ระบบรับรองและตรวจสอบใบประกาศนียบัตรออนไลน์ด้วยเทคโนโลยีบล็อคเชน

ONLINE CERTIFICATE APPROVAL AND VALIDATION USING BLOCKCHAIN TECHNOLOGY

กรินทร์ อ่อนวงศ์

จุฬพัฒน์ อมตฉายา

ปริญญานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

สาขาวิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์

สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

ปีการศึกษา 2563

ปริญญานิพนธ์ปีการศึกษา 2563

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง

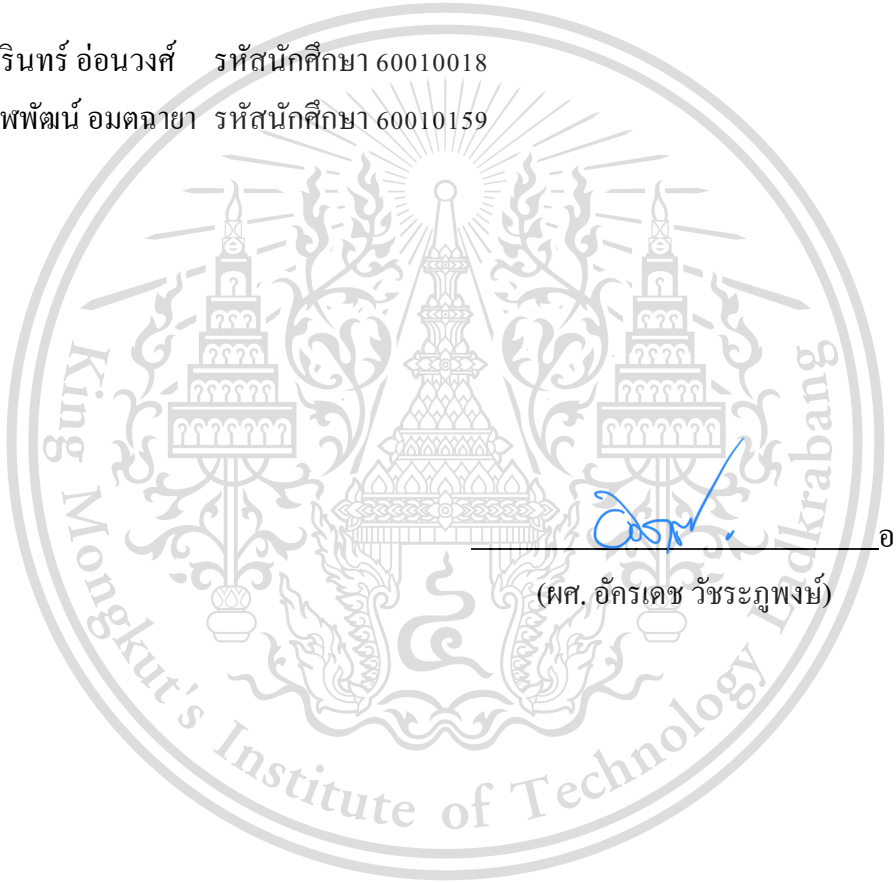
เรื่อง ระบบรับรองและตรวจสอบใบประกาศนียบัตรออนไลน์ด้วยเทคโนโลยีบล็อคเชน

ONLINE CERTIFICATE APPROVAL AND VALIDATION USING BLOCKCHAIN TECHNOLOGY

ผู้จัดทำ

1. นายกรินทร์ อ่อนวงศ์ รหัสนักศึกษา 60010018

2. นายจุฬพัฒน์ อมตฉายา รหัสนักศึกษา 60010159



_____อาจารย์ที่ปรึกษา

(ผศ. อัครเดช วัชระภูพงษ์)

ระบบรับรองและตรวจสอบใบประกาศนียบัตรออนไลน์ด้วยเทคโนโลยีบล็อคเชน

นายกรินทร์ อ่อนวงศ์ 60010018
นายจุฬพัฒน์ อมตฉายา 60010159
ผศ.อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษา
ปีการศึกษา 2563

