกรรมแบบ Peer-to-Peer มาประยุกต์ใช้งาน โดยคอมพิวเตอร์ภายในสถาปัตยกรรมจะใช้ซอฟต์แวร์ชนิดเดียวกัน มีการเชื่อมต่อกันและจัดการธุรกรรมต่างๆ ที่เกิดขึ้น ทุกเครื่องสามารถจัดการและแลกเปลี่ยนข้อมูลระหว่างกัน อย่างเช่น เมื่อเราต้องการโอนข้อมูลให้ใครคนใดคนหนึ่งภายในบิตคอยน์ คอมพิวเตอร์ทุกเครื่องที่เชื่อมต่อบนเครือข่ายจะมีข้อมูลของเราที่ทำการโอนเงินไปยังผู้อื่นบนระบบและข้อมูลนี้จะถูกบันทึกและจัดเก็บเหมือนกันหมดทุกเครื่อง ซึ่งมีลักษณะการทำงานคล้ายการเล่น Bit Torrent

การใช้งานบิตคอยน์ ผู้ใช้ต้องติดตั้งซอฟต์แวร์บิตคอยน์และทำการเชื่อมต่อซอฟต์แวร์ที่เกี่ยวข้องกับบัญชีแยกประเภทแบบเปิด (Open/Public Ledger) ของบิตคอยน์ทั่วโลกและทำการสำรองข้อมูลที่เครื่องผู้ใช้ รายการบัญชีแยกประเภท (Ledger) ทุกธุรกรรมและการแลกเปลี่ยนต่างๆ ที่เกิดในบิตคอยน์ จะถูกบันทึกที่โหนดและจะมีการขอคัดลอกรายการบัญชีแยกประเภทจากโหนดมาเก็บไว้ที่เครื่องผู้ใช้ เมื่อมีโหนดใหม่เกิดขึ้นจะมีการขอคัดลอกข้อมูลใหม่และถูกคัดลอกไว้ที่โหนดเก่าของทุกโหนด โดยธุรกรรมบนบิตคอยน์มีการจัดการเก็บข้อมูลของทุกคนบนระบบเป็นลักษณะสาธารณะและกระจายข้อมูลให้ทุกคนรับรู้ทั้งหมด หรือที่เรียกว่า ระบบบัญชีสาธารณะแบบกระจาย (Public Distributed Ledger)

1. คุณสมบัติของบิตคอยน์

บิตคอยน์มีลักษณะเหมือนสกุลเงินแบบดั้งเดิมในด้านกำลังการซื้อและการลงทุน โดยใช้เครื่องมือการซื้อขายออนไลน์เหมือนกับการใช้จ่ายเงินบนโลกดิจิตอล หนึ่งในคุณลักษณะเฉพาะที่แตกต่างกับสกุลเงินระบบไฟแอทเคอเรินซี่ คือ การกระจายอำนาจ บิตคอยน์ไม่ได้ดำเนินการภายใต้องค์กรปกครองหรือสถาบันใดๆ หมายความว่าองค์กรเหล่านี้ไม่สามารถควบคุมได้ ทำให้ผู้ใช้เป็นเจ้าของผลิตภัณฑ์ของตนได้อย่างเต็มที่ นอกจากนี้ธุรกรรมที่เกิดขึ้นบนบิตคอยน์ไม่มีการเชื่อมโยงกับชื่อที่อยู่หรือข้อมูลส่วนบุคคลใดๆ อย่างระบบการชำระเงินแบบเดิมที่มีธนาคารเป็นตัวกลาง ทุกรายการธุรกรรมของบิตคอยน์จะถูกเก็บไว้ในบัญชีแยกประเภทที่ทุกคนสามารถเข้าถึงได้เรียกว่า เทคโนโลยีบล็อกเชน หากผู้ใช้มีที่อยู่สำหรับการใช้งานสาธารณะหรือบัญชีผู้ใช้ (Bitcoin Address) ข้อมูลจะถูกแชร์เพื่อให้ทุกคนเห็น ระบบบัญชีสาธารณะแบบกระจายเป็นบัญชีที่แตกต่างจากธนาคารทั่วไปที่ต้องการข้อมูลมากมาย ซึ่งอาจทำให้ผู้ใช้ตกอยู่ในอันตรายเนื่องจากการฉ้อฉลและแผนการต่างๆ บิตคอยน์ได้นำเทคโนโลยีบล็อกเชนมาใช้ทำให้มีคุณสมบัติไม่รวมศูนย์ ใช้งานง่ายด้วยซอฟต์แวร์หลายประเภท ไม่เปิดเผยชื่อจริงโดยผู้ใช้สามารถใช้นามแฝงในการทำธุรกรรมได้ มีความ

สมบูรณ์โปร่งใส ค่าธรรมเนียมต่ำ ใช้เวลาการโอนเงินรวดเร็วและผู้ใช้ไม่สามารถปฏิเสธความรับผิดชอบในการกระทำใดๆ บนบิตคอยน์ได้ [8]

2. ซอฟต์แวร์บิตคอยน์

ซอฟต์แวร์บิตคอยน์หรือกระเป๋าสตางค์บิตคอยน์ (Bitcoin Wallet) โดยแบ่งออกเป็น 4 ประเภทดังนี้ [9]

2.1 กระเป๋าสตางค์แบบฮาร์ดแวร์ (Hardware Wallet) เป็นอุปกรณ์อิเล็กทรอนิกส์ ที่สร้างขึ้นโดยเฉพาะเพื่อใช้จัดเก็บบิตคอยน์ให้ปลอดภัย หลักการทำงานคือ อุปกรณ์จะทำการจัดเก็บบิตคอยน์และสร้างกุญแจส่วนตัวในระบบออฟไลน์ทำให้ไม่สามารถโจรกรรมข้อมูลได้ เมื่อใช้งานต้องนำอุปกรณ์เชื่อมต่อกับคอมพิวเตอร์หรืออุปกรณ์สื่อสารจึงสามารถใช้งานได้ ตัวอย่างเช่น Ledger Nano, KeepKey, Trezor, Digital Bitbox เป็นต้น

