การสร้างระบบออกใบปริญญาบัตรและโอนหน่วยกิตด้วยเหรียญดิจิทัล

สุธิดา ณรงค์ศักดิ์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
บัณฑิตวิทยาลัย สาขาเทคโนโลยีสารสนเทศ
สถาบันเทคโนโลยีไทย-ญี่ปุ่น
ปีการศึกษา 2565

DIGITAL TOKEN-BASED DEGREE CERTIFICATE WITH CREDIT TRANSFER SYSTEM

Sutida Narongsak

A Thesis Submitted in Partial Fulfillment of the Requirements

For the Degree of Master of Science Program in Information Technology

Graduate School

Thai-Nichi Institute of Technology

Academic Year 2022

หัวข้อวิทยานิพนธ์ การสร้างระบบออกใบปริญญาบัตรและโอนหน่วยกิตด้วยเหรียญดิจิทัล

โดย สุธิดา ณรงค์ศักดิ์

สาขาวิชา เทคโนโลยีสารสนเทศ

อาจารย์ที่ปรึกษา ดร.ศรายุทธ นนท์ศิริ

บัณฑิตวิทยาลัย สถาบันเทคโนโลยีไทย-ญี่ปุ่น อนุมัติให้นับวิทยานิพนธ์ฉบับนี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญามหาบัณฑิต

.....คณบดีบัณฑิตวิทยาลัย

(รองศาสตราจารย์ ดร.วรากร ศรีเชวงทรัพย์)

วันที่.....เดือน.....พ.ศ.....

คณะกรรมการสอบวิทยานิพนธ์

.....ประธานกรรมการ

(รองศาสตราจารย์ ดร.อรรณพ หมั่นสกุล)

.....กรรมการ

(ว่าที่ร้อยตรี ดร.พิชิตชัย คำอินทร์)

.....กรรมการ

(ดร.ประมุข บุญเสี่ยง)

.....อาจารย์ที่ปรึกษาวิทยานิพนธ์

(ดร.ศรายุทธ นนท์ศิริ)

สถาบันเทคโนโลยีไทย-ญี่ปุ่น
THAI - NICHI INSTITUTE OF TECHNOLOGY
TNI

สุธิดา ณรงค์ศักดิ์: การสร้างระบบออกใบปริญญาบัตรและโอนหน่วยกิตด้วยเหรียญดิจิทัล

อาจารย์ที่ปรึกษา: : ดร.ศรายุทธ นนท์ศิริ, 64 หน้า.

ปัญหาการปลอมแปลงใบปริญญาบัตร เป็นปัญหาใหญ่ในระดับสากลที่ส่งผลกระทบต่อบริษัทและองค์กรต่าง ๆ โดยในปัจจุบันใบปริญญาบัตรปลอมสามารถเข้าถึงและซื้อขายได้ง่ายมากขึ้นผ่านเว็บไซต์และสื่อสังคมออนไลน์ ทำให้ธุรกิจการปลอมใบปริญญาบัตรยิ่งขยายตัวและเติบโตอย่างรวดเร็ว การว่าจ้างพนักงานที่ใช้ใบปริญญาบัตรปลอมในการสมัครงาน นอกจากจะได้คนที่ไม่มีประสิทธิภาพเพียงพอแล้ว ยังสามารถสร้างความเสียหายต่อรายได้และชื่อเสียงอีกด้วย ด้วยเหตุนี้หลาย ๆ องค์กรและบริษัทเลือกว่าจ้างผู้เชี่ยวชาญเพื่อเข้ามาตรวจสอบความถูกต้องของใบปริญญาโดยเฉพาะ ทว่าขั้นตอนในการตรวจสอบนั้นมีความยุ่งยาก ซับซ้อน และใช้เวลานาน

งานวิจัยนี้เสนอการใช้เทคโนโลยีบล็อกเชนบนเครือข่ายมัลติเชนและการสร้างเหรียญดิจิทัลเพื่อสร้างระบบในการออกใบปริญญา โดยเหรียญดิจิทัลจะถูกสร้างขึ้นเพื่อใช้แทนหน่วยกิตรายวิชาที่มหาวิทยาลัยจะทำการโอนให้กับนักศึกษาหลังจากที่นักศึกษาสำเร็จการศึกษารายวิชา นักศึกษาจะต้องสะสมเหรียญดิจิทัลแทนหน่วยกิตรายวิชาให้ครบตามเงื่อนไขที่กำหนดเพื่อนำไปแลกเปลี่ยนเป็นใบปริญญา ที่จะถูกสร้างขึ้นโดยใช้เหรียญดิจิทัลที่ไม่สามารถทดแทนได้

งานวิจัยนี้พบว่าระบบออกใบปริญญาบัตรที่พัฒนาโดยใช้เทคโนโลยีบล็อกเชนบนเครือข่ายมัลติเชน สามารถใช้งานได้จริง โดยสามารถตรวจสอบข้อมูลทางการศึกษาและการได้มาซึ่งใบปริญญาผ่านระบบที่พัฒนาขึ้นได้ นอกจากนี้การใช้มัลติเชนยังช่วยลดค่าใช้จ่ายที่อาจเกิดขึ้นจากกการเผยแพร่ธุรกรรมในระบบ และการสร้างเครือข่ายบล็อกเชนแบบส่วนตัวช่วยรักษาความเป็นส่วนตัวของข้อมูล และควบคุมการเข้าถึงข้อมูลของผู้ใช้งานแต่ละคนได้

บัณฑิตวิทยาลัย ล า ย มื อ ชื่ อ นั ก ศึ ก ษ า

.....

สาขาวิชา เทคโนโลยีสารสนเทศ ล า ย มื อ ชื่ อ อ า จ า ร ย์ ที่ ป รึ ก ษ า

.....

ปีการศึกษา 2565

SUTIDA NARONGSAK: DIGITAL TOKEN-BASED DEGREE CERTIFICATE WITH CREDIT TRANSFER SYSTEM. ADVISOR: DR. SARAYUT NONSIRI, 64 PP.

The fake degree, diploma, or certificate is a global issue that affects many organizations, companies, and industries. With a rapid increase in the numbers of websites and social platforms, the fake degree certificate can be sold online by diploma mills or individuals. institutions or employers that they have obtained the legitimate degree. This issue may have severe consequences for employers, universities, individuals, and public safety. There are companies that have hired specialists to specifically review applicants' degrees. The traditional way of proving documents is difficult, time-consuming, and involves many intermediates that make the process more complicated.

This research paper presents the method of using blockchain technology and digital token to develop certificate system. We developed digital token as credit, which will be transferred to the students when they complete the course. The student must collect the credit token for the specific amount to exchange it for an NFT certificate. All transactions related to certificates will be stored in a university blockchain on a multichain network which can be tracked and verified.

The result of this research paper shows that the proposed system is working properly. All transactions are trackable and verifiable. The use of multichain provides the gas-fee free environment which can reduce the costs. Also, the proposed system is working in private network which gives more data privacy and can control data accessible.

Graduate School Student’s Signature.....

Field of Study Information Technology Advisor’s

Signature……..

Academic Year 2022

กิตติกรรมประกาศ

การทำวิทยานิพนธ์นี้สำเร็จสำเร็จลุล่วงได้ด้วยดี ผู้วิจัยขอขอบพระคุณดร.ศรายุทธ นนท์ศิริ ที่ให้ความกรุณาช่วยเหลือ แนะนำ ให้คำปรึกษา ตรวจสอบแก้ไขข้อบกพร่องต่าง ๆ ด้วยความเอาใจใส่อย่างดีอย่างยิ่ง รวมถึงขอขอบพระคุณคณะกรรมการทุก ๆ ท่าน ได้แก่ รองศาสตราจารย์ ดร.อรรณพ หมั่นสกุล ว่าที่ร้อยตรี ดร.พิชิตชัย คำอินทร์ และ ดร.ประมุข บุญเสี่ยง ที่ได้กรุณาให้ข้อเสนอแนะและช่วยตรวจสอบข้อบกพร่องของวิทยานิพนธ์ฉบับนี้จนเสร็จสมบูรณ์

นอกจากนี้ ผู้วิจัยขอขอบคุณเจ้าหน้าที่บัณฑิตวิทยาลัยของสถาบันเทคโนโลยีไทย-ญี่ปุ่นที่ช่วยอำนวยความสะดวกในการจัดทำและตรวจสอบเล่มวิทยานิพนธ์ฉบับนี้ให้เสร็จสมบูรณ์

สุธิดา ณรงค์ศักดิ์

สารบัญ

หน้า

สารบัญ (ต่อ)

สารบัญตาราง

ตาราง

หน้า

สารบัญรูป

สารบัญรูป (ต่อ)

รูป
หน้า

สารบัญรูป (ต่อ)

รูป หน้า


สถาบันเทคโนโลยีไทย-ญี่ปุ่น
THAI - NICHI INSTITUTE OF TECHNOLOGY
TNI

บทที่ 1
บทนำ

1.1 ที่มาและความสำคัญของปัญหา

ปริญญาบัตร (Degree Certificate) คือเอกสารที่ออกโดยสถานที่ศึกษาให้แก่ผู้เรียนที่สำเร็จการศึกษาในระดับอุดมศึกษา ถือเป็นสินทรัพย์ส่วนบุคคลที่มีความสำคัญ เนื่องจากเป็นหลักฐานที่ใช้ในการสมัครงาน หรือใช้ในการสมัครเรียนต่อในระดับที่สูงขึ้น โดยหลายครั้งมักใช้ร่วมกันกับบล็อกการศึกษา (Transcript) เพื่อยืนยันว่าผู้เรียนมีความรู้ความสามารถเพียงพอที่จะปฏิบัติงานหรือศึกษาต่อได้

ปัญหาหนึ่งที่อยู่คู่กับวงการศึกษามานานคือปัญหาการปลอมแปลงวุฒิการศึกษา ธุรกิจการสร้างและจัดจำหน่ายใบปริญญาบัตรปลอมถูกเรียกว่าเป็น “ธุรกิจพันล้าน” ที่มีโรงงานผลิตมากกว่า 3,000 แห่ง [1] ขายใบปริญญาบัตรปลอมไปแล้วกว่าหนึ่งล้านฉบับ [2] และมีแนวโน้มที่จะขยายตัวอย่างต่อเนื่อง ซึ่งเป็นผลมาจากการเติมโตของสังคมออนไลน์ที่ทำให้มนุษย์ทุกเพศทุกวัยเข้าถึงสื่อต่าง ๆ ได้อย่างรวดเร็วและง่ายดาย

การแพร่ระบาดของใบปริญญาปลอมถือเป็นภัยคุกคามที่สร้างความเสียหายต่อองค์กรเป็นอย่างมาก เนื่องจากเป็นการจ้างพนักงานที่ไม่มีความรู้ความสามารถที่เหมาะสมในการปฏิบัติงานนั้นๆ ซึ่งนอกจากจะเป็นการสร้างความเสียหายให้กับองค์กรแล้ว ยังสามารถสร้างความเสียหายให้กับบุคคลอื่นได้อีกด้วย โดยสามารถศึกษาได้จากข่าวต่าง ๆ เช่น กรณีการจ้างแพทย์ที่ใช้ใบประกอบวิชาชีพปลอมเข้าทำงานในสถาบันเสริมความงาม เป็นเหตุให้ผู้ป่วยได้รับความเสียหายจากการรักษาที่ไม่ถูกต้อง ซึ่งส่งผลต่อชีวิต ทรัพย์สิน และชื่อเสียงของสถานพยาบาล เป็นต้น ด้วยเหตุนี้ปัญหาใบปริญญาปลอมจึงถือเป็นภาระต่อองค์กรต่าง ๆ ที่ต้องพิสูจน์วุฒิการศึกษาของผู้สมัครงาน หลายบริษัทมีการจ้างผู้เชี่ยวชาญมาเพื่อตรวจสอบใบปริญญาบัตรของผู้สมัครงานโดยเฉพาะ ซึ่งขั้นตอนในการพิสูจน์เอกสารเป็นขั้นตอนที่มีความยุ่งยากและใช้เวลานาน นอกจากนี้ใบปริญญาบัตรในรูปแบบกระดาษยังง่ายต่อการเสียหายหรือสูญหาย โดยการขอออกใบปริญญาใหม่จะต้องใช้เวลาและเสียค่าใช้จ่ายในการดำเนินงาน

เทคโนโลยีเข้ามามีบทบาทกับสังคมและการเป็นอยู่ของมนุษย์ในปัจจุบันมากขึ้น เกิดเศรษฐกิจรูปแบบใหม่ที่เรียกว่า เศรษฐกิจดิจิทัล ซึ่งเป็นการประยุกต์ใช้เทคโนโลยีเพื่อเพิ่มประสิทธิภาพในทางธุรกิจและบริการ เป็นส่วนสำคัญที่ส่งผลให้การดำเนินกิจกรรมของมนุษย์มีรูปแบบเปลี่ยนไป เช่น การประยุกต์ใช้เทคโนโลยีกับการค้าปลีก เกิดเป็นธุรกิจการขายสินค้าออนไลน์ที่ผู้บริโภคสามารถซื้อสินค้าได้สะดวกมากขึ้นผ่านเว็บไซต์แอปพลิเคชัน ผู้ค้าสามารถขายสินค้าของตนได้มากขึ้น และช่วยลดต้นทุนการเช่าพื้นที่ หรือการประยุกต์ใช้เทคโนโลยีกับ

การขนส่ง ที่ทำให้เราสามารถเรียกใช้บริการรถรับจ้างได้ง่าย ๆ ผ่านแอปพลิเคชันบนโทรศัพท์มือถือ เป็นต้น

หนึ่งในเทคโนโลยีที่กำลังได้รับความนิยมเป็นอย่างมาก คือบล็อกเชน (Blockchain) เทคโนโลยีบล็อกเชนคือเทคโนโลยีการจัดเก็บข้อมูลแบบกระจายศูนย์หรือไร้ตัวกลาง โดยข้อมูลที่จัดเก็บจะมีการเข้ารหัสคอมพิวเตอร์และบันทึกอยู่ใน (Block) ต่อกันไปเรื่อย ๆ คล้ายกับห่วงโซ่ (Chain) ซึ่งไม่สามารถย้อนกลับไปแก้ไขหรือเปลี่ยนแปลงได้ ข้อมูลที่บันทึกอยู่ในบล็อกเชนจึงถือว่าเป็นข้อมูลที่มีความถูกต้อง โปร่งใส และสามารถตรวจสอบได้ เทคโนโลยีบล็อกเชนถูกนำไปประยุกต์ใช้ในแวดวงต่าง ๆ มากมาย ไม่ว่าจะเป็นธุรกิจการเงิน การประกันภัย หรือสถานพยาบาล

เหรียญดิจิทัล คือหน่วยอิเล็กทรอนิกส์ที่สร้างขึ้นจากระบบบล็อกเชนเพื่อทำหน้าที่เป็นสื่อกลางในการแลกเปลี่ยนหรือซื้อขายสินค้าและบริการต่าง ๆ หรือใช้ในจุดประสงค์บางอย่าง สามารถแบ่งออกได้หลายประเภท เช่น กลุ่มของเหรียญเพื่อการชำระเงิน (Payment Token) ที่มีคุณสมบัติในการใช้ซื้อหรือแลกเปลี่ยนสินค้าและบริการ หรือกลุ่มเหรียญที่ไม่สามารถทดแทนได้ (Non-Fungible Token: NFT) ที่มีคุณสมบัติเฉพาะของตัวเอง ไม่สามารถแลกเปลี่ยนหรือทดแทนกันได้

ผู้วิจัยจึงต้องการประยุกต์ใช้เทคโนโลยีบล็อกเชนในการสร้างระบบออกใบปริญญาบัตร โดยเปลี่ยนหน่วยกิตการศึกษาให้เป็นเหรียญดิจิทัลเพื่อใช้ในการรับส่งธุรกรรมที่เกิดขึ้นเพื่อให้ได้มาซึ่งใบปริญญาบัตรที่อยู่ในรูปแบบของสินทรัพย์ดิจิทัล ตามเงื่อนไขจริงที่กำหนดโดยสถาบันการศึกษา เพื่อเป็นการรับรองว่านักเรียนนักศึกษาได้รับปริญญามาอย่างถูกต้อง โดยสามารถตรวจสอบได้จากข้อมูลธุรกรรมที่บันทึกอยู่บนเครือข่ายซึ่งยากต่อการปลอมแปลง

1.2 วัตถุประสงค์

1.2.1 เพื่อวิเคราะห์และสร้างกรอบความคิดในการออกใบปริญญาบัตรด้วยการประยุกต์ใช้เทคโนโลยีบล็อกเชนและเหรียญดิจิทัลที่สามารถนำไปใช้ได้จริง

1.2.2 เพื่อวิเคราะห์ ออกแบบ และพัฒนาระบบที่สามารถตรวจสอบความถูกต้องของใบปริญญา

1.3 เป้าหมายของงานวิจัย

เพื่อเสนอแนวทางในการออกใบปริญญาบัตรในรูปแบบใหม่ที่ช่วยแก้ไขปัญหาการใบปริญญาบัตรปลอม และสามารถตรวจสอบความถูกต้องได้

บทที่ 2
ทฤษฎี หลักการ และงานวิจัยที่เกี่ยวข้อง

ในการทำวิจัยเรื่องการสร้างระบบออกใบปริญญาบัตรและโอนหน่วยกิตด้วยเหรียญดิจิทัล ผู้วิจัยได้ทำการรวบรวมองค์ความรู้ ทฤษฎี หลักการและงานวิจัยที่เกี่ยวข้อง โดยมีเนื้อหาดังนี้

2.1 ทฤษฎีและหลักการที่เกี่ยวข้อง

2.1.1 ปริญญาบัตร

2.1.2 เทคโนโลยีบล็อกเชน

2.1.3 วิทยาการเข้ารหัสลับ

2.1.4 สินทรัพย์ดิจิทัล

2.1.5 กระเป๋าเงินดิจิทัล

2.1.6 มัลติเซน

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 การสร้างระบบตรวจสอบเอกสารปริญญาบัตรด้วยรหัส QR code

2.2.2 การตรวจสอบใบปริญญาบัตรออนไลน์ด้วยเทคโนโลยีบล็อกเชน

2.2.3 การโอนหน่วยกิตในการศึกษาด้วยระบบบล็อกเชน

2.2.4 การสร้างใบปริญญา NFT พร้อมช่องทางการชำระเงินออนไลน์

2.1 ทฤษฎีและหลักการที่เกี่ยวข้อง

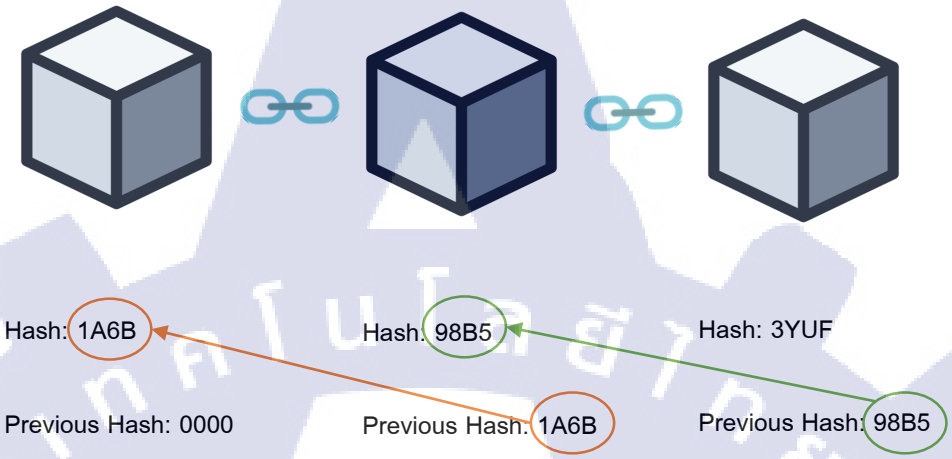
2.1.1 ปริญญาบัตร

ปริญญาบัตร (Graduate Certificate) คือเอกสารหลักฐานที่แสดงถึงการสำเร็จการศึกษาตามหลักสูตรที่มหาวิทยาลัยกำหนดไว้ โดยพจนานุกรมฉบับราชบัณฑิตสถานปี พุทธศักราช 2554 ได้ให้ความหมายของปริญญาบัตรไว้ว่า “คือบัตรที่แสดงวิทยฐานะของผู้สำเร็จการศึกษาว่ามีศักดิ์และสิทธิ์ระดับปริญญา” [3] หากสำเร็จการศึกษาต่ำกว่าระดับปริญญาตรี หรือต่ำกว่าระดับอุดมศึกษา จะเรียกเอกสารนั้นว่า ประกาศนียบัตร

2.1.2 เทคโนโลยีบล็อกเชน

เทคโนโลยีบล็อกเชน (Blockchain Technology) คือเทคโนโลยีการจัดเก็บข้อมูลแบบกระจายศูนย์ (Distributed Ledger Technology: DLT) ที่บันทึกข้อมูลหรือประวัติการทำธุรกรรมต่าง ๆ [4] ซึ่งจะถูกตรวจสอบและดูแลโดยเครื่องคอมพิวเตอร์ภายในเครือข่าย เมื่อมีข้อมูลทางธุรกรรมเกิดขึ้น คอมพิวเตอร์จะทำการตรวจสอบและยืนยันความถูกต้องของข้อมูลด้วยวิธี

คำนวณทางคณิตศาสตร์ ข้อมูลที่ได้รับการตรวจสอบแล้วจะถูกเชื่อมต่อกับข้อมูลก่อนหน้าเป็นห่วงโซ่ (Chain) [5] ดังรูปที่ 2.1