บทคัดย่อ

ปัจจุบันในระบบการศึกษาต่างๆ เมื่อนักเรียนสำเร็จการศึกษา ผู้เรียนจะได้รับใบประกาศนียบัตรหรือวุฒิการศึกษา โดยส่วนมากสถานศึกษามักจะออกใบประกาศนียบัตรให้เป็นแบบกระดาษ ซึ่งจะมีกลวิธีในการป้องกันการปลอมแปลงบนใบประกาศนียบัตรกระดาษเหล่านั้นแตกต่างกันออกไป อย่างไรก็ตาม ถึงแม้กลวิธีในการป้องกันการปลอมแปลงจะดีแค่ไหนก็ตาม ผู้ที่ปลอมแปลงก็ยังสามารถปลอมแปลงใบประกาศนียบัตรได้เสมอ และบางครั้งปลอมแปลงได้แนบเนียนจนการตรวจสอบด้วยตาเปล่าไม่สามารถบอกได้ว่าเป็นของปลอม หรือบางครั้งใบประกาศนียบัตรนั้นอาจเป็นของจริง แต่ข้อมูลบางอย่างบนใบประกาศนียบัตรนั้นถูกแก้ไข การจะตรวจจับการปลอมแปลงหรือแก้ไขใบประกาศนียบัตรที่เป็นกระดาษจึงทำได้ยาก และอาจตรวจจับใบที่ถูกปลอมแปลงหรือแก้ไขไม่ได้ทั้งหมด ครั้นจะเปลี่ยนมาใช้การให้ใบประกาศนียบัตรแบบไฟล์ดิจิตอล ก็ยังไม่มีระบบใดที่จะตรวจจับการปลอมแปลงและแก้ไขได้อย่างมีประสิทธิภาพมากพอ ปริญญานิพนธ์ “ระบบรับรองและตรวจสอบใบประกาศนียบัตรออนไลน์ด้วยเทคโนโลยีบล็อคเชน” นี้จึงถูกจัดทำขึ้นเพื่อแก้ไขปัญหาดังกล่าวโดยการนำเทคโนโลยี Blockchain เข้ามาช่วยให้การรับรองประกาศนียบัตรออนไลน์นั้นมีประสิทธิภาพมากยิ่งขึ้น เพื่อให้สามารถตรวจสอบว่าประกาศนียบัตรออนไลน์นั้นเป็นใบประกาศนียบัตรที่ออกโดยผู้จัดการเรียนการสอนออนไลน์จริงๆ และข้อมูลบนใบประกาศนียบัตรออนไลน์เป็นข้อมูลที่ถูกต้อง มิใช่ใบประกาศนียบัตรที่ถูกปลอมแปลงหรือแก้ไขโดยมิจฉาชีพ

ONLINE CERTIFICATE APPROVAL AND VALIDATION USING BLOCKCHAIN TECHNOLOGY

Mr. Karin	Onwong	60010018
Mr. Chulapat	Amatachaya	60010159
Asst. Prof. Akkradach	Watcharapupong	Advisor

Academic Year 2020

ABSTRACT

Currently, in various educational academy, students receive their certificate after they graduate or finish their courses. In most cases, educational institutions will issue paper certificates to students. There are different anti-counterfeiting strategies on those paper certificates, but the counterfeiters are still able to forge a certificate. A well forged certificate is still very difficult to be identified perhaps mistakenly identified as a genuine certificate. In another case, some of certificate were genuinely issued by the academy but some of the information on the certificate have been changed without authority of the academy which is also difficult to identify. Switching to a digital certificate file is a better practice to make the certificate more difficult to be counterfeited but there is not yet a system that can effectively detect certificate counterfeit and tampering.

"Online Certificate Approval and Validation using Blockchain Technology" is a solution to solve certificate counterfeit and tampering problem with a better procedure. Using advantages of Blockchain Technology makes it impossible to counterfeit or tamper the information on the certificate. We look forward to the future that all certificates can be trusted using the system we developed.