2.2 กระเป๋าสตางค์แบบออนไลน์ (Web Wallet) ผู้ใช้ต้องมีกุญแจส่วนตัวไว้ใช้ออนไลน์ โดยสามารถเข้าใช้งานด้วยบิตคอยน์แอดเดรสที่ผู้ใช้กำหนด ข้อดีคือ สามารถใช้บิตคอยน์ได้จากอุปกรณ์ใดๆ ที่มีการเชื่อมต่อกับอินเทอร์เน็ต ข้อเสียคือ มีความปลอดภัยน้อยที่สุด หากมีการใช้งานกับเครื่องสาธารณะ ตัวอย่างเช่น Coin.Space, Coinbase, Xapo, Coinapult, BitGo, BTC.com, GreenAddress [10]

2.3 กระเป๋าสตางค์สำหรับระบบปฏิบัติการมือถือ (Mobile Wallet) มีให้เลือกใช้ทั้งบน Android และ iOS ซึ่งสามารถใช้งานบนอุปกรณ์ที่เป็นส่วนตัว ตัวอย่างเช่น Mycelium, breadwallet, Copay, Airbitz, GreenBits, Bitcoin Wallet, Coinomi เป็นต้น

2.4 กระเป๋าสตางค์แบบเดสก์ท็อป (Desktop Wallet) เป็นโปรแกรมที่ดาวน์โหลดและติดตั้งไว้ในคอมพิวเตอร์ สามารถใช้งานกระเป๋าสตางค์จากบิตคอยน์กลางได้โดยตรงซึ่งมีความปลอดภัย โดยจะทำการเก็บบิตคอยน์ไว้ในเครื่องคอมพิวเตอร์ที่ไม่ได้มีการเชื่อมต่อออนไลน์ ตัวอย่างเช่น Electrum, Copay, Bitcoin Core, Bitcoin Knots, MultiBit HD, Armory, mSIGNA, Bither, BitGo เป็นต้น

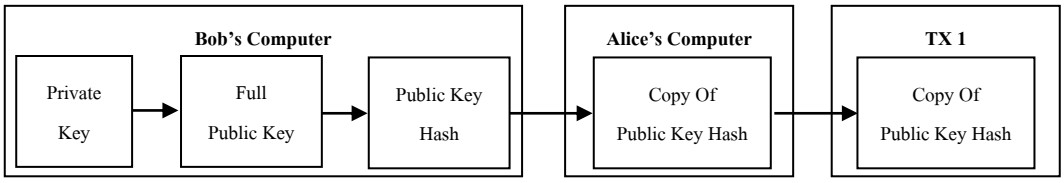
สำหรับการเปิดบัญชีเพื่อใช้งานบิตคอยน์ ประการแรกคือ ผู้ใช้ต้องทำการดาวน์โหลดซอฟต์แวร์สำหรับใช้งาน จากนั้นสร้างบัญชีผู้ใช้ (Bitcoin Address) ระบบบิตคอยน์จะกำหนดตัวเลขขึ้นเพื่อแทนที่อยู่ (Address) เช่น 1XKp7DsovCSS7RstXwkpNqFsjfwma YLvX [11-12] ในการอ้างอิงบิตคอยน์ เพื่อการทำธุรกรรมต่างๆ ซอฟต์แวร์หรือสกุลเงินที่นิยมใช้กัน ตัวอย่างเช่น Dogecoin, Ethereum, Ripple, HyperStake เป็นต้น [13]

3. การใช้จ่ายและเงื่อนไขการทำธุรกรรมบนบิตคอยน์

การใช้เงินบนบิตคอยน์ ผู้ใช้ต้องทำการระบุเงื่อนไขการทำธุรกรรมบนกระเป๋าสตางค์บิตคอยน์ เพื่อใช้ในการส่งข้อมูลตามที่กำหนด สำหรับการจ่ายเงินและการแลกเปลี่ยนของบิตคอยน์จะทำบนทรานเซกชัน ซึ่งต้องมีเงื่อนไข “Bitcoin Scripts” ที่ถูกต้องและสมบูรณ์ จึงจะสามารถใช้จ่ายเงินบนบิตคอยน์ได้และข้อมูลเงื่อนไขนั้นจะถูกเก็บไว้บน Transaction Bitcoin เงื่อนไขทั้ง 4 คือ Send X bitcoins, From address A, To address B, Under condition C โดยการใช้งานบนซอฟต์แวร์บิตคอยน์ของเงื่อนไขทั้ง 4

4. ความปลอดภัยของการทำธุรกรรม

ธุรกรรมบนอินเทอร์เน็ตทั่วไปจะมีระบบการป้องกันที่ดี แสดงให้เห็นจากการทำธุรกรรมบนแอพพลิเคชั่นของธนาคารทั่วไป URL ของระบบจะใช้ https นั่นแสดงให้เห็นว่ามีความปลอดภัยในการทำธุรกรรม โดยมีระบบการจัดการเรื่องการซ่อนข้อมูลของลูกค้าให้เป็นความลับ



ภาพที่ 1 ขั้นตอนการสร้างกุญแจด้วยฟังก์ชันแฮช [16]

ส่วนบิตคอยน์มีการนำเทคโนโลยีบล็อกเชนและการนำกุญแจส่วนตัว (Private Key) มาใช้สร้างกุญแจสาธารณะ (Public Key) ด้วยทฤษฎีทางคณิตศาสตร์ที่เราเรียกว่า ECC (Elliptic curve cryptography) [14-15] ดังภาพที่ 1 ผู้ใช้สามารถสร้างกุญแจส่วนตัวจากรหัสผ่าน ซึ่งเป็นกุญแจที่เป็นความลับด้วยการย่อยข้อมูลก่อนส่งข้อมูลบนบิตคอยน์ให้ผู้รับ