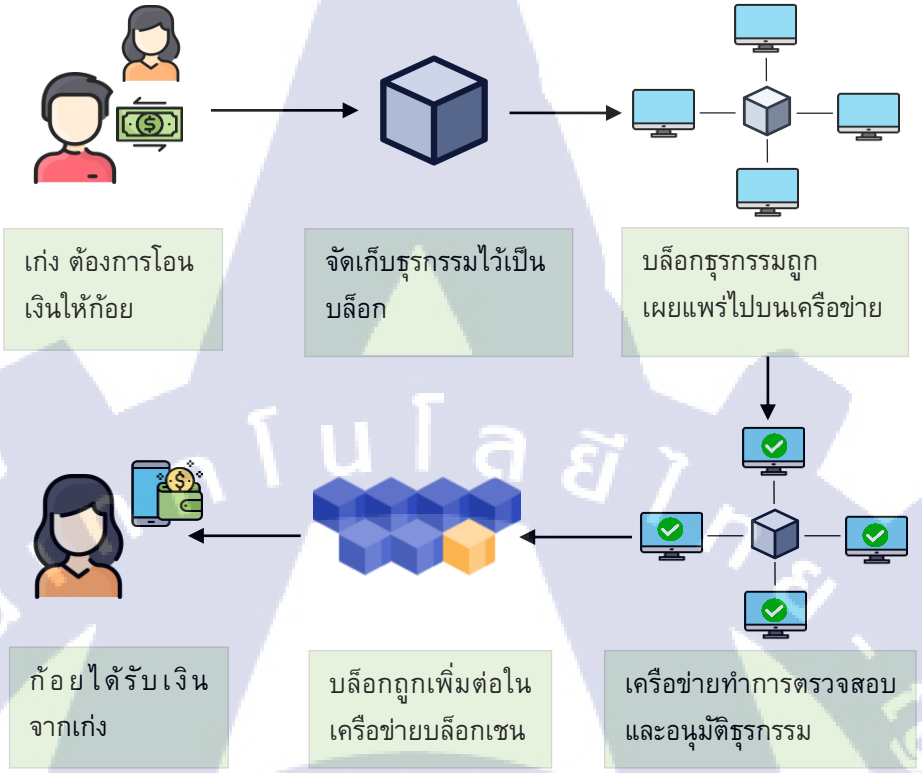


รูปที่ 2.1 การเชื่อมต่อกันของข้อมูลบนระบบบล็อกเชน

ด้วยคุณสมบัตินี้จึงทำให้ข้อมูลที่อยู่ในบล็อกเชนมีความปลอดภัยสูง สามารถดัดแปลงหรือแก้ไขได้ยาก เนื่องจากเครื่องคอมพิวเตอร์ทุกเครื่องบนเครือข่ายแบ่งปันและบันทึกข้อมูลเดียวกัน หากเครื่องคอมพิวเตอร์เครื่องใดพยายามทำการเปลี่ยนแปลงข้อมูล ข้อมูลที่ถูกเปลี่ยนแปลงจะขัดแย้งกับข้อมูลที่อยู่ในคอมพิวเตอร์เครื่องอื่น ทำให้ข้อมูลดังกล่าวไม่สามารถบันทึกในเครื่องคอมพิวเตอร์บนเครือข่ายได้ อีกทั้งยังมีความโปร่งใส สามารถตรวจสอบได้ และสามารถทำธุรกรรมหรือส่งข้อมูลต่าง ๆ ได้อย่างอิสระ เนื่องจากไม่มีตัวกลางมาจัดการ

วิวัฒนาการของเทคโนโลยีบล็อกเชน เริ่มขึ้นในยุคแรก คือบล็อกเชน 1.0 เกิดขึ้น Satoshi Nakamoto ได้เสนอไว้ใน “Bitcoin: A Peer-to-Peer Electronic Cash System” [6] ซึ่งเป็นแนวคิดเกี่ยวกับการสร้างเครื่องมือที่มีความปลอดภัยในการแลกเปลี่ยนเงินสกุลดิจิทัล เพื่อแก้ไขปัญหาการจ่ายเงินซ้ำซ้อนและเป็นการดำเนินธุรกรรมทางการเงินที่ไม่ต้องผ่านตัวกลาง โดยประยุกต์ใช้วิทยาการเข้ารหัสลับ (Cryptography) เพื่อสร้างธุรกรรมบนเครือข่ายอินเทอร์เน็ต จากนั้นจะทำการเผยแพร่และบันทึกข้อมูลธุรกรรมเหล่านั้นไว้บนเครื่องคอมพิวเตอร์ทุกเครื่องที่อยู่บนเครือข่าย

บิทคอยน์ถือเป็นการประยุกต์ใช้เทคโนโลยีบล็อกเชนครั้งแรกที่มาพร้อมกับระบบการจ่ายเงินออนไลน์ผ่านระบบอินเทอร์เน็ต [7] จึงทำให้เป็นที่น่าสนใจและได้รับความนิยม นอกจากนี้บิทคอยน์ยังเป็นพื้นฐานของการสร้างสกุลเงินดิจิทัลเพื่อทำธุรกรรมต่าง ๆ แบบกระจายศูนย์ ดังรูปที่ 2.2

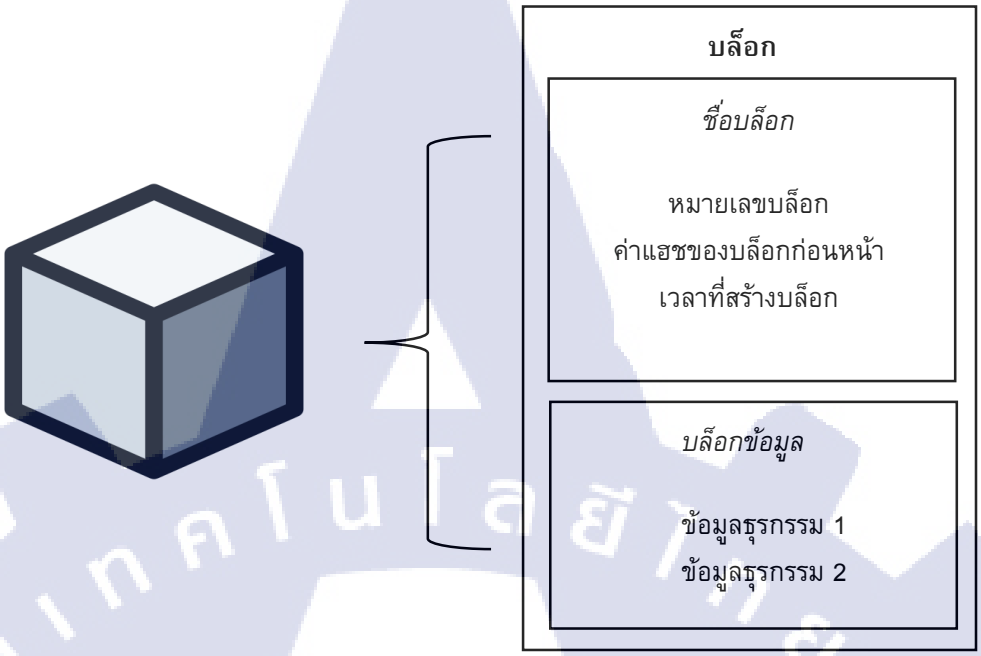


รูปที่ 2.2 ตัวอย่างการทำงานของเทคโนโลยีบล็อกเชน

บล็อกเชน 2.0 ถูกพัฒนาขึ้น โดย Vitalik Buterin ได้ให้กำเนิดสกุลเงินดิจิทัลที่ชื่อว่า อีเธอเรียม (Ethereum) [8] ที่มีความสามารถในการสร้างสัญญาอัจฉริยะ (Smart Contract) บนระบบบล็อกเชน ซึ่ง Nick Szabo เป็นผู้เสนอแนวคิดในการสร้างสัญญาในรูปแบบของโปรแกรมคอมพิวเตอร์เพื่อให้ข้อตกลงและเงื่อนไขของสัญญาสามารถดำเนินการได้ด้วยตนเอง ลดข้อผิดพลาดที่เกิดจากความตั้งใจหรือไม่ตั้งใจ และลดความต้องการของตัวกลางที่เชื่อถือได้ [9]

โครงสร้างของบล็อกเชน 1.0 และบล็อกเชน 2.0 มีองค์ประกอบคล้ายกัน ซึ่งมีส่วนประกอบหลัก ๆ 3 ส่วน ได้แก่ บล็อก เครือข่าย และฉันทามติ [7]

(1) บล็อก (Block) คือ ส่วนที่ทำหน้าที่เก็บรวมรวมข้อมูลหรือธุรกรรมที่เกิดขึ้น สามารถแบ่งได้เป็น 2 ส่วนใหญ่ ๆ คือ ชื่อบล็อก (Block Header) ที่ใช้ระบุให้ทราบถึงข้อมูลภายในบล็อก เช่น หมายเลขบล็อก เวลาที่สร้างบล็อก ค่าแฮช เป็นต้น และข้อมูลในบล็อก (Block data) ที่ใช้บรรจุข้อมูลต่าง ๆ [10] โดยบล็อกแรกที่ถูกสร้างขึ้นบนเครือข่ายบล็อกเชนเรียกว่า “Genesis Block” หรือ หรือ “Block 0” ดังรูปที่ 2.3



รูปที่ 2.3 ส่วนประกอบของบล็อก

(2) เครือข่าย (Network) คือ ส่วนที่ทำหน้าที่เชื่อมต่ออุปกรณ์ใด ๆ เข้ากับระบบบล็อกเชน โดยจะมีการบันทึกและตรวจสอบความถูกต้องของข้อมูลธุรกรรมและแบ่งปันข้อมูลให้กับผู้ใช้งานทุกเครื่องที่อยู่ในระบบ และเป็นส่วนที่ควบคุมสิทธิ์ในการเข้าถึงข้อมูล [7] เครือข่ายของเทคโนโลยีบล็อกเชน ใช้การเชื่อมต่อไร้สายแบบโครงข่ายตรงระหว่างเครื่องคอมพิวเตอร์โดยไม่ต้องผ่านตัวกลาง (Peer-to-peer network: P2P) [5]

(3) ฉันทามติ (Consensus) คือข้อตกลงที่ยอมรับร่วมกันระหว่างระหว่างสมาชิกในเครือข่าย เพื่อใช้ในกระบวนการตรวจสอบยืนยันความถูกต้องของธุรกรรม [11] โดยฉันทามติสามารถทำได้หลายวิธี [10] เช่น

การพิสูจน์ด้วยการทำงาน (Proof of Work: PoW) คือการยืนยันธุรกรรมที่ต้องใช้กำลังในด้านการประมวลผลเพื่อแก้โจทย์ปัญหาทางคณิตศาสตร์ โดยเครื่องคอมพิวเตอร์หรือ โหนด (Node) แรกที่สามารถแก้โจทย์ปัญหาได้ก่อนจะเป็นผู้เผยแพร่ข้อมูลในบล็อกนั้น ๆ

การพิสูจน์ด้วยการวางเงิน (Proof of Stake: PoS) คือการยืนธุรกรรมโดยดูจากสินทรัพย์หรือเงินดิจิทัลที่วางไว้ในระบบ โดยหากเงินที่วางไว้ยิ่งมีจำนวนมาก ก็ยิ่งเพิ่มโอกาสที่ธุรกรรมนั้นจะได้รับการยืนยันจากระบบ

ฉันทามติแบบผลัดกันทั้งหมด (Round Robin) คือการยืนยันธุรกรรมที่นิยมใช้ในเครือข่ายบล็อกเชนแบบส่วนตัว โดยแต่ละโหนดจะผลัดกันเป็นผู้สร้างบล็อก และจะมีการ

กำหนดระยะรอคอยในการสร้างบล็อกถัดไป เพื่อไม่ให้โหนดใดโหนดหนึ่งสร้างบล็อกมากกว่าโหนดอื่น ๆ

บล็อกเชน 3.0 คือเทคโนโลยีบล็อกเชนให้มีความปลอดภัยมากขึ้น และสามารถขยายขีดความสามารถ ทำให้นำไปประยุกต์ใช้กับอุตสาหกรรมอื่นนอกเหนือจากธุรกิจการเงินได้ [5] โดยมุ่งเน้นไปที่การพัฒนาแอปลิเคชันแบบกระจายศูนย์ (Decentralized Application)

โครงสร้างทางสถาปัตยกรรมของเทคโนโลยีบล็อกเชน 3.0 สำหรับใช้พัฒนาแอปพลิเคชันแบบกระจายศูนย์ สามารถแบ่งได้เป็น 6 ชั้น คือ ชั้นข้อมูล ชั้นเครือข่าย ชั้นฉันทามติ ชั้นผลตอบแทน ชั้นสัญญา และชั้นโปรแกรมประยุกต์ [12] ดังรูปที่ 2.4

รูปที่ 2.4 โครงสร้างทางสถาปัตยกรรมของเทคโนโลยีบล็อกเชน 3.0

เทคโนโลยีบล็อกเชน สามารถแบ่งออกได้เป็น 4 ประเภท [13] ได้แก่ บล็อกเชนสาธารณะ บล็อกเชนส่วนตัว บล็อกเชนเฉพาะกลุ่ม และบล็อกเชนผสมผสาน ดังรูปที่ 2.5

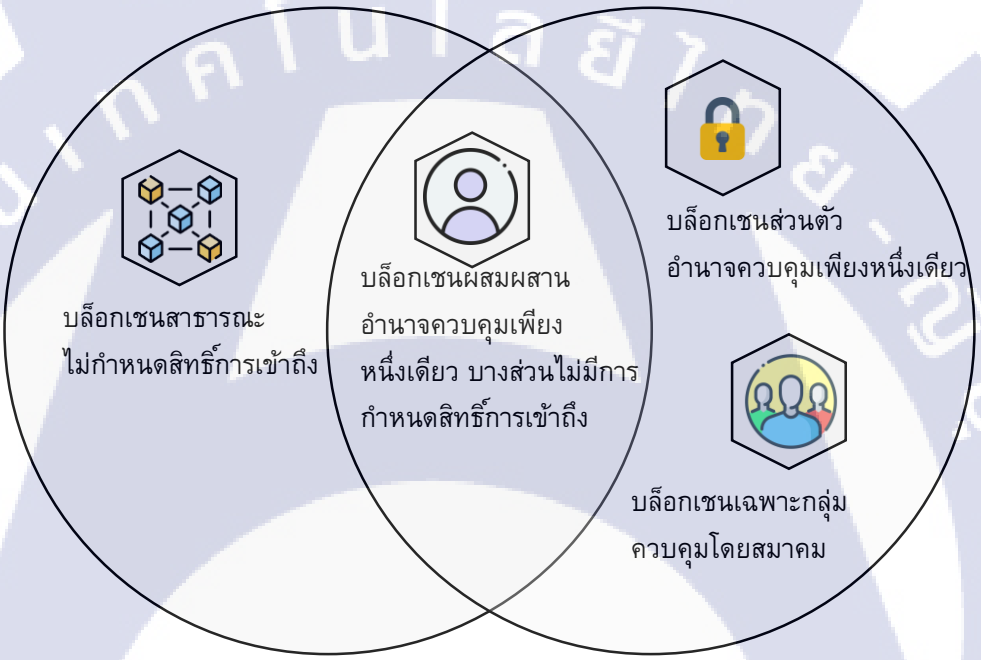
(1) บล็อกเชนสาธารณะ (Public Blockchain หรือ Permissionless Blockchain) คือระบบที่อนุญาตให้ทุกคนมีสิทธิ์ในการเข้าถึงเครือข่ายและข้อมูลได้อย่างอิสระ [13] โดยส่วนใหญ่เครือข่ายบล็อกเชนสาธารณะมักจะเป็นซอฟต์แวร์ที่เปิดเผยที่มาและหลักการให้บุคคลภายนอกใช้งานได้โดยไม่เสียค่าใช้จ่าย (Open-source software) เช่น บิทคอยน์ (Bitcoin) และอีเธอเรียม (Ethereum)

(2) บล็อกเชนส่วนตัว (Private Blockchain หรือ Permissioned Blockchain) คือระบบที่อนุญาตให้เฉพาะบุคคลที่กำหนดมีสิทธิ์เข้าถึงข้อมูลได้ โดยผู้ที่มีอำนาจบริหารจัดการ

จะมีเพียงหนึ่งเดียว (Single Authority) บล็อกเชนส่วนตัวมักนิยมใช้ในบริษัทที่ต้องการความปลอดภัยสูง [13] เช่น ไฮเปอร์เลดเจอร์ (Hyperledger) เป็นต้น

(3) บล็อกเชนเฉพาะกลุ่ม (Consortium Blockchain) คือบล็อกเชนที่จำกัดการเข้าถึงเฉพาะกลุ่มที่กำหนด บริหารจัดการโดยสมาคมที่เป็นการรวมกลุ่มระหว่างบริษัทหรือองค์กร มากกว่าบริหารจัดการโดยองค์กรใดองค์กรหนึ่ง เช่น คาร์โกสมาร์ท (Cargo Smart) [14]

(4) บล็อกเชนผสมผสาน (Hybrid Blockchain) คือบล็อกเชนที่ประยุกต์ใช้ระหว่างบล็อกเชนสาธารณะและบล็อกเชนส่วนตัวเข้าด้วยกัน กำกับและควบคุมโดยหนึ่งองค์กรเพื่อกำหนดสิทธิ์ในการเข้าถึงข้อมูล [13]



รูปที่ 2.5 ประเภทของเทคโนโลยีบล็อกเชน

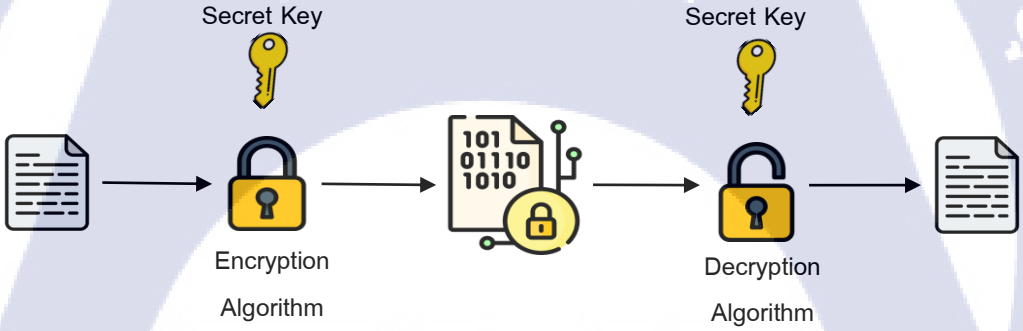
2.1.3 วิทยาการเข้ารหัสลับ

วิทยาการเข้ารหัสลับ (Cryptography) คือวิธีการทางคณิตศาสตร์ที่ใช้ในการเข้ารหัสและถอดรหัสข้อมูล [15] โดยจะมีกลไกในการเปลี่ยนข้อมูลหรือข้อความธรรมดาให้อยู่ในรูปแบบข้อความที่ไม่สามารถอ่านได้ และเปลี่ยนข้อความที่อ่านไม่ได้นั้น กลับมาอยู่ในรูปแบบที่อ่านได้เช่นเดิม วิทยาการเข้ารหัสลับมีหลักการพื้นฐาน 4 อย่าง คือ การรักษาความลับ การรักษาข้อมูลให้มีความถูกต้อง การพิสูจน์ความถูกต้อง และการห้ามปฏิเสธความรับผิด [16] ดังรูปที่ 2.6

รูปที่ 2.6 การเข้ารหัสข้อมูล

วิทยาการเข้ารหัสลับสามารถแบ่งได้เป็น 3 ประเภท [17] คือ การเข้ารหัสแบบกุญแจสมมาตร การเข้ารหัสแบบกุญแจอสมมาตร และการเข้ารหัสแบบฟังก์ชันแฮช

(1) การเข้ารหัสแบบกุญแจสมมาตร (symmetric-key cryptography) หรือกุญแจลับ (Secret Key) คือการเข้ารหัสและถอดรหัสข้อมูลที่ผู้รับและผู้ส่งใช้กุญแจเดียวกัน ผู้รับและผู้ส่งจะต้องมีกุญแจรหัสลับแบบเดียวกันเพื่อใช้ในการเข้ารหัสและถอดรหัสข้อมูล [15] ดังรูปที่ 2.7

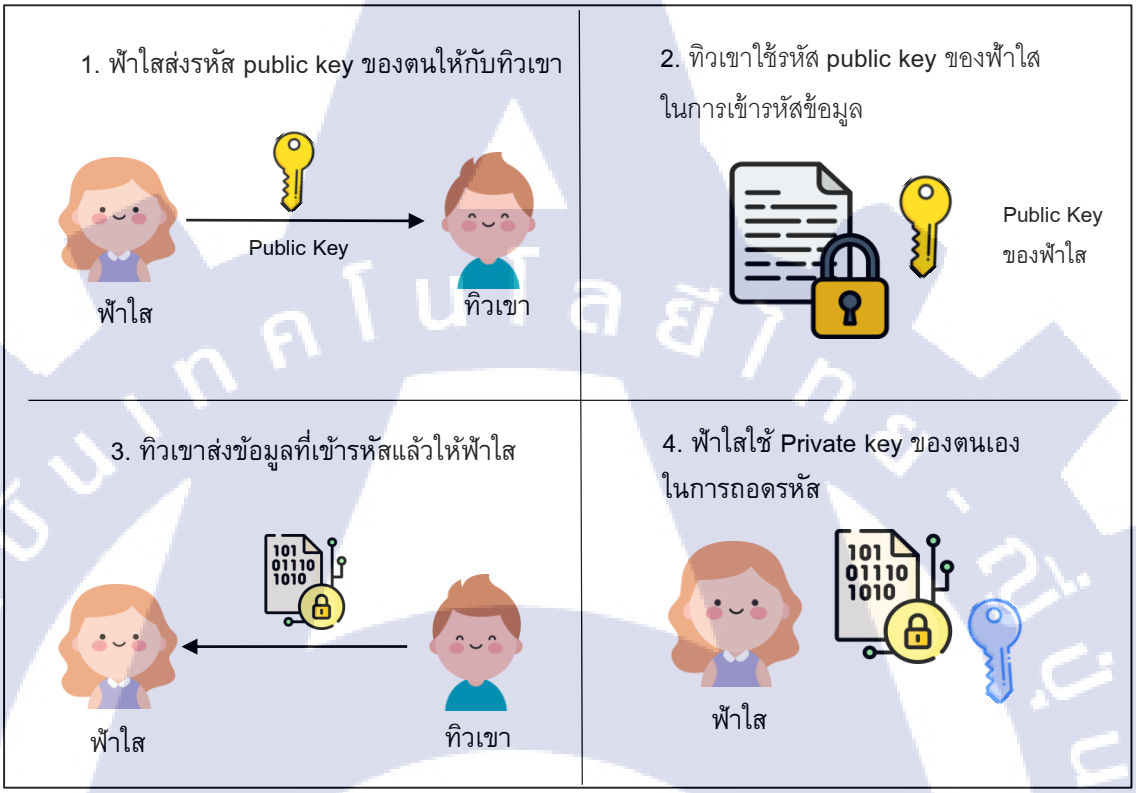


รูปที่ 2.7 การเข้ารหัสแบบกุญแจสมมาตร

การเข้ารหัสแบบกุญแจสมมาตรยังสามารถแบ่งออกเป็น 2 รูปแบบย่อย ได้แก่ การเข้ารหัสบล็อก (Block Cipher) คือการแบ่งข้อมูลเป็นส่วน ๆ ที่มีความยาวเท่ากันและทำการเข้ารหัสไปทีละบล็อก และการเข้ารหัสกระแส (Stream Cipher) คือการเข้ารหัสครั้งละหนึ่งบิตหรือหนึ่งไบต์ [17]

(2) การเข้ารหัสแบบกุญแจอสมมาตร (Asymmetric-key cryptography) หรือกุญแจสาธารณะ (Public Key) คือการเข้ารหัสและถอดรหัสข้อมูลด้วยกุญแจหนึ่งคู่ นั่นคือ กุญแจสาธารณะ (Public Key) ใช้ในการเข้ารหัสข้อมูล และกุญแจส่วนตัว (Private Key) ใช้ใน

การถอดรหัสข้อมูล โดยผู้รับข้อมูลจะต้องเปิดเผยกุญแจสาธารณะของตนเองให้คนอื่นทราบ เพื่อให้ผู้อื่นส่งข้อมูลที่เข้ารหัสแล้วมาให้ และเก็บกุญแจส่วนตัวไว้เป็นความลับเพื่อใช้ในการถอดรหัสข้อมูล [15] ดังรูปที่ 2.8