กิตติกรรมประกาศ

ปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี เนื่องจากได้รับคำแนะนำ คำปรึกษา และความช่วยเหลือด้านอื่นๆจากหลายฝ่ายทั้งในทางตรงและทางอ้อม ปริญญานิพนธ์ฉบับนี้จะสำเร็จลุล่วงไปไม่ได้ หากปราศจากการชี้แนะให้ดำเนินการไปในทางที่ถูกต้องตลอดการทำปริญญานิพนธ์จากผู้ช่วยศาสตราจารย์อัครเดช วัชระภูพงษ์ อาจารย์ที่ปรึกษาที่คอยให้คำปรึกษาทั้งในและนอกเวลาเรียน ตั้งแต่เริ่มต้นจนปริญญานิพนธ์ฉบับนี้สำเร็จลุล่วงไปได้ด้วยดี

ขอขอบคุณห้องวิจัย Hardware และห้องวิจัย Information Security Advisory Group(ISAG) ที่เอื้อเฟื้อสถานที่ในการศึกษาและจัดทำปริญญานิพนธ์

สุดท้ายนี้ ขอกราบขอบคุณบิดา มารดา ที่คอยส่งเสริม และสนับสนุนโอกาสในการศึกษา และสนับสนุนในทุกๆด้านในชีวิตเสมอมา

กรินทร์ อ่อนวงศ์

จุฬพัฒน์ อมตฉายา

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

ตาราง **หน้า**

สารบัญรูป

รูป **หน้า**

สารบัญรูป (ต่อ)

รูป **หน้า**

บทที่ 1
บทนำ

1.1 ความเป็นมาของปัญหา

ปัจจุบันระบบการเรียนการสอนผ่านระบบออนไลน์ ได้เข้ามามีบทบาทในชีวิตประจำวันมากขึ้น เนื่องจากมีความสะดวกสบายในการเรียนสูง เมื่อเรียนจบคอร์สทางสถาบันมักจะมีใบประกาศนียบัตรออนไลน์ให้กับผู้เรียนเพื่อเป็นการรับรองว่าผู้เรียนได้ผ่านการเรียนในคอร์สนั้นๆแล้ว อย่างไรก็ตามประกาศนียบัตรนั้นย่อมถูกปลอมแปลงได้ และปัจจุบันยังไม่มีวิธีตรวจสอบที่ดีมากพอ

ปริญญานิพนธ์ “การรับรองใบประกาศนียบัตรออนไลน์ด้วยเทคโนโลยีบล็อคเชน” นี้จึงถูกจัดทำขึ้นโดยการนำเทคโนโลยี Blockchain เข้ามาช่วยให้การรับรองประกาศนียบัตรออนไลน์นั้นมีประสิทธิภาพมากยิ่งขึ้น เพื่อให้สามารถตรวจสอบว่าประกาศนียบัตรออนไลน์นั้นเป็นใบประกาศนียบัตรที่ออกโดยผู้จัดการเรียนการสอนออนไลน์จริงๆ มิใช่ใบประกาศนียบัตรที่ถูกปลอมแปลงขึ้นมาโดยมิจฉาชีพ

1.2 วัตถุประสงค์ของปริญญานิพนธ์

1) เพื่อให้สามารถตรวจสอบว่าใบประกาศนียบัตรออนไลน์เป็นใบประกาศนียบัตรที่มีความถูกต้อง
2) เพื่อให้สามารถมั่นใจได้ว่าใบประกาศนียบัตรออนไลน์เป็นใบประกาศนียบัตรที่ออกโดยผู้จัดการเรียนการสอนอย่างแท้จริง
3) เพื่อศึกษาเกี่ยวกับการพัฒนาแอปพลิเคชั่นที่ทำงานร่วมกับเครือข่ายบล็อคเชน

1.3 ประโยชน์ที่คาดว่าจะได้รับ

1) ผู้จัดทำได้รับความรู้ความเข้าใจในระบบ Blockchain
2) ได้นำเทคโนโลยี Blockchain มาพัฒนาให้เกิดประโยชน์
3) เพื่อเป็นแนวทางให้เป็นแนวทางในการที่พัฒนาแอปพลิเคชั่นในแพลตฟอร์มอื่นๆ มาร่วมกับเครือข่าย Blockchain Ethereum นี้

