บล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล
BLOCKCHAIN-BASED DATA INTEGRITY FRAMEWORK

สิรวิศ จันทะสี[1], ราชันย์ มูลสมบัติ[1] และ ปิยวัจน์ ค้าสบาย[1,*]
สาขาวิชาวิทยาการคอมพิวเตอร์และเทคโนโลยีสารสนเทศ คณะวิทยาศาสตร์ มหาวิทยาลัยราชภัฏอุดรธานี
Sirawit Chanthasri[1], Rachan Munsombat[1] Piyawat Kasabai[1]
[1]Department of Computer Science and Information Technology, Faculty of Science,
Udon Thani Rajabhat University.

(Received: January 9, 2023; Revised: April 15, 2023; Accepted: April 20, 2023)

*ผู้ประสานงาน : ปิยวัจน์ ค้าสบาย อีเมล์: piyawad.k@udru.ac.th

บทคัดย่อ

แอพพลิเคชันบนเครือข่ายอินเทอร์เน็ตมีการเก็บข้อมูลขององค์กรและผู้ใช้บริการ การจัดเก็บข้อมูลส่วนใหญ่นั้นเก็บไว้ที่ศูนย์กลาง อาจจะมีข้อมูลที่มีความสำคัญหรือเกี่ยวข้องกับหลายองค์กร หากมีคนเข้าถึงข้อมูล ข้อมูลทั้งหมดอาจถูกบุกรุกได้ง่าย นอกจากนี้ ผู้ประสงค์ร้ายยังสามารถแก้ไขข้อมูลได้ ดังนั้นความสมบูรณ์ของข้อมูลโดยไม่ต้องเชื่อถือในการรวมศูนย์หรือบุคคลที่สามจึงมีความจำเป็น โครงงานนี้มีวัตถุประสงค์นำเสนอบล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล เพื่อให้แอพพลิเคชันต่างๆ บันทึกข้อมูลที่สำคัญลงในบล็อกเชน โดยใช้อัลกอริทึมฉันทามัติแบบพีโอดับเบิลยู ทำให้แอพพลิเคชันดังกล่าวไม่ต้องพึ่งพาตัวกลางในการตรวจสอบความสมบูรณ์ของข้อมูล ผลการทดสอบโปรแกรมต้นแบบพบว่าการทดสอบบันทึกและตรวจสอบความสมบูรณ์ของข้อมูลแสดงให้เห็นถึงประสิทธิผลของการแก้ปัญหาที่นำเสนอ

คำสำคัญ: ความสมบูรณ์, บล็อกเชน, อัลกอริทึมฉันทามัติ

ABSTRACT

The majority of online application control organization or user’s data. The data which is stored in the centralization, also contains sensitive and essential information that could be relevant to the organizations. if someone accesses to the data, the entire data can easily be compromised. In addition, malicious actors can alter database data. Thus, data integrity without trusted in centralization or third party is required. The

purpose of the study is to design and develop blockchain-based data integrity framework in order to provide any applications to record information on the blockchain. Proof-of-Work (PoW) algorithm has been used for the consensus. The framework enables the applications to check the integrity without relying on intermediary or third party. From experimental results, it revealed that this prototype has demonstrated the effectiveness of the proposed solution.

Keywords: Integrity, Blockchain, Consensus algorithm.

1. บทนำ

ปัจจุบันอินเทอร์เน็ตได้เข้ามามีบทบาทสำคัญต่อชีวิตประจำวันของคนมากยิ่งขึ้นและความนิยมของ Internet of Things (IoT) ทำให้มีการเก็บข้อมูลขนาดใหญ่ของทั้งด้านธุรกิจและข้อมูลส่วนบุคคลมากขึ้น ข้อมูลจึงเป็นทรัพยากรที่สำคัญมากที่เป็นปัจจัยในการขับเคลื่อนสังคมและใช้ในการตัดสินใจทางด้านธุรกิจต่าง ๆ ทั้งด้านการเงิน สุขภาพ อาหาร การเกษตร การศึกษาและในองค์กรของรัฐทำให้มนุษย์พึ่งพาข้อมูลมากขึ้นเรื่อย ๆ ข้อมูลที่น่าเชื่อถือและความสมบูรณ์ของข้อมูลจึงเป็นสิ่งสำคัญ การจัดเก็บข้อมูลขนาดใหญ่นั้นส่วนมากจะจัดเก็บไว้ที่ศูนย์กลาง ซึ่งจัดการโดยตัวกลางและอาจมีความเป็นได้ว่าตัวกลางนั้นจะแอบแก้ไขข้อมูลโดยที่เจ้าของข้อมูลไม่รู้ตัว ซึ่งอาจส่งผลกระทบและสร้างความเสียหายต่อธุรกิจต่าง ๆ ได้ปัญหาเหล่านี้ส่วนมากเกิดขึ้นจากการที่เจ้าของข้อมูลจัดเก็บข้อมูลไว้ที่ศูนย์กลางและจัดการโดยตัวกลาง ทำให้เจ้าของข้อมูลควบคุมการรักษาความลับ ความสมบูรณ์ของข้อมูล และการเข้าถึงข้อมูลไม่ได้ เป็นเหตุให้ข้อมูลอาจถูกปลอมแปลงแก้ไขโดยตัวกลาง

บล็อกเชน (Blockchain) เป็นรูปแบบการจัดเก็บข้อมูลแบบกระจายโดยที่ไม่อาศัยตัวกลางตรวจสอบความถูกต้องของข้อมูล ซึ่งใช้กลไกวิทยาการรหัสลับ (Cryptography) เพื่อรักษาความปลอดภัยของข้อมูลและการทำธุรกรรมที่มีการติดตามได้อย่างเป็นระบบ โดยมีลักษณะเป็นบล็อกของข้อมูลที่ถูกเชื่อมต่อกัน ด้วยเทคโนโลยีเข้ารหัสแบบเสริมการทำงาน เพื่อให้มั่นใจว่าข้อมูลไม่ถูกแก้ไขหรือเปลี่ยนแปลงได้ และเก็บไว้ในแต่ละบล็อก ทำให้ไม่มีการแก้ไขข้อมูลหรือการทำธุรกรรมได้โดยไม่ได้รับอนุญาตจากผู้ถือสิทธิ์