รูปที่ 2.8 การเข้ารหัสแบบกุญแจอสมมาตร

(3) การเข้ารหัสแบบฟังก์ชันแฮช (Hash Function Cryptography) คือการเข้ารหัสทางเดียวที่ใช้คำนวณหาอัตลักษณ์หรือเอกลักษณ์ของข้อมูล ผลลัพธ์จากการคำนวณจะมีขนาดคงที่ และข้อความหรือข้อมูลเดียวกันจะได้ผลลัพธ์เหมือนกันเสมอ ในขณะเดียวกันเมื่อข้อมูลถูกเปลี่ยนแปลงไปเพียงเล็กน้อย ผลลัพธ์ที่ได้จะเปลี่ยนแปลงไปอย่างสิ้นเชิง [17] นอกจากนี้การเข้ารหัสแบบฟังก์ชันแฮชยังถือเป็นหัวใจของเทคโนโลยีบล็อกเชน เนื่องจากเป็นกระบวนการที่ใช้ตรวจสอบความถูกต้องของข้อมูลภายในบล็อก [10] ดังรูปที่ 2.9

รูปที่ 2.9 การเข้ารหัสแบบฟังก์ชันแฮช

การเข้ารหัสแบบฟังก์ชันแฮชมีมาตรฐานในการใช้งานอยู่หลายแบบ โดยจะแตกต่างกันที่รูปแบบการทำงานและขนาดของผลลัพธ์ที่ได้หลังการเข้ารหัส เช่น มาตรฐาน SHA-256 ผลลัพธ์ที่ได้จะมีขนาด 256 บิท และผลลัพธ์จากมาตรฐาน SHA-512 จะมีขนาด 512 บิท เป็นต้น

2.1.4 สินทรัพย์ดิจิทัล

สินทรัพย์ดิจิทัล (Digital Asset) คือ สิ่งใด ๆ ในรูปแบบระบบเลขฐานสองที่มีสิทธิ์ในการใช้งาน โดยครอบคลุมถึงสินทรัพย์เสมือน (Virtual Asset) เช่น วีดีโอเกมส์ และสินทรัพย์อิเล็กทรอนิกส์ที่ควบคุมและกำกับโดยหน่วยงาน เช่น สกุลเงินดิจิทัล เป็นต้น [18]

ในประเทศไทย สินทรัพย์ดิจิทัลถูกจัดให้เป็นผลิตภัณฑ์ในการลงทุนประเภทหนึ่ง กำกับและดูแลการประกอบธุรกิจและการดำเนินกิจกรรมโดยสำนักงานกำกับหลักทรัพย์และตลาดหลักทรัพย์ (ก.ล.ต.) ภายใต้พระราชกำหนดการประกอบธุรกิจสินทรัพย์ดิจิทัล (พ.ร.ก.) ปีพุทธศักราช 2561 [19] ซึ่งสามารถแบ่งสินทรัพย์ดิจิทัลออกเป็น 2 ประเภท ตามลักษณะการใช้งานและสิทธิที่กำหนดไว้ ได้แก่ สกุลเงินดิจิทัล และโทเคนดิจิทัล

สกุลเงินดิจิทัล (Digital Currency) หรือ คริปโตเคอร์เรนซี (Cryptocurrency) คือ หน่วยอิเล็กทรอนิกส์ที่สร้างขึ้นบนระบบหรือเครือข่ายอิเล็กทรอนิกส์ที่ใช้เป็นสื่อกลางในการแลกเปลี่ยนสินค้า บริการ สิทธิอื่นใด หรือแลกเปลี่ยนระหว่างสินทรัพย์ดิจิทัล [19] เช่น บิทคอยน์ (Bitcoin) และ อีเธอเรียม (Ethereum) เป็นต้น

โทเคนดิจิทัล (Digital Token) คือ หน่วยอิเล็กทรอนิกส์ที่สร้างขึ้นบนระบบเพื่อใช้กำหนดสิทธิของบุคคล สิทธิในการซื้อสินค้าหรือบริการ หรือสิทธิเฉพาะเจาะจงอื่น ๆ [19] สามารถแบ่งได้เป็น 2 ประเภทย่อย ๆ ได้แก่ โทเคนดิจิทัลเพื่อการลงทุน (Investment Token) คือ หน่วยอิเล็กทรอนิกส์ที่สร้างขึ้นเพื่อกำหนดสิทธิในการร่วมลงทุน เช่น สิทธิในส่วนแบ่งรายได้ผลกำไรจากการลงทุน เป็นต้น [20] และโทเคนดิจิทัลเพื่อการใช้ประโยชน์ (Utility Token) คือ หน่วยอิเล็กทรอนิกส์ที่สร้างขึ้นเพื่อกำหนดสิทธิในการได้รับสินค้าหรือบริการที่เจาะจง [20] เช่น สิทธิในการเข้าถึงโครงการ หรือสิทธิในการแลกสินค้าในโครงการ

สินทรัพย์ดิจิทัล หรือเรียกรวม ๆ ว่าเหรียญดิจิทัล มีการสร้างและพัฒนาเหรียญต่าง ๆ ขึ้นมาอย่างต่อเนื่องเพื่อใช้ตอบโจทย์ความต้องการที่หลากหลาย ซึ่งในแต่ละเหรียญอาจสร้างขึ้นโดยใช้มาตรฐานที่แตกต่างกัน เช่น การใช้มาตรฐาน ERC-20 เพื่อใช้สร้างเหรียญในระบบสัญญาอัจฉริยะ ซึ่งมีความสามารถในการโอนถ่ายระหว่างบัญชี สามารถตรวจสอบยอดคงเหลือในบัญชีและจำนวนเหรียญที่อยู่ในระบบได้ [21] หรือการใช้มาตรฐาน ERC-721 ในการสร้างเหรียญที่ไม่สามารถทดแทนได้ เพื่อใช้ในวงการของสะสมและงานศิลปะ เป็นต้น [22] โดยในปัจจุบันเหรียญดิจิทัลสามารถแบ่งประเภทตามวัตถุประสงค์ของการใช้งานได้ 8 กลุ่ม [23] ดังนี้

(1) กลุ่มเหรียญดิจิทัลเพื่อใช้ชำระเงิน (Payment Token) คือเหรียญดิจิทัลที่ทำงานบนระบบบล็อกเชนที่มีการเชื่อมต่อโดยตรงระหว่างคอมพิวเตอร์ (Peer to Peer Network) สามารถทำธุรกรรมต่าง ๆ ได้โดยไม่ต้องผ่านตัวกลาง และรองรับการทำธุรกรรมจำนวนมาก [24] มีจุดประสงค์เพื่อใช้เป็นสื่อกลางในการชำระหรือแลกเปลี่ยนสินค้าและบริการ เช่น บิทคอยน์ (Bitcoin: BTC) [6] และ ไลท์คอยน์ (Litecoin: LTC) [25]

(2) กลุ่มเหรียญสัญญาอัจฉริยะ (Smart Contract Token) คือเหรียญดิจิทัลที่มีความสามารถในการสร้างสัญญาอัจฉริยะผ่านระบบบล็อกเชน มีจุดประสงค์เพื่อใช้ตรวจสอบยืนยัน และบังคับใช้สัญญาตามเงื่อนไขที่ระบุไว้โดยไม่ต้องผ่านตัวกลาง [26] เช่น อีเธอเรียม (Ethereum: ETH) [8] และ คาร์ดาโน (Cardono: ADA) [27]

(3) กลุ่มเหรียญส่วนตัว (Privacy Token) คือเหรียญดิจิทัลที่มีการปกปิดข้อมูลการทางธุรกรรม และไม่สามารถติดตามหรือแกะรอยได้ [23] มีจุดประสงค์เพื่อรักษาความเป็นส่วนตัวในการดำเนินธุรกรรม เช่น โมเนโร (Monero: XMR) [28]

(4) กลุ่มเหรียญเพื่อการใช้ประโยชน์ (Utility Token) คือเหรียญดิจิทัลที่สร้างขึ้นเพื่อใช้ดำเนินการตามจุดประสงค์ที่กำหนดเอาไว้ [23] เช่น เหรียญ BAT (Basic Attention Token: BAT) ที่พัฒนาเพื่อใช้งานสำหรับอุตสาหกรรมโฆษณาดิจิทัลโดยเฉพาะ [29]

(5) กลุ่มเหรียญหลักทรัพย์ (Security Token) คือเหรียญดิจิทัลที่ใช้แทนการลงทุนที่ถูกบันทึกอยู่ในระบบบล็อกเชน ถูกควบคุมภายใต้กฎหมายหรือองค์กรรัฐ [30] เช่น หุ้น ตราสารหนี้ ตราสารอนุพันธ์ เป็นต้น สร้างขึ้นเพื่อใช้การลงทุนหรือระดมทุน โดยผู้ลงทุนจะได้รับเหรียญดิจิทัลแทนผลกำไร

(6) กลุ่มเหรียญมูลค่าคงที่ (Stablecoin) คือเหรียญดิจิทัลที่อ้างอิงมูลค่ากับสินทรัพย์อื่น ๆ ในอัตราการแลกเปลี่ยนคงที่ 1:1 [31] มีจุดประสงค์เพื่ออำนวยความสะดวกให้กับนักลงทุนสินทรัพย์ดิจิทัล สามารถแบ่งออกเป็นกลุ่มย่อย ๆ ได้อีก 4 กลุ่มตามประเภทของสินทรัพย์ที่อ้างอิง ได้แก่

(6.1) เหรียญมูลค่าคงที่ที่อ้างอิงมูลค่าจากเงินตรา (Fiat – collateralized) [32] จะอ้างอิงมูลค่าจากสกุลเงินต่าง ๆ บนโลก เช่น เหรียญ USD Coin (USDC) ที่ผูกมูลค่าไว้กับสกุลเงินดอลลาร์สหรัฐ สามารถแลกเหรียญ USDC [33] ในอัตรา 1 เหรียญ ต่อ 1 ดอลลาร์สหรัฐ

(6.2) เหรียญมูลค่าคงที่ที่ผูกมูลค่าไว้กับสินค้าโภคภัณฑ์ (Commodity – collateralized) [34] จะอ้างอิงมูลค่ากับสินทรัพย์ที่จับต้องได้ ไม่ว่าจะเป็นน้ำมัน ทองคำ หุ้น หรือโลหะ เช่น เหรียญ DGX [35] ที่ผูกมูลค่าไว้กับทองคำ สามารถแลกเหรียญ DGX ในอัตรา 1 เหรียญ ต่อทองคำ 1 กรัมได้

(6.3) เหรียญมูลค่าคงที่ที่อ้างอิงมูลค่าไว้กับสกุลเงินดิจิทัล (Crypto-collateralized) จะอ้างอิงมูลค่ากับสกุลเงินดิจิทัลอื่น ๆ ซึ่งอัตราการแลกเปลี่ยนเหรียญมูลค่าคงที่จะไม่ใช่ 1:1 แต่จะต้องค้ำประกันด้วยเหรียญดิจิทัลที่มีจำนวนมากกว่า [34] เช่น เหรียญ DAI [36] ที่สามารถนำโทเคน ERC-20 ที่ MakerDAO ยอมรับในการค้ำประกันมูลไปแลกเปลี่ยนได้

(6.4) เหรียญมูลค่าคงที่ที่ไม่อ้างอิงมูลค่า (Non- collateralized หรือ Algorithmic Stablecoins) คือเหรียญที่ไม่มีการอ้างอิงมูลค่ากับสิ่งใด แต่จะใช้กระบวนการควบคุมอุปทาน [34]

(7) กลุ่มเหรียญสำหรับใช้ในธุรกรรมแบบกระจายศูนย์ (Decentralized Finance) คือเหรียญดิจิทัลบนระบบที่สามารถทำธุรกรรมที่ไม่ต้องผ่านตัวกลาง แต่ใช้เทคโนโลยีบล็อกเชนและควบคุมกลไกการทำงานให้เป็นไปตามเงื่อนไขที่กำหนดผ่านสัญญาอัจฉริยะ [23] เช่น เหรียญ Aave คือเหรียญที่ใช้กำกับดูแล Aave Protocol [37] ซึ่งเป็นระบบกู้ยืมเหรียญดิจิทัลแบบกระจายศูนย์ ซึ่งผู้ถือเหรียญสามารถเสนอนโยบายเพื่อพัฒนาปรับปรุงระบบต่าง ๆ ได้

(8) กลุ่มเหรียญที่ไม่สามารถทดแทนได้ (Non-Fungible Token: NFT) คือเหรียญดิจิทัลที่มีความเป็นเอกลักษณ์ในตัวเอง ไม่สามารถแลกเปลี่ยนระหว่างกันได้ [38] และสามารถแสดงความเป็นเจ้าของในสินทรัพย์ดิจิทัล เช่น รูปภาพ เพลง หรือวีดีโอ โดยใช้เทคโนโลยีบล็อกเชนและสัญญาอัจฉริยะในการสร้างและดำเนินธุรกรรม [39]

2.1.5 กระเป๋าเงินดิจิทัล

กระเป๋าเงินดิจิทัล (Digital Wallet) คือ โปรแกรมประยุกต์ที่ใช้สร้าง จัดการ และจัดเก็บกุญแจส่วนตัว (Private Key) และกุญแจสาธารณะ (Public Key) ที่อยู่ในรูปของโปรแกรมหรืออุปกรณ์ใด ๆ [40] เพื่อใช้เข้าถึงสินทรัพย์ดิจิทัลหรือทำธุรกรรมต่าง ๆ บนเครือข่ายบล็อกเชน ดังรูปที่ 2.10

รูปที่ 2.10 การทำงานของกระเป๋าเงินดิจิทัล

กระเป๋าเงินดิจิทัลสามารถแบ่งได้เป็น 2 ประเภทใหญ่ ๆ คือ กระเป๋าเงินร้อน และกระเป๋าเงินเย็น

กระเป๋าเงินร้อน (Hot Wallets) คือกระเป๋าเงินดิจิทัลที่มีการเชื่อมต่ออินเตอร์เน็ตเข้าถึงสินทรัพย์ดิจิทัลและการทำธุรกรรมต่าง ๆ ได้อย่างรวดเร็ว [40] โดยกระเป๋าเงินประเภทนี้สามารถแบ่งได้เป็น 4 รูปแบบย่อย [41] คือ

(1) กระเป๋าเงินบนเว็บไซต์ (Web Wallet หรือ Online Wallets) คือกระเป๋าเงินดิจิทัลที่ติดตั้งและใช้งานผ่านเว็บไซต์

(2) กระเป๋าเงินบนมือถือ (Mobile Wallets) คือกระเป๋าเงินดิจิทัลที่ติดตั้งและใช้งานผ่านโทรศัพท์มือถือที่มีการเชื่อมต่ออินเตอร์เน็ต

(3) กระเป๋าเงินบนเครื่องคอมพิวเตอร์ (Desktop Wallets) คือกระเป๋าเงินดิจิทัลที่ติดตั้งและใช้งานผ่านโปรแกรมบนเครื่องคอมพิวเตอร์

(4) กระเป๋าเงินหลายลายเซ็น (Multisignature Wallets) คือกระเป๋าเงินดิจิทัลที่ต้องใช้กุญแจส่วนตัวมากกว่าหนึ่งในการทำธุรกรรม เหมาะสำหรับบริษัทหรือองค์กร

กระเป๋าเงินเย็น (Cold Wallets) คือกระเป๋าเงินดิจิทัลที่ไม่มีการเชื่อมต่ออินเตอร์เน็ตทำให้มีความปลอดภัยต่อการถูกโจมตีหรือโจรกรรมมากกว่า [40] ซึ่งกระเป๋าเงินเย็นสามารถแบ่งได้ 2 รูปแบบย่อย [41] คือ

(1) กระเป๋าเงินแบบอุปกรณ์ (Hardware Wallets) คือกระเป๋าเงินดิจิทัลที่ใช้งานผ่านอุปกรณ์ เหมาะสำหรับการจัดเก็บสินทรัพย์ดิจิทัลในระยะยาว

(2) กระเป๋าเงินแบบกระดาษ (Paper Wallets) คือการจดบันทึกกุญแจส่วนตัวไว้ในรูปแบบกระดาษ

2.1.6 มัลติเชน

มัลติเชน (Multichain) คือ โครงสร้างพื้นฐานของเทคโนโลยีบล็อกเชนแบบ Open Source ที่เปิดเผยและอนุญาตให้บุคคลภายนอกนำรหัสต้นฉบับ (Source Code) ไปสร้างและใช้งานบล็อกเชนส่วนตัวแบบภายในหรือระหว่างองค์กร มีจุดประสงค์เพื่อแก้ไขปัญหาด้านความเป็นส่วนตัว การควบคุม และการเปิดเผยข้อมูลผ่านการจัดการสิทธิ์ของผู้ใช้งานในรูปแบบที่สามารถใช้งานได้ง่าย [42] นอกจากนี้มัลติเชนยังรองรับการเชื่อมต่อระหว่างบล็อกเชนต่างเครือข่ายให้สามารถติดต่อสื่อสาร หรือแลกเปลี่ยนสินทรัพย์กันได้ ทำให้มัลติเชนมีความโดดเด่นในด้านการสร้างแอพลิเคชั่นแบบต่างโซ่ (Cross-chain)

เพื่อแก้ไขปัญหาด้านความเป็นส่วนตัว มัลติเชนได้ให้บริการเครือข่ายบล็อกเชนแบบส่วนตัว (Private Blockchain) ที่มั่นใจว่ากิจกรรมที่เกิดขึ้นทั้งหมดบนเครือข่ายจะถูกเผยแพร่ให้เฉพาะบุคคลที่ได้รับอนุญาตเท่านั้น โดยสิทธิ์ในการควบคุมการเข้าถึงข้อมูลของผู้ใช้งานจะถูกมอบหมายให้กับบล็อกแรกที่สร้างขึ้นบนเครือข่ายเรียกว่าผู้ดูแล (Administrator)

เพื่อหลีกเลี่ยงค่าใช้จ่ายและการผูกขาดจากการยืนยันธุรกรรม มัลติเชนกำหนดฉันทามติแบบผลัดกันทั้งหมด (Round Robin consensus) ซึ่งนักขุดทั้งหมดที่อยู่บนเครือข่ายจะผลัดกันสร้างบล็อก โดยมีข้อกำหนดเรื่องระยะการรอคอยที่นักขุดจะสามารถสร้างบล็อกถัดไปได้ และเมื่อไม่มีการแข่งขันในการขุดหรือสร้างบล็อก จึงไม่จำเป็นต้องให้ผลตอบแทนเป็นเงินรางวัลแก่นักขุด ทำให้ต้นทุนในการสร้างหรือเผยแพร่ธุรกรรมเป็นศูนย์

2.2 งานวิจัยที่เกี่ยวข้อง

2.2.1 การสร้างระบบตรวจสอบเอกสารปริญญาบัตรด้วยรหัส QR code

H. A. Ahmed และ J. W. Jang [43] ได้เสนอแนวคิดในการพัฒนาระบบตรวจสอบเอกสารปริญญาบัตรโดยใช้รหัส QR Code ที่มีการรับรองด้วยลายเซ็นดิจิทัล เพื่อแก้ไขปัญหาใบ

ปริญญาปลอมและการตรวจสอบใบปริญญาที่ใช้เวลานาน โดยมีรายละเอียดในการพัฒนาระบบดังนี้

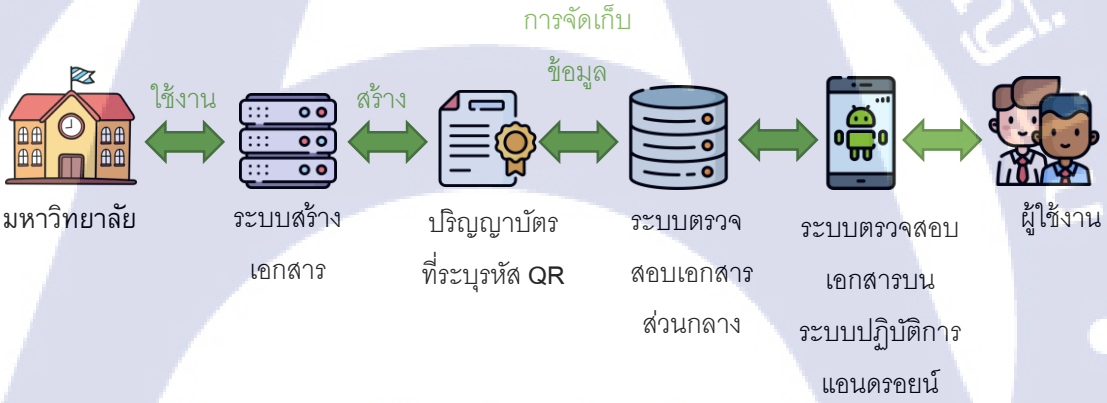
(1) ระบบตรวจสอบเอกสาร (Document Certificate Authentication System: DCAS) ถูกพัฒนาขึ้นให้เป็นระบบส่วนกลางที่จะทำหน้าที่จัดเก็บเอกสารปริญญาบัตร

(2) สถาบันการศึกษาใช้ระบบสร้างเอกสาร (Document Certificate Generate System: DCGS) เพื่อออกใบปริญญาบัตร โดยข้อมูลส่วนตัวของนักศึกษาจะถูกนำไปเข้ารหัสเพื่อสร้างลายเซ็นดิจิทัล และเปลี่ยนให้อยู่ในรูปแบบของ QR Code ซึ่งจะระบุอยู่บนปริญญาบัตรที่สร้างขึ้น

(3) สถาบันการศึกษาจะทำการส่งเอกสารไปยังระบบตรวจสอบเอกสาร (Document Certificate Authentication System: DCAS) ซึ่งเป็นระบบส่วนกลาง เพื่อจัดเก็บเอกสาร

(4) ในการตรวจสอบความถูกต้อง จะดำเนินการผ่านแอปพลิเคชันที่พัฒนาขึ้น โดยใช้โทรศัพท์มือถือสแกนรหัส QR Code

ภาพรวมการทำงานของระบบตรวจสอบเอกสารด้วยรหัส QR ได้แสดงไว้ดังรูปที่ 2.11



รูปที่ 2.11 ภาพรวมการทำงานของระบบตรวจสอบเอกสารด้วยรหัส QR Code [43]

งานวิจัยนี้แสดงให้เห็นว่าการรหัส QR Code ที่มีข้อมูลลายเซ็นดิจิตอล สามารถใช้ตรวจสอบความถูกต้องของปริญญาบัตรได้ และใช้เวลาเพียง 1 วินาทีโดยเฉลี่ย อีกทั้งระบบยังออกแบบให้บันทึกประวัติการตรวจสอบไว้ เพื่อหลีกเลี่ยงการเรียกดูเอกสารจำนวนมากจนเป็นเหตุทำให้ระบบทำงานหนักเกินความจำเป็น