1.4 วิธีการดำเนินงาน

วิธีการดำเนินงานปริญญานิพนธ์นี้แบ่งออกเป็น 9 ขั้นตอนหลัก ดังนี้

1) กำหนดปัญหาที่จะทำในปริญญานิพนธ์
2) วิเคราะห์เพื่อหาแนวทางแก้ไขปัญหา
3) ศึกษาและรวบรวมทฤษฎีที่จะใช้ในการแก้ปัญหา
4) ออกแบบโครงสร้างของระบบ
5) ออกแบบแอปพลิเคชัน ทั้งเชิงตรรกะและรูปร่างหน้าตา
6) พัฒนาแอปพลิเคชัน
7) ทดสอบเพื่อหาข้อบกพร่อง
8) นำไปใช้งานจริงและวัดผล
9) จัดทำเอกสารและคู่มือการใช้งาน

1.5 ขอบเขตของปริญญานิพนธ์

1) แอปพลิเคชันนี้เป็นแอปพลิเคชันที่ใช้เทคโนโลยี Blockchain เฉพาะบนเครือข่าย Ethereum
2) ขณะใช้งานแอปพลิเคชันจะต้องมีการเชื่อมต่ออินเตอร์เน็ต
3) สถาบันผู้ออกใบ Digital Certificate จะต้องประกาศ Public key ของ Account Blockchain ให้ทราบโดยทั่วกัน
4) Third-party App ต้อง implement ตาม Requirement ที่กำหนด

บทที่ 2
ทฤษฎีที่เกี่ยวข้อง

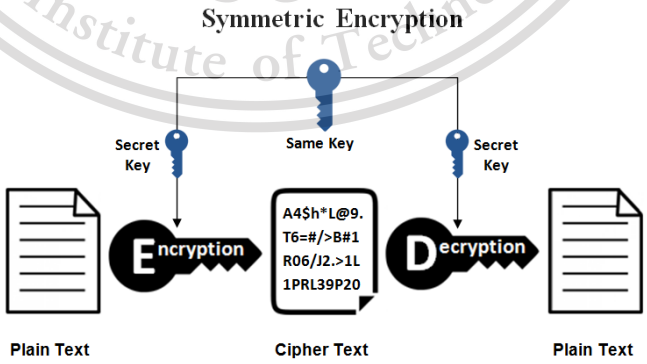
2.1 ทฤษฎีที่เกี่ยวข้อง

2.1.1 Cryptography

การเข้ารหัสข้อมูลโดยพื้นฐานแล้วจะเกี่ยวข้องกับวิธีการทางคณิตศาสตร์เพื่อใช้ในการป้องกันข้อมูลหรือข้อความตั้งต้นที่ต้องการส่งไปถึงผู้รับ ข้อมูลตั้งต้นจะถูกแปรเปลี่ยนไปสู่ข้อมูลหรือข้อความอีกรูปแบบหนึ่งที่ไม่สามารถอ่านเข้าใจได้โดยใครก็ตามที่ไม่มีกุญแจสำหรับเปิดดูข้อมูลนั้น เราเรียกกระบวนการในการแปรรูปของข้อมูลตั้งต้นว่า "การเข้ารหัสข้อมูล" (Encryption) และกระบวนการในการแปลงข้อความที่ไม่สามารถอ่าน และทำความเข้าใจให้กลับไปสู่ข้อความดั้งเดิม ว่าการถอดรหัสข้อมูล (Decryption)