โครงงานนี้ได้นำเสนอการใช้บล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล เพื่อให้ระบบไม่ต้องพึ่งพาตัวกลางและรองรับการตรวจสอบความสมบูรณ์ของข้อมูลทั้งข้อความ ซอฟต์แวร์หรือรูปแบบต่างๆของข้อมูลในระบบคอมพิวเตอร์ โดยตรวจสอบจากค่าตัวแทนของข้อมูล (Hash) รองรับการนำไปใช้ในแอปพลิเคชันหลากหลายรูปแบบ

2. ทฤษฎีและงานวิจัยที่เกี่ยวข้อง

2.1 ความสมบูรณ์ของข้อมูล (Data Integrity)

คุณภาพของข้อมูลที่มีความถูกต้อง แม่นยำ และไม่ถูกแก้ไขหรือปลอมแปลงโดยไม่ได้รับอนุญาต ซึ่งเป็นสิ่งสำคัญในการจัดการข้อมูล เช่นในระบบฐานข้อมูล และระบบเครือข่าย การรักษา Data Integrity สามารถทำได้โดยใช้วิธีการต่างๆ เช่น การใช้ระบบ Checksum เพื่อตรวจสอบว่าข้อมูลไม่ได้ถูกเปลี่ยนแปลงหรือสูญหาย การใช้ Digital Signature เพื่อยืนยันความถูกต้องและความปลอดภัยของข้อมูล การเข้ารหัสข้อมูล (Encryption) เพื่อป้องกันการเข้าถึงและการแก้ไขข้อมูลโดยไม่ได้รับอนุญาต และการสร้าง Backup ของข้อมูลเพื่อป้องกันการสูญหายของข้อมูล

2.2 Peer to Peer (P2P) Network

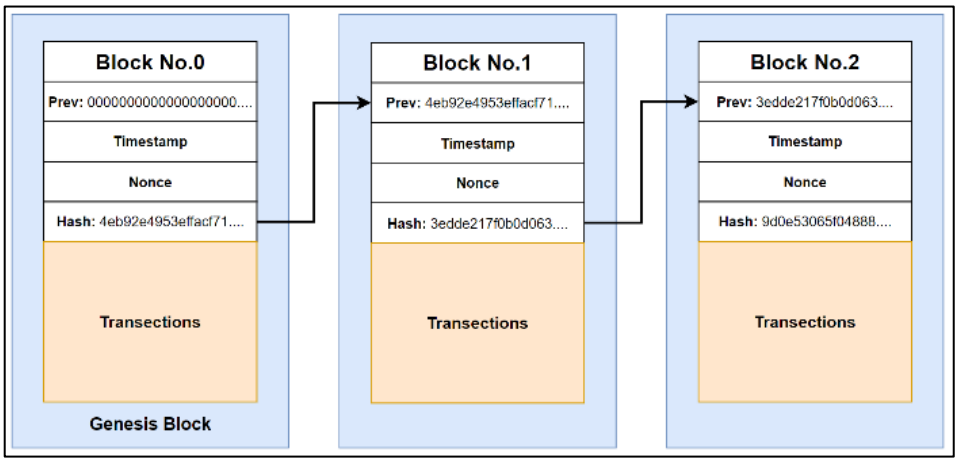
P2P เป็นการเชื่อมต่อเครือข่ายคอมพิวเตอร์โดยตรงระหว่างคอมพิวเตอร์ คอมพิวเตอร์แต่ละเครื่องจะมีสิทธิเท่าเทียมกันในการจัดการเครือข่าย P2P มีการทำงานแบบกระจายศูนย์ ไม่จำเป็นต้องมีผู้ดูแลและจัดการระบบ คอมพิวเตอร์ทุกเครื่องที่อยู่ในเครือข่ายจะทำหน้าที่เป็นทั้งไคลเอนท์และเซิร์ฟเวอร์แทนและผู้ใช้เครื่องคอมพิวเตอร์แต่ละเครื่องจะเป็นคนกำหนดข้อมูลหรือทรัพยากรของเครื่องนั้นที่ต้องการจะส่งผ่านเครือข่ายให้กับผู้ใช้คนอื่น ๆ

2.3 Blockchain

บล็อกเชนเป็นเทคโนโลยีการจัดเก็บข้อมูลแบบ Shared Database หรืออาจเรียกว่า Distributed Ledger Technology (DLT) ใช้หลักการของเครือข่าย P2P ซึ่งไม่มีตัวกลางคอยควบคุม โดยเป็นรูปแบบการบันทึกข้อมูลที่รับประกันความปลอดภัยว่าข้อมูลที่ถูกบันทึกไปก่อนหน้านั้นไม่สามารถที่จะเปลี่ยนแปลงหรือแก้ไข ข้อมูลที่ถูกจัดเก็บจะถูกแชร์และจัดเก็บเป็นสำเนาไว้ในทุกเครื่องที่รัน Node และใช้กระบวนการ Consensus ในการทำให้สำเนาข้อมูลที่ได้รับตรงกันทั้งหมด

2.3.1 หลักการทำงานของ Blockchain

หลักการทำงานของบล็อกเชนเป็นการแชร์ข้อมูลและจัดเก็บเป็นสำเนาไว้กับทุก Node ที่อยู่ในเครือข่ายของบล็อกเชนทุก Node จะได้รับสำเนาข้อมูลมาเก็บไว้และจะมีการอัปเดตข้อมูลแบบอัตโนมัติเมื่อมีข้อมูลใหม่เกิดขึ้นและจะใช้กระบวนการ Consensus ในการทำให้สำเนาข้อมูลที่ได้รับตรงกันทั้งหมด



