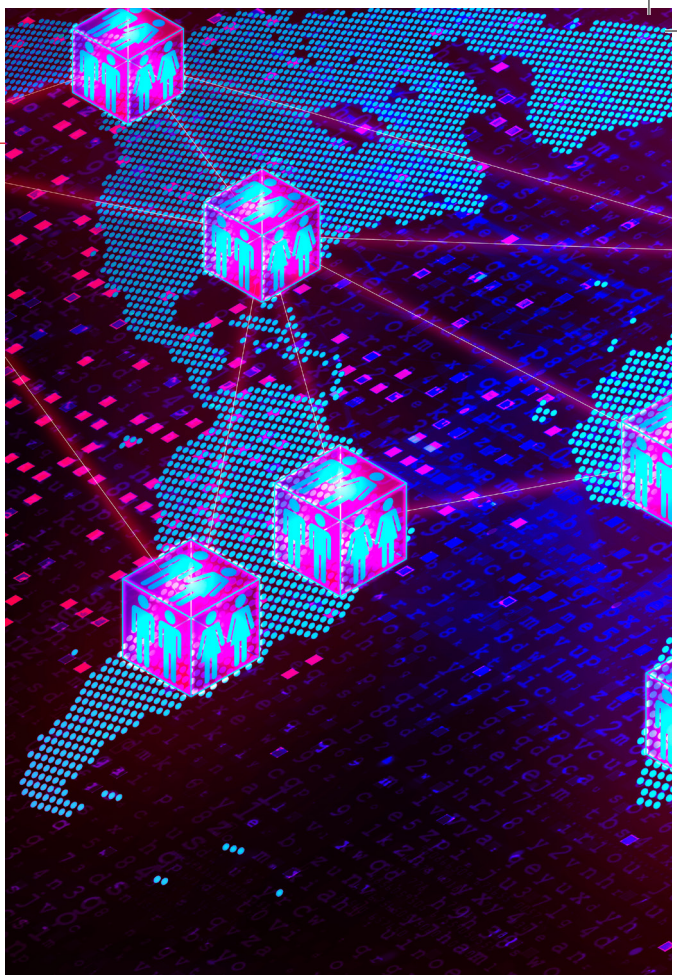
บล็อกเชน พื้นฐาน Blockchain Fundamental

- จุดกำเนิดของบล็อกเชน (Beginning of Blockchain)
- ฐานข้อมูลแบบกระจาย (Decentralized Database)
- Peer-to-Peer Network
- ธุรกรรมแบบไหนถึงเข้าข่าย
- องค์ประกอบของบล็อกเชน
- บล็อก (Block)
- กุญแจสาธารณะและกุญแจส่วนบุคคล (Public and Private Keys)
- การขุดเหมือง (Mining)
- โทเคน หรือ เหรียญ (Tokens or Coins)
- Smart Contracts (สัญญาอัจฉริยะ)