เทคโนโลยีบล็อกเชน: Blockchain Technology

เทคโนโลยีบล็อกเชน คือ สายโซ่ของกล่องหรือก้อน แนวความคิดนี้ถูกสร้างจาก 3 เทคโนโลยี ได้แก่ Private Key Cryptography, Peer-to-Peer Network, และ Program (The Blockchain's protocol) บล็อกเชนได้เปลี่ยนแปลงระบบการเงินจากที่มีธนาคารเป็นศูนย์กลางให้กลายเป็นการสร้างเครือข่ายข้อมูลในรูปแบบของระบบบัญชีสาธารณะแบบกระจาย เพื่อให้เกิดความปลอดภัยและโปร่งใสมากขึ้น รวมถึงช่วยลดต้นทุนในการทำธุรกรรมทางการเงิน ซึ่งไม่เพียงแต่ใช้ประโยชน์ในเรื่องของการเงินเพียงอย่างเดียว แต่สามารถนำไปใช้ในเรื่องการซื้อขายหุ้น อสังหาริมทรัพย์ การจัดการเอกสารจากลายเซ็นดิจิตอล และอื่นๆ ได้อีกมากมาย โดยระบบจะทำงานเชื่อมต่อผ่านเครือข่ายอินเทอร์เน็ต ในประเทศจีนมีการลงทุนสร้าง Server Mining ขนาดใหญ่ที่ตั้งขึ้นเพื่อ "ขุด" ของ แชนด์เลอร์ กั๋ว (Chandler Guo) ผู้ก่อตั้ง BitBank [17]

1. ประเภทของบล็อกเชน

ผู้ใช้สามารถนำเทคโนโลยีบล็อกเชนมาใช้ประโยชน์ได้อย่างหลากหลายไม่ว่าจะเป็นเครือข่ายขนาดเล็กหรือใหญ่ ซึ่งแต่ละประเภทจะเหมาะสมกับการใช้งานต่างกัน โดยพิจารณาจากประเภทของบล็อกเชนทั้ง 3 ประเภทดังนี้

1.1 Public Blockchain เป็นบล็อกเชนที่ใช้งานจริงกับผู้คนทั่วโลกอย่างบิตคอยน์ ข้อดีคือ หากนำมาใช้ไม่จำเป็นต้องลงทุนฮาร์ดแวร์และซอฟต์แวร์ราคาสูง สามารถส่งข้อมูลไปผู้รับปลายทางได้โดยไม่ต้องสร้างช่องทางส่งข้อมูลระหว่างกัน ข้อเสียคือ ข้อมูลที่ถูกส่งผ่าน Public Blockchain จะกลายเป็นข้อมูลที่ถูกเปิดเผยแก่สาธารณะชน

1.2 Private Blockchain เป็นบล็อกเชนที่ใช้งานภายในองค์กรหรือเครือข่ายปิด ข้อดีคือ ลดการเปิดเผยข้อมูล สามารถปรับเกณฑ์ต่างๆ ของเครือข่ายบล็อกเชนให้เหมาะกับลักษณะการใช้งาน โดยอ้างอิงการออกแบบโครงสร้างของ Public Blockchain ซึ่งปกติการส่งเงินบนบิตคอยน์ระบบได้ออกแบบให้มีการรอการตอบรับการทำธุรกรรม 10 – 15 นาทีตามกฎของบิตคอยน์ แต่ถ้ามีการวางระบบ Private Blockchain นั้นสามารถออกแบบให้การรอการตอบรับการทำธุรกรรมให้เสร็จภายใน 2 วินาที ข้อเสียคือ ใช้งบประมาณในการสร้างระบบโครงสร้างในราคาสูง

1.3 Consortium Blockchain เป็นบล็อกเชนที่ใช้งานเฉพาะผู้ได้รับอนุญาต ใช้งานภายในองค์กรเครือข่ายเท่านั้น สำหรับบล็อกเชนประเภทนี้คือ มีการรวมแนวคิดและข้อดีของทั้ง 2 ประเภทข้างต้นเข้าด้วยกัน เป็นแนวคิดที่กำลังได้รับความนิยมสูงในปัจจุบัน เช่น ธนาคารใช้ในการแลกเปลี่ยนข้อมูลการโอนเงินภายในสมาคมธนาคารและธนาคารอื่น หากต้องการเข้าร่วมต้องได้รับอนุญาตจากตัวแทนก่อนจึงจะมีสิทธิ์เข้าใช้งานเครือข่ายร่วมกัน ข้อดีคือ ผู้ใช้ไม่ต้องกังวลว่าข้อมูลสำคัญขององค์กรและลูกค้าจะถูกเปิดเผย ใช้งบประมาณน้อยกว่าการสร้าง Private Blockchain ขึ้นภายในองค์กร ข้อเสียคือ อาจเกิดความไม่คล่องตัวในการปรับปรุงเปลี่ยนแปลงเงื่อนไขการใช้งาน

ดังนั้นการเลือกใช้งานบล็อกเชนประเภทใดนั้นไม่มีข้อกำหนดตายตัว ซึ่งขึ้นอยู่กับลักษณะของงาน เงินลงทุน การบริการและการออกแบบ เพื่อให้รอบรับการขยายตัวในอนาคต

2. โครงสร้างการทำงานของบล็อกเชน

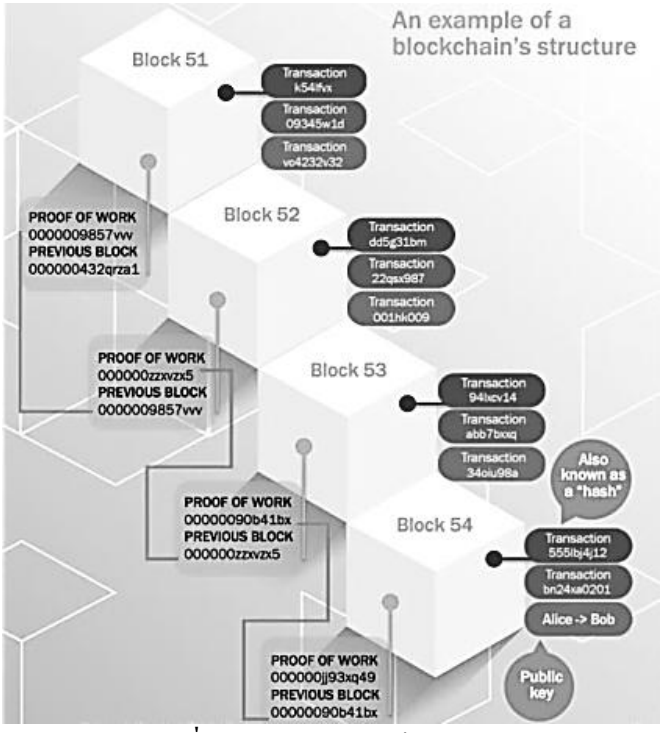
ทำหน้าที่ควบคุมข้อมูลและป้องกันการซ้ำซ้อนของข้อมูล มีโครงสร้างการทำงานดังภาพที่ 2 ซึ่ง Block เป็นหน่วยต่ำสุดของบล็อกเชน และมีโครงสร้างของบล็อก ดังภาพที่ 3 [18] โดยใน 1 Block เก็บข้อมูลได้มากกว่า 1 ทรานเซกชันประกอบด้วย 4 ส่วนหลักๆ คือ