2.1.1.1 Symmetric-key cryptography

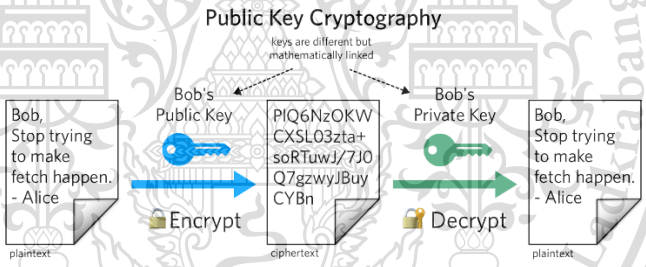
เป็นระบบกี่เข้ารหัสลับที่ใช้กุญแจชุดเดียวกันทั้งฝั่งผู้ส่งและฝั่งผู้รับในการเข้ารหัสลับและถอดรหัสลับ จากหลักการนี้ จึงเป็นที่มาของชื่อระบบรหัสแบบสมมาตร เนื่องจากคำว่า “สมมาตร” เป็นการสื่อถึงความเท่าเทียมกันหรือเหมือนกันของทั้งสองฝั่ง ซึ่งในที่นี้ก็คือตัวกุญแจนั่นเอง กุญแจซึ่งอยู่ในรูปรหัสคอมพิวเตอร์นี้เป็นตัวแปรสำคัญสำหรับการเข้าและถอดรหัสลับข้อมูล ซึ่งยิ่งขนาดของกุญแจมาก (มีหน่วยเป็นบิต) ก็ยิ่งแสดงถึงระดับความปลอดภัยของข้อมูลที่ได้รับการเข้ารหัสลับที่สูงขึ้น เพราะยิ่งรหัสลับมีขนาดใหญ่ ก็ยิ่งลดความน่าจะเป็นในการคาดเดารหัสลับ



รูป 2.1 รูปแบบการเข้ารหัสแบบ Symmetric-key

2.1.1.2 Asymmetric-key cryptography

เป็นระบบรหัสที่ใช้กุญแจคู่ (Key Pair) ซึ่งประกอบด้วย 2 ส่วน คือ กุญแจส่วนบุคคล (Private Key) และกุญแจสาธารณะ (Public Key) โดย ผู้ใช้ 1 คนจะสามารถใช้กุญแจคู่นี้ในการติดต่อสื่อสารและส่งข้อมูลกับบุคคลอื่นโดยไม่จำเป็นต้องมีกุญแจเป็นจำนวนมากเฉกเช่นเดียวกับกรณีของระบบรหัสแบบสมมาตร ทั้งนี้ กุญแจส่วนบุคคลจะต้องถูกเก็บรักษาไว้กับเจ้าของกุญแจเพียงผู้เดียว และห้ามมิให้ผู้อื่นล่วงรู้โดยเด็ดขาด ส่วนกุญแจสาธารณะนั้นต้องมีการประกาศให้ผู้อื่นรับรู้ หรือเก็บไว้ในที่ซึ่งบุคคลอื่นสามารถเข้าถึงได้ ในการเข้ารหัสลับข้อมูลแบบอสมมาตร จะต้องใช้กุญแจชุดหนึ่งในการเข้ารหัสลับ และใช้กุญแจอีกชุดหนึ่งที่เป็นคู่กันในการถอดรหัสลับ กล่าวคือ หากใช้กุญแจสาธารณะชุดหนึ่งในการเข้ารหัสลับก็จะต้องใช้กุญแจส่วนบุคคลชุดที่เป็นคู่กันในการถอดรหัสลับข้อมูลเท่านั้น และหากใช้กุญแจส่วนบุคคลชุดหนึ่งในการเข้ารหัสลับก็จะต้องใช้กุญแจสาธารณะชุดที่เป็นคู่กันในการถอดรหัสลับข้อมูลเท่านั้น