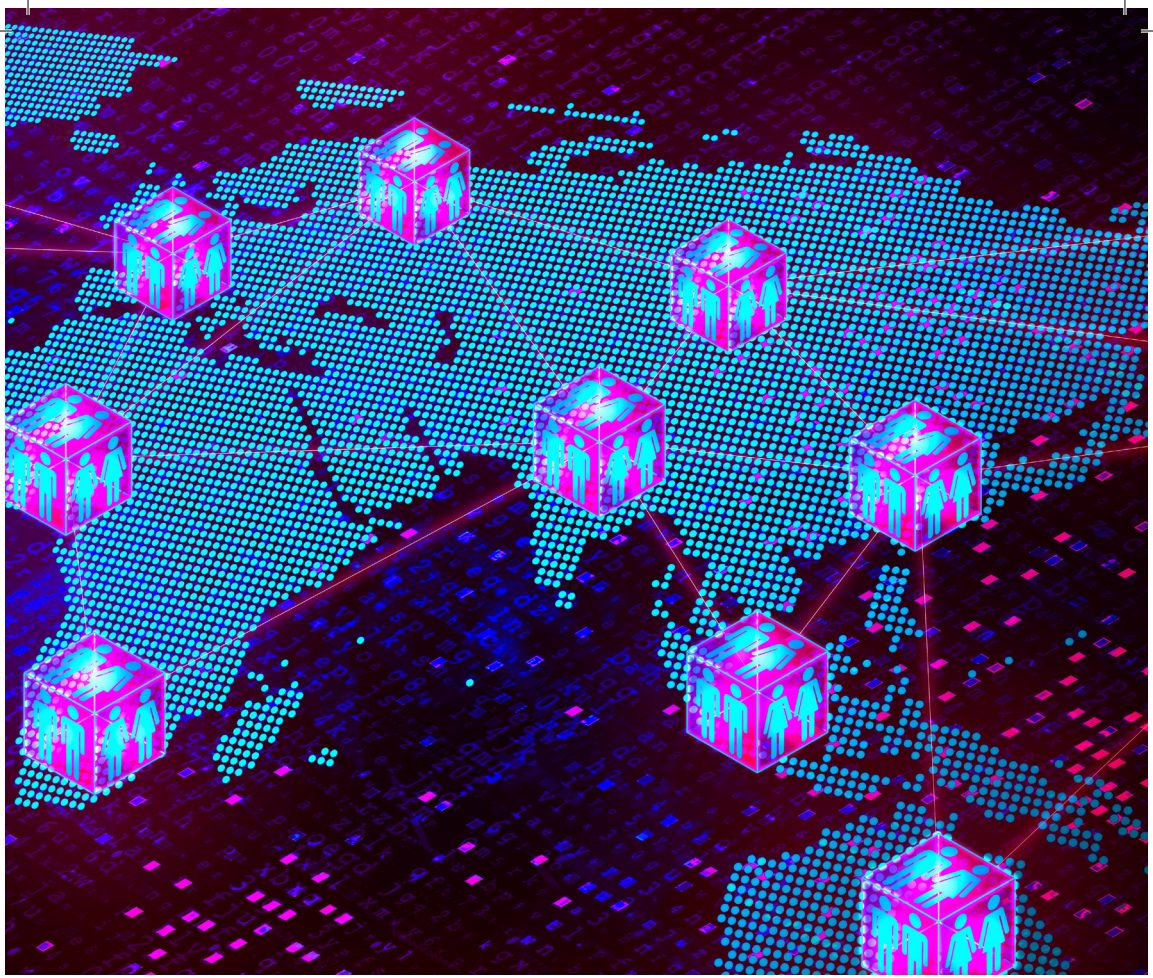
จุดกำเนิดของบล็อกเชน Beginning of Blockchain

ไอเดียของเทคโนโลยีบล็อกเชนนั้นเริ่มต้นเป็นที่รู้จักครั้งแรกในช่วงปี ค.ศ.2008 ซึ่งเป็นช่วงเดียวกับที่โลกใบนี้กำลังเผชิญหน้ากับวิกฤตการณ์เงินครั้งใหญ่ของโลกที่มีชื่อว่า วิกฤตแฮมเบอร์เกอร์ หรือ วิกฤตสินเชื่อซับไพรม์ (Subprime Mortgage Crisis) ซึ่งสร้างความหายนะให้แก่ความมั่งคั่งของคนจำนวนมากไปทั่วโลก แต่ท่ามกลางวิกฤตที่ร้ายแรงครั้งหนึ่งของมวลมนุษยชาติก็มีโอกาสด้านเทคโนโลยีใหม่ๆ เกิดขึ้นเช่นกัน นั่นก็คือการถือกำเนิดขึ้นของบล็อกเชน อย่างที่ได้กล่าวไป มันถือกำเนิดขึ้นมาเคียงคู่กับสิ่งที่เรียกว่า คริปโทเคอร์เรนซี ซึ่งมีชื่อว่า บิตคอยน์ (Bitcoin) จากบุรุษนิรนามที่มีชื่อว่า ซาโตชิ นากาโมโตะ (Satoshi Nakamoto) ในเดือนตุลาคม ค.ศ.2008 พร้อมกระดาษ 9 หน้าที่ถือเป็นสาระสำคัญที่พูดถึง

ระบบ “Bitcoin: A Peer-to-Peer Electronic Cash System” แปลเป็นไทยว่า บิตคอยน์: ระบบการเงินอิเล็กทรอนิกส์แบบไร้ตัวกลาง โดยการมาของเทคโนโลยีนี้ได้เข้ามาแก้ไขปัญหาสำคัญ 2 เรื่องที่เรียกว่า The Double-Spend Problem เพราะบิตคอยน์ผ่านการมีเทคโนโลยีบล็อกเชนอยู่เบื้องหลังได้เข้าแก้ไขปัญหาธุรกรรมทั้งโลกจริงและโลกดิจิทัลที่ไม่เคยแก้ไขได้คือ การใช้ตราประทับบอกเวลาของเหตุการณ์และการเข้ารหัสธุรกรรม (Time-Stamps and Cryptography) เข้ามาแก้ไขปัญหาการทำธุรกรรมซึ่งตรงนี้เป็นการเพิ่มมูลค่าให้แก่โลกของอินเทอร์เน็ตแบบก้าวกระโดด พร้อมตอบโจทย์ด้านความปลอดภัย ความยืดหยุ่น และต้นทุนในการทำธุรกรรมที่คาดกันว่าจะถูกลงจากการมาของเทคโนโลยีบล็อกเชนที่เป็นหนึ่งในเทคโนโลยีของโลก 4.0 นี้