2.1 ID ประจำบล็อก ซึ่งเป็นตัวเลขสุ่มที่ทำการสร้างขึ้นด้วยตัวเลขและตัวอักษรภาษาอังกฤษที่มีขอบเขตเรียกว่า วิธีการฟังก์ชันแฮช

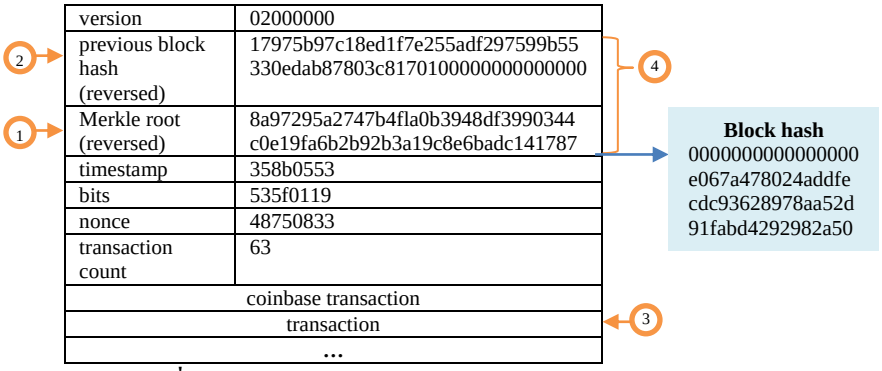
2.2 ID ของบล็อก ก่อนหน้านี้ ที่ทำการป้องกันด้วยการเข้ารหัสฟังก์ชันแฮชไว้เช่นกัน

2.3 ข้อมูลทรานเซกชัน ซึ่งอาจจะมีเพียง 1 ทรานเซกชัน หรือมากกว่านั้นก็ได้

2.4 กุญแจสาธารณะ สำหรับระบุว่าบล็อกนี้เป็นของใคร ใครส่งให้ใคร ใครเป็นผู้รับ



ภาพที่ 2 โครงสร้างของบล็อกเชน [19]



ภาพที่ 3 โครงสร้างภายในบล็อกของบิตคอยน์ [20]

ในทางด้านฐานข้อมูลนั้น บล็อกเชนก็คือ รายการโยงหรือลิงค์ลิสต์ (Linked list) นั่นเอง ภายในบล็อกจะมี Header และทรานเซกชัน สิ่งที่บล็อกเชนเก็บคือ ค่าที่ถูกสร้างขึ้นเพื่อแสดงตัวตนและรักษาความปลอดภัยของผู้ใช้ ด้วยวิธีการฟังก์ชันแฮชโดยไม่ซ้ำกันกับผู้ใช้รายอื่น การอ้างอิงด้วย Block Header มีความสำคัญและจะถูกเก็บไว้ในบล็อกตนเอง บล็อกก่อนหน้าและบล็อกถัดไปที่มีความเกี่ยวข้องในการทำธุรกรรมต่างๆ

ทรานเซกชัน

ทรานเซกชัน (Transaction) ถือเป็นหัวใจหลักของบิตคอยน์และบล็อกเชน ซึ่งมีความเกี่ยวข้องในการเชื่อมต่อจ่ายเงิน คัดลอกไฟล์ข้อมูล ปรับปรุงข้อมูลและทุกเรื่องบนระบบ บล็อกเชนนั้นมีโครงสร้างแบบไม่มีตัวกลางจัดการแตกต่างจากระบบการเงินในปัจจุบันที่มีโครงสร้างแบบมีตัวกลาง (Centralized) ทำหน้าที่จัดการเรื่องการโอนเงินให้บุคคลอย่างระบบธนาคาร บล็อกเชนเป็นระบบฐานข้อมูลแบบกระจายที่มีจุดเด่นแตกต่างจากระบบฐานข้อมูลทั่วไป ดังภาพที่ 4 โดยมีความแตกต่างกัน 5 ประการดังนี้

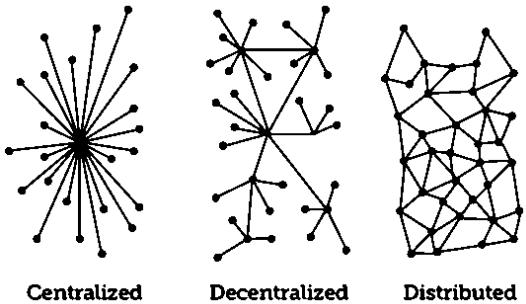
1) แชร์ข้อมูลออกสู่สาธารณะ – เครื่องแม่ข่ายหรือโหนดต่างๆ จะมีหน้าที่ดูแลข้อมูล “แหล่งเก็บบันทึกข้อมูล” หรือเรียกว่า “Block” และทุกโหนดจะมีความสามารถที่ดูได้ว่าข้อมูลทรานเซกชันนั้นๆ ถูกจัดเก็บในบล็อกใด โดยข้อมูลจะมีการรักษาความปลอดภัยแบบ Cryptographic Hash Functions