รูปที่ 1 ตัวอย่างโครงสร้างการเชื่อมโยง Block ของ Bitcoin

จากรูปที่ 1 การจัดเก็บข้อมูลของบล็อกเชนจะถูกจัดเก็บในรูปแบบของ Block ซึ่งการที่จะเกิดเป็นบล็อกเชนได้นั้นจะต้องเชื่อมแต่ละ Block เข้าหา Block ก่อนหน้าด้วยค่า Hash Function ของ Block ก่อนหน้านี้เสมอหรือก็คือค่า Previous Hash ทำให้เชื่อมต่อกันเป็น Chain จึงยากต่อการปลอมแปลงแก้ไขหรือถ้ามีการแก้ไขข้อมูลที่อยู่ใน Block Chain จะขาดโดยอัตโนมัติทันที นอกจากนี้ยังสามารถตรวจสอบความถูกต้องของข้อมูลได้ทุกๆ Block ตลอดทั้ง Chain และตรวจสอบย้อนกลับไปจนถึง Block เริ่มต้น หรือ Genesis Block ได้

2.3.2 Consensus Algorithms

กระบวนการที่มีการตัดสินใจในระบบบล็อกเชนโดยใช้โปโตคอลที่เป็นระเบียบเรียงเหมือนกัน ซึ่งจะทำให้ผู้ใช้ทุกคนในระบบสามารถเห็น และยอมรับข้อมูลเดียว โดยไม่มีความขัดแย้งหรือความไม่เหมือนกันของข้อมูลที่อาจเกิดขึ้น การใช้อัลกอริทึม Consensus จะช่วยให้ระบบบล็อกเชนสามารถทำงานได้อย่างมีประสิทธิภาพโดยมีหลายๆ อัลกอริทึมที่ใช้งานได้ เช่น

1) Proof of Stake (PoS)

Proof of stake (PoS) มีการทำงานโดยไม่ต้องทำการยืนยันธุรรกรรม ด้วยการประมวลผลแข่งขันเพื่อหาคำตอบให้ได้ก่อน แต่จะต้องว่าง stake ในการเข้ามามีส่วนในการยืนยันธุรกรรม แต่ละรอบของการยืนยันธุรกรรม ระบบจะสุ่มเลือกโหนดมายืนยันตามสัดส่วนของ Stake ที่ว่างไว้ โดยที่การทำงานของโหนดที่ได้รับเลือกมีเพียงการตรวจสอบยืนยันธุรกรรมเท่านั้น [2]

2) Proof of Authority (PoA)

เป็นอัลกอริทึมสำหรับการยืนยันการทำธุรกรรมในระบบ บล็อกเชนโดย PoA ใช้วิธีการกำหนดผู้ควบคุมระบบ (Validator) ที่ได้รับการยอมรับจากผู้ใช้งานเพื่อทำหน้าที่ตรวจสอบและยืนยันการทำธุรกรรม โดยที่ผู้ควบคุมระบบจะมีสิทธิ์ในการสร้างบล็อกในระบบบล็อกเชน [2]

3) Proof of Work (PoW)

Proof of Work (PoW) เป็นการแก้ปัญหาทางคณิตศาสตร์ซึ่งมีความซับซ้อนและต้องใช้เวลาในการแก้ปัญหานั้น ๆ จาก Nodes ต่าง ๆ ด้วยการทำงานของ PoW ที่ถูกใช้ใน Bitcoin โดยข้อมูลทั้งหมดที่อยู่ใน Block จะถูกนำมา Hash ด้วยอัลกอริทึม SHA-256 เมื่อได้ผลลัพธ์ของการ Hash จะต้องนำผลลัพธ์นั้นมา Hash อีกรอบโดยอัลกอริทึม SHA-256 เพื่อให้ได้ผลลัพธ์ที่มีค่าน้อยกว่าหรือเท่ากับ Target โดย Miners จะทำการสุ่มหาค่า Nonce ไปเรื่อย ๆ ซึ่งค่า Nonce จะมีค่าตั้งแต่ 0 - 4,294,967,296 จนกว่าจะได้ค่า Nonce ที่นำไปรวมกับข้อมูลทั้งหมดที่อยู่ภายใน Block แล้วทำการ Hash ผลลัพธ์ที่ได้จะต้องมีค่าน้อยกว่าหรือเท่ากับ Target ดังสูตร

$$\text{SHA-256 (SHA-256 (Block\_Header)) } \leq \text{ Target}$$

ความยากของการสุ่มค่า Nonce ให้สามารถหาค่าที่ต่ำกว่าหรือเท่ากับ Target ได้จะใช้เวลาเฉลี่ยประมาณ 10 นาที หากมี Miners จำนวนมากความยากในการสุ่มก็จะสูงขึ้น หากมีจำนวนน้อยความยากก็จะต่ำลง เพื่อให้สอดคล้องกับระยะเวลาที่ตั้งไว้ เมื่อ Miner สุ่มหาค่า Nonce เจอเป็นคนแรก ระบบจะประกาศให้ทุก Nodes ทราบและ Miner คนนั้นจะได้รับเหรียญเป็นรางวัลค่าตอบแทน

การหาค่า Target จะเป็นการนำเอาค่า Bits ที่อยู่ใน Block Header ซึ่งเป็นเลขฐาน 16 มาเข้าฟังก์ชั่นทางคณิตศาสตร์ ตัวอย่างเช่น Bits = 0x1D00FFFF โดยกำหนดให้ 2 ตัวแรกของ Bits คือ index และ 6 ตัวหลังของ Bits คือ coefficient นำมาคำนวณตามสูตรดังนี้

$$\text{Targer = coefficient * 2 ^ (8 * (index - 3))}$$

นอกจากนี้ค่า Target จะถูกคำนวณค่าใหม่ในทุก 2016 Blocks หรือประมาณ 2 สัปดาห์และค่า Difficulty หรือค่าความยากง่ายในการทำ PoW จะถูกกำหนดโดยระบบภายใต้สูตร