บล็อกเชนพื้นฐาน Blockchain Fundamental



ความหมายของบล็อกเชนหากเราไปค้นหาในอินเทอร์เน็ตก็มักจะได้ความรู้ที่ค่อนข้างจะสับสน เพราะว่าอ่านจากตรงไหนก็มีความหมายคล้ายๆ กันหรือแบบเดียวกันหมด จนอ่านจบแล้วก็ยังไม่แน่ใจว่าตัวเราคนอ่านเองเข้าใจมันจริงๆ ไหม ที่จริงแล้วความหมายของบล็อกเชนหรือจะเรียกคำนิยามก็ได้นั้นค่อนข้างจะสั้นและเรียบง่ายมากนั่นก็คือ ฐานข้อมูลแบบไม่รวมศูนย์ซึ่งทำงานไปพร้อมๆ กันผ่านข้อตกลงเก่าๆ ที่เชื่อมโยงกันเท่านั้นของธุรกรรมทั้งหลายทั่วทั้งเครือข่ายแบบ Peer-to-Peer (P2P เดี๋ยวจะอธิบายต่อไป)

ฐานข้อมูลแบบกระจาย Decentralized Database

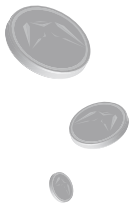
หนึ่งในจุดเด่นสำคัญของบล็อกเชนที่คนพูดถึงกันมากคือ มีฐานข้อมูลแบบกระจายศูนย์ แต่ก่อนจะไปถึงเรื่องนั้นหลายคนยังงงกับคำว่า ‘ฐานข้อมูล’ (Database) อยู่ จึงขอยกตัวอย่างให้เห็นภาพง่ายๆ เช่น สมุดหน้าเหลือง หรือ เยลโล่เพจเจส ที่คนยุคเก่ารู้จักกัน หรือคนยุคใหม่หน่อยก็ให้สังเกตว่าเวลาเราเข้าเว็บไซต์มันจะมี ‘ช่องค้นหา’ การค้นหาของเราผ่านช่องนั้นระบบมันจะไปค้นมาจากฐานข้อมูลที่ถูกเก็บเอาไว้ทั้งหมดตามข้อความที่เราระบุหรือข้อความที่ใกล้เคียงมาแสดงให้เราดู เพราะฉะนั้นฐานข้อมูลก็คือคลังของข้อมูลนั่นเอง

เราจะเห็นว่าจากความหมายด้านบนที่บอกไปนั้นทำให้ภาพของคำว่า ฐานข้อมูลแบบกระจาย (Decentralized Database) เด่นชัดขึ้นมา เพราะแม้มันจะมีคำว่ากระจายอยู่แต่ไม่ได้หมายความว่า การเก็บข้อมูล

จะเป็นไปในลักษณะต่างคน (คนในที่นี้หมายถึง โหนด (Node)) แต่เพื่อความเข้าใจที่ง่ายขอเรียกว่าคนแทน) ต่างเก็บ การเก็บข้อมูลของบล็อกเชนนั้นยังคงรวมศูนย์อยู่แค่ที่เดียวเท่านั้น แต่ชุดสำเนานี้จะถูกกระจายออกไปให้หลายคนช่วยกันเก็บ และเมื่อมันเป็นสำเนาหรือชุดที่คัดลอกกันมามันก็จะเหมือนกัน ขณะที่ตัวบล็อกเชนเองไม่มีคนควบคุมระบบแบบเบ็ดเสร็จเด็ดขาดเพียงลำพังแต่เพียงผู้เดียว ตรงนี้จะต่างจากระบบจำนวนมากที่เราใช้กันในปัจจุบัน เช่น ธนาคาร ที่จะเป็นคนดูแลและควบคุมการกิจกรรมเกี่ยวกับเงินของเราทั้งหมด เราโอนเงินไปไหน ให้ใคร เวลาใด ที่ไหน ธนาคารจะเป็นคนจดบันทึกให้ อำนาจจึงอยู่ที่ธนาคารแต่เพียงผู้เดียวทำให้ธนาคารจึงมีลักษณะเป็นระบบฐานข้อมูลแบบรวมศูนย์ (Centralized Database System) ซึ่งอยู่ขั้วตรงข้ามกับบล็อกเชน