2.2.2 การตรวจสอบใบปริญญาบัตรออนไลน์ด้วยเทคโนโลยีบล็อกเชน

R. Shanmuga Priya และ N. Swetha [44] ได้นำเสนอแนวคิดการใช้เทคโนโลยีบล็อกเชนในการพัฒนาโปรแกรมและระบบใบปริญญาแบบกระจายศูนย์ เพื่อแก้ไขปัญหาในแบบ

เดียวกัน โดย N. Swetha และ R. Shanmuga Priya ได้ออกแบบให้โปรแกรมทำงานอยู่บนอีเธอเรียม ซึ่งขั้นตอนในการทำงานของระบบสามารถสรุปได้ดังนี้

(1) สถานศึกษาบันทึกข้อมูลของนักศึกษาลงในระบบ ระบบจะทำการบันทึกข้อมูลลงในบล็อกเชน

(2) สถานศึกษาให้ปริญญาบัตรกับนักศึกษาในรูปแบบของรหัส QR Code

(3) เมื่อนักศึกษาสมัครงาน จะส่งรหัส QR Code ให้กับบริษัท

(4) บริษัททำการตรวจสอบใบปริญญาผ่านระบบโดยใช้ QR Code

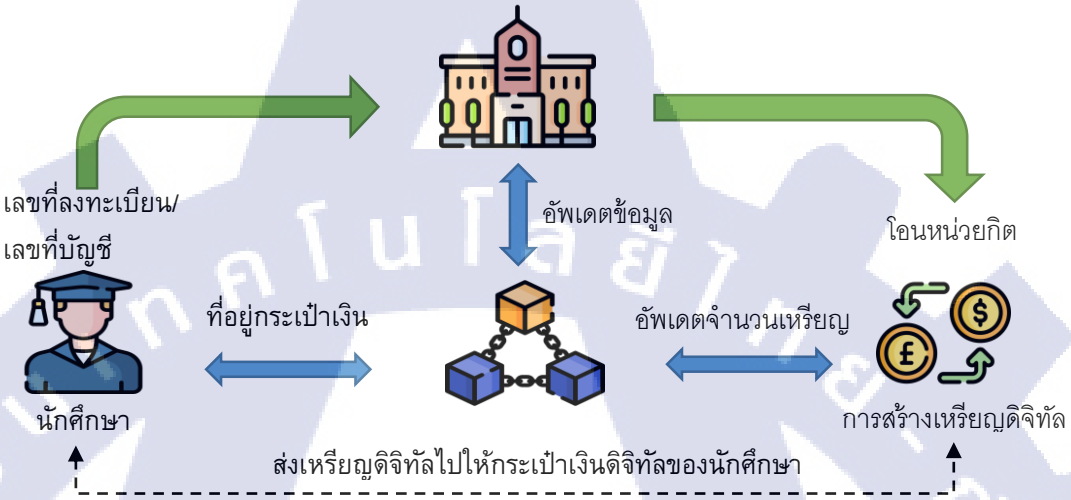
ภาพรวมการทำงานของระบบตรวจสอบปริญญาบัตรด้วยระบบบล็อกเชนได้แสดงไว้ดังรูปที่ 2.12

รูปที่ 2.12 การทำงานของระบบตรวจสอบปริญญาบัตรด้วยระบบบล็อกเชน [44]

งานวิจัยนี้แสดงให้เห็นว่า ระบบที่ประยุกต์ใช้เทคโนโลยีบล็อกเชนช่วยลดโอกาสความน่าจะเป็นของใบปริญญาปลอม เนื่องจากระบบมีความโปร่งใส สามารถตรวจสอบได้ ข้อมูลที่ได้มีความถูกต้อง และมีความปลอดภัย

2.2.3 การโอนหน่วยกิตในการศึกษาด้วยระบบบล็อกเชน

R. Manoj และคณะ [45] ได้เสนอแนวคิดการประยุกต์ใช้เทคโนโลยีบล็อกเชนและสัญญาอัจฉริยะ เพื่อพัฒนาระบบโอนหน่วยกิตให้กับนักศึกษาผ่านกระเป๋าเงินดิจิทัล โดยเมื่อนักศึกษาเรียนจบและสอบผ่านรายวิชา มหาวิทยาลัยจะทำการโอนหน่วยกิตในรายวิชานั้นในรูปแบบของโทเคน ดังรูปที่ 2.13



รูปที่ 2.13 การทำงานของระบบโอนหน่วยกิต [45]

งานวิจัยได้มีการออกแบบการทำงานของระบบ ซึ่งมีรายละเอียดดังต่อไปนี้

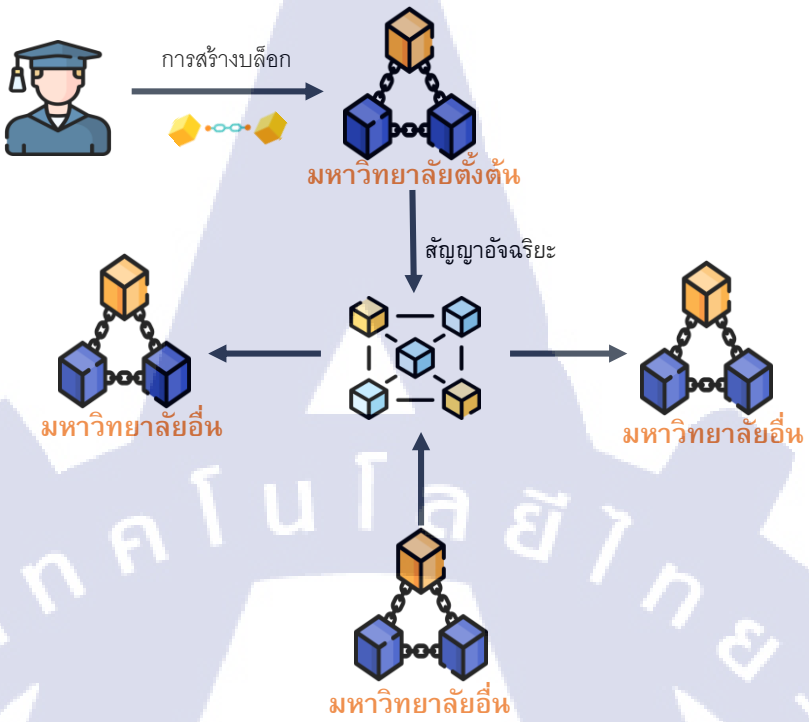
(1) ใช้กระเป๋าเงินดิจิทัลหลายเซ็นในการตรวจสอบและรองรับเอกสาร

(2) มหาวิทยาลัยลงทะเบียนเข้าสู่ระบบบล็อกเชน โดยระบบจะทำการส่งลิ้งค์ให้กับมหาวิทยาลัยใหม่เพื่อใช้เข้าร่วมเครือข่าย โหนดของมหาวิทยาลัยใหม่นั้นก็จะทำการสร้างกระเป๋าเงินดิจิทัล ที่อยู่ รหัสกุญแจส่วนตัว กุญแจสาธารณะ และทำการเชื่อมต่อเครือข่ายเข้ากับโหนดของมหาวิทยาลัยอื่น ๆ โทเคนจะถูกสร้างขึ้นจากโหนดที่มีอยู่ก่อนหน้า และจะทำการส่งไปยังโหนดใหม่

(3) นักศึกษาลงทะเบียนเข้าร่วมเครือข่ายบล็อกเชน โดยระบบจะสร้างรหัสนักศึกษา และกระเป๋าเงินดิจิทัลให้กับนักศึกษาแต่ละคน

(4) ใช้พื้นฐาน ERC-20 ในการสร้างโทเคน

การเชื่อมต่อระหว่างเครือข่ายบล็อกเชนระหว่างมหาวิทยาลัยได้แสดงไว้ดังรูปที่ 2.14



รูปที่ 2.14 การเชื่อมต่อของเครือข่ายบล็อกเชนระหว่างมหาวิทยาลัย [45]

ผลลัพธ์จากงานวิจัยแบ่งออกเป็นผลลัพธ์ด้านความปลอดภัย และผลลัพธ์ด้านการรองรับจำนวนผู้ใช้งานที่มากขึ้น โดยได้ระบุว่า ระบบสามารถป้องกันการโจมตีแบบเล่นซ้ำ (Replay Attack) และการโจมตีของซีบิล (Sybil Attack) ได้ สำหรับการโจมตีแบบการชนกัน (Collusion Tamper Attack) โอกาสที่ถูกโจมตีจะลดลงเมื่อข้อมูลบนบล็อกเชนเพิ่มมากขึ้น และระบบสามารถรองรับจำนวนผู้ใช้งานที่มากขึ้นได้ โดยใช้เวลาน้อยกว่า 10 มิลลิวินาทีเมื่อมีมหาวิทยาลัยที่ลงทะเบียน 800 แห่ง

2.2.4 การสร้างใบปริญญา NFT พร้อมช่องทางการชำระเงินออนไลน์

X. Zhao และ Y.W. Si [46] ได้นำเสนอกรอบแนวคิดในการสร้างระบบการจัดการใบปริญญาโดยใช้เหรียญ NFT เพื่อป้องกันไม่ให้ผู้ฉ้อฉลผลิตใบปริญญาปลอมหรือผิดกฎหมาย โดยให้กลุ่มสถาบันการศึกษาเข้าร่วมเครือข่ายบล็อกเชนที่กำหนดเพื่อสร้างความน่าเชื่อถือให้กับผู้ใช้งาน และค่าใช้จ่ายในการออกปริญญาบัตรจะถูกเรียกเก็บผ่านช่องทางการชำระเงินออนไลน์ ซึ่งมีขั้นตอนดังนี้

(1) สถาบันการศึกษาสร้างปริญญาบัตรด้วยเหรียญ NFT และรอข้อมูลการชำระเงินจากนักศึกษา

(2) ระบบ Oracle จะส่งคำขอไปที่ผู้ให้บริการการชำระเงินออนไลน์ เพื่อสร้างรายการรอชำระเงินตามเงื่อนไขที่ระบุไว้ในสัญญาอัจฉริยะ

(3) เมื่อได้รับรายการรอชำระเงิน นักศึกษาดำเนินการชำระเงินผ่านช่องทางที่กำหนด

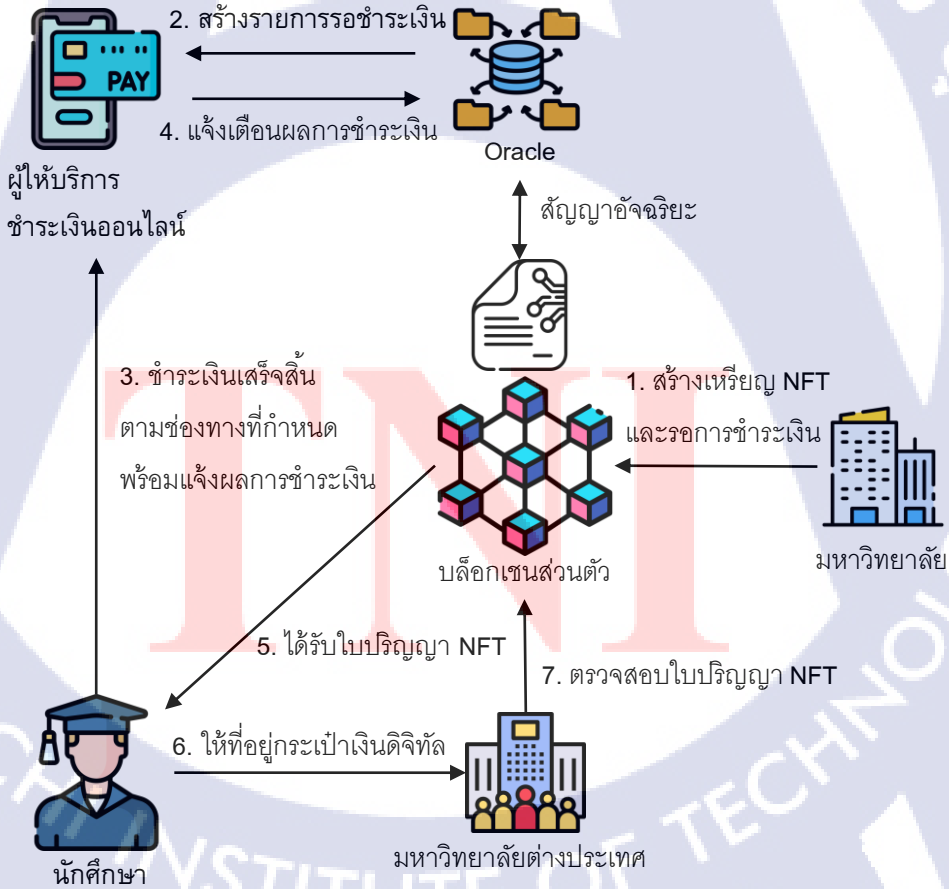
(4) ผลการชำระเงินจะส่งไปที่สัญญาอัจฉริยะผ่านระบบ Oracle

(5) เมื่อได้รับผลการชำระเงินเรียบร้อยแล้ว สัญญาอัจฉริยะจะทำการส่งเหรียญ NFT ไปที่กระเป๋าเงินดิจิทัลของนักศึกษา

(6) นักศึกษาสามารถเผยแพร่ใบปริญญาบัตร NFT ของตนให้กับบริษัทหรือหน่วยงานต่าง ๆ ได้ โดยบริษัท หรือหน่วยงานต่าง ๆ สามารถตรวจสอบความถูกต้องได้อย่างง่ายดาย

(7) สถาบันการศึกษาในต่างประเทศหรือบริษัทใด ๆ ที่เชื่อมต่อกับเครือข่ายบล็อกเชนส่วนตัว สามารถเข้าถึงใบปริญญาบัตร NFT ที่จัดเก็บไว้ได้

ภาพรวมการทำงานของระบบใบปริญญา NFT พร้อมช่องทางการชำระเงินออนไลน์ได้แสดงไว้ดังรูปที่ 2.15



รูปที่ 2.15 การทำงานของระบบใบปริญญา NFT พร้อมช่องทางการชำระเงินออนไลน์ [46]

X. Zhao และ Y.W. Si ระบุว่ากรอบแนวคิดนี้สามารถแทนที่วิธีการแบบเก่า โดยไม่ต้องพึ่งพาสกุลเงินดิจิทัล ในขณะที่ยังคงคุณสมบัติการใช้งาน การรับรองความถูกต้อง ความน่าเชื่อถือ ความโปร่งใส และความพร้อมใช้งาน

อีธีเลียมเป็นแพลตฟอร์มที่ได้รับความนิยมในการนำมาประยุกต์ใช้และพัฒนาระบบในงานวิจัยต่าง ๆ [47] [48] [49] [50] [51] [52] ทั้งนี้ระบบบล็อกเชนที่สร้างขึ้นบนแพลตฟอร์มของอีธีเลียมอาจมีค่าใช้จ่ายสูงจากค่าแก๊สในการเผยแพร่ธุรกรรม เพื่อลดค่าใช้จ่ายที่อาจเกิดขึ้น งานวิจัยนี้จึงพัฒนาระบบบนเครือข่ายมัลติเชนที่มีความสามารถในการเผยแพร่ธุรกรรมได้โดยไม่เสียค่าใช้จ่าย สามารถแนบรายละเอียดที่เกี่ยวข้องกับการศึกษา เช่น วิชาที่สำเร็จ หน่วยกิตที่ได้รับ ไปกับการโอนหน่วยกิตได้ และยังสามารถแลกเปลี่ยนหน่วยกิตรายวิชาให้เป็นใบปริญญาบัตรได้โดยการประยุกต์ใช้ Atomic Exchange ที่เปรียบเสมือนสัญญาอัจฉริยะบนเครือข่ายมัลติเชน โดยหน่วยกิตและใบปริญญาบัตรที่ได้รับจะจัดเก็บอยู่ในกระเป๋าเงินดิจิทัลเพื่อให้ง่ายต่อการเข้าถึงและเรียกใช้งาน ทั้งนี้ผู้วิจัยได้ทำการเปรียบเทียบความสามารถของระบบที่พัฒนากับงานวิจัยอื่น ๆ ไว้ในตารางที่ 2.1

ตารางที่ 2.1 การเปรียบเทียบระบบที่พัฒนากับงานวิจัยอื่น ๆ

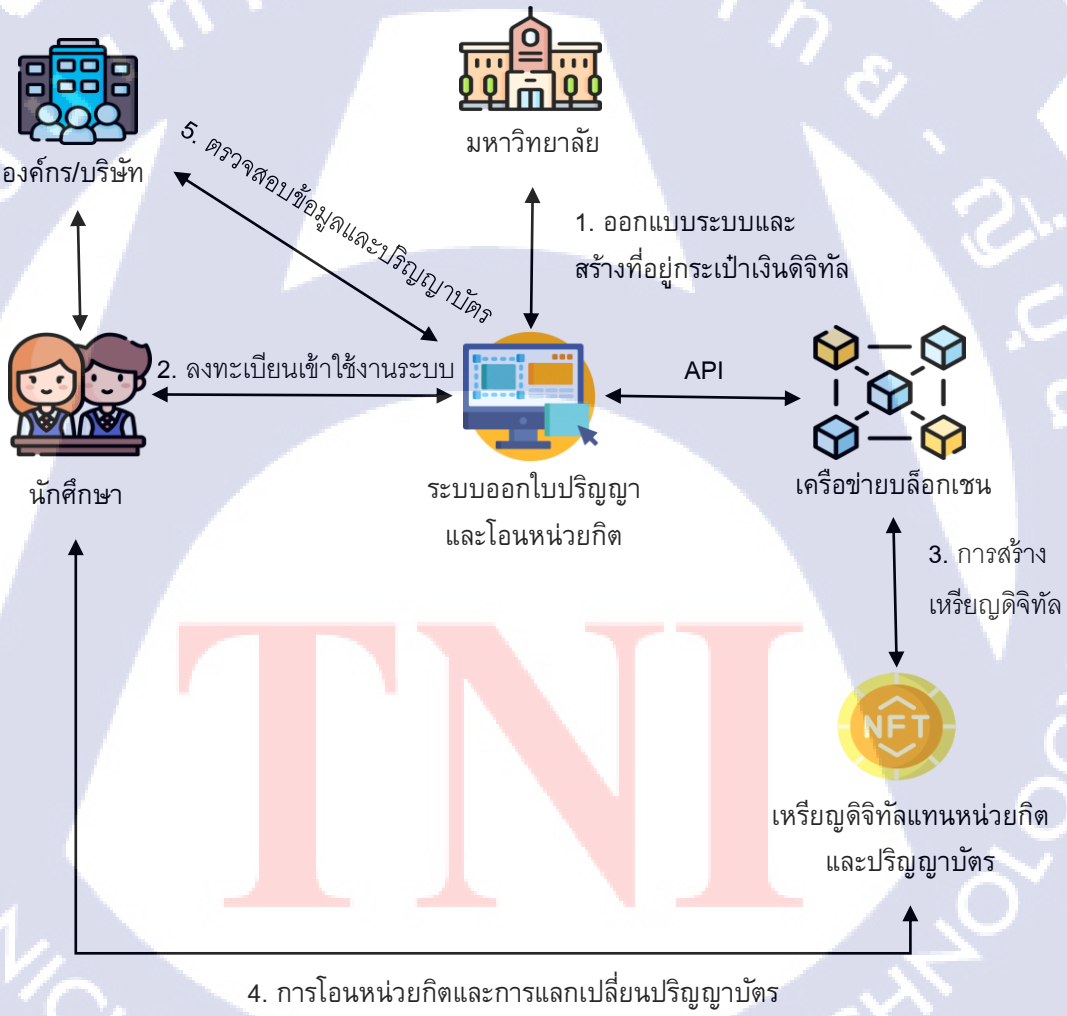
งานวิจัย	1	2	3	4	5	6
Document Certificate Authentication System Using Digitally Signed QR Code Tag [43]	x	✓	x	x	✓	x
Online Certificate Validation Using Blockchain [44]	✓	x	x	x	✓	x
Blockchain Ecosystem for Credit Transfer in Education [45]	✓	x	✓	x	✓	✓
NFTCert: NFT-Based Certificates With Online Payment Gateway [46]	✓	x	x	✓	✓	✓
Token-based Degree Certificate with Credit Transfer System (Proposed approach)	✓	✓	✓	✓	✓	✓

หมายเหตุ: 1. ระบบการประมวลผลแบบกระจาย

2. ไม่มีค่าใช้จ่ายในการเผยแพร่ธุรกรรม
3. มีระบบโอนหน่วยกิต
4. จัดเก็บใบปริญญาบัตรไว้ในกระเป๋าเงินดิจิทัล
5. ข้อมูลส่วนตัวมีความปลอดภัย 6. สัญญาอัจฉริยะ

บทที่ 3
ระเบียบและวิธีดำเนินงานวิจัย

ในการดำเนินงานวิจัยเรื่องการสร้างระบบออกใบปริญญาบัตรและโอนหน่วยกิตด้วยเหรียญดิจิทัล ผู้วิจัยได้ทำการแบ่งขั้นตอนในการดำเนินงานออกเป็น 5 ขั้นตอน ได้แก่ ขั้นตอนการออกแบบโครงสร้างเครือข่ายบล็อกเชนและสร้างที่อยู่กระเป๋าเงินดิจิทัล ขั้นตอนการลงทะเบียนเข้าใช้ระบบ ขั้นตอนการสร้างเหรียญแทนหน่วยกิตและปริญญาบัตร ขั้นตอนการโอนและแลกเปลี่ยนปริญญาบัตร และขั้นตอนการตรวจสอบข้อมูลและปริญญาบัตร โดยได้แสดงขั้นตอนทั้งหมดไว้ดังรูปที่ 3.1



รูป 3.1 ขั้นตอนการทำงานของระบบสร้างปริญญาบัตรด้วยเหรียญ NFT

การทำงานของระบบจะเริ่มต้นจากการสร้างระบบบล็อกเชนส่วนตัวของมหาวิทยาลัย จากนั้นมหาวิทยาลัยจะทำการสร้างที่อยู่กระเป๋าเงินดิจิทัลและส่งข้อมูลให้กับนักศึกษาใหม่ชั้นปีที่ 1 เมื่อนักศึกษาได้รับที่อยู่กระเป๋าเงินดิจิทัลแล้วจะทำการนำรหัสที่ได้ไปลงทะเบียนเข้าใช้งานระบบ เพื่อแสดงตัวตนและความเป็นเจ้าของในที่อยู่กระเป๋าเงินดิจิทัลนั้น ๆ ในขณะเดียวกันมหาวิทยาลัยก็จะทำการสร้างเหรียญดิจิทัลที่ใช้แทนหน่วยกิตการศึกษา และเหรียญดิจิทัลแทนใบปริญญาบัตรรอไว้ในระบบเพื่อใช้ในการรับส่งธุรกรรม โดยเมื่อนักศึกษาสำเร็จการศึกษารายวิชาแล้ว มหาวิทยาลัยจะทำการส่งเหรียญดิจิทัลแทนหน่วยกิตการศึกษาไปที่ที่อยู่กระเป๋าเงินดิจิทัลของนักศึกษา เมื่อนักศึกษาเรียนครบตามหลักสูตร หรือสะสมหน่วยกิตครบตามจำนวนที่มหาวิทยาลัยกำหนด ก็จะทำการยื่นคำร้องขอแลกเปลี่ยนหน่วยกิตของตนกับเหรียญดิจิทัลแทนใบปริญญาผ่านเว็บไซต์ มหาวิทยาลัยเมื่อได้รับคำร้องขอแล้วจะดำเนินการตรวจสอบและยืนยันการแลกเปลี่ยนธุรกรรม ในกรณีที่บริษัทหรือองค์กรต้องการที่จะตรวจสอบข้อมูลใบปริญญา ก็สามารถดำเนินการได้ผ่านเว็บไซต์ที่ได้พัฒนาขึ้น