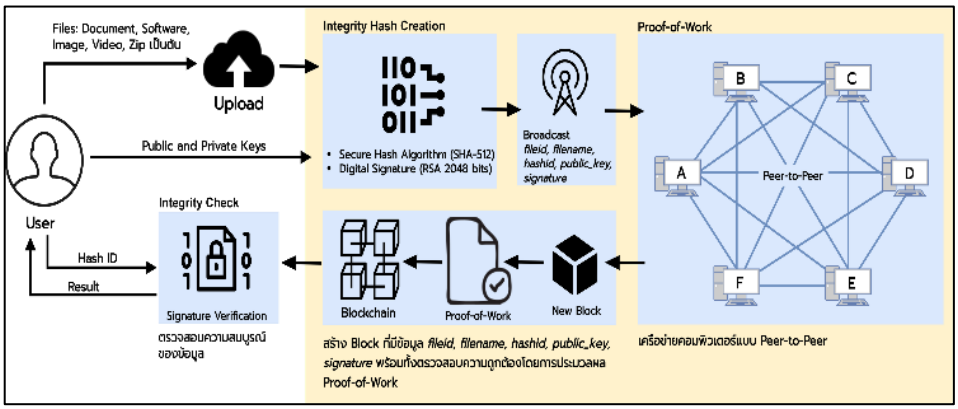
$$Difficulty = \frac{0x00ffff0000000000000000000000000000000000000000000000000000}{CurrentTarget}$$

2.4 วรรณกรรมที่เกี่ยวข้อง

ด้วยแอปพลิเคชันขนาดใหญ่ของที่เก็บข้อมูลบนคลาวด์ วิธีการตรวจสอบความสมบูรณ์ของข้อมูลบนคลาวด์จึงกลายเป็นประเด็นสำคัญ แม้ว่าจะมีการเสนอวิธีการต่างๆ มากมาย แต่ก็ยังมีข้อจำกัด ในงานวิจัย [4] นำเสนอการปรับปรุงข้อบกพร่องบางประการของวิธีการก่อนหน้านี้ และเสนอแผนการตรวจสอบความสมบูรณ์ของข้อมูลบนคลาวด์ที่มีประสิทธิภาพด้วยระบบบล็อกโดยใช้อัลกอริทึม lattice signature เพื่อลดการคำนวณแบบควอนตัม และตัวกรอง cuckoo เพื่อลดความซับซ้อนของการคำนวณของขั้นตอนการยืนยันผู้ใช้ สุดท้ายนี้เครือข่ายบล็อกเชนแบบกระจายศูนย์ได้รับการแนะนำเพื่อแทนที่การตรวจสอบแบบรวมศูนย์แบบดั้งเดิมบล็อกเชนเทคโนโลยีถูกนำมาใช้ตรวจสอบความสมบูรณ์ของข้อมูลบน Internet of Things (IoT) โดยการดึงตัวแทนของข้อมูลหรือ Hash มาเก็บไว้ในบล็อกเชน โดยข้อมูลที่อยู่ในบล็อกเชนจะถูกเก็บไว้ทุกเครื่องที่รันบล็อกเชนโหนด Bin Liu และคณะ [5] ได้นำเสนอบล็อกเชนสำหรับความสมบูรณ์ของข้อมูล IoT โดยนำเสนอการใช้งานบล็อกเชนสำหรับเฟรมเวิร์คบริการความสมบูรณ์ของข้อมูล ทำให้ไม่ต้องมีตัวกลางในการจัดการข้อมูลและสามารถตรวจสอบความสมบูรณ์ข้อมูลทำให้ข้อมูลน่าเชื่อถือมากขึ้น Haiyan Wang และ Jiawei Zhang [6] ได้นำเสนอบล็อกเชนสำหรับตรวจสอบความสมบูรณ์ของข้อมูล IoT ขนาดใหญ่ โดยได้นำเสนอวิธีแก้ปัญหาการวิเคราะห์ข้อมูล IoT ขนาดใหญ่ โดยใช้ Bilinear mapping based Data Integrity Scheme (BB-DIS) สำหรับการคำนวณข้อมูลซึ่งรูปแบบของข้อมูลนั้นจะทำตาม Bilinear mapping ในรูปแบบธุรกรรมของบล็อกเชน Zikratov และคณะ [7] นำเสนอการใช้เทคโนโลยีบล็อกเชนในหลากหลายด้าน เช่น สินทรัพย์ดิจิทัลและหุ้น สัญญาอัจฉริยะ การเก็บบันทึกระบบ ID ที่เก็บข้อมูลบนคลาวด์ โดยตรวจสอบกิจกรรมของบล็อกเชนในแง่ของวิธีการจัดเก็บ ดึงข้อมูล และแชร์ไฟล์ เทคโนโลยีบล็อกเชนสามารถรักษาความสมบูรณ์ของไฟล์ที่จัดเก็บในฐานข้อมูลธุรกรรม การพิสูจน์ตัวตน การตรวจสอบ ทำให้จำนวนของภัยคุกคามที่เป็นไปได้ต่อความสมบูรณ์ของข้อมูลลดลง

3. วิธีดำเนินการวิจัย

งานวิจัยนี้ได้นำเสนอบล็อกเชนเพื่อความสมบูรณ์ของข้อมูล ซึ่งได้พัฒนาระบบโดยใช้เทคโนโลยีบล็อกเชนเพื่อตรวจสอบตรวจสอบความสมบูรณ์ของข้อมูลผ่านทาง Web service โดยมีรายละเอียดดังนี้



รูปที่ 2 ภาพรวมระบบ

จากรูปที่ 2 สามารถอธิบายได้ออกเป็น 2 ส่วน ส่วนที่ 1 ผู้ใช้งานต้องการตรวจความสมบูรณ์ของข้อมูลผ่าน Web service โดยผู้ใช้ทำการเลือกบันทึกไฟล์ข้อมูลได้หลากหลายชนิด เช่น Document, Software, Image, Video และ Zip เป็นต้น และส่ง Public and Private Key เพื่อนำไปจัดเก็บลงในบล็อกเชนเพื่อให้ผู้ใช้สามารถนำค่าตัวแทนข้อมูล (hashid) เพื่อนำมาตรวจสอบความสมบูรณ์ ส่วนที่ 2 การทำงานของระบบบล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล จะทำการส่งข้อมูลที่ได้จากการบันทึกได้แก่ fileid, filename, hashid, public_key และ signature ซึ่งมีรายละเอียดดังหัวข้อ 3.1 จะนำไปสร้างเป็น block ข้อมูล และกระจายข้อมูลไปยังทุกเครื่องคอมพิวเตอร์ที่อยู่ในเครือข่าย Peer-to-Peer พร้อมทั้งตรวจตสอบความถูกต้องโดยการประมวลผล Proof-of-Work ดังหัวข้อ 2.3.2 โดยระบบจะทำการนำเอาข้อมูลที่บันทึกของเครื่องใดเครื่องหนึ่งที่อยู่ในเครือข่าย เพื่อค้นหาเครื่องคอมพิวเตอร์ที่บันทึกข้อมูลได้เป็นอันดับแรกสามารถนำ block ข้อมูลของเครื่องที่บันทึกนำไปเก็บลงในบล็อกเชนได้ก่อนเครื่องอื่นๆ (เป็นกรณีที่มีผู้ใช้งานหลายเครื่องบันทึกข้อมูลพร้อมกันต้องมีการแก้สมการเพื่อหาเครื่องที่แก้ได้เร็วที่สุด)