2) ไม่มีศูนย์กลาง – ในการตรวจสอบทรานเซกชันใดๆ ที่เกิดขึ้น

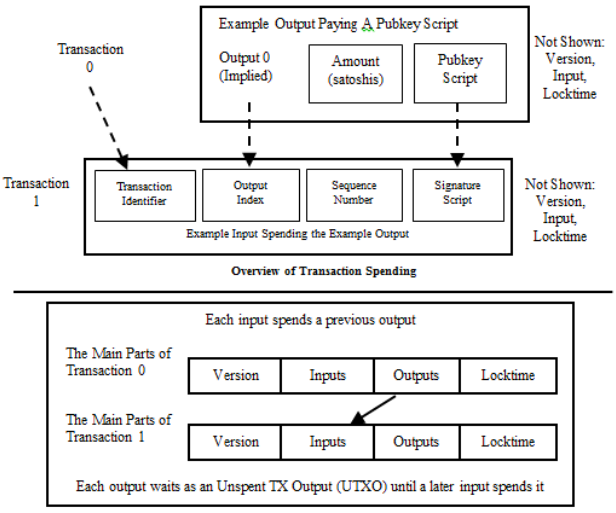
3) มีความปลอดภัย – ข้อมูลจะถูกเก็บในบล็อก ซึ่งไม่มีการเปลี่ยนแปลง ไม่สามารถเอาค่าคืนกลับมาได้หรือแม้กระทั่งจะทำลายข้อมูลเหล่านั้น

4) มีความน่าเชื่อถือ – ด้วยการจัดการแบบไม่มีศูนย์กลางจัดเก็บข้อมูล เมื่อมีทรานเซกชันเกิดขึ้นจากผู้ใช้รายใหม่ ทุกโหนดจะทำการปรับปรุงหรือคัดลอกข้อมูลใหม่

5) ทำงานอัตโนมัติ – ซอฟต์แวร์จะถูกเขียนขึ้นเพื่อป้องกันการเขียนข้อมูลซ้ำซ้อนและการจัดเก็บข้อมูลทรานเซกชันที่เกิดขึ้นจากคนที่ไม่รู้จัก



ภาพที่ 4 ความแตกต่างของเทคโนโลยีบัญชีแยกประเภท [21]



ภาพที่ 5 โครงสร้างทรานเซกชัน

1. โครงสร้างทรานเซกชัน

ทุกทรานเซกชันต้องมีลายเซ็นแบบดิจิตอล (Signature) โดยใช้กุญแจส่วนตัวในการสร้างทรานเซกชันที่เกิดจากบุคคล 2 ฝ่ายคือ ผู้จ่ายและผู้รับ ซึ่งเกิดขึ้นจากเงื่อนไขการทำธุรกรรมบนบิตคอยน์ที่ถูกต้องและสมบูรณ์ สำหรับ

การเก็บข้อมูลของบิตคอยน์แตกต่างจากธนาคารตรงที่ ธนาคารจะทำการเก็บข้อมูลจำนวนเงินปัจจุบัน ส่วนบิตคอยน์ไม่มีการเก็บจำนวนเงินปัจจุบันไว้ สิ่งที่บิตคอยน์เก็บคือ ข้อมูลที่ผู้ใช้ได้รับเงินมา ดังภาพที่ 5 แสดงส่วนสำคัญของธุรกรรมบิตคอยน์ ในแต่ละรายการมีอินพุตและเอาต์พุตอย่างน้อยหนึ่งรายการ โดยระบุการป้อนข้อมูลแต่ละครั้งที่ใช้จ่ายเงินไปให้กับผู้รับก่อนหน้านี้

กระบวนการทำธุรกรรมจะเกิดขึ้นดังตัวอย่างเช่น สมมติ A มีเงินและต้องการจ่ายเงินให้ B 150 BTC โดย A มีเงิน BTC อยู่บนระบบ 2 ก้อน ก้อนแรกจำนวนเงิน 200 BTC และก้องที่สองจำนวนเงิน 300 BTC ภายใต้เงื่อนไขการทำธุรกรรมบนบิตคอยน์นั้นไม่สามารถจ่ายให้ B ได้โดยตรง แต่ต้องทำการจ่ายเงินโดยสร้างทรานเซกชันตามเงื่อนไขให้ถูกต้อง กระบวนการจ่ายเงินจึงจะสมบูรณ์ดังภาพที่ 6

200 > A	มีการส่งเงินมาให้ A ทรานเซกชันที่ 1 จำนวน 200 BTC
300 > A	มีการส่งเงินมาให้ A ทรานเซกชันที่ 2 จำนวน 300 BTC
A > 150 > B	A ทำการจ่ายเงินให้ B 150 BTC จาก ทรานเซกชันที่ 1
A > 50 > A	A ทำการ โอนเงินให้ A 50 BTC จาก ทรานเซกชันที่ 1 เพื่อเป็นการทอนกลับให้ตนเอง

ภาพที่ 6 ตัวอย่างขั้นตอนการทำธุรกรรมบนบิตคอยน์

จากภาพที่ 6 หากต้องการจ่ายเงิน 150 BTC นั้น A จะต้องเอาเงินก้อนหนึ่งก้อนใดมาใช้ เนื่องจากบิตคอยน์มองข้อมูลเป็นก้อน แต่ถ้ายอดจ่ายเงินเกินหรือเงินก้อนนั้นเหลือต้องทำการจ่ายกลับให้ตนเอง และในกรณีนี้ A ใช้เงินก้อน 200 BTC จากทรานเซกชันที่ 1 โดย A โอนเงินให้ B 150 BTC และโอนเพื่อทอนกลับให้ตนเอง 50 BTC ดังนั้นทรานเซกชันที่ 1 จะไม่สามารถใช้ได้อีก หากจะตรวจสอบว่า A เหลือเงินเท่าไหร่ให้ดูจาก ทรานเซกชันที่ยังไม่ถูกใช้งานเรียกว่า Unspent Transaction Outputs หรือ UTXO