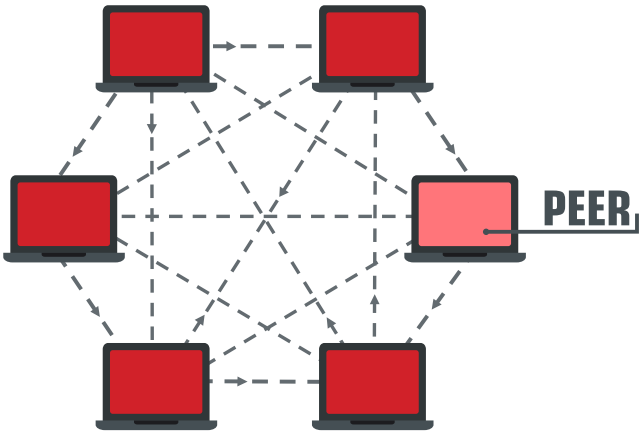
โดยปกติแล้ว ฐานข้อมูลแบบกระจายมีผู้อ่านและผู้เขียนจำนวนมาก เมื่อเซิร์ฟเวอร์ (Server) หรือ เครื่องบริการ หรือ เครื่องแม่ข่ายบนเครือข่ายส่งข้อมูลไปยังลูกค้า รูปแบบของสถาปัตยกรรมข้อมูล (รูปร่างหน้าตาของชุดข้อมูลรวมไปถึงการจัดเรียงด้วย) การส่งนั้นจะเป็นฐานข้อมูลแบบกระจาย (Distributed Database) นั่นก็คือทุกคนที่อยู่บนเครือข่ายนี้จะได้รับข้อมูล โดยข้อมูลที่ได้จะมีจำนวนเท่ากันและได้สิทธิที่จะมีได้เท่ากัน (ตรงนี้ทำให้ทุกคนมีอิสระหรือมีสิทธิตอบโต้ได้อย่างเต็มที่) และตรงนี้เองที่ทำให้บล็อกเชนจึงมีฐานะเป็นฐานข้อมูลแบบกระจายเพราะไม่มีผู้กำหนดบนระบบทั้งหมดหรือข้อมูลทั้งหมด

เพราะฉะนั้นในข้อเท็จจริงแล้ว บล็อกเชนคือการที่ทุกคนเห็นด้วยกับข้อตกลงนี้ที่สุดท้ายจะกลายเป็นประวัติศาสตร์ธุรกรรม แต่เทคโนโลยีบล็อกเชนมีความพิเศษในแง่ของฐานข้อมูลที่ถูกเรียกว่า Distributed Ledger แปลเป็นไทยแบบตรงตัวก็คือ การจดบัญชีแบบกระจาย แต่อ่านแล้วก็ยังงงอยู่ดี เพราะฉะนั้นขออนุญาตขยายความเพิ่มเพื่อความเข้าใจ มันคือฐานข้อมูลที่ถูกยินยอมให้แบ่งปันและมีความเชื่อมโยงกับหลากหลายสถานที่สถาบันภูมิศาสตร์ และที่สำคัญคือผู้คนเข้าไปใช้งานง่าย ตรงนี้ทำให้การทำธุรกรรมจะต้องมี ‘พยาน’ เกิดขึ้น นั่นหมายความว่า Ledger ถูกออกแบบให้สามารถติดตามร่องรอยของธุรกรรมได้ ผ่านการมีส่วนร่วมของแต่ละคนในเครือข่ายที่สามารถเข้าถึงข้อมูลที่ถูกแบ่งปันทั่วทั้งเครือข่าย และเป็นเจ้าของสำเนาข้อมูลชุดนั้นได้ด้วย