รูป 2.2 รูปแบบการเข้ารหัสแบบ Asymmetric-key

การเข้ารหัสแบบอสมมาตร สามารถนำไปประยุกต์ใช้ได้ 2 ลักษณะ ดังนี้

2.1.1.2.1 การเข้า/ถอดรหัสลับ เพื่อรักษาความลับของข้อมูล

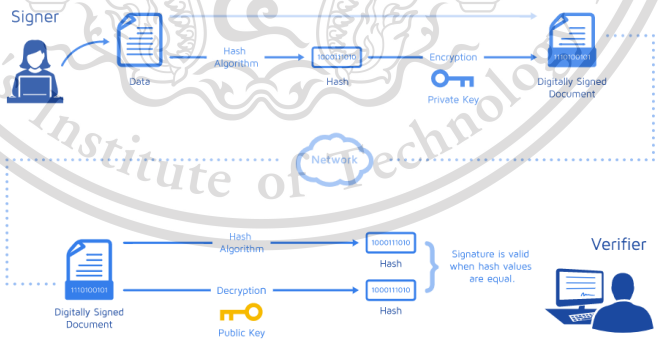
ระบบรหัสลับแบบอสมมาตรสำหรับการเข้า/ถอดรหัสลับซึ่งนำมาสู่การรักษาความลับของข้อมูลนั้น จะใช้ในกรณีผู้ส่งต้องการส่งข้อมูลที่เป็นความลับเพื่อให้ผู้รับเท่านั้นที่สามารถอ่านข้อมูลชุดนั้นได้ โดยผู้ส่งจะใช้กุญแจสาธารณะของผู้รับในการเข้ารหัสลับ(Encryption) กับข้อมูลอิเล็กทรอนิกส์ หลังจากนั้น เมื่อข้อมูลที่ถูกเข้ารหัสลับนั้นถูกส่งไปยังผู้รับ ผู้รับจะใช้กุญแจส่วนบุคคลของตนเองในการถอดรหัสลับ (Decryption) เพื่อให้สามารถอ่านข้อมูลดังกล่าวได้ ข้อสังเกต คือ ผู้รับเท่านั้นที่รู้กุญแจส่วนบุคคลของตน นั่นคือ จะมีผู้รับเพียงผู้เดียวที่สามารถถอดรหัสลับและอ่านข้อมูลนั้นได้(แม้แต่ผู้ส่งก็ไม่สามารถอ่านข้อมูลที่ถูกเข้ารหัสลับแล้วได้)

2.1.1.2.2 ลายมือชื่อดิจิทัล (Digital Signature)

ลายมือชื่อดิจิทัลเป็นข้อมูลในรูปอิเล็กทรอนิกส์ที่สร้างขึ้นโดยนำสมการทางคณิตศาสตร์มาใช้เพื่อระบุตัวตนของผู้ส่งข้อมูลอิเล็กทรอนิกส์นั้น ทั้งนี้ การลงลายมือชื่อดิจิทัลจะสร้างปลอดภัยให้กับข้อมูลได้ 3 ประการ คือ การยืนยันตัวตนบุคคล(Authentication) ความถูกต้องของข้อมูล (Data Integrity) และการห้ามปัดความรับผิดชอบ (Non-repudiation)

การสร้างลายมือชื่อดิจิทัลนั้นจะนำข้อมูลที่ต้องการส่งมาเข้ากระบวนการย่อยข้อมูล (Hash Function) เพื่อให้มีขนาดเล็กลงแต่ยังคงสามารถใช้แทนข้อมูลเดิมได้ จากนั้นจะนำกุญแจส่วนบุคคลของผู้ส่งและข้อมูลที่ผ่านการย่อยแล้วมาผ่านกระบวนการทางคณิตศาสตร์ ผลลัพธ์ที่ได้จะกลายเป็นลายมือชื่อดิจิทัล ซึ่งจะถูกส่งไปให้ผู้รับพร้อมกับข้อมูลอิเล็กทรอนิกส์ กุญแจส่วนบุคคลของผู้ส่งสร้างลายมือชื่อดิจิทัลจะถูกใช้ยืนยันได้ว่าข้อมูลนั้นมาจากผู้ส่งจริงๆ เนื่องจากมีเพียงผู้ส่งคนเดียวเท่านั้นที่มีหรือรู้ถึงกุญแจส่วนบุคคล

ในการตรวจสอบลายมือชื่อดิจิทัล ผู้รับจะนำข้อมูลอิเล็กทรอนิกส์มาผ่านขั้นตอนการย่อยแบบเดียวกับที่ผู้ส่งใช้ และนำกุญแจสาธารณะของผู้ส่งมาทำการถอดรหัสลับลายมือชื่อดิจิทัลที่ถูกแนบมากับข้อมูล จากนั้นนำผลลัพธ์ที่ได้จากกระบวนการทั้งสองมาเปรียบเทียบกัน หากเหมือนกันทุกประการ นั่นหมายความว่าข้อมูลที่ส่งมาเป็นข้อมูลที่ถูกส่งมาจากผู้ที่กล่าวอ้างจริง และไม่ได้ผ่านการเปลี่ยนแปลงหรือแก้ไขใดๆ (หากมีการเปลี่ยนแปลงข้อมูลอิเล็กทรอนิกส์ของเดิม ข้อมูลสองชุดที่นำมาเปรียบเทียบกันจะไม่เท่ากันทันที)



