

Smart Contract สัญญาอัจฉริยะบนความมั่นคงปลอดภัยของ Blockchain

บล็อกเชน (Blockchain) นับได้ว่าเป็นที่จัดเก็บข้อมูลที่มีความปลอดภัยสูง สามารถนำมาปรับใช้กับการทำงานได้อย่างมีประสิทธิภาพทั้งในส่วนของผู้ประกอบการขนาดใหญ่จนถึงขนาดย่อมหรือ SMEs ซึ่งในบทความนี้จะยกตัวอย่างกรณีศึกษาเกี่ยวกับการนำเทคโนโลยีบล็อกเชนมาใช้เพื่อเพิ่มประสิทธิภาพการทำงานกับสัญญาอัจฉริยะ (smart contract)

แต่ก่อนจะไปถึงการประยุกต์ใช้สัญญาอัจฉริยะ เรามาดูทำความเข้าใจและเข้าใจเทคโนโลยีบล็อกเชนกันให้มากขึ้นก่อนว่าทำไมจึงได้รับการยอมรับถึงความน่าเชื่อถือและความมั่นคงปลอดภัยสูงมากกว่าการเก็บข้อมูลบนระบบเซิร์ฟเวอร์หรือบนระบบคลาวด์แบบเดิม

ทำความเข้าใจบล็อกเชนคืออะไร

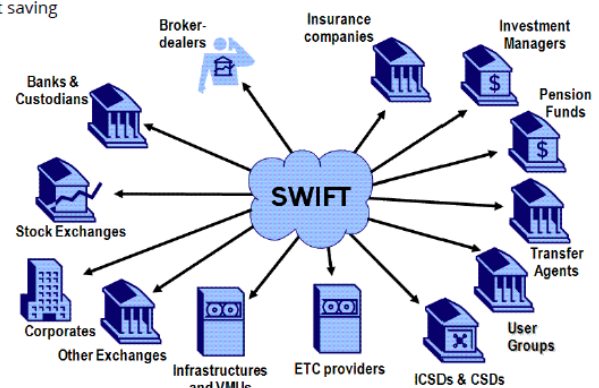
ย้อนไปในอดีต ตัวอย่างกรณี ธนาคารกลางของประเทศสหรัฐอเมริกา เคยเกิดเหตุเครื่องแม่ข่ายซึ่งทำหน้าที่อนุญาตให้สถาบันการเงินส่งเงินระหว่างกัน เกิดขัดข้องขึ้นมาจนทำให้ระบบธนาคารหยุดทำงานไปหลายชั่วโมงกว่าจะกลับมาทำงานได้เหมือนเดิม ก่อให้เกิดความเสียหายอย่างมากกับระบบการฝาก การจ่ายเงินเดือน ประกันสังคม การคืนภาษีเงินได้ และอื่นๆ ระบบที่มีการจ่ายเงินอัตโนมัติ ดังนั้นเพื่อลดปัญหาเครื่องแม่ข่ายขัดข้องนี้ ธนาคารจึงต้องทำสำรองข้อมูลไว้เป็นประจำ ซึ่งต้องทำไว้หลายสำเนาและเก็บไว้ต่างศูนย์กลางข้อมูล (data center) ด้วย ซึ่งการมี Data Center หลายแห่ง ก็จะต้องลงทุน และมีค่าใช้จ่ายในหลายๆ ด้านโดยเฉพาะค่าไฟฟ้าเพิ่มมากขึ้น

วิธีการแก้ไขกรณีนี้ที่ทำได้โดยทั่วไปคือ การเปลี่ยนมาใช้บริการเครื่องแม่ข่ายบนระบบคลาวด์ (on cloud) จากบริษัทผู้ให้บริการอย่าง Amazon Web Service (AWS) หรือ Microsoft Cloud ซึ่งจะช่วยให้ธนาคารลดค่าใช้จ่าย ไม่ต้องดูแลบริหารจัดการและลงทุนระบบทั้งหมดด้วยตัวเอง (on premise) ลงไปได้มาก แต่ก็ต้องแลกมาด้วยความเสี่ยงเรื่องความปลอดภัยของข้อมูลลูกค้าและรายการข้อมูลธุรกรรมของผู้บริโภค ที่อาจถูกเข้าถึงได้ง่ายขึ้นจากการถูกโจมตีไปที่บริการระบบคลาวด์

หรือตัวอย่าง ระบบ SWIFT (Society for Worldwide Interbank Financial Telecommunication) ซึ่งเป็นระบบเครือข่ายการสื่อสารของผู้ให้บริการสถาบันทางการเงินระหว่างประเทศ (ในรูปที่ 1) ในหนึ่งรายการประมวลผล (transaction) อาจมีการติดต่อกับอีกหลายระบบย่อยของธนาคารที่เกี่ยวข้องได้ โอกาสที่จะเกิดปัญหาที่ระบบใดระบบหนึ่งแล้วพาล่มทั้งระบบ หรือ Single point of failure จึงสามารถเกิดขึ้นได้ง่าย