ดังนั้น การจ่ายหรือการโอนเงินบิตคอยน์ต้องมีบัญชีรายการนำเข้าและรายการผลลัพธ์ อย่างน้อย 1 รายการ ซึ่งรายการผลลัพธ์ก่อนหน้านี้จะต้องเป็นรายการบัญชีนำเข้าของทรานเซกชันถัดไป หากมีทรานเซกชันเป็นหมื่นเป็นแสน Wallet จะจัดการให้เราทั้งหมด การใช้จ่ายบิตคอยน์นั้นหากสร้างรายการผลลัพธ์กลับคืนไม่ครบเงินจะสูญหายไป และรายการผลลัพธ์ที่ถูกใช้แล้วจะใช้ได้ครั้งเดียว ดังนั้นต้องจ่ายเงินทอนกลับคืนตนเองในทรานเซกชันเดียวกันกับที่ใช้จ่ายออกไปเท่านั้น

2. วัฏจักรการทำงานของทรานเซกชัน: Transaction Life Cycle มีขั้นตอนดังนี้

1) ผู้ใช้เป็นคนสร้าง ทรานเซกชันใหม่

2) ทำการส่งกระจาย (Broadcast) ไปยังฐานข้อมูลที่มีการเชื่อมต่อใช้งานบิตคอยน์ร่วมกัน

3) จากนั้น ECDSA (Elliptic Curve Digital Signature Algorithm) มีหน้าที่ตรวจสอบกุญแจสาธารณะ เมื่อถูกต้องจะเก็บไว้ในฐานข้อมูล

4) ส่งต่อไปยังฐานข้อมูลผู้ใช้รายอื่นๆ เมื่อได้รับข้อมูลจะกระจายส่งต่อไปเรื่อยๆ

5) ถ้า ทรานเซกชัน ซึ่งประกอบด้วย ID ประจำบล็อก ID ของบล็อกก่อนหน้า ข้อมูลทรานเซกชันและกุญแจสาธารณะมีความถูกต้อง จึงจะถูกเพิ่มรายการที่ได้รับการตรวจสอบว่าถูกต้องในบล็อกเชน

3. การตรวจสอบความถูกต้องของบล็อกเชน

บล็อกจะถูกสร้างขึ้นได้ เมื่อมีหลายๆ โหนดทำการตกลงว่าจะยอมรับและมีการตรวจสอบว่า ทรานเซกชันนั้นถูกต้อง กระบวนการนี้จึงถูกเรียกว่า บัญชีแยกประเภทแบบกระจาย (Distributed Ledger) ซึ่งเป็นกระบวนการที่ไม่ต้องใช้การเก็บข้อมูลไว้ส่วนกลางเพื่อใช้ในการตรวจสอบ บล็อกที่ได้รับเลือกต้องผ่านเงื่อนไข 4 ข้อดังนี้

1) มีทรานเซกชันถูกต้อง และมีเงินจ่ายได้จริง

2) แต่ละโหนดจะรวมทรานเซกชันเข้ามา โดยการทำเหมืองข้อมูลเพื่อสร้างบล็อกขึ้นมา

3) ต้องส่งข้อมูลไปให้บล็อกอื่นๆ และต้องถูกเช็คด้วยว่าถูกต้อง

4) จากนั้นถึงจะได้รับการยอมรับให้เลือกเป็นบล็อก

ปัจจุบันมีการสร้างเซิร์ฟเวอร์ ไว้ให้บริการกระบวนการนี้ หรือเรามักจะเรียกว่า การขุด (Mining) สำหรับการตรวจสอบความถูกต้องบล็อกนั้นมีอยู่ด้วยกัน 2 ขั้นตอนคือ

ขั้นตอนที่ 1 พิสูจน์ด้วยกระบวนการ Proof of Work (POW) เพื่อตรวจสอบว่าบัญชีแยกประเภทหรือบัญชีข้อมูลนี้ไม่ได้ถูกแฮกเข้ามา สำหรับเรื่องการป้องกันการโจมตีระบบ จะต้องใช้เหมืองข้อมูล (Block Mining) เข้ามาช่วยตรวจสอบด้วยการคำนวณค่าแฮช โดยการนำค่าตัวเลข (Nonce) มาใส่และคำนวณให้ได้ค่าน้อยกว่า ค่า difficulty ที่ใช้สำหรับคำนวณความยากของสูตรที่ให้เหมืองข้อมูลทำการประมวลผล เพื่อสร้างบล็อกใหม่ต่อไป ซึ่งค่า difficulty จะเพิ่มขึ้นทุกครั้งที่มีบล็อกใหม่เกิดขึ้น โดยใช้ฟังชัน SHA-256 กระบวนการของ POW มีขั้นตอนดังนี้

- รายการใหม่แต่ละรายการจะถูกประกาศไปยังทุกโหนด
- แต่ละโหนดจะทำการเก็บข้อมูลของรายการและเก็บรวบรวมเป็นบล็อก
- แต่ละโหนดจะเป็นผู้ตรวจสอบความถูกต้องของแต่ละบล็อก โดยใช้การคำนวณแก้โจทย์ทางคณิตศาสตร์เพื่อหาค่าตัวเลขที่อยู่ในแต่ละบล็อก ถ้ามีค่าบล็อกแฮช เริ่มต้นด้วย 0 จะประกาศเป็นบล็อกที่ถูกต้องและเชื่อมต่อในบล็อกเชน
- ค่าความยากจะมีการปรับขึ้นไปเรื่อยๆ เมื่อมีการประกาศบล็อกที่ถูกต้องได้ทุกๆ 2016 บล็อก (ปัจจุบันต้องทำการหาค่าแฮช ที่มีเลข 0 นำหน้าถึง 17 หลัก)

ขั้นตอนที่ 2 Proof of Stake ในขณะที่เหมืองข้อมูลดำเนินการตรวจสอบข้อมูลที่เข้ารหัส Proof of Stake จะตรวจสอบความเป็นเจ้าของด้วยจำนวนที่มีการเพิ่มขึ้น

ภายในรายการบัญชีแยกประเภทนั้น ไม่มีการเก็บข้อมูลเจ้าของแต่จะเก็บเพียงข้อมูล ทรานเซกชัน ทั้งหมดที่ผ่านมาเท่านั้น ซึ่งในส่วนนี้กระเป๋าเงินบิตคอยน์จะสามารถอ้างอิงไปยังเจ้าของผ่านทางข้อมูลทรานเซกชันที่ผ่านมานั่นเอง