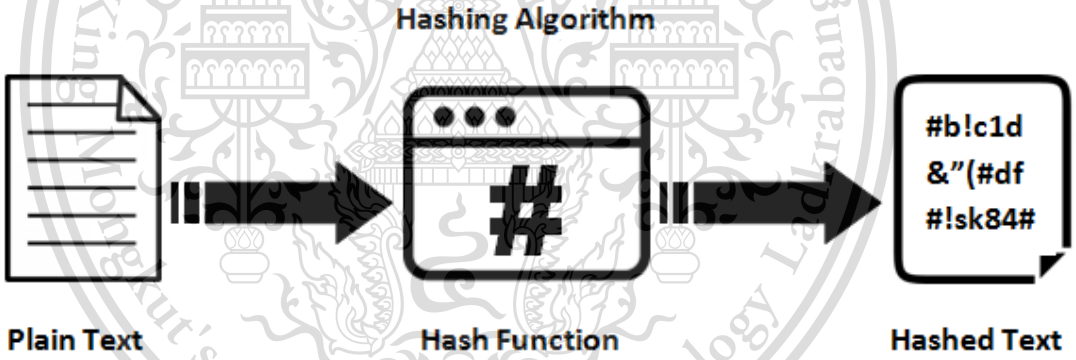
รูป 2.3 การทำสัญญาและตรวจสอบลายเซ็นดิจิทัล

2.1.1.3 Cryptographic Hash Function

วิธีการที่ทำให้ข้อมูลมีขนาดย่อลงแต่ยังคงมีลักษณะจำเพาะของข้อมูลนั้นเช่นเดิม โดยอาจกระทำโดยการแบ่งข้อมูลออกเป็นส่วนๆ ผ่านวิธีการใดๆแล้วนำกลับมารวมกัน เรียกว่า ค่าแฮช (hash value)

คุณสมบัติของฟังก์ชันแฮช (Hash function)

1) ข้อมูลแต่ละตัวเมื่อผ่านฟังก์ชันแฮชแล้วจะต้องมีค่าไม่เท่ากัน มีลักษณะที่จำเพาะแต่ล่ะข้อมูล
2) หาค่าแฮชจากข้อมูลควรทำได้ง่ายและรวดเร็ว
3) เมื่อข้อมูลผ่านฟังก์ชันแฮชแล้วต้องไม่สามารถทำย้อนกลับได้
4) การบวนการแฮชควรมีการกระจายตัวสูง ข้อมูลใดๆที่ผ่านฟังก์ชันแฮช ควรมีขนาดเท่ากัน แต่ไม่เหมือนกัน



รูป 2.4 รูปแบบของฟังก์ชั่นแฮช

2.1.2 Blockchain

Blockchain คือเทคโนโลยีการจัดเก็บข้อมูลแบบ Shared Database หรือ ที่รู้จักกันในชื่อ “Distributed Ledger Technology (DLT)” โดยเป็นรูปแบบการจัดเก็บข้อมูลที่สามารถรับประกันความปลอดภัยว่าข้อมูลที่ถูกบันทึกไปก่อนหน้านั้น ไม่สามารถที่จะถูกเปลี่ยนแปลง หรือแก้ไขได้ ซึ่งทุกผู้ใช้งานจะได้รับข้อมูลชุดเดียวกันทั้งหมด โดยใช้หลักการของ Cryptography และ Distributed Computing เพื่อสร้างกลไกที่มีความน่าเชื่อถือโดยไม่จำเป็นต้องมีคนกลางเข้ามาเกี่ยวข้อง เช่น ธนาคาร หรือหน่วยงานอื่นๆ ที่