Benefits of blockchain technology in banking:

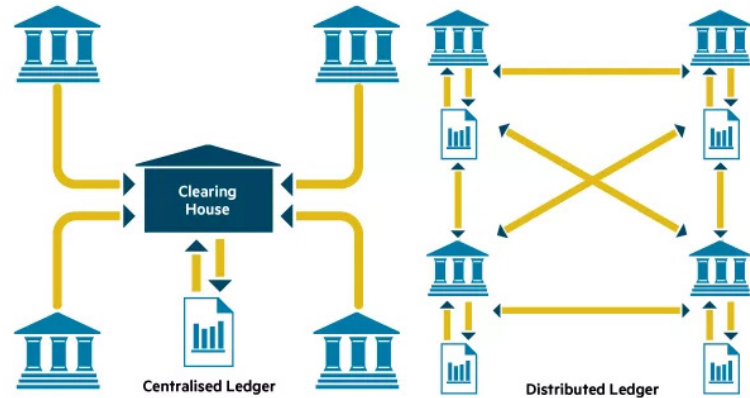
1. Instant settlement 24/7
2. Faster transaction
3. Cost saving



รูปที่ 1. ระบบ SWIFT เครือข่ายธนาคารที่ถูกใช้ระหว่างประเทศ

บล็อกเชน (blockchain) สามารถเข้ามาช่วยป้องกันกรณีเหล่านี้ได้ โดยเปลี่ยนจากระบบที่เป็นแบบรวมศูนย์เดิมที่ทุกคนต้องมีสมุดบัญชีกับธนาคารที่เป็นตัวกลางแห่งใดแห่งหนึ่ง มาเป็นระบบบล็อกเชนแบบกระจาย ที่ให้ทุกคนถือสมุดบัญชีของตนเองไว้ที่ตัว โดยเรียกสมุดบัญชีนี้ว่าโหนด (node) ดังแสดงในรูปที่ 2

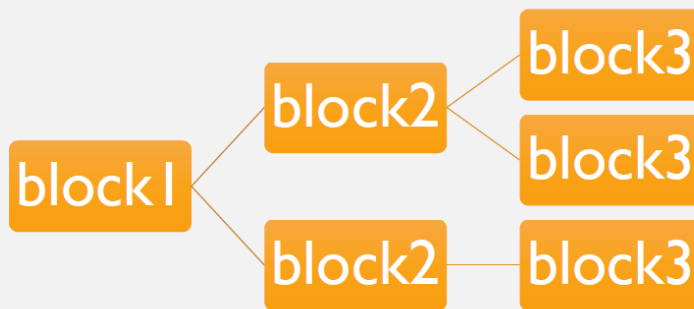
ผู้ช่วยศาสตราจารย์ Eunjin (EJ) Jung A กล่าวถึงการบริหารจัดการข้อมูลบล็อกเชน (blockchain for data management) ว่า บล็อกเชนคือห่วงโซ่ที่เชื่อมต่อกันด้วยฟังก์ชันแฮช ดังแสดงในรูปที่ 3 ซึ่งฟังก์ชันแฮชจะเป็นการเข้ารหัสข้อมูลทำให้ไม่สามารถย้อนกลับไปยังรูปแบบเดิมได้ แต่สามารถใช้ฟังก์ชันแฮชเพื่อตรวจสอบความถูกต้องของข้อมูล เช่น ถ้าใส่เงินไปในบล็อกที่ 2 แล้วเปลี่ยนใจเข้าไปแก้ไขข้อมูลตัวแฮชของบล็อกที่ 2 การเชื่อมโยงไปยังบล็อกที่ 3 ก็จะไม่ถูกต้อง ซึ่งเหตุการณ์นี้ทำให้ตัวแฮชในบล็อกที่ 3 ไม่สามารถถูกเชื่อมโยงได้ เรียกว่าเป็น canonical block นี่คือการสมบัติ Immutability คือไม่สามารถแก้ไขข้อมูลได้นั่นเอง



ที่มา: Scan Pay (2017)

รูปที่ 2. การใช้เทคโนโลยีสมุดบัญชีแบบกระจาย

IRREVERSIBILITY OF HASH FUNCTION = IMMUTABLE DATA STORAGE



รูปที่ 3. บล็อกเชนคือห่วงโซ่ที่เชื่อมต่อกันด้วยฟังก์ชันแฮช

เทคโนโลยีบล็อกเชนจึงเกิดความน่าเชื่อถือจากการเก็บประวัติของรายการประมวลผล ที่ถูกเขียนลงบล็อกแล้วจะไม่สามารถแก้ไขได้ จึงรับประกันได้ว่าข้อมูลที่บันทึกในบล็อกเชนนั้นมีความสมบูรณ์ สอดคล้องกัน