3.1 ขั้นตอนการออกแบบโครงสร้างเครือข่ายบล็อกเชนและสร้างที่อยู่กระเป๋าเงินดิจิทัล

งานวิจัยนี้เสนอการสร้างเครือข่ายบล็อกเชนแบบส่วนตัวบนแพลตฟอร์มมัลติเชน (Multichain) ที่อนุญาตให้เฉพาะผู้ที่เกี่ยวข้องสามารถเชื่อมต่อเข้ากับเครือข่ายบล็อกเชนของมหาวิทยาลัย ซึ่งหากเครื่องคอมพิวเตอร์เครื่องใดเครื่องหนึ่งจะทำการเชื่อมต่อเข้ากับระบบจะต้องทำการขออนุญาตจากมหาวิทยาลัยก่อน โดยผู้ดูแลระบบมีทำหน้าที่ในการให้สิทธิ์ในการเชื่อมต่อ และสร้างที่อยู่ของกระเป๋าเงิน (Wallet address) ซึ่งเป็นตัวระบุการทำงานของกุญแจสาธารณะ (Public Key) และกุญแจส่วนตัว (Private Key) ให้กับผู้ใช้งานเพื่อใช้ในการโอนและรับเหรียญดิจิทัล หรือเรียกดูธุรกรรมต่าง ๆ ที่เกิดขึ้น ซึ่งมีการกำหนดสิทธิ์การเข้าถึงและใช้งานไว้ดังตารางที่ 3.1

ตารางที่ 3.1 สิทธิ์ในการเข้าถึงและใช้งานของผู้ใช้งาน

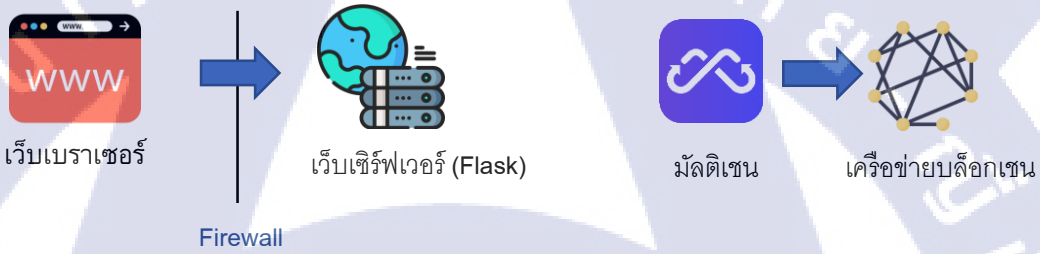
สิทธิ์ในการเข้าถึงและใช้งาน	**มหาวิทยาลัย**	**นักศึกษา**	**บริษัท**
สิทธิ์ในการเชื่อมต่อ (Connect)	✓	✓	✓
สิทธิ์ในการส่ง (Send)	✓	✓	X
สิทธิ์ในการรับ (Receive)	✓	✓	X
สิทธิ์ในการสร้าง (Create)	✓	X	X
สิทธิ์ในการออก (Issue)	✓	X	X

สิทธิ์ในการขุด (Mine)	✓	X	X

ตารางที่ 3.1 สิทธิ์ในการเข้าถึงและใช้งานของผู้ใช้งาน (ต่อ)

สิทธิ์ในการเข้าถึงและใช้งาน	**มหาวิทยาลัย**	**นักศึกษา**	**บริษัท**
สิทธิ์ในการเปิดใช้งาน (Activate)	✓	X	X
สิทธิ์ผู้ดูแลระบบ (Admin)	✓	X	X

ระบบได้พัฒนาเว็บไซต์ที่มีการเชื่อมต่อ API กับเครือข่ายบล็อกเชนที่ให้บริการโดยมัลติเชน และใช้ Flask ทำหน้าที่เป็นเว็บเซิร์ฟเวอร์ ซึ่งผู้ใช้งานสามารถเข้าถึงระบบที่พัฒนาได้ผ่านเว็บเบราเซอร์ ดังรูปที่ 3.2



รูป 3.2 การออกแบบและพัฒนาระบบบล็อกเชนและเว็บไซต์สำหรับใช้งาน

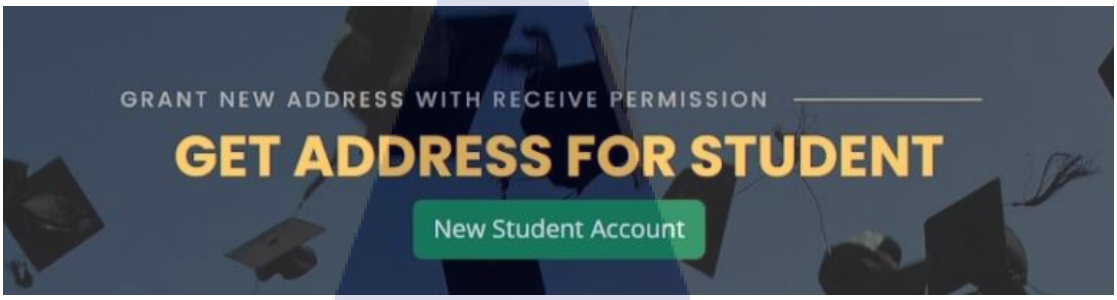
ฮาร์ดแวร์ที่ใช้ในการทดลอง

เครื่องคอมพิวเตอร์ที่ใช้ในการทดลองนี้ประกอบไปด้วยเครื่องคอมพิวเตอร์ 3 เครื่องที่เชื่อมต่อกันแบบเครื่องต่อเครื่อง (Peer-to-peer) โดยใช้ระบบปฏิบัติการ Intel® Xeon ® CPU E3-1270 v5 3.60 GHz processor ที่มีหน่วยความจำขนาด 16 GB

ซอฟต์แวร์ที่ใช้ในการทดลอง

ภาษาคอมพิวเตอร์ที่ใช้ในการพัฒนาโปรแกรมคือภาษา Python เวอร์ชั่น 3.10.8 เนื่องจากเป็นภาษาที่ได้รับความนิยม เข้าใจง่าย และเป็นภาษาที่รองรับบนเครือข่ายมัลติเชน ร่วมกับการใช้ภาษาคอมพิวเตอร์ HTML และ CSS ในการพัฒนาหน้าเว็บไซต์

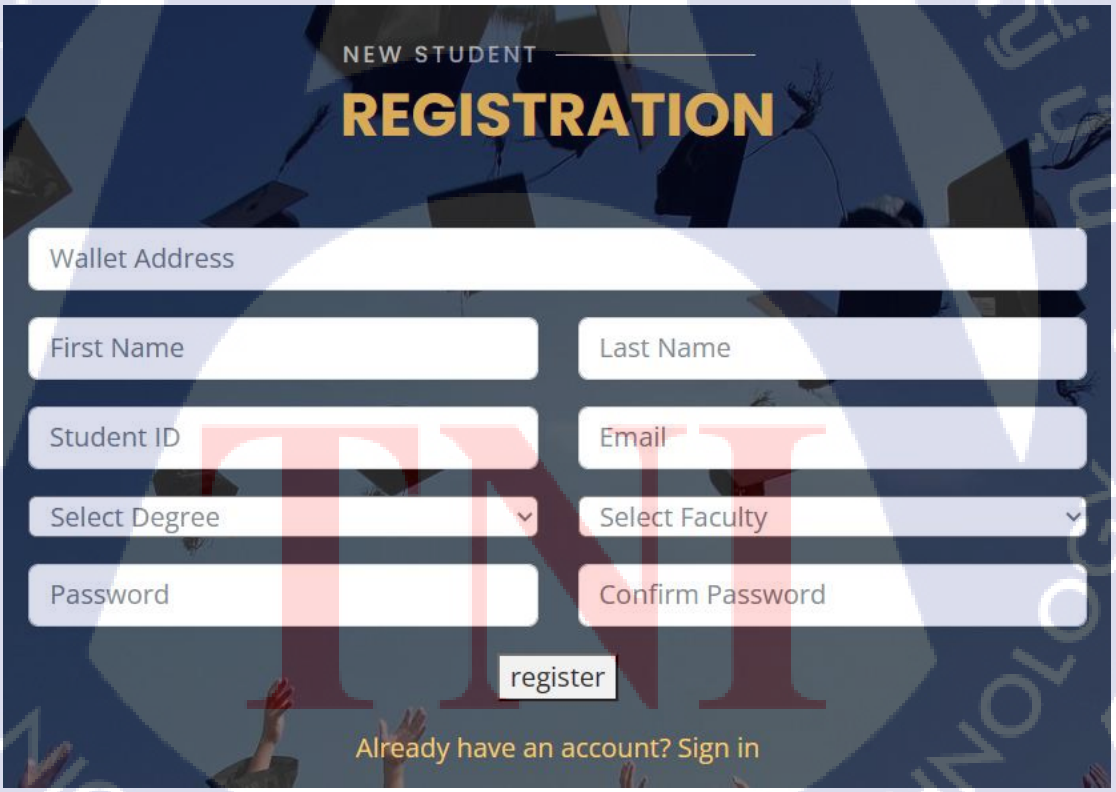
ในการเริ่มต้น ผู้ดูแลระบบจะดำเนินการสร้างที่อยู่กระเป๋าดิจิทัลที่ใช้รับส่งธุรกรรมผ่านระบบการใช้งานบนเว็บไซต์ ซึ่งจะเป็นส่วนที่เก็บบันทึกข้อมูลส่วนตัวของนักศึกษา ได้แก่ ชื่อ-นามสกุล รหัสนักศึกษา คณะ สาขา วิชาเรียน ผลการเรียน หน่วยกิตที่ได้รับ และใบปริญญาบัตรในรูปแบบของเหรียญดิจิทัล ดังรูปที่ 3.3



รูป 3.3 กระเป๋าเงินดิจิทัลของผู้ใช้งาน

3.2 ขั้นตอนการลงทะเบียนและการเข้าใช้งานระบบ

หลังจากที่มหาวิทยาลัยได้สร้างที่อยู่กระเป๋าเงินดิจิทัลแล้ว ระบบจะทำการส่งที่อยู่กระเป๋าเงินดิจิทัลนั้นให้กับนักศึกษา ซึ่งนักศึกษาจะต้องดำเนินการลงทะเบียนเพื่อเข้าใช้งานผ่านหน้าเว็บไซต์ พร้อมทั้งกรอกรายละเอียดข้อมูลส่วนบุคคลให้ครบถ้วน โดยข้อมูลการลงทะเบียนจะถูกเก็บบันทึกไว้ในฐานข้อมูล SQLite ดังรูปที่ 3.4



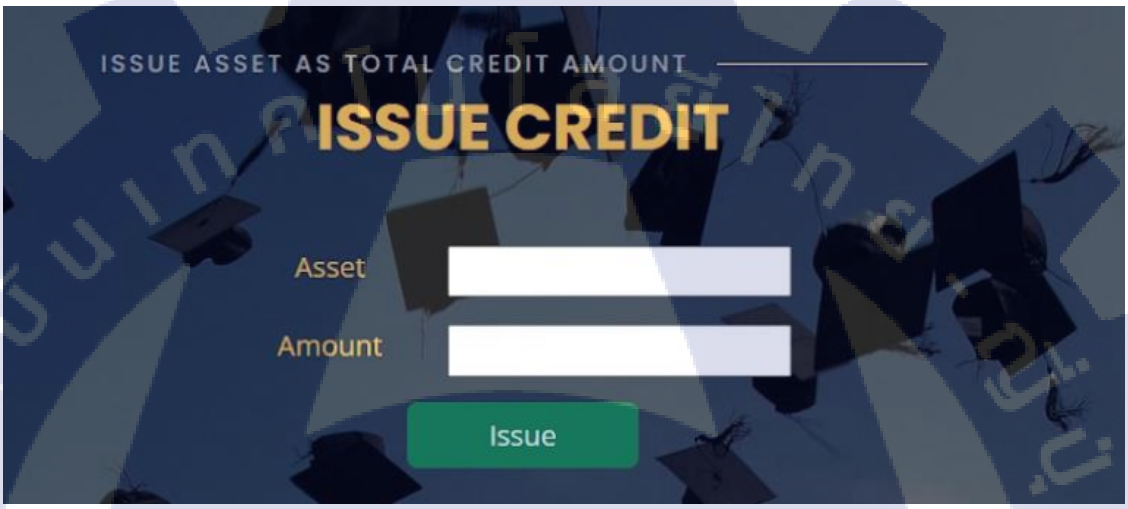
รูป 3.4 การลงทะเบียนเข้าใช้งานผ่านหน้าเว็บไซต์

หลังจากลงทะเบียนเรียบร้อยแล้ว นักศึกษาจะใช้อีเมล์และรหัสผ่านที่กำหนดไว้เพื่อเข้าใช้งานระบบในครั้งถัดไป

3.3 ขั้นตอนการสร้างเหรียญดิจิทัล

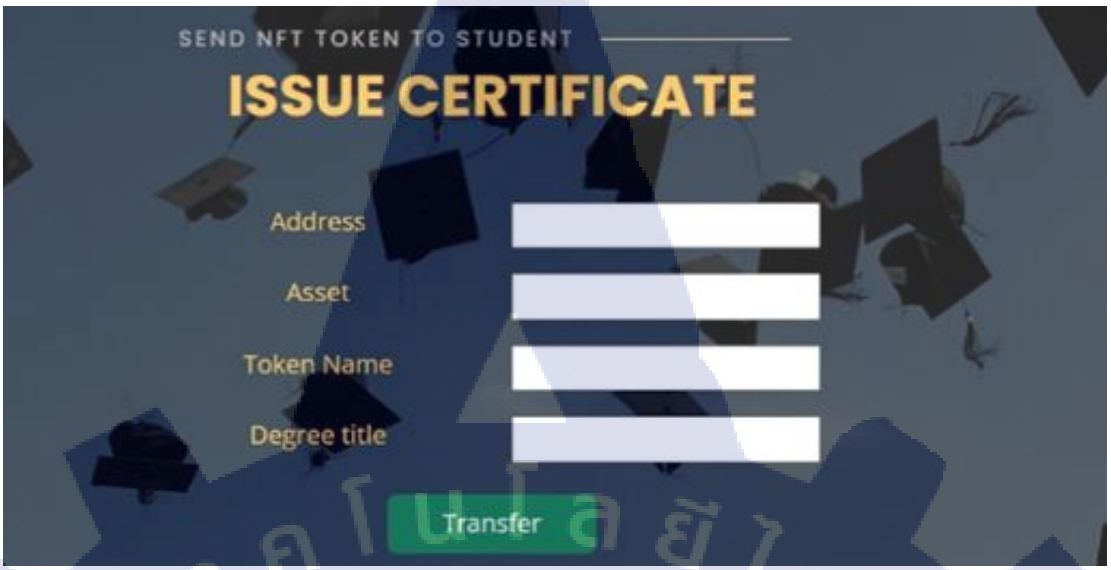
ผู้ดูแลระบบจะดำเนินการสร้างเหรียญดิจิทัล โดยแบ่งออกเป็น 2 ประเภท

(1) Credit Token คือเหรียญที่ใช้แทนหน่วยกิตรายวิชา สร้างขึ้นในรูปแบบของสินทรัพย์ที่สามารถทดแทนกันได้ (Fungible Asset) โดยมหาวิทยาลัยจะทำการส่งเหรียญดิจิทัลนี้ให้กับนักศึกษาที่สำเร็จการศึกษารายวิชา เป็นจำนวนเท่ากับหน่วยกิตที่ได้รับจริงในวิชานั้น ๆ ดังรูปที่ 3.5



รูป 3.5 การสร้างเหรียญหน่วยกิต

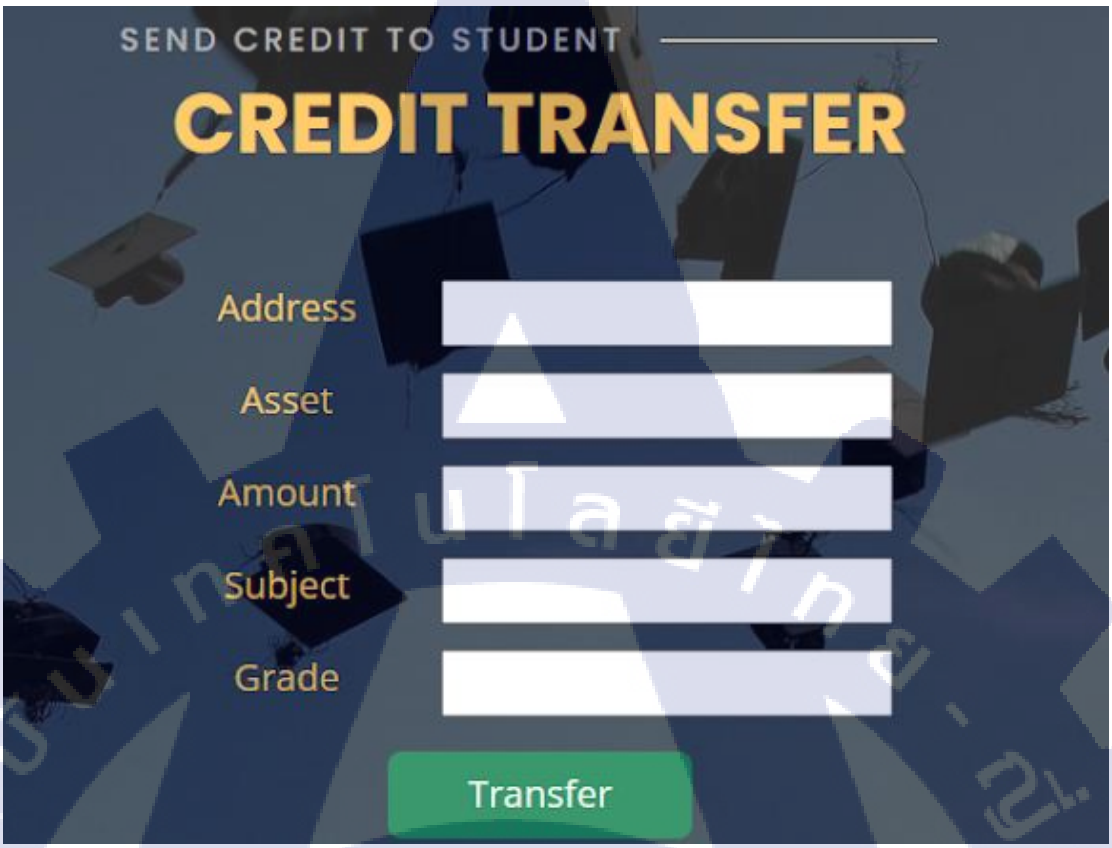
(2) NFT Certificate Token คือเหรียญที่ใช้แทนปริญญาบัตร มอบให้เมื่อนักศึกษาสำเร็จการศึกษาตามหลักสูตรที่มหาวิทยาลัยกำหนด สร้างขึ้นในรูปแบบของสินทรัพย์ที่ไม่สามารถทดแทนได้ (Non-Fungible Asset) เพื่อสร้างเหรียญแทนปริญญาบัตรที่มีเอกลักษณ์และไม่ซ้ำใคร ซึ่งจะมีการแนบข้อมูลใบปริญญาบัตรเพื่อแสดงถึงประเภทของใบปริญญาที่นักศึกษาได้รับ ดังรูปที่ 3.6



รูป 3.6 การสร้างเหรียญแทนปริญญาบัตร

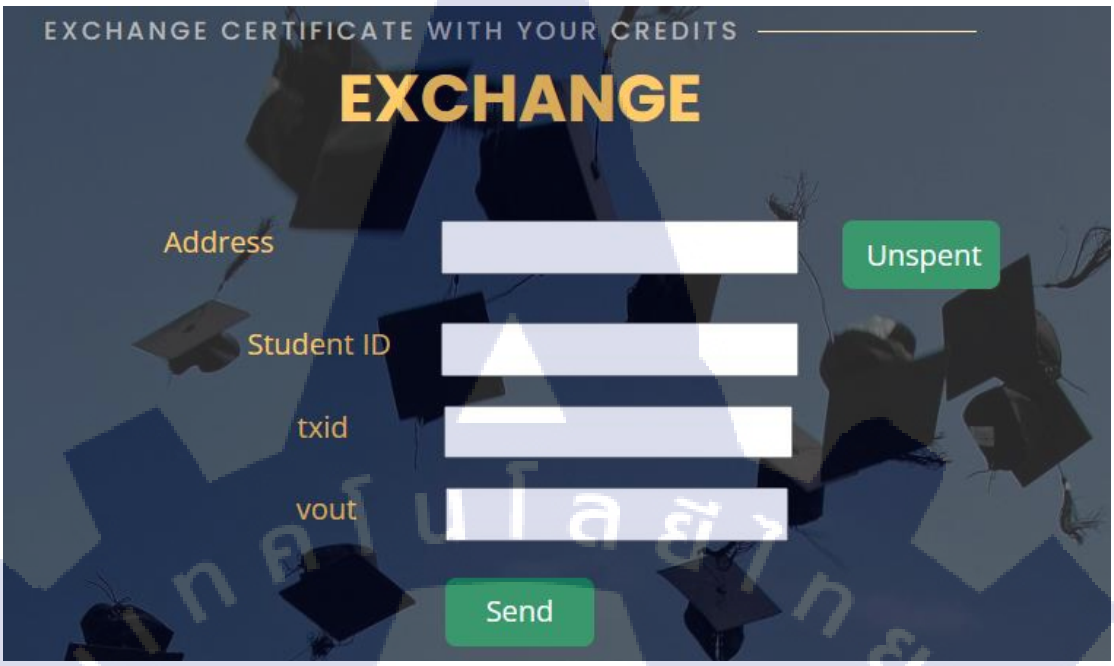
3.4 ขั้นตอนการสร้างโอนและแลกเหรียญดิจิทัล

หลังจากที่นักศึกษาสำเร็จการศึกษาในภาควิชาที่กำหนด ผู้ดูแลระบบจะทำการโอนเหรียญแทนหน่วยกิตรายวิชาให้กับนักศึกษา พร้อมทั้งแนบข้อมูลรายวิชาและผลการศึกษาลงใน Metadata ดังรูปที่ 3.7