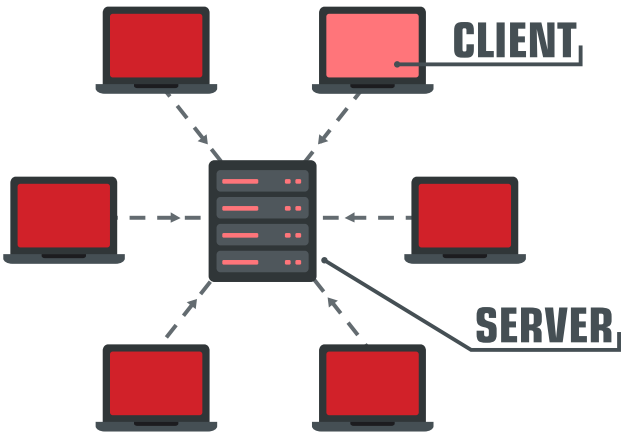


NETWORK TYPES

PEER-TO-PEER (P2P) NETWORK



CLIENT-SERVER NETWORK



Peer-to-Peer Network

บล็อกเชนนั้นถือเป็นหนึ่งในลักษณะของ Distributed Ledger Technology (DLT) การเปลี่ยนแปลงทั้งหมดของ DLT จะถูกออกแบบ 2 ลักษณะหลักๆ ได้แก่

1. ดำเนินการบนระบบที่เรียกว่า Peer-to-Peer Network เป็นระบบเครือข่ายของคอมพิวเตอร์ที่เชื่อมต่อเครื่องคอมพิวเตอร์ในแต่ในละเครื่องโดยไม่ต้องผ่านคอมพิวเตอร์หลัก

2. ใช้ต้นแบบการยอมรับจากคนส่วนใหญ่ที่เรียกว่า Consensus Protocol

นั่นหมายความว่า บล็อกเชนจะต้องมีเครือข่ายระบบคอมพิวเตอร์เบื้องหลังอาจจะเป็นคนหรือไม่ก็ได้ แต่มีคนจำนวนมากโดยใช้คนจำนวนที่มากนี้ช่วยกันตรวจสอบฐานข้อมูลหากมีการเปลี่ยนแปลงเพื่อสร้างการยอมรับจากการคนส่วนใหญ่ แทนที่การมีศูนย์กลางอำนาจที่คอยจัดการ

คนเดียวแบบเบ็ดเสร็จเด็ดขาด โดยข้อดีของการใช้กลไกความคิดเห็นส่วนรวม (Consensus Mechanism) ก็คือมันสามารถอนุญาตให้เกิดการมีส่วนร่วมจำนวนมากเพื่อที่จะรักษาความจริงร่วมกันผ่านการใช้ต้นแบบนี้ ช่วยลดการโต้เถียงสำหรับการทำงานของธุรกรรมแบบดั้งเดิมไป เช่น เมื่อเราเข้าไปซื้อของในร้านค้าแล้วได้ของมาตรงแต่ปัญหาคือรายละเอียดด้านในไม่ตรง คราวนี้พอจะเปลี่ยนใบเสร็จรับเงินดันหายเพราะไม่คิดว่าจะมีปัญหาอีกแล้ว ตรงนี้หากอยู่ในรูปของเทคโนโลยี DLT ก็จะไม่มีปัญหาเพราะมีเครือข่ายคอยรับรองความถูกต้องทั้งหมดแม้แต่รายละเอียดเอาไว้ให้แล้ว ตรงส่วนนี้เขาจะเรียกกันว่า “Agreed-Upon” ขณะที่อีกส่วนคือ “Append-Only” หมายถึงธุรกรรมเหล่านี้ถูกบันทึกและถือโดยบุคคลต่างๆ (หรือจะเรียกว่า โหนด (Node) หรือ Peer ก็ได้) โดยที่พวกเขาจะสามารถเพิ่มได้เท่านั้น แต่ลบไม่ได้ โดยบันทึกเหล่านี้จะมีความเชื่อมโยงกันเพื่อสะท้อนความเปลี่ยนแปลงและสถานะปัจจุบันของเครือข่าย ขณะที่ฐานข้อมูลเหล่านี้จะคงอยู่ถาวร ให้นึกภาพคุณเข้าไปยืมหนังสือในห้องสมุดแล้วบรรณารักษ์จะมีการบันทึกคนยืมก่อนหน้านี้เป็นใคร ยืมไปเมื่อไร เวลาใด และจะต้องคืนวันไหน เอาไว้ทั้งหมด นั่นหมายความว่าไม่ว่าจะเกิดอะไรขึ้นกับหนังสือเล่มนี้มันจะถูกบันทึกเอาไว้หมดอย่างละเอียดถึงช่วงเวลาก่อนหน้านี้และไม่มีใครลบมันได้