ตัวอย่างเช่น ถ้านายเอวิส โอน 1 บาทคอยน์ ให้กับนายเดวิด ประวัติรายการประมวลผลจะถูกบันทึกในบล็อกเชน ดังนั้นผู้คนที่เกี่ยวข้องก็สามารถทราบจากบันทึกรายการนี้ว่า นายเอวิสได้โอนให้นายเดวิดไปแล้วนั่นเอง เหมือนกับประกาศสาธารณะไว้ให้ทราบโดยทั่วกันนั่นเอง

อีกตัวอย่างคือ บริษัทไอบีเอ็ม (IBM) ได้จัดทำโครงการห่วงโซ่อุปทาน (supply chain project) โดยสามารถติดตามย้อนกลับแหล่งที่มาทรัพยากร โดยบริษัทไอบีเอ็มใช้เทคโนโลยีที่อยู่บน Hyper Ledger (แพลตฟอร์มบล็อกเชนที่เป็น opensource) และ Spirit of the SCM เพื่อวัตถุประสงค์ในการติดตามการขนส่งทางเรือ และจัดการห่วงโซ่อุปทาน

ตัวอย่างที่ 2 : การนำสัญญาอัจฉริยะมาใช้งานกับบริการรถแท็กซี่ คล้ายกับ Uber ดังแสดงในรูปที่ 6

- กำหนดเงื่อนไขที่จะเกิดการกระตุ้น และต้องแปลงเงื่อนไขเชิงตรรกะให้เป็นขั้นตอนวิธี (algorithm)
- นำไปใช้ในรูปแบบฟังก์ชันการจ่ายเงิน หรือ Payment function
- เงื่อนไขเริ่มจาก ผู้ขับขี่กำหนดสถานที่ต้นทางของผู้โดยสาร ไปยังสถานที่ปลายทางของผู้โดยสาร
- ด้วยตรรกะรูปแบบคล้ายกัน GPS ของทั้งผู้ขับขี่ ของบริษัท และผู้โดยสาร ต้องมี GPS ที่สอดคล้องตรงกัน
- เส้นทางจากสถานที่ต้นทางไปยังปลายทางที่ผู้โดยสารต้องจ่ายเงิน (ตกลงให้เป็นไปตามสัญญาอัจฉริยะ)
- GPS ของผู้ขับขี่ ของบริษัท ของผู้โดยสาร ต้องมีสถานะเหมือนกัน ดังนั้นผู้โดยสารต้องจ่ายเงินจากบัญชีของผู้โดยสารไปยังบัญชีของผู้ขับขี่

Case Study: Smart Contract: Sensing alcohol → Insurance fee changes



รูปที่ 6. ตัวอย่างการนำสัญญาอัจฉริยะมาให้กับบริษัทรถแท็กซี่

ตัวอย่างที่ 3 : กรณีศึกษาเรื่อง Podcasting 2.0 ซึ่งเป็นระบบนิเวศ (ecosystem) ที่ผู้สร้างสามารถอัปโหลดเสียงหรือเพลงลงโปรแกรมพอดแคสต์ และผู้ฟังสามารถฟังผ่านพอดแคสต์ได้เช่นกัน ทั้งผู้สร้างและผู้ฟังสามารถเรียกเก็บเงิน หรือชำระเงินหรือบริจาคเงินเพื่อผู้สร้างได้ ซึ่งจะกระจายอยู่บนเครือข่ายบล็อกเชน โดยที่ไม่อาจทราบได้ว่าเป็นไฟล์พอดแคสต์ ดังนั้นจึงไม่มีตัวกลาง ไม่ขึ้นกับแพลตฟอร์มผู้ให้บริการอย่าง แอปเปิลพอดแคสต์ หรือกูเกิลพอดแคสต์ ที่เก็บบนเครื่องแม่ข่ายหรือระบบคลาวด์ แล้วเป็นผู้กำหนดราคาค่าบริการในแต่ละพอดแคสต์ 🎧

เอกสารอ้างอิง

ส่วนความร่วมมือระหว่างประเทศ สถาบันเพิ่มผลผลิตแห่งชาติ. 2564. การอบรม หลักสูตร Digital Multicountry Workshop on Blockchain Solutions for SME Productivity Enhancement ภายใต้โครงการ APO. กรุงเทพฯ: สถาบันเพิ่มผลผลิตแห่งชาติ.

Scan Pay. 2017. How Blockchain Technology Disrupts Traditional Banking Architecture. [online]. Available at: <https://medium.com/@scanpayasia/how-blockchain-technology-disrupts-traditional-banking-architecture-9bd81bae0d19>, [accessed 3 July 2023].