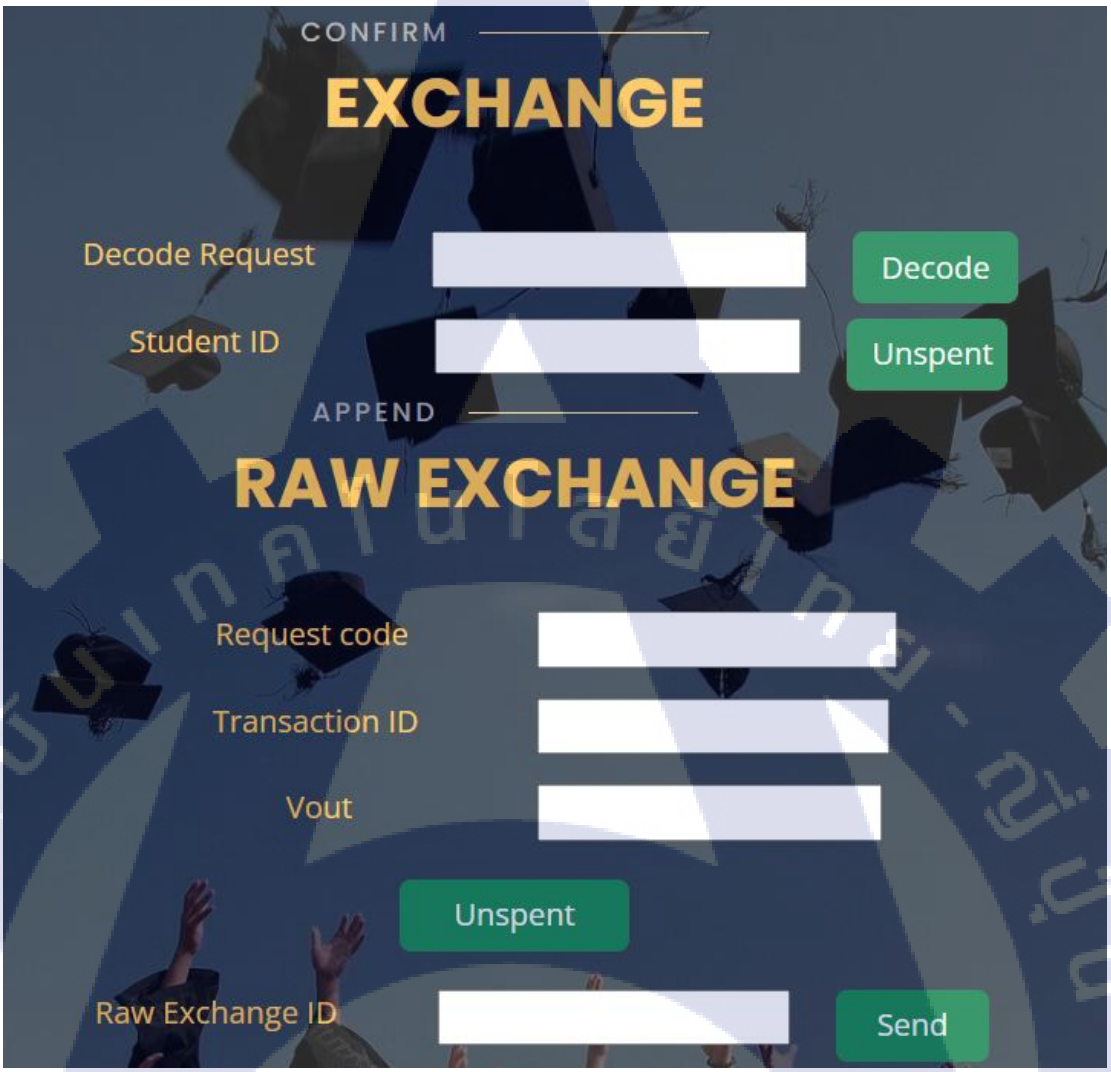
รูป 3.7 การโอนเหรียญแทนหน่วยกิตให้กับนักศึกษา

นักศึกษาจะต้องทำการสะสมเหรียญแทนหน่วยกิตรายวิชาให้ครบตามที่หลักสูตรกำหนด เพื่อนำเหรียญแทนหน่วยกิตมาแลกเป็นเหรียญแทนใบปริญญาบัตร โดยนักศึกษาจะทำการยื่นคำขอแลกเปลี่ยนผ่านระบบ ดังรูปที่ 3.8



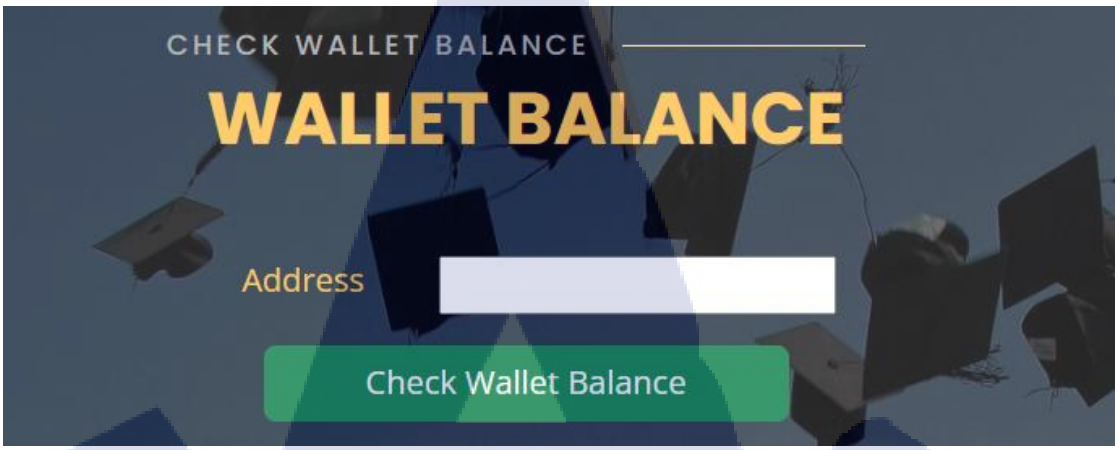
รูปที่ 3.8 การขอแลกเปลี่ยนเหรียญหน่วยกิตกับเหรียญปริญญาบัตร

ผู้ดูแลระบบจะทำการตรวจสอบคำขอที่ได้รับจากนักศึกษา และจะทำดำเนินการยืนยันการแลกเปลี่ยนหน่วยกิตกับใบปริญญาบัตรผ่านระบบที่ได้พัฒนาไว้ ดังรูปที่ 3.9



รูปที่ 3.9 การยืนยันการแลกเปลี่ยนโดยผู้ดูแลระบบบล็อกเชนของมหาวิทยาลัย

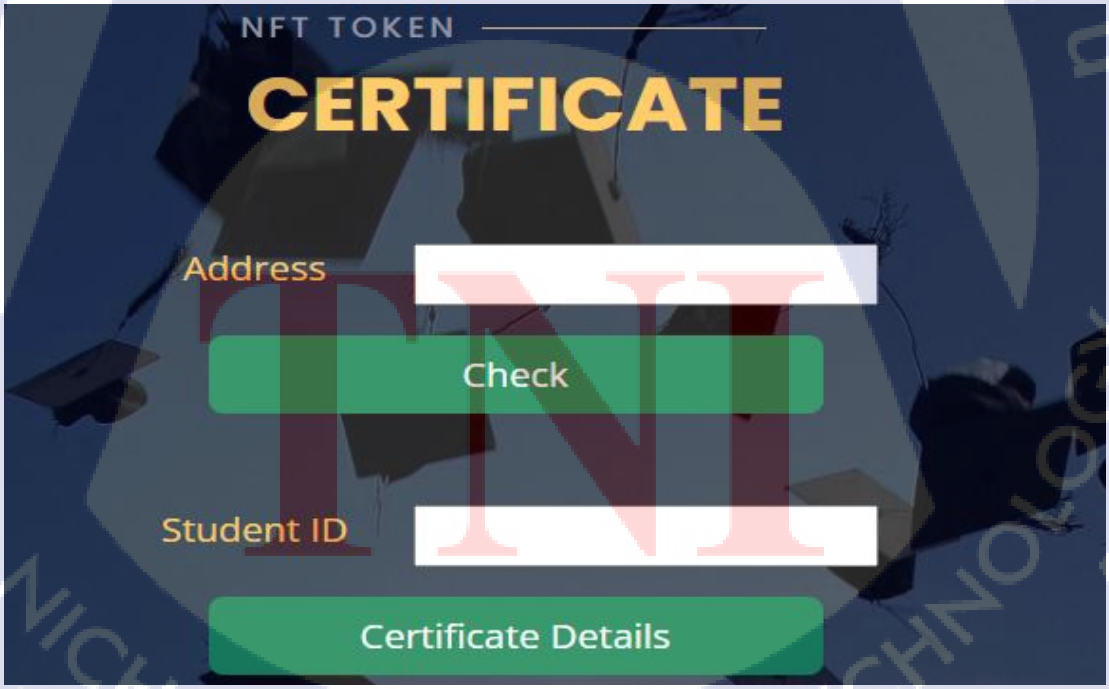
เมื่อทำการตรวจสอบยอดคงเหลือในที่อยู่กระเป๋าเงินของนักศึกษา จะพบว่าจำนวนเหรียญแทนหน่วยกิตมีจำนวนลดลงเท่ากับจำนวนที่ได้ทำการแลกเปลี่ยนในระบบ และจะพบเหรียญแทนปริญญาบัตรเพิ่มเข้ามา ซึ่งสามารถตรวจสอบได้จากหน้าเว็บไซต์ ดังรูปที่ 3.10



รูปที่ 3.10 การตรวจสอบยอดคงเหลือในกระเป๋าเงินดิจิทัล

3.5 การตรวจสอบปริญญาบัตร

ในการตรวจสอบปริญญาบัตร บริษัทหรือหน่วยงานต่าง ๆ สามารถเชื่อมต่อเข้าถึงเครือข่ายบล็อกเชนของมหาวิทยาลัยเพื่อเรียกดูธุรกรรมต่าง ๆ เกิดขึ้นทั้งหมดได้โดยใช้ที่อยู่กระเป๋าเงินของนักศึกษา โดยยังสามารถทราบถึงผลการศึกษาของวิชาเรียน และเรียกดูใบปริญญาบัตรในรูปแบบอิเล็กทรอนิกส์ได้จาก metadata ที่แนบไว้ผ่านเว็บไซต์ ดังรูปที่ 3.11



รูปที่ 3.11 การตรวจสอบข้อมูลและใบปริญญาบัตรโดยองค์กรหรือบริษัทที่ได้รับอนุญาต

บทที่ 4
ผลลัพธ์การวิจัย วิเคราะห์และอภิปรายผลการทดลอง

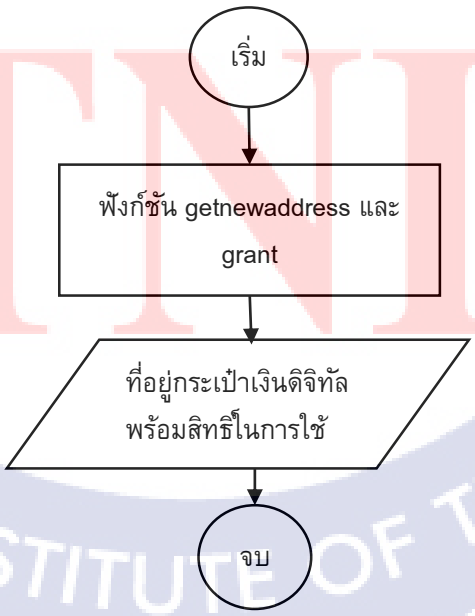
ผู้วิจัยได้ทำการสร้างและทดสอบระบบโอนหน่วยกิตและออกใบปริญญาบัตรด้วยการสร้างเหรียญดิจิทัลบนเครือข่ายมัลติเชน โดยจะแสดงผลลัพธ์ทั้งในส่วนของผู้ดูแลระบบ นักศึกษา และบุคคลทั่วไป ดังนี้

4.1 การสร้างที่อยู่กระเป๋าเงินดิจิทัล

ผู้ดูแลระบบจะเป็นผู้ดำเนินการสร้างที่อยู่กระเป๋าเงินให้กับนักศึกษาในแต่ละคน ซึ่งกระเป๋าเงินดิจิทัลของนักศึกษาจะได้รับสิทธิ์ในการเชื่อมต่อ รับ และส่งธุรกรรม สามารถทำได้ผ่านการใช้งานร่วมกันของฟังก์ชัน getnewaddress และ grant ดังรูปที่ 4.1 และ 4.2

```
@app.route('/admindashboard/newacc')
def new_acc():
    addr = api.getnewaddress()
    api.grant(addr, 'connect,receive,send')
    return addr
```

รูปที่ 4.1 การสร้างที่อยู่กระเป๋าเงินและสิทธิ์ในการเข้าถึง



รูปที่ 4.2 ขั้นตอนการสร้างที่อยู่กระเป๋าเงินดิจิทัลบนหน้าเว็บไซต์

4.2 การลงทะเบียนใช้งานระบบของนักศึกษา

หลังจากที่ผู้ดูแลระบบได้สร้างที่อยู่กระเป๋าเงินดิจิทัลแล้ว จะทำการส่งที่อยู่กระเป๋าเงินดิจิทัลนั้นให้กับนักศึกษาเพื่อนำไปใช้ลงทะเบียนผ่านหน้าเว็บไซต์ที่ได้พัฒนาขึ้น ซึ่งนักศึกษาจะทำการกรอกข้อมูลส่วนบุคคล ได้แก่ ชื่อ-นามสกุล รหัสนักศึกษา ที่อยู่กระเป๋าเงินดิจิทัล ที่อยู่อีเมล์ ระดับการศึกษา คณะที่ศึกษา และรหัสผ่าน ซึ่งระบบจะมีการตรวจสอบความถูกต้องของข้อมูล ดังนี้

1) ที่อยู่กระเป๋าเงินดิจิทัล หากระบบพบว่าที่อยู่กระเป๋าเงินดิจิทัลที่ระบุมีการลงทะเบียนใช้งานมาแล้ว จะไม่สามารถลงทะเบียนซ้ำได้

2) ที่อยู่อีเมล์ หากระบบพบว่าอีเมล์ที่ระบุมีการลงทะเบียนใช้งานมาแล้ว จะไม่สามารถลงทะเบียนซ้ำได้

3) รหัสนักศึกษา หากระบบพบว่ารหัสนักศึกษาที่ระบุมีการลงทะเบียนใช้งานมาแล้วจะไม่สามารถลงทะเบียนซ้ำได้

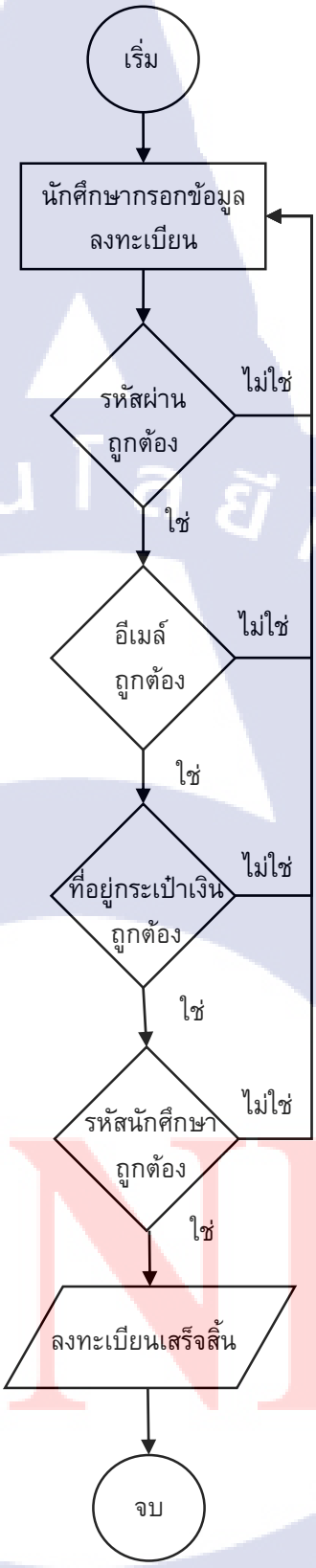
4) รหัสผ่าน ระบบจะให้นักศึกษาทำการกำหนดรหัสผ่าน และทำการยืนยันรหัสผ่านโดยหากรหัสผ่านที่ระบุไม่ตรงกัน จะไม่สามารถลงทะเบียนได้

ขั้นตอนการทำงานของระบบสามารถดูได้ดังรูปที่ 4.3 และ 4.4

```
register():
form = RegisterForm()
if request.method == 'POST':
    firstname = request.form.get('firstname')
    lastname = request.form.get('lastname')
    email = request.form.get('email')
    password = request.form.get('password')
    confirm_password = request.form.get('confirm_password')
    hashed_password = bcrypt.generate_password_hash(form.password.data)
    student_id = request.form.get('student_id')
    address = request.form.get('address')
    faculty = request.form.get('faculty')
    degree = request.form.get('degree')
    date_added = datetime.today()

    if password != confirm_password:
        flash("Not same password, please check again!")

    else:
        user_email = User.query.filter_by(
        email=email).first()
        if user_email:
            raise ValidationError(
            'Email already exists, please go to login page')
        else:
            user_address = User.query.filter_by(
            address=address).first()
            if user_address:
                raise ValidationError(
                'Wallet already exists, please go to login page')
```

```
            else:
                user_student_id = User.query.filter_by(
                student_id=student_id).first()
                if user_student_id:
                    raise ValidationError(
                    'Student ID already exist, please go to login page'                    )

                else:
                    new_user = User(firstname=firstname, lastname=lastname, email=email, password=hashed_password,
                                    student_id=student_id, address = address, faculty=faculty, degree=degree, date_added=date_added)
                    db.session.add(new_user)
                    db.session.commit()
                    return render_template('login.html', form=form)
return render_template('register.html', form=form)
```

รูปที่ 4.3 การสร้างส่วนลงทะเบียนเข้าใช้งาน



รูปที่ 4.4 ขั้นตอนการทำงานส่วนลงทะเบียนเข้าใช้งานบนหน้าเว็บไซต์

ข้อมูลที่นักศึกษาทำการลงทะเบียนจะถูกบันทึกไว้ในฐานข้อมูล SQLite โดยข้อมูลรหัสผ่านเพื่อใช้เข้าระบบจะถูกเก็บให้รูปแบบของค่าแฮชเพื่อป้องกันการถูกโจรกรรม ดังรูปที่ 4.5

```
app = Flask(__name__)
app.config['SQLALCHEMY_DATABASE_URI'] = 'sqlite:///database.db'
app.config['SECRET_KEY'] = 'thisisasecretkey'
db = SQLAlchemy(app)
bcrypt = Bcrypt(app)
```

รูปที่ 4.5 การเชื่อมต่อกับฐานข้อมูล SQLite

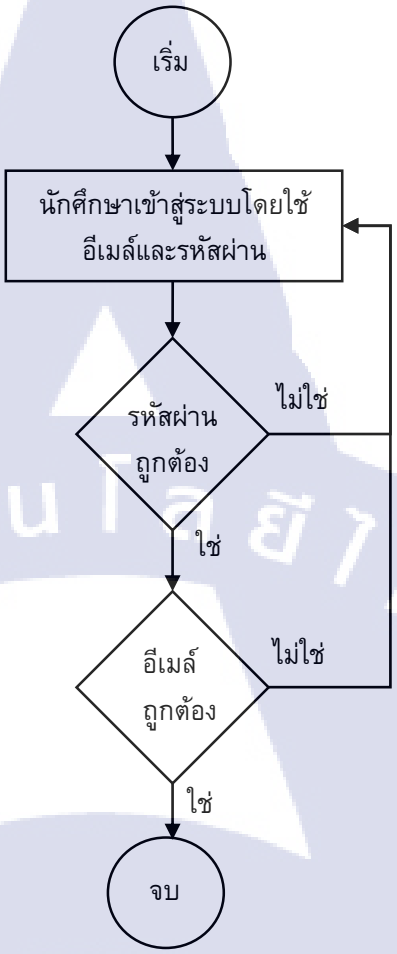
ตารางที่ 4.1 ตัวอย่างข้อมูลการลงทะเบียนที่ถูกจัดเก็บบนฐานข้อมูล SQLite

id	firstname	lastname	student_id	address	email	faculty	degree	password	date_added
1	Sutida	Narongsak	2163110030	113rXtvRD6F ThKdPN61N LEsdLzaWAXdl S3P1z	snzine.1012@gmail.com	Information Technology	Master of Science	$2b$12$E4e9 AmFnYcoJvL pkyXjNce/Xp EPvGc1UV6k W43ygUbHKf JtU9gneC	24/4/2023 21:26:42

หลังจากลงทะเบียนเสร็จสิ้น นักศึกษาสามารถเข้าใช้งานระบบได้ผ่านหน้า Sign in โดยการระบุที่อยู่อีเมล์และรหัสผ่านที่กำหนดไว้ ดังรูปที่ 4.6 และ 4.7

```
@app.route('/login', methods=['GET', 'POST'])
def login():
    form = LoginForm()
    if form.validate_on_submit():
        user = User.query.filter_by(email=form.email.data).first()
        if user:
            if bcrypt.check_password_hash(user.password, form.password.data):
                login_user(user)
                return redirect(url_for('dashboard'))
    return render_template('login.html', form=form)
```

รูปที่ 4.6 การเข้าใช้งานระบบ



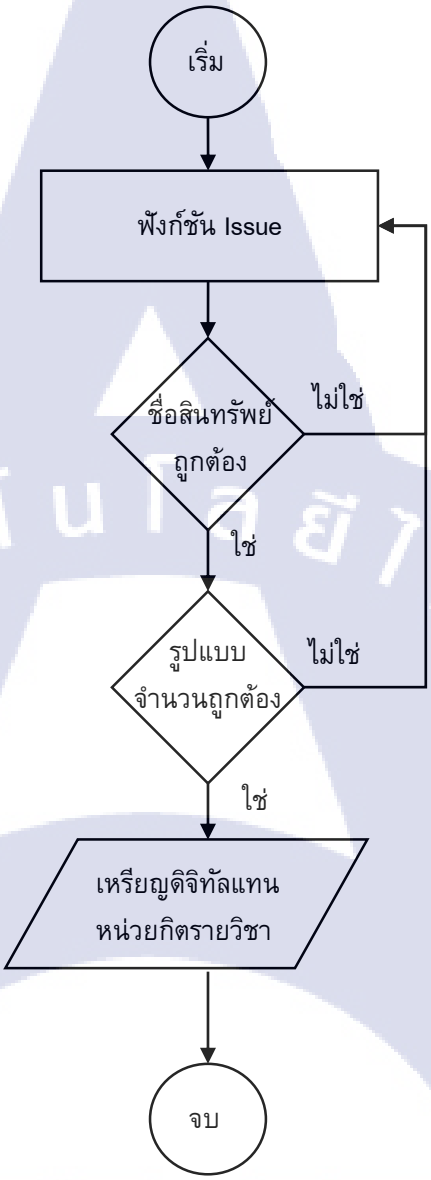
รูปที่ 4.7 ขั้นตอนการเข้าสู่ระบบผ่านหน้าเว็บไซต์