การประยุกต์ใช้งานบล็อกเชน: Benefit of Blockchain

การประยุกต์ใช้งานบล็อกเชนทำให้บิตคอยน์ถูกใช้ในการแลกเปลี่ยนกันอย่างถูกกฎหมายในประเทศสหรัฐอเมริกา เยอรมนี แคนาดา และญี่ปุ่น นอกจากนั้นยังส่งผลให้เกิดประโยชน์บนการทำธุรกรรมของบิตคอยน์ ดังนี้

1. การใช้บิตคอยน์ เป็นการทำธุรกรรมที่ถูกและเร็วมาก:

เวลาที่ทำธุรกรรมทางการเงินโดยใช้บิตคอยน์ ค่าธรรมเนียมที่เกิดขึ้นนั้นถูกมากๆ เมื่อเทียบกับวิธีการทำธุรกรรมอื่นๆ โดยปกติค่าธรรมเนียมอยู่ที่ 0.0005 BTC ต่อ 1 รายการการทำธุรกรรม (หรือน้อยกว่า 25 สตางค์) ซึ่งหากเทียบกับการทำธุรกรรมทางไกลวิธีอื่น จะเสียประมาณ 700-1300 บาทต่อรายการธุรกรรม และหากใช้บัตรเครดิตจะเสียประมาณ 3-5% ของจำนวนเงินในการทำธุรกรรมนั้นๆ ซึ่งแพงกว่าค่าธรรมเนียมของการธุรกรรมโดยใช้บิตคอยน์ นอกจากนี้การทำธุรกรรมทั่วไปถ้าเป็นการทำธุรกรรมทางไกลจะใช้เวลาประมาณ 2-3 วัน หรือบางครั้งเป็นสัปดาห์ แต่ถ้าหากใช้ Bitcoin การทำธุรกรรมจะสำเร็จภายในไม่กี่ชั่วโมง

2. การโอนเงินบิตคอยน์จะไม่สามารถเรียกคืนได้:

ในการซื้อขายของออนไลน์โดยปกติ ผู้ขายออนไลน์จะมีความกังวลว่าหากรับซื้อด้วยบัตรเครดิต ผู้ซื้อมีสิทธิ์แจ้งเรียกเงินคืนได้ ด้วยเหตุผลต่างๆนานา เช่น ลูกค้าไม่ได้เป็นผู้ใช้งานบัตร บัตรถูกขโมย แต่ผู้ขายของออนไลน์ได้ส่งสินค้าแล้ว แต่กลับได้รับข้อความจากทางธนาคาร และโดนเรียกเงินคืนด้วยเหตุผลต่างๆ ผู้ขายอาจไม่สามารถทำอะไรได้ นอกจากส่งเอกสารยืนยันว่าส่งสินค้าจริง ซึ่งอาจทำให้เสียเวลาและความไว้ใจในการทำธุรกิจ ทำให้ผู้ขายสูญเสียโอกาสและรายได้ส่วนนั้นไป ถ้าเป็นการทำธุรกรรมทางการเงินของบิตคอยน์จะไม่สามารถเรียกคืนได้ 100% ด้วยเหตุผลนี้ หากต้องการส่งจะรับด้วยบิตคอยน์ ผู้ใช้บิตคอยน์มั่นใจว่าได้ทำการส่งเงินให้กับผู้รับที่ไว้ใจได้ และที่อยู่ของบิตคอยน์นั้นมีความถูกต้อง

3. การทำธุรกรรมทางการเงินของบิตคอยน์ ไม่ต้องมีเอกสารให้ยุ่งยาก :

การซื้อ – ขายบิตคอยน์ สามารถเป็นใครหรือจากประเทศใดก็สามารถทำธุรกรรมด้วยบิตคอยน์ได้ทั้งนั้น โดยลดความยุ่งยากเรื่องเอกสารและใช้เวลาน้อยในการดำเนินงาน

หลายปีที่ผ่านมาทางหน่วยงานที่ปรึกษาด้านวิทยาศาสตร์และเทคโนโลยีของรัฐบาลสหราชอาณาจักรได้ตีพิมพ์และนำเสนอการนำบล็อกเชนมาใช้กับภาครัฐบาลสหราชอาณาจักร ซึ่งมีแนวทางที่นำเสนอ 5 ประการ [22]

1) เพื่อใช้ในการจัดเก็บข้อมูลที่ต้องการความปลอดภัยจากการโจมตีในโลกไซเบอร์

2) เพื่อใช้ในการจัดเก็บข้อมูลรวมถึงการจ่ายสวัสดิการและบำนาญ เพื่อแก้ไขปัญหาความผิดพลาดและความซ้ำซ้อนของข้อมูลด้านการจ่ายเงิน

3) เพื่อการจ่ายเงินช่วยเหลือให้กับต่างประเทศโดยเฉพาะในประเทศด้อยพัฒนา ที่มักพบว่าการจ่ายเงินไม่เป็นไปตามวัตถุประสงค์ ซึ่งบล็อกเชนจะช่วยในเรื่องของการตรวจสอบการใช้เงินได้ง่ายขึ้น

4) เพื่อลดภาระค่าใช้จ่ายในการทำธุรกรรมของ SMEs ในการบันทึกข้อมูลสินทรัพย์ต่างๆ อย่างสิทธิบัตร ที่ดินและทะเบียนต่างๆ ด้วยระบบบล็อกเชน

5) เพื่อการจัดเก็บภาษีมูลค่าเพิ่ม ทวีปยุโรปมีระเบียบที่ยุ่งยากและซับซ้อน เนื่องจากมีสมาชิกหลายประเทศ ระบบบล็อกเชนสามารถช่วยเก็บข้อมูลด้านการซื้อขาย ซึ่งทำให้ง่ายต่อการตรวจสอบชำระภาษีต่างๆ