3.1 การออกแบบบล็อกเชน

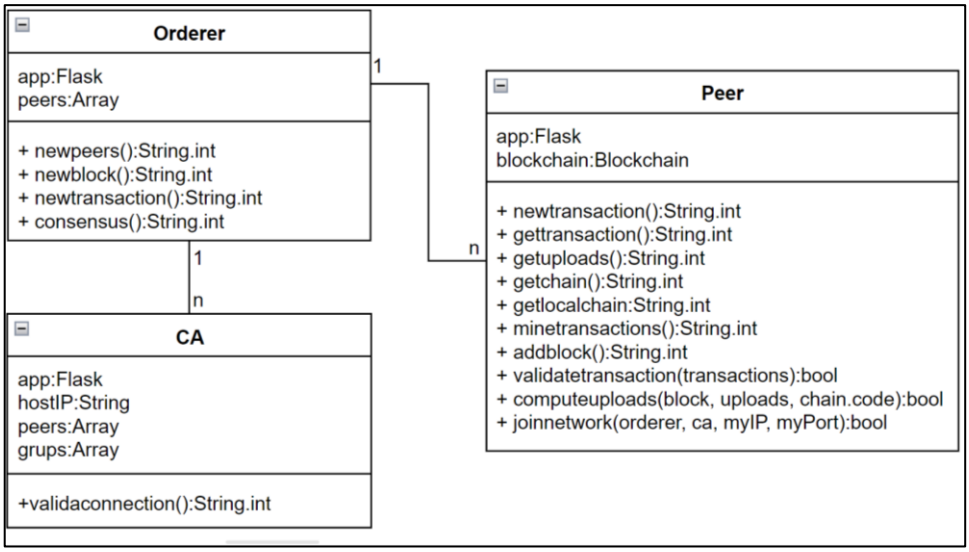
งานวิจัยนี้ได้นำเสนอการตรวจสอบความสมบูรณ์ของข้อมูล โดยออกแบบระบบบล็อกเชนให้เหมาะสมกับวัตถุประสงค์ของงานวิจัย ดังรูปที่ 3

รูปที่ 3 การออกแบบบล็อกเชน

จากรูปที่ 3 การแบบบล็อกเชนเป็นการจำลองการจัดเก็บข้อมูลของบล็อกเชน โดยมีตัวอย่างบล็อกข้อมูล 2 บล็อก ที่มีค่า hash ที่ได้จากการแปลงข้อมูล โดยการนำเอาข้อมูลต่าง ๆ มาผ่านอัลกอริทึม SHA-512, index ใช้แสดงหลายเลขของบล็อกว่าอยู่ลำดับที่เท่าไรของบล็อกเชน, nonce เป็นตัวเลขสุ่มเพื่อใช้ในกระบวนการของ Proof-of-Work, previous_hash ใช้แสดงค่า hash ของบล็อกก่อนหน้าเพื่อให้รู้ว่าบล็อกใหม่ได้เชื่อมต่อบล็อกก่อนหน้าสำเร็จ, timetamp ใช้ระบุเวลาเมื่อสร้างบล็อกสำเร็จ และ transaction คือธุรกรรมข้อมูลที่ถูกบันทึกลงในบล็อกโดยมีข้อมูลได้แก่ fileid คือ id ของไฟล์ข้อมูลที่ถูกบันทึก, filename คือชื่อของไฟล์ข้อมูลที่ทำการบันทึก, hashid คือค่ารหัสตัวแทนของไฟล์ข้อมูลที่ถูกบันทึก และสามารถนำไปตรวจสอบความสมบูรณ์ของข้อมูล, public_key คือกุญแจสาธารณะของผู้บันทึกลงในบล็อกเชน, sig ใช้ในการตรวจสอบลายเซ็นดิจิทัล เพื่อพิสูจน์ความเป็นเจ้าของไฟล์ข้อมูล และ timestamp ใช้บอกเวลาของไฟล์ข้อมูลที่ถูกบันทึก

sig = RSA(hashid, private_key)

3.2 การออกแบบคลาสสำหรับการเชื่อมต่อ



รูปที่ 4 ออกแบบระบบเชื่อมต่อเครือข่าย

จากรูปที่ 4 ด้วยการออกแบบระบบเชื่อมต่อเครือข่ายโดยจะใช้รูปแบบของ P2P ดังข้อ 2.2 โดยจะมีโปรแกรมทั้งหมด 4 โปรแกรมเพื่อให้ระบบสามารถทำงานได้อย่างมีประสิทธิภาพ และรายละเอียดของโปรแกรมมีดังนี้