4.3 การสร้างเหรียญดิจิทัลแทนหน่วยกิตรายวิชาและปริญญาบัตร

ผู้ดูแลระบบทำการสร้างเหรียญดิจิทัลแทนหน่วยกิตและใบปริญญาบัตรให้กับที่อยู่กระเป๋าดิจิทัลของมหาวิทยาลัยเพื่อใช้ในการรับส่งธุรกรรม โดยจะแบ่งการสร้างเหรียญดิจิทัลแทนหน่วยกิตรายวิชาออกเป็น 2 ประเภท ได้แก่ เหรียญดิจิทัลแทนหน่วยกิตวิชาหลัก และเหรียญดิจิทัลแทนหน่วยกิตวิชาเลือก ซึ่งระบบจะมีการตรวจสอบชื่อของสินทรัพย์ และจำนวนเหรียญที่จะสร้าง ดังรูปที่ 4.8 และ 4.9

```python
## Issue asset to an address.
@app.route('/admindashboard/issue', methods=['POST'])
def issue():

    ## The asset must not already exist.
    asset = request.form['asset']
    if is_valid_asset(asset):
        return 'The asset already exist.'

    ## The amount must be valid.
    amount = request.form['amount']
    if not is_valid_amount(amount):
        return 'Invalid amount.'

    ## The asset subdivide is always 1.0.
    r = api.issue(root_addr(), asset, float(amount), 0.01)
    try:
        if r['error']:
            return str(r['error']['message'])
    except:
        pass
    return 'Success.'
```

รูปที่ 4.8 การสร้างเหรียญดิจิทัลแทนหน่วยกิตรายวิชา



รูปที่ 4.9 ขั้นตอนการสร้างเหรียญดิจิทัลแทนหน่วยกิตรายวิชาบนหน้าเว็บไซต์

โดยหากพิจารณาจากคุณสมบัติของเหรียญที่ถูกสร้างขึ้น จะพบว่าระบบมีการระบุให้ fungible = true ซึ่งหมายถึงเหรียญดิจิทัลทุกเหรียญมีค่าเท่ากัน สามารถทดแทนกันได้

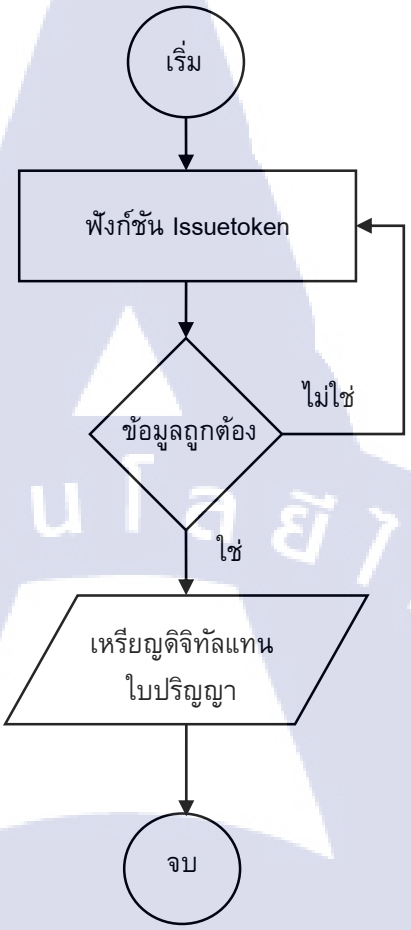
```
{
        "name" : "credit",
        "issuetxid" : "SHA256",
        "assetref" : "25-265-61589",
        "multiple" : 1,
```

```
"units" : 1,
"open" : false,
"restrict" : {
"send" : false,
"receive" : false,
"issue" : true
},
"fungible" : true,
"issueqty" : 1000,
"issueraw" : 1000,
}
```

ในส่วนของการสร้างเหรียญดิจิทัลแทนใบปริญญา ผู้ดูแลระบบจะทำการเหรียญดิจิทัลที่อยู่ในรูปแบบเหรียญที่ไม่สามารถทดแทนกันได้ โดยกำหนดให้ใช้รหัสนักศึกษาแทนชื่อของเหรียญดิจิทัล เพื่อให้ง่ายต่อการเรียกใช้ ส่งมอบ หรือแลกเปลี่ยน ผ่านฟังก์ชัน Issuetoken ที่กำหนดจำนวนให้เท่ากับ 1 เสมอ และมีการแนบข้อมูลไว้ในแต่ละเหรียญที่สร้างขึ้น เพื่อแสดงความเป็นเจ้าของในสินทรัพย์ ดังรูปที่ 4.10 และ 4.11

```python
@app.route('/admindashboard/token', methods=['POST'])
def issue_token():

    t = request.form['token_name']
    d = request.form['degree_title']
    f = request.form['faculty_name']
    pic = request.form['pic_hash']

    r = api.issuetoken( root_addr(), "TNI", t, 1, 0, {"json":({"authority":"Thai-Nichi Institute of Technology",
                                                               "degree_title":d,"faculty_name":f,"URL": pic})})

    try:
        if r['error']:
            return str(r['error']['message'])
    except:
        pass
    return 'Success.'
```

รูปที่ 4.10 การสร้างเหรียญดิจิทัลแทนใบปริญญา



รูปที่ 4.11 ขั้นตอนการสร้างเหรียญดิจิทัลแทนใบปริญญา

โดยหากพิจารณาจากคุณสมบัติของเหรียญที่ถูกสร้างขึ้น จะพบว่าระบบมีการระบุให้ fungible = false ซึ่งหมายถึงเหรียญดิจิทัลที่มีเอกลักษณ์เฉพาะตัว

```
{
    "name" : “certificate",
    "issuetxid" : "SHA256",
    "assetref" : "33-265-26573",
    "multiple" : 1,
    "units" : 1,
    "open" : true,
    "restrict" : {
    "send" : false,
    "receive" : false,
```

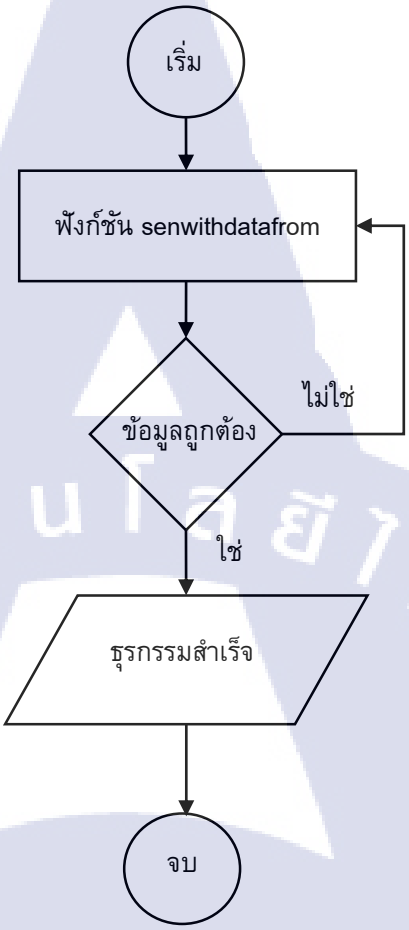
```
            "issue" : true
            },
            "fungible" : false,
            "issueqty" : 1,
            "issueraw" : 1,
    }
```

4.4 การโอนเหรียญดิจิทัลแทนหน่วยกิตรายวิชา

หลังจากที่นักศึกษาสำเร็จการศึกษารายวิชา ผู้ดูแลระบบจะทำการส่งเหรียญดิจิทัลแทนหน่วยกิตไปที่ที่อยู่กระเป๋าเงินของนักศึกษา ซึ่งระบบจะทำการตรวจสอบความถูกต้องของที่อยู่กระเป๋าเงินของผู้รับ พร้อมแนบรายละเอียดรายวิชาและผลการศึกษา ผ่านฟังก์ชัน sendwithdatafrom ดังรูปที่ 4.12 และ 4.13

```python
@app.route('/admindashboard/transfer', methods=['POST'])
def send_from():
    ## 'add1' and 'addr2' must be valid.
    add1 = request.form['add1']
    if not is_valid_addr(add1):
        return 'Invalid sender address.'

    ## 'root' cannot receive assets.
    if add1 == root_addr():
        return 'admin cannot receive assets.'

    ## The asset must valid.
    asset = request.form['asset']

    ## The amount must valid.
    amount = request.form['amount']
    if not is_valid_amount(amount):
        return 'Invalid amount.'

    s = request.form.get('subject')


    g = request.form.get('grade')


    r = api.sendwithdatafrom(root_addr(), add1, {asset:float(amount)},
                             {"json":({"subject":s,"grade":g})})

    try:
        if r['error']:
            return str(r['error']['message'])
    except:
        pass
    return 'Success.'
```

รูปที่ 4.12 การโอนเหรียญดิจิทัลแทนหน่วยกิตรายวิชา



รูปที่ 4.13 ขั้นตอนการโอนเหรียญดิจิทัลแทนหน่วยกิตรายวิชาผ่านหน้าเว็บไซต์

นักศึกษาสามารถตรวจสอบจำนวนเหรียญที่ได้รับผ่านหน้าเว็บไซต์ โดยใช้ฟังก์ชัน getaddressbalances ซึ่งจะแสดงผลรวมของเหรียญที่ได้รับทั้งหมด ดังรูปที่ 4.14

```python
@app.route('/dashboard/addbal', methods=['POST'])
def addr_bal():
    add1 = request.form['add1']
    if not is_valid_addr(add1):
        return 'Invalid sender address.'
    s = ''
    for b in api.getaddressbalances(add1):
        s += b['name'] + '  ' + str(b['qty']) + '<br/>'
    return s
```

รูปที่ 4.14 การตรวจสอบยอดคงเหลือของที่อยู่กระเป๋าเงิน

ในกรณีที่นักศึกษาต้องการดูรายละเอียดธุรกรรมทั้งหมดที่เกิดขึ้น สามารถเรียกดูได้ผ่านฟังก์ชัน listaddresstransactions โดยระบบจะแสดงผลลัพธ์ในรูปแบบรายละเอียดรายวิชา ผลการศึกษา จำนวนและผลรวมของเหรียญที่ได้รับ ดังรูปที่ 4.15 และ 4.16

```python
@app.route('/dashboard/addtrans', methods=['POST'])
def addr_trans():
    core_credit = 0
    elective_credit = 0
    add1 = request.form['add1']
    if not is_valid_addr(add1):
        return 'Invalid wallet address.'
    s = ''
    for b in api.listaddresstransactions(add1):

        if len(b["data"]) > 0:
            s += 'Subject: ' + str(b["data"][0]["json"]["subject"])
            + ' Type: '+str(b["balance"]["assets"][0]["name"])
            + ' Grade: '+ str(b["data"][0]["json"]["grade"])
            + ' credit: ' + str(b["balance"]["assets"][0]["qty"])
            s += '<br>'

            print(s)
            if b["balance"]["assets"][0]["name"]=="core_subject":
                core_credit += int(b["balance"]["assets"][0]["qty"])
            elif b["balance"]["assets"][0]["name"]=="elective_subject":
                elective_credit += int(b["balance"]["assets"][0]["qty"])
    s += 'Total Core Credit: ' + str(core_credit)
    s += '<br>'
    s += 'Total Elective Credit: ' + str(elective_credit)

    return s
```

รูปที่ 4.15 การเรียกดูรายละเอียดธุรกรรมที่เกิดขึ้นทั้งหมด

Subject: AI Type: core_subject Grade: A credit: 3
Subject: Network Type: core_subject Grade: A credit: 3
Subject: Eng Type: elective_subject Grade: B credit: 3
Total Core Credit: 6
Total Elective Credit: 3

รูปที่ 4.16 ผลลัพธ์ที่ได้จากการเรียกดูรายการธุรกรรม

4.5 การแลกเปลี่ยนเหรียญดิจิทัลแทนใบปริญญาบัตร

หลังจากที่นักศึกษาสะสมจำนวนเหรียญดิจิทัลได้ครบตามจำนวนที่มหาวิทยาลัยกำหนด ก็จะสามารถดำเนินการขอแลกเปลี่ยนเหรียญดิจิทัลแทนหน่วยกิตรายวิชาที่ตนเองมีกับเหรียญดิจิทัลแทนใบปริญญาจากมหาวิทยาลัยได้ผ่านหน้าเว็บไซต์ เบื้องต้นระบบจะทำการจำกัดการใช้เหรียญดิจิทัลแทนหน่วยกิตรายวิชาผ่านฟังก์ชัน preparelockunspent เพื่อให้มั่นใจว่าเหรียญดิจิทัลเหล่านั้นจะไม่ถูกส่งหรือโอนไปยังที่อยู่กระเป๋าเงินดิจิทัลอื่นระหว่างการแลกเปลี่ยน ซึ่งจำนวนเหรียญที่ใช้จะถูกกำหนดโดยมหาวิทยาลัย หากนักศึกษามีจำนวนเหรียญดิจิทัลเท่ากับหรือมากกว่าจำนวนเหรียญที่ระบุไว้ในระบบก็จะสามารถดำเนินการได้ โดยผลลัพธ์ที่ได้จะอยู่ในรูปแบบของรหัสอ้างอิงการทำธุรกรรม ดังรูปที่ 4.17 และ 4.18

```
@app.route('/dashboard/exchange', methods=['POST'])
def exchange_request():
    a = request.form['add1']

    s=''
    r = api.preparelockunspentfrom(a, {"core_subject":15,"elective_subject":9})
    s += 'txid: ' + str(r["txid"]) +'<br>'+'vout: '+ str(r["vout"])

    return s
```

รูปที่ 4.17 การจำกัดการใช้งานเหรียญดิจิทัลที่จะใช้สำหรับแลกเปลี่ยน

Txid: 44db71c0afdd237a4166f3f45f1c9aeacca020402a5047678081434ffc606843

Vout: 0

รูปที่ 4.18 ผลลัพธ์ที่ได้จากการจำกัดการใช้งานเหรียญดิจิทัล

หลังจากที่ทำการจำกัดการใช้งานเหรียญดิจิทัลแทนหน่วยกิตรายวิชาแล้ว นักศึกษาจะต้องทำการส่งคำร้องขอแลกเปลี่ยนเหรียญดิจิทัลแทนใบปริญญา ซึ่งจะต้องใช้รหัสอ้างอิงการทำธุรกรรมที่ได้จากขั้นตอนก่อนหน้ามาระบุลงไปในคำร้องด้วย ดังรูปที่ 4.19

```python
@app.route('/dashboard/sendexchange', methods=['POST'])
def create_raw():
    i = request.form['student_id']
    t = request.form['txid']
    v = request.form['vout']

    s = ''
    s = api.createrawexchange(t, int(v), {"TNI":{"token":i,"qty":1}})
    return s
```

รูปที่ 4.19 การสร้างคำร้องขอแลกเปลี่ยน

ผลลัพธ์ที่ได้จากการสร้างคำขอแลกเปลี่ยนจะอยู่ในรูปแบบรหัสที่เปรียบเสมือนเป็นเลขที่เอกสารคำขอ ดังรูปที่ 4.20

```
0100000001436860fc4f4381806747502a4020a0ccea9a1c5ff4f366417a23ddafc071db44000000
006a47304402202f6d8ec15e86ea754a2e351d2784bf940c31f347d7fe329d51e0b39ca6554180
02207c3232849a193eae0888629ce76c8ca76bbcd23b14c50ffa45a0d9733fc058a18321027b63
d58b484254a9a1b6c09f8c0489a52dbf6bdc0d86e2b038b81bf21855cce6ffffffff01000000000000
00003776a9144aaede32ef48d6b0006ceb27485bb6a8ef478ff688ac1c73706b715ad3126503ed
37bb32e089993657905c0100000000000000007500000000
```

รูปที่ 4.20 ผลลัพธ์ที่ได้จากการสร้างคำขอแลกเปลี่ยน

นักศึกษาจะต้องส่งรหัสที่ได้จากการสร้างคำขอแลกเปลี่ยนไปให้มหาวิทยาลัยเพื่อทำการตรวจสอบ โดยผู้ดูแลระบบสามารถถอดรหัสคำร้องขอเพื่อดูรายละเอียดการแลกเปลี่ยนได้ผ่านฟังก์ชัน decoderawexchange ดังรูปที่ 4.21 และ 4.22

```python
@app.route('/admindashboard/decode_request', methods=['POST'])
def decode_raw():
    r = request.form['request']


    s = api.decoderawexchange(r)
    return s
```

รูปที่ 4.21 การถอดรหัสคำขอแลกเปลี่ยน

```
{
 "ask": {
  "amount": 0,
  "assets": [
   {
    "assetref": "8-265-39743",
    "name": "TNI",
    "qty": 1,
    "token": "2163110031"
   }
  ]
 },
 "cancomplete": true,
 "candisable": true,
 "complete": false,
 "offer": {
  "amount": 0,
  "assets": [
   {
    "assetref": "7-265-3122",
    "name": "core_subject",
    "qty": 3
   }
  ]
 },
 "requiredfee": 0
}
```


รูปที่ 4.22 ผลลัพธ์ที่ได้จากการถอดรหัสคำขอแลกเปลี่ยน

เมื่อตรวจสอบความถูกต้องของข้อมูลแล้ว ผู้ดูแลระบบจะต้องทำการจำกัดการใช้งานของเหรียญดิจิทัลแทนใบปริญญาบัตรที่ถูกร้องขอแลกเปลี่ยนผ่านฟังก์ชัน preparelockunspent จากนั้นจะทำการส่งข้อมูลเพื่อยืนยันการทำธุรกรรม ซึ่งจะต้องใช้รหัสคำขอแลกเปลี่ยนธุรกรรมจากนักศึกษา และผลลัพธ์จากการจำกัดการใช้งานเหรียญดิจิทัลแทนใบปริญญา พร้อมทั้งกำหนดจำนวนของสินทรัพย์ที่ต้องการแลกเปลี่ยน ผ่านฟังก์ชัน appendrawexchange และ sendrawtransaction ดังรูปที่ 4.23 และ 4.24

```python
@app.route('/admindashboard/append_raw', methods=['POST'])
def append_raw():
    h = request.form['hex_exchange']
    t = request.form['txid']
    v = request.form['vout']

    s = ''
    s = api.appendrawexchange(h,t,int(v),{"core_subject":15,"elective_subject":9})
    return s
```

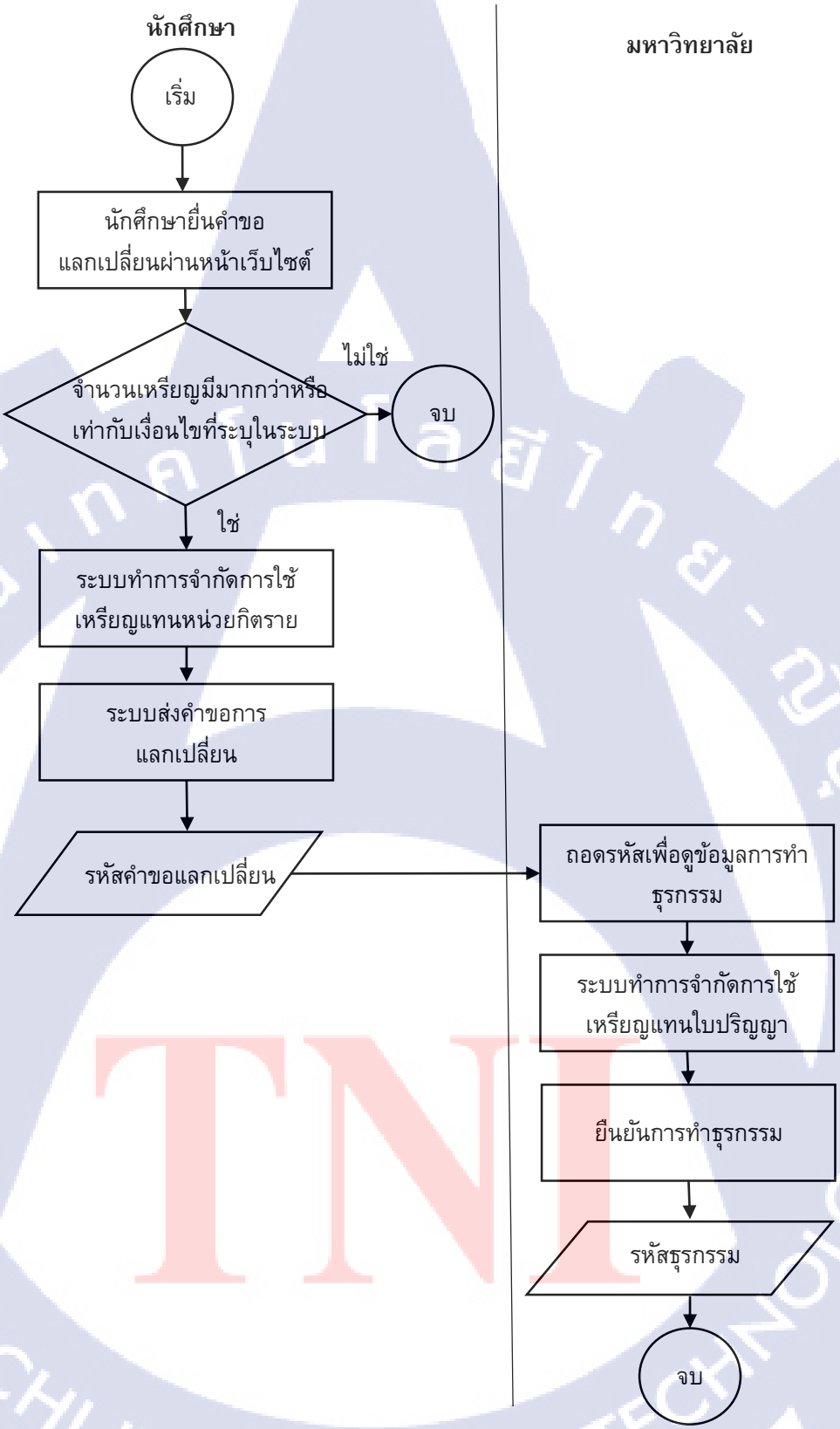
รูปที่ 4.23 การส่งข้อมูลเพื่อยืนยันธุรกรรม

```python
@app.route('/admindashboard/send_raw', methods=['POST'])
def send_raw():
    h = request.form['hex']

    r = api.sendrawtransaction(h)
    try:
        if r['error']:
            return str(r['error']['message'])
    except:
        pass
    return 'Success.'
```

รูปที่ 4.24 การยืนยันธุรกรรม

เมื่อการแลกเปลี่ยนเสร็จสิ้น จำนวนเหรียญดิจิทัลแทนหน่วยกิตรายวิชาของนักศึกษาจะหายไป โดยแลกมากับเหรียญดิจิทัลแทนใบปริญญาที่เพิ่มขึ้น โดยเหรียญดิจิทัลแทนหน่วยกิตรายวิชาที่ทำการแลกเปลี่ยน จะวนกลับเข้าสู่ระบบบล็อกเชนเพื่อใช้ส่งธุรกรรมให้นักศึกษารายอื่นต่อไป

จากกระบวนการทั้งหมดที่กล่าวมาในข้างต้น สามารถสรุปเป็นขั้นตอนการทำงานโดยรวมของระบบได้ดังรูปที่ 4.25