นอกจากนั้นรัฐบาลเวียดนามกำลังเตรียมร่างกฎหมายรองรับสกุลเงินบิตคอยน์ออกมาใช้งานในปลายปี 2017 [23] และในปีเดียวกันธนาคารภายในประเทศไทยเริ่มมีบริการระบบโอนเงินระหว่างประเทศไทยและญี่ปุ่นโดยใช้เทคโนโลยีบล็อกเชนของ Ripple จากแนวคิดทฤษฎีต่างๆ หากนำมาวิเคราะห์กับปัญหาของประเทศไทยนั้น พบว่าแนวทางที่น่าจะมีศักยภาพสำหรับภาครัฐบาลไทยในการนำเทคโนโลยีบล็อกเชนมาประยุกต์เพื่อสร้างความโปร่งใสในการจัดเก็บข้อมูลโฉนดที่ดิน การเชื่อมต่อข้อมูลเวชระเบียนผู้ป่วยระหว่างสถานพยาบาล การเบิกจ่ายเงินสวัสดิการภาครัฐหรือการช่วยเหลือคนยากจน การใช้ Smart Contract ในการเบิกจ่ายเงินในโครงการของรัฐ และด้านอื่นๆ อีกหลากหลายมิติ [24] ซึ่งประโยชน์ของบล็อกเชนสามารถนำมาเป็นเครื่องมือที่ช่วยผลักดันให้เกิดการพัฒนามากขึ้น

สรุปผลการศึกษา

หลายประเทศทั่วโลกทั้งภาครัฐบาลและเอกชนได้ให้ความสนใจกับบิตคอยน์และบล็อกเชน เพื่อจะนำเทคโนโลยีดังกล่าวไปประยุกต์ใช้ในการแก้ปัญหาและเพิ่มประสิทธิภาพการจัดการข้อมูล บิตคอยน์เป็นสกุลเงินดิจิตอลที่ทำงานอยู่บนเทคโนโลยีบล็อกเชน สามารถใช้เป็นสื่อกลางในการแลกเปลี่ยนกันทั่วโลก Satoshi Nakamoto เป็นผู้คิดค้นและนำทฤษฎี Cryptographic Hash Function มาใช้ในการรักษาความปลอดภัยด้วยกุญแจสาธารณะและ

กุญแจส่วนตัวแก่ผู้ใช้งานบิตคอยน์ ทุกธุรกรรมจะทำงานอยู่บนโครงสร้างทรานเซกชันแบบบัญชีแยกประเภทแบบกระจาย ซึ่งทำให้ทุกข้อมูลบนบล็อกเชนสามารถตรวจสอบความถูกต้องบนบล็อก โดยกระบวนการ Poof of Work และ Poof of Stake นอกจากนั้นด้วยคุณสมบัติที่ไม่รวมศูนย์ ใช้งานง่าย ไม่เปิดเผยชื่อจริง มีความสมบูรณ์โปร่งใส ค่าธรรมเนียมต่ำ มีความรวดเร็วและไม่สามารถปฏิเสธความรับผิดชอบในการกระทำใดๆ บนบิตคอยน์ได้ ทำให้บิตคอยน์และบล็อกเชนเป็นอีกเทคโนโลยีหนึ่งที่อาจเปลี่ยนแปลงระบบการจัดการฐานข้อมูลที่เกี่ยวข้องกับการแลกเปลี่ยนเงินตราและระบบไอทีในอนาคต

เอกสารอ้างอิง

1. Lakakul N. Saranukromthai. Thailand encyclopedia project for youth. Bangkok: the whim of the king; 2001.
2. Luo GY. The evolution of money as a medium of exchange. Journal of Economic Dynamics and Control. 1998; 23(3): 415-458.
3. Drake PJ. Classical Economics to Development Economics. New York: Springer; 1994. 94-103.
4. Mckinnon RI. Money in international exchange: the convertible currency system. Oxford University Press; 1979.
5. Taub B. Private fiat money with many suppliers. Journal of Monetary Economics. 1985; 16(2): 195-208.
6. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system; 2008.
7. Grinberg R. "Bitcoin: An innovative alternative digital currency."; 2011.
8. Bitcoin & blockchain technology. [Internet]. 2017. Retrieved May, 2017, from https://www.slideshare.net/dendej/bitcoin-blockchain-technology-kmutnbit
9. Bitcoin wallet. [Internet]. 2017. Retrieved May, 2017, from https://bitcoin.org/en/choose-your-wallet
10. Bitcoin. [Internet]. 2017. Retrieved May, 2017, from https://greenaddress.it/th/
11. Bitcoin address. [Internet]. 2017. Retrieved May, 2017, from https://payniex.com/
12. Bitcoin address. [Internet]. 2017. Retrieved May, 2017, from https://coin.co.th/wallet
13. Bitcoin currency. [Internet]. 2017. Retrieved May, 2017, from https://bx.in.th
14. Hankerson D, Menezes AJ, Vanstone S. Guide to elliptic curve cryptography. Springer Science & Business Media, 2006.
15. Anoop MS. Elliptic curve cryptography. An Implementation Guide, 2007.
16. Bitcoin. [Internet]. 2017. Retrieved May, 2017, from https://bitcoin.org/en/developer-guide#transactions
17. Blockchain revolution. [Internet]. 2017. Retrieved May, 2017, from http://thaipublica.org/2016/07/ blockchain-revolution/
18. Walport M. Distributed Ledger Technology: Beyond Blockchain. UK Government Office for Science, 2016.
19. Blockchain structure. [Internet]. 2017. Retrieved May, 2017, from https://www.pinterest.com/oeroeboeroe/ blockchain/
20. Structure of a Bitcoin block [Internet]. 2017. Retrieved May, 2017, from https://bitcoin.stackexchange.com/ questions/51300/how-to-prevent-a-minner-steal-another-miners-blockby-what-validation

21. Blockchain-distributed ledger technology. [Internet]. 2017. Retrieved May, 2017, from https://www.linkedin.com/pulse/blockchain-distributed-ledger-technology-david-cox
22. Distributed Ledger Technology: beyond block chain. [Internet]. 2015. Retrieved May, 2017, from https://www.gov.uk/ government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledgertechnology.pdf
23. Vietnam will support legislation Bitcoin in 2017. [Internet]. 2017. Retrieved May, 2017, from http://www.eworldmag.com
24. Blockchain & Thailand 4.0. [Internet]. 2017. Retrieved May, 2017, from http://www.nbtc.go.th/