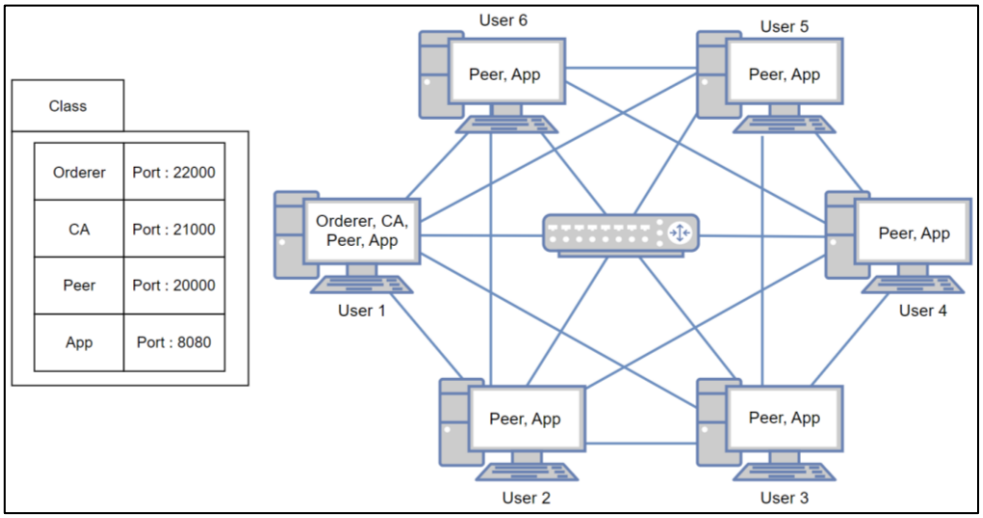
1) โปรแกรม Orderer คือโปรแกรมที่ทำงานในการเก็บ Node (Peer) ของเครื่องคอมพิวเตอร์ที่เข้าร่วมเครือข่าย P2P พร้อมทั้งกระจายข้อมูลทั้งหมดของบล็อกเชน (newblock) และมีฟังก์ชันการคำนวณอัลกอริทึมฉันทามติ (consensus) โดยใช้ Proof-of-Work เพื่อให้ระบบนำบล็อกข้อมูลที่มีการสร้าธุรกรรมใหม่มาเชื่อมต่อกับบล็อกล่าสุดหรือบล็อกสุดท้ายของบล็อกเชน

2) โปรแกรม Ca (Certificate Authority) คือโปรแกรมตรวจสอบ และอนุญาตเข้าร่วมเครือข่าย (connection)

3) โปรแกรม Peer คือโปรแกรมที่มีฟังก์ชันการทำงานของระบบบล็อกเชนทั้งหมดได้แก่ การขุด (transactions), ตรวจสอบธุรกรรม (transaction), ส่งคืนค่าไปเก็บในบล็อกเชน (addblock) และอื่นๆ

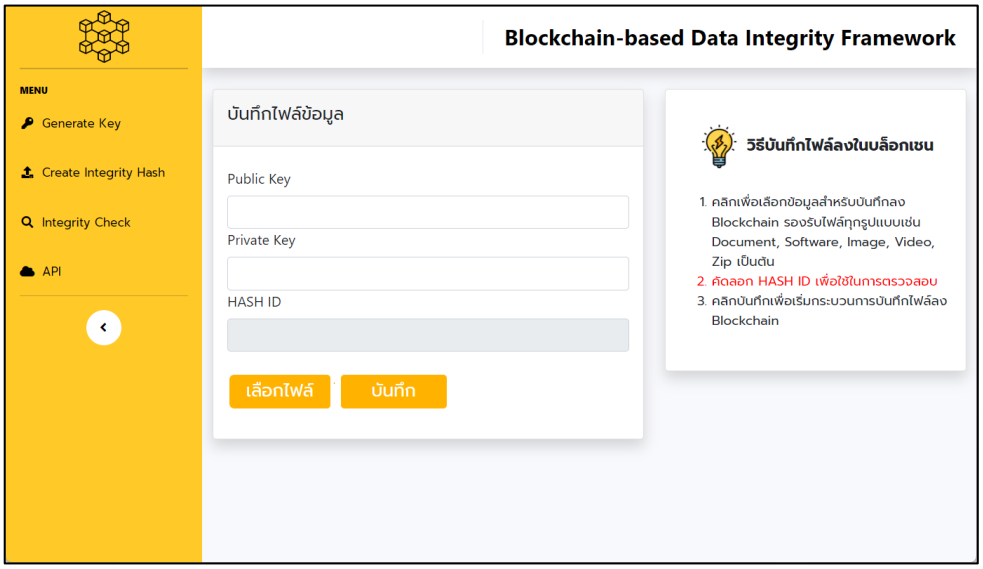
4) โปรแกรม App คือ โปรแกรมที่เปิดใช้งานแอปพลิเคชันบล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล

4. ผลการวิจัยและอธิปรายผล



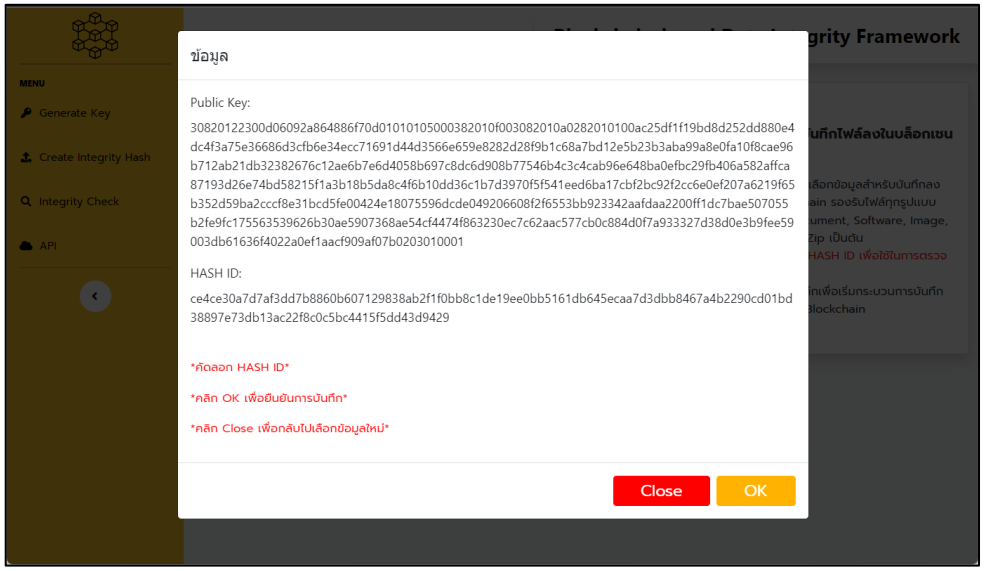
รูปที่ 6 เครือข่ายทดสอบ

การทดสอบระบบดังรูปที่ 6 ระบบบล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูลพัฒนาด้วยภาษา Python โดยใช้ Flask และ Cryptodome Library ร่วมกับ Visual Studio Code ของระบบปฏิบัติการ Windows ในการสร้าง Web service ที่ทำงานพร้อมกับบล็อกเชนเพื่อตรวจสอบความสมบูรณ์ของข้อมูล เมื่อทำการเปิดทั้ง 4 โปรแกรม ดังข้อ 3.2 จะแสดงหน้าจอหลักของโปรแกรมดังรูปที่ 7