รูปที่ 4.25 ขั้นตอนการทำงานของการแลกเปลี่ยนเหรียญดิจิทัล

4.5 การเรียกดูและตรวจสอบข้อมูลปริญญาบัตร

ในการเรียกดูใบปริญญาบัตรที่ได้รับมานั้น นักศึกษาจะต้องกรอกที่อยู่กระเป๋าเงินดิจิทัลของตนเองลงบนเว็บไซต์ที่ได้พัฒนาขึ้น กรณีบริษัทหรือองค์กรอื่น ๆ ต้องการที่จะเรียกดูหรือตรวจสอบข้อมูลปริญญาบัตรของนักศึกษาคนใดคนหนึ่ง จะต้องรู้ที่อยู่กระเป๋าเงินดิจิทัลของนักศึกษาคนนั้น ๆ โดยสามารถเรียกดูข้อมูลใบปริญญาได้ผ่านฟังก์ชัน getaddressbalances gettokenbalance และ gettokeninfo ดังรูปที่ 4.26

```python
@app.route('/verify/cer_status', methods=['POST'])
def addr_bal():
    add1 = request.form['add1']
    if not is_valid_addr(add1):
        return 'Invalid sender address.'
    s = ''
    for b in api.getaddressbalances(add1):
        if b['name'] == "TNI":
            return "This student has been graduated from Thai Nichi Institute of Technology " + "<br/>"+ "No. of certificate received: "+str(b['qty'])
        else:
            s += b['name'] + '  ' + str(b['qty']) + '<br/>'         #check address balance by provide the address
    return s
```

```python
@app.route('/verify/cer', methods=['POST'])
def verify_cer():
    add1 = request.form['add1']
    if not is_valid_addr(add1):
        return 'Invalid wallet address.'
    #token_name = request.form['token_name']

    if not is_valid_addr(add1):
        return 'Invalid wallet address.'
    s = ''
    s = api.gettokenbalances(add1, "TNI" )
    return s

@app.route('/verify/cer_details', methods=['POST'])
def verify_nft_details():
    token_name = request.form['token_name']

    s = ''
    s = api.gettokeninfo("TNI", token_name )
    return s
```

รูปที่ 4.26 การเรียกดูข้อมูลใบปริญญาบัตร

ข้อมูลที่ได้รับจะแสดงสถานะจบการศึกษาของนักศึกษา พร้อมระบุจำนวนใบปริญญาที่ได้รับ โดยหากตรวจสอบแล้วไม่เจอข้อมูล สามารถระบุได้ว่าที่อยู่กระเป๋าเงินดิจิทัลที่ได้รับอาจไม่ถูกต้อง หรือที่อยู่กระเป๋าเงินดิจิทัลนั้นไม่มีอยู่จริง ดังรูปที่ 4.27

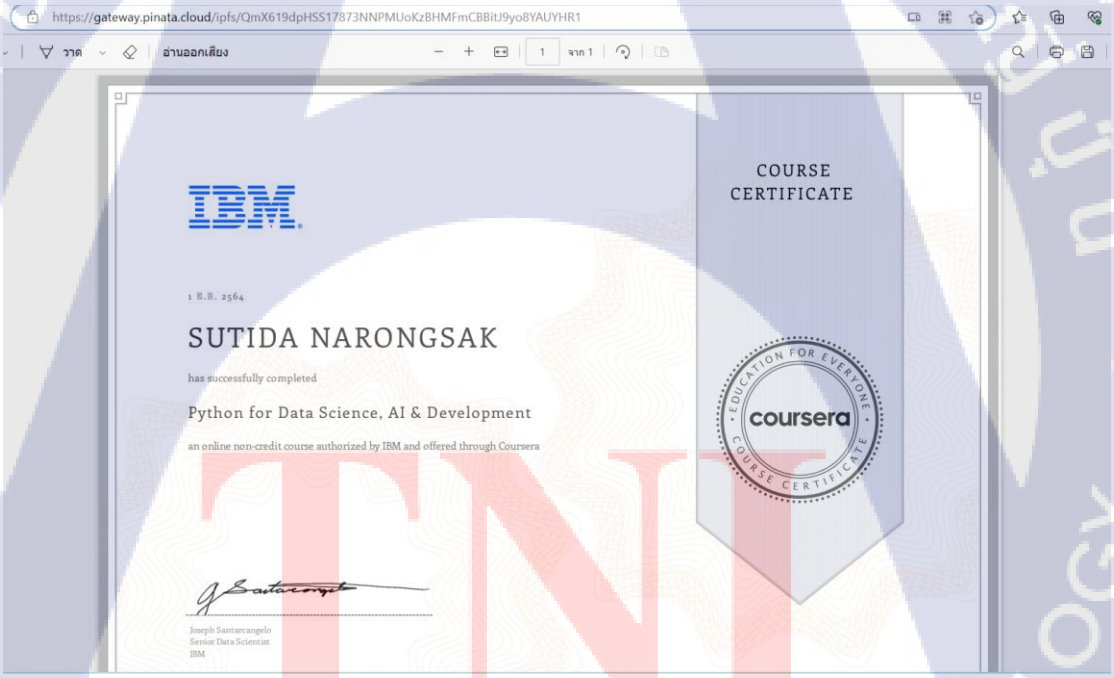
This student has been graduated from Thai Nichi Institute of Technology
No. of certificate received: 1

รูปที่ 4.27 ระบบแจ้งสถานการณ์ได้รับใบปริญญา

นอกจากนี้ระบบยังสามารถแสดงให้เห็นถึงรายละเอียดใบปริญญาที่ได้รับ และสามารถเรียกดูใบปริญญาฉบับจริงได้ผ่านที่อยู่ URL ที่ระบุไว้ใน metadata ดังรูปที่ 4.28 และ 4.29

```
{
  "details": {
    "json": {
      “URL”: “QmX619dpHSS17873NNPMUoKzBHMFmCBBitJ9yo8YAUYHR1”,
      "authority": "Thai-Nichi Institute of Technology",
      "degree_title": "Master of Science",
      "faculty_name": "Information Technology"
    }
  },
  "qty": 1,
  "raw": 1,
  "token": "2163110030",
  "txid": "a1257f6e65fa06bea6ccb8811133e02190d15c5f49a21a4f7430e0391c8646c1"
}
```


รูปที่ 4.28 รายละเอียดใบปริญญาที่ได้รับ



รูปที่ 4.29 การเรียกดูใบปริญญาบัตรโดยใช้ URL ที่ระบุไว้ใน metadata

หลังจากที่ผู้วิจัยได้ทำการสร้างและทดสอบการใช้งานของระบบ พบว่าระบบที่สร้างขึ้นมีข้อจำกัดบางประการที่ส่งผลต่อการทำงานภาพรวม ดังนี้

1) ระบบมีข้อจำกัดที่ไม่สามารถสร้างเหรียญดิจิทัลที่มีชื่อแบบเดียวกันได้ ดังนั้น ผู้ดูแลระบบจึงต้องกำหนดจำนวนเหรียญที่สร้างให้เพียงพอกับการใช้งานในระบบ

2) เนื่องจากข้อมูลที่บันทึกอยู่บนระบบบล็อกเชนไม่สามารถลบหรือเปลี่ยนแปลงข้อมูลได้ ดังนั้นขั้นตอนในการส่งธุรกรรมจึงมีความสำคัญมาก ก่อนการส่งข้อมูลทุกครั้งจำเป็นต้องตรวจสอบความถูกต้องให้ละเอียดก่อนเสมอ

บทที่ 5
บทสรุป และข้อเสนอแนะ

การสร้างระบบโอนหน่วยกิตและออกใบปริญญาบัตรด้วยการสร้างเหรียญดิจิทัล มีวัตถุประสงค์คือ 1) เพื่อวิเคราะห์และสร้างกรอบความคิดที่สามารถนำไปใช้ได้จริงในการออกใบปริญญาบัตรด้วยการประยุกต์ใช้เทคโนโลยีบล็อกเชนและเหรียญดิจิทัล 2) เพื่อวิเคราะห์และออกแบบเครื่องมือที่สามารถตรวจสอบความถูกต้องของใบปริญญา ได้ทำการสรุปการวิจัยตามลำดับดังนี้

5.1 สรุปผลงานวิจัย

5.2 ข้อเสนอแนะงานวิจัย

5.1 สรุปผลงานวิจัย

จากการพัฒนาระบบระบบโอนหน่วยกิตและออกใบปริญญาบัตรด้วยการสร้างเหรียญดิจิทัลบนเครือข่ายมัลติเชนด้วยภาษาไพธอน โดยใช้ SQLite เป็นฐานข้อมูล ร่วมกับการพัฒนาเว็บไซต์ด้วยภาษา HTML และ CSS ระบบสามารถทำงานได้ ข้อมูลการรับส่งธุรกรรมมีการบันทึกและจัดเก็บลงในเครือข่ายบล็อกเชนได้อย่างถูกต้อง เมื่อเครื่องแม่ข่ายถูกปิดหรือไม่สามารถเข้าถึงได้ เครื่องคอมพิวเตอร์เครื่องอื่น ๆ บนเครือข่ายก็ยังสามารถทำงานได้ตามปกติ ในกรณีที่เครื่องแม่ข่ายหรือเครื่องคอมพิวเตอร์อื่น ๆ กลับเข้ามาเชื่อมต่อบนเครือข่ายหลังจากหลุดการเชื่อมต่อ ระบบจะมีการอัพเดตข้อมูลธุรกรรมที่เกิดขึ้นให้เป็นปัจจุบัน ทำให้มั่นใจได้ว่าข้อมูลที่เกิดขึ้นมีความถูกต้อง ไม่สูญหาย และเป็นข้อมูลเดียวกันทั้งระบบ ยิ่งเครื่องคอมพิวเตอร์บนเครือข่ายเพิ่มมากขึ้น ข้อมูลบนเครือข่ายก็ยิ่งมีความปลอดภัยมากขึ้น เนื่องจากการปลอมแปลงหรือแก้ไขข้อมูลก็ยิ่งทำได้ยาก อีกทั้งเวลาในการเผยแพร่ธุรกรรมลงบนเครือข่ายบล็อกเชนก็ยังมีความรวดเร็ว และไม่มีค่าธรรมเนียมในการดำเนินการ ช่วยลดค่าใช้จ่ายในการพัฒนาระบบ นอกจากนี้การแลกเปลี่ยนระหว่างสินทรัพย์ที่แตกต่างกันก็ยังสามารถดำเนินการได้อย่างง่ายดายผ่าน Atomic Exchange ซึ่งช่วยลดขั้นตอนในการดำเนินการและตรวจสอบ และการออกใบปริญญาบัตรด้วยเหรียญดิจิทัลยังเป็นการเปลี่ยนใบปริญญาในรูปแบบกระดาษให้เป็นใบปริญญาบัตรแบบดิจิทัล ซึ่งช่วยลดค่าใช้จ่ายในการผลิตใบปริญญา และช่วยลดค่าใช้จ่ายและขั้นตอนในการดำเนินการขอใบปริญญาบัตรใหม่กรณีสูญหายหรือเสียหาย ในกรณีที่ต้องการนำใบปริญญาบัตรไปใช้เพื่อสมัครเข้าศึกษาต่อในระดับสูง หรือการสมัครเข้าทำงาน บริษัทหรือองค์กรภายนอกสามารถตรวจสอบความถูกต้องของใบปริญญาได้ง่าย ๆ ผ่านระบบที่ได้พัฒนาไว้ ทำให้มั่นใจได้ว่าใบปริญญาที่ได้มาเป็นของจริง

5.2 ข้อเสนอแนะงานวิจัย

งานวิจัยนี้ได้พัฒนาระบบโอนหน่วยกิตและออกใบปริญญาบัตรให้กับ หนึ่งมหาวิทยาลัย ซึ่งสามารถนำแนวทางไปใช้งานได้จริง โดยอาจนำไปประยุกต์เพื่อสร้างเครือข่ายบล็อกเชนของมหาวิทยาลัยและสถาบันการศึกษาในสังกัดกระทรวงการศึกษา เพื่อเชื่อมต่อข้อมูลและขยายเครือข่ายบล็อกเชนให้มีความปลอดภัยมากขึ้น นอกจากนี้ยังเป็นการอำนวยความสะดวกให้กับนักศึกษาที่ทำการย้ายสถาบันการศึกษาจากที่หนึ่งไปยังอีกที่หนึ่ง โดยสามารถอ้างอิงจากหน่วยกิตและผลการศึกษาที่เคยได้รับ ทำให้นักศึกษาไม่ต้องเสียเวลาและค่าใช้จ่ายในการเรียนซ้ำวิชาเดิม

บรรณานุกรม

บรรณานุกรม

[1] S. G. Linda Ronnie, *"The Conversation,"* [Online]. Available: https://theconversation.com/fake-qualifications-are-on-the-rise-how-universities-can-manage-the-risk-109962. [Accessed: August 15, 2022].

[2] G. Grolleau and N. Mzoughi, "An introduction to the economics of fake degrees," *Journal of Economic Issues*, vol. 42, no. 43, pp. 673-693, September 2008.

[3] ราชบัณฑิตยสถาน, *"พจนานุกรมฉบับราชบัณฑิตยสถาน พ.ศ. 2554,"* [Online]. Available: https://dictionary.orst.go.th. [Accessed : 15 สิงหาคม 2565].

[4] M. Crosby et al, "Blockchain technology: beyond bitcoin," *Applied Innovation Review*, vol. 2, pp. 6-10, June 2016.

[5] S. S. Sarmah, "Understanding blockchain technology," *Computer Science and Engineering 2018*, vol. 8, no. 2, pp. 23-29, August 2018.

[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," [Online]. Available: https://bitcoin.org/bitcoin.pdf. [Accessed : August 20, 2022].

[7] M. N. M. Bhutta et al., "A survey on blockchain technology: evolution, architecture and security," *IEEE Access 2021*, vol. 9, no. 9, pp. 61048-61073, April 2021.

[8] V. Buterin, "*Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform,"* [Online] . Available: https://ethereum.org/669c9e2e2027310b6b3cdce6e1c52962/Ethereum_Whitepaper_-_Buterin_2014.pdf. [Accessed : August 1, 2022].

[9] N. Szabo, *"Smart Contracts,"* [Online] . Available: https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html. [Accessed : September 5, 2022].

[10] D. Yaga, et al., *"Blockchain Technology Overview,"* [Online] Available: https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf [Accessed: August 1, 2022].

[11] มณฑา ชยากรวิกรม และคณะ, *การใช้เทคโนโลยีบล็อกเชนสำหรับภาครัฐฯ*, กรุงเทพฯ: สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน), 2564.

[12] J. Xie et al, “A survey of blockchain technology applied to smart cities: research issues and challenges,” *IEEE Communications Surveys & Tutorials*, vol. 23, no. 21, pp. 2794-2830, July 2019.

[13] K. E. Wegrzyn and E. Wang, *“Types of Blockchain: Public, Private, or Something in Between,”* Foley, [Online] . Available: https://www.foley.com/en/insights/ publications /2021/08/types-of-blockchain-public-private-between. [Accessed : September 13, 2022].

[14] S. Jose, *“CargoSmart launches Blockchain Initiative to Simplify Shipment Documentation Processes,”* CargoSmart, [Online] . Available: https://www. cargosmart.com/en/news/cargosmart-launches-blockchain-initiative-to-simplify-shipment-documentation-processes.htm. [Accessed: September 13, 2022].

[15] PGP Corporation, *An Introduction to Cryptography*, California: PGP Corporation, 2002.

[16] M. Barakat, C. Eder and T. Hanke, *“An Introduction to Cryptography,”* [Online]. Available: https://www.mathematik.uni-kl.de/~ederc/download/ Cryptography.pdf. [Accessed : October 2, 2022].

[17] C. Paar and J. Pelzl, *Understanding Cryptography*, London: Springer, 2010.

[18] W. A. Kaal, “Digital asset market evolution,” *Journal of Corporation Law*, vol.46, no. 20-02, May 2020.

[19] *“พระราชกำหนดการประกอบธุรกิจดิจิทัล พ.ศ. 2561,”* ราชกิจจานุเบกษา, เล่มที่ 135, หน้าที่ 43, 13 พฤษภาคม 2561.

[20] สำนักงานคณะกรรมการกำกับหลักทรัพย์และตลาดหลักทรัพย์, *“SEC,”* [Online]. Available: https://www.sec.or.th/TH/Documents/Seminars/seminar-digitalas set - 110762.pdf. [Accessed : 7 กันยายน 2564].

[21] P. Wackerow, *“ERC-20 Token Standard,”* [Online] . Available: https://ethereum.org/en/developers/docs/standards/tokens/erc-20/. [Accessed : October 3, 2022].

[22] P. Wackerow, *"ERC-721 Non-Fungible Token Standard,"* [Online]. Avalables: https://ethereum.org/en/developers/docs/standards/tokens/erc-721. [Accessed : October 3, 2022].

[23] Wirex, *"The 8 Different Types of Crypto Assets,"* [Online]. Available: https://wirexapp.com/blog/post/the-8-different-types-of-crypto-assets-0471. [Accessed : September 21, 2022].

[24] นเรศ เหล่าพรรณราย, *Digital Asset Cryptocurrency Bitcoin มือใหม่เริ่มต้นลงทุนสินทรัพย์ดิจิทัล*, กรุงเทพฯ: พราว, 2564.

[25] Litecoin, *"Lite Coin White Paper,"* [Online]. Available: https://api-new.whitepaper.io/documents/pdf?id=SkGJbIbEO. [Accessed : September 20, 2022].

[26] Bitkub, *"New Normal Digital Economy Cryptocurrency and Blockchain,"* [Online]. Available: https://www.oic.or.th/sites/default/files/institute/course/91919/public/20-5-65_khunphiirasiththi_cchiwaphngs_new_normal_digital_economy_cryptocurrency_blockchain_samhrabthurkicchprakanphay.pdf. [Accessed : September 21, 2022].

[27] C. Hoskinson, *"Why We Are Building Cardano,"* [Online]. Available: https://whitepaper.io/document/581/cardano-whitepaper. [Accessed : September 21, 2022].

[28] N. V. Saberhagen, *"Crypto Note v 2.0,"* [Online]. Available: https://github.com/monero-project/research-lab/blob/master/whitepaper/whitepaper.pdf. [Accessed : September 21, 2022].

[29] BAT, *"Basic Attention Token (BAT) Blockchain Based Digital Advertising,"* [Online]. Available: https://basicattentiontoken.org/static-assets /documents /BasicAttentionTokenWhitePaper-4.pdf. [Accessed : September 21, 2022].

[30] T. Lambert, D. Liebau and P. Roosenboom, "Security token offerings," *Small Business Economics*, vol. 59 no. 1, pp. 299-325, June 2022.

[31] D. Arner, R. Auer and J. Frost, *"Stablecoins: Risks, Potential and Regulation,"* [Online]. Available: https://www.bis.org/publ/work905.pdf. [Accessed : September 22, 2022].

[32] W. K. Härdle, C. R. Harvey, and R. C. G. Reule, "Understanding cryptocurrencies," *Capital Markets: Market Microstructure eJournal*, vol.18, no.2, pp.181-208, March 2019.

[33] Coinbase, *"USD Coin,"* [Online]. Available: https://www.coinbase.com/th/ usdc. [Accessed : September 22, 2022].

[34] G. Iredale, *"What Are The Different Types Of Stablecoins?,"* [Online]. Available: https://101blockchains.com/types-of-stablecoins/. [Accessed : September 22, 2022].

[35] A. C. Eufemio, S. Djie, and K. C. Chng, *"Digix's Whitepaper: The Gold Standard in Crypto-Assets,"* [Online] . Available: https://cryptorating.eu/whitepapers /DigixDAO/whitepaper.pdf. [Accessed : September 22, 2022].

[36] The Maker Team, *"The DAI Stablecoin System White Paper,"* [Online]. Available: https://makerdao.com/whitepaper/DaiDec17WP.pdf. [Accessed : September 22, 2022].

[37] E. Frangella and L. Herskind, *"Aave Technical Paper,"* [Online]. Available: https://github.com/aave/aave-v3-core/blob/master/techpaper/Aave_V3_Te chnical_Paper.pdf. [Accessed : September 22, 2022].

[38] B. Sakız and A. Hiç, "Blockchain beyond cryptocurrency: non-fungible tokens," *International Conference on Eurasian Economies 2021*, Istanbul, Turkey and Online, August 24-25, 2022, pp. 144-151.

[39] K. E. Busch, *"Non-Fungible Tokens (NFTs),"* [Online]. Available : https:// crsreports.congress.gov/product/pdf/R/R47189. [Accessed : September 22, 2022].

[40] D. Yaga et al., *"Blockchain Networks: Token Design and Management Overview,"* [Online]. Available : https://nvlpubs.nist.gov/nistpubs/ir/2021/ NIST.IR.8301.pdf [Accessed : September 23, 2022].

[41] S. JokiĆ et al., "Comparative analysis of cryptocurrency wallets vs traditional wallets," *Ekonomika*, vol. 65, no. 3, pp. 65-75, October 2019.

[42] G. Greenspan, *"Multichain Private Blockchain — White Paper,"* [Online]. Available : https://www.multichain.com/white-paper/. [Accessed : March 28, 2023].

[43] H. A. Ahmed and J. W. Jang, “Document certificate authentication system using digitally signed QR code tag,” *IMCOM '18: Proceedings of the 12th International Conference on Ubiquitous Information Management and Communication*, Langkawi, Malaysia, January 5, 2018, pp 1-5.

[44] R. Shanmuga Priya and N. Swetha, “Online certificate validation using blockchain,” *International Journal of Advanced Networking & Applications (IJANA)*, vol. 1, no. 1, pp. 132-135, January 2019.

[45] R. Manoj et al., “Blockchain ecosystem for credit transfer in education,” *Mathematical Problems in Engineering*, vol. 2021, no. 4, pp. 1-12, December 2021.

[46] X. Zhao and Y.W. Si, “NFTCert: NFT-based certificates with online payment gateway,” *IEEE International Conference on Blockchain (Blockchain)*, Melbourne, Australia, December 6-8, 2021, pp. 538-543.

[47] R. A. Mishra et al., “Privacy protected blockchain based architecture and implementation for sharing of students’ credentials,” *Information Processing & Management*, vol. 58, no. 3, pp. 1-25, May 2021.

[48] S. Badlani et al., “EduCrypto: transforming education using blockchain,” *6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, Madurai, India, May 25-27, 2022. pp. 829-836.

[49] H. A. Alsobhi et al., “Blockchain-based micro-credentialing system in higher education institutions: systematic literature review,” *Knowledge-Based Systems*, vol. 265, no.1, pp. 281-190, April 2023.

[50] S. Guerreiro et al., “Integrating an academic management system with blockchain: a case study,” *Blockchain: Research and Applications*, vol. 3, no. 4, pp.192-199, December 2022.

[51] N. Nizamuddin et al., “Decentralized document version control using ethereum blockchain and IPFS,” *Computers & Electrical Engineering*, vol. 76, pp. 183-197, March 2019.

[52] N. Nousias et al., “A process-aware approach for blockchain-based verification of academic qualifications,” *Simulation Modelling Practice and Theory*, vol. 121, no. 1, pp. 429-433, September 2022.