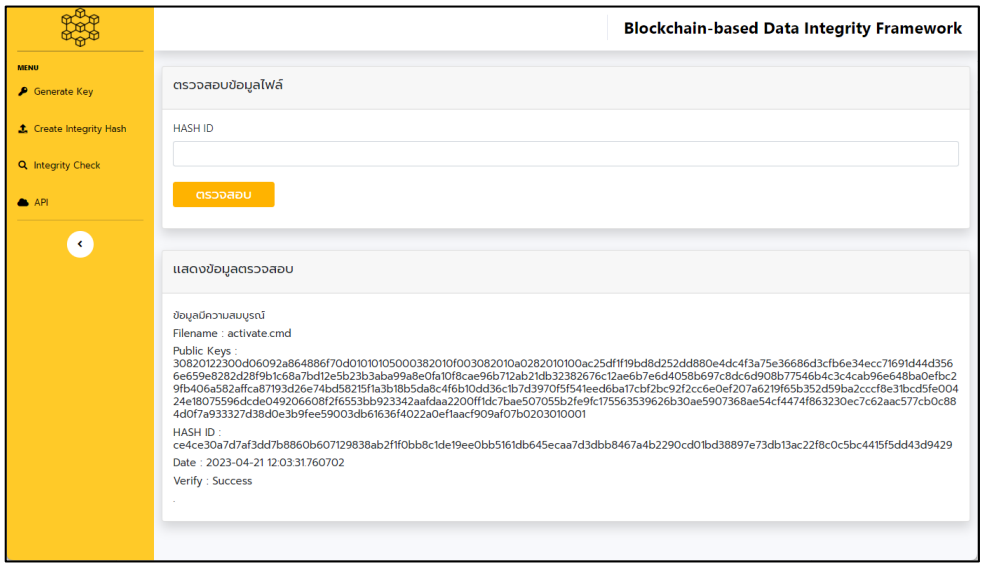
รูปที่ 7 หน้าจอหลักบันทึกข้อมูลลง Blockchain

จากรูปที่ 7 แสดงหน้าจอหลักของเว็บไซต์ เมื่อผู้ใช้งานเปิดใช้งานโปรแกรม แบ่งเป็น 2 ส่วน ส่วนแรกจะพบกับช่องกรอกข้อมูลของ Public Key และ Private Key ส่วนที่สองจะพบปุ่มกดเลือกไฟล์ใช้สำหรับเลือกไฟล์ข้อมูลที่ต้องการบันทึก หลังจากเลือกสำเร็จค่าตัวแทนของข้อมูลจะแสดงขึ้นที่ช่อง HASH ID และปุ่มบันทึกใช้สำหรับบันทึกไฟล์ข้อมูลที่เลือกไว้



รูปที่ 8 หน้าจอยืนยันการบันทึกข้อมูล

จากรูปที่ 8 หน้าจอยืนยันการบันทึกข้อมูล หลังจากที่ผู้ใช้งานคลิก บันทึก จะขึ้นแสดงกล่องข้อความรายละเอียดของข้อมูลที่บันทึกได้แก่ Public Key และ hashid โดยให้ผู้ใช้งานต้องคัดลอก Public key และค่ารหัสตัวแทนข้อมูล (hashid) เพื่อใช้ในการตรวจสอบความสมบูรณ์ของข้อมูล และผู้ใช้งานสามารถระบุว่าข้อมูลไหนเป็นข้อมูลของผู้ใช้ โดยตรวยสอบผ่านทาง Public key เมื่อคัดลอกข้อมูลสำเร็จ หลังจากนั้นผู้ใช้งานคลิก OK เพื่อยืนยันการบันทึกข้อมูล แล้วจะขึ้นแจ้งเตือนบันทึกข้อมูลสำเร็จ



รูปที่ 9 หน้าจอแสดงผลการตรวจสอบ

จากรูปที่ 9 ระบบแสดงผลการตรวจสอบความสมบูรณ์ จะพบช่องกรอกค่าตัวแทนข้อมูล (hash id) ใช้สำหรับตรวจสอบค่าตัวแทนของข้อมูลตรงกับข้อมูลที่ได้บันทึก โดยจะแสดงผลข้อมูลจากการตรวจสอบได้แก่ Filename, Public Key, HASH ID, Date และ Verify


```
"hash": "00634a1eb6755949869ef7dc288528407f398b468e93876cc575ef0d93e47f8fb3036428c36570680f137c15e62e9af60ec0aeabd91b4dc6db34255b6114e8ad",
"index": 0,
"nonce": 533,
"previous_hash": "0",
"timestamp": 1682052982.5525791,
"transactions": []


"hash": "00a1eb2c95a390868fe86576b123388b4b81a990e3ae0f19f05f79e6d8d31dd9aba9d8dda3cb4c38026311e3b001c2dbb03d67185ccafeb0d4c5cf6e65dbd75b",
"index": 1,
"nonce": 149,
"previous_hash": "00634a1eb6755949869ef7dc288528407f398b468e93876cc575ef0d93e47f8fb3036428c36570680f137c15e62e9af60ec0aeabd91b4dc6db34255b6114e8ad"
  ,
"timestamp": 1682053411.773894,
"transactions": [
  {
    "content": {
      "fileid": "1682053042999",
      "filename": "activate.cmd",
      "hashid": "ce4ce30a7d7af3dd7b8860b607129838ab2f1f0bb8c1de19ee0bb5161db645ecaa7d3dbb8467a4b2290cd01bd38897e73db13ac22f8c0c5bc4415f5dd43d9429",
      "public_key": "30820122300d06092a864886f70d01010105000382010f003082010a0282010100ac25df1f19bd8d252dd880e4dc4f3a75e36686d3cfb6e34ecc71691d44d3
        566e659e8282d28f9b1c68a7bd12e5b23b3aba99a8e0fa10f8cae96b712ab21db32382676c12ae6b7e6d4058b697c8dc6d908b77546b4c3c4cab96e648ba0efbc29fb406a58
        2affca87193d26e74bd58215f1a3b18b5da8c4f6b10dd36c1b7d3970f5f541eed6ba17cbf2bc92f2cc6e0ef207a6219f65b352d59ba2cccf8e31bcd5fe00424e18075596dcd
        e049206608f2f6553bb923342aafdaa2200ff1dc7bae507055b2fe9fc175563539626b30ae5907368ae54cf4474f863230ec7c62aac577cb0c884d0f7a933327d38d0e3b9fe
        e59003db61636f4022a0ef1aacf909af07b0203010001",
      "sig": "047f3f3103ae91e6130406e4a80b1a03d04e8c6889875fb91bc149d8ea0e8e3ad16aaf6091f576cbb2c3bb7be6a17030baf6d6c2ba06aa29ab8b293006b44051f85bd
        63a524eac247ec88548a710cfbfd0d80dd4339a473afbe61a7d00d81bc111f2cc12f7f025c50f2abbe1ef50c1a2a8da07430913f58b03cd7e19bccb48e1a11a9490997c304c
        a2166c4223864104a45ef6972df55c7855ae0d0fd04e7cd096620bb860707e2ad63eb9175d88b2202b400170b2dccb807c1c14f6c25c20d6d00aff1b7b386f6f158dd122c59
        491967c8842a37e06b29fa6a8031a3499021919152O5bd486cb70a57fdf609eafa7fd9082a391212314d855563b1666696131",
      "timestamp": 1682053411.7607016
```


รูปที่ 10 หน้าจอข้อมูลบล็อกเชน

จากรูปที่ 10 จากการทดลองบล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล จะเห็นได้ว่าข้อมูลทั้งหมดในบล็อกเชนถูกจัดเก็บเป็นไฟล์ .JSON โดยจะมีรายละเอียดของข้อมูล ดังข้อ 3.1

จากการศึกษาซอฟต์แวร์บล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล ได้ตอบสนองความต้องการของขอบเขต ซึ่งผู้ใช้งานสามารถใช้งานซอฟต์แวร์ได้ เพื่อให้ผู้ใช้งานสามารถตรวจสอบความสมบูรณ์ของข้อมูลผ่านทางเว็บเซอร์วิส รวมถึงผลการทดสอบโปรแกรมต้นแบบ พบว่ามีประสิทธิผลในการตรวจสอบความสมบูรณ์ของข้อมูล และสามารถนำไปใช้ได้โดยง่าย การใช้งานหรือขั้นตอนการใช้งานซอฟต์แวร์บล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล

5. สรุปผลการวิจัย

สรุปผลที่ได้ในการพัฒนาระบบบล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูล บล็อกเชนสำหรับเฟรมเวิร์คความสมบูรณ์ของข้อมูลที่ทำการพัฒนาขึ้นนั้น ในระบบทำงานในลักษณ์ของเซิร์ฟเวอร์แบ่งเป็นสองส่วน ได้แก่ ส่วนของระบบ และส่วนของผู้ใช้งาน ส่วนของระบบนั้นจะทำการเริ่มระบบของโปรแกรมการทำงานของบล็อกเชนและการเชื่อมของเครื่องคอมพิวเตอร์ส่งผ่านข้อมูลถึงกันโดยตรวจสอบขออนุญาตเข้ารวมการเชื่อมต่อในระบบบล็อกเชนเริ่มทำการสร้างบล็อกที่มีข้อมูลและนำไปเชื่อมต่อในบล็อกเชน ส่วนของผู้ใช้งาน ผู้ใช้งานสามารถบันทึกข้อมูลเช่น Document, Software, Image, Video, Zip เป็นต้น เพื่อนำไปใช้ตรวจสอบความสมบูรณ์ของข้อมูลที่ ผู้ใช้สามารถตรวจสอบได้โดยการใช้ Hash ID ของข้อมูลที่บันทึกลงในบล็อกเชนมาเรียกดูความสมบูรณ์ ผลการทดสอบระบบพบว่าสามารถตรวจความสมบูรณ์ของข้อมูลถูกต้อง

เอกสารอ้างอิง

[1] A. Iftekhar, X. Cui, Blockchain-Based Traceability System That Ensures Food Safety Measures to Protect Consumer Safety and COVID-19 Free Supply Chains, Wuhan University, 2021.

[2] Andreas M. Antonopoulos, “Mastering Bitcoin (Second Edition)” https://github.com/bitcoinbook/bitcoinbook (accessed Apr. 3, 2023).

[3] BlockChain for Government Services, พิมพ์ครั้งที่ 2, สำนักงานพัฒนารัฐบาลดิจิทัล พ.ศ. 2564.

[4] G. Xie, Y. Liu, G. Xin, Q. Yang, Blockchain-Based Cloud Data Integrity Verification Scheme with High Efficiency, Hunan University of Chinese Medicine, Volume 2021.

[5] B. Liu, X.L. Yu, S. Chen, X. Xu, L. Zhu, Blockchain Based Data Integrity Service Framework for IoT Data, 2017 **IEEE International Conference on Web Services (ICWS)**, pp. 468 - 475.

[6] D. Yue, R. Li, Y. Zhang, W. Tian, C. Peng, Blockchain Based Data Integrity Verification in P2P Cloud Storage, 2018 **IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS)**, pp. 561 – 568.

[7] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, Ensuring data integrity using blockchain technology, 2017 **20th Conference of Open Innovations Association (FRUCT),** pp. 534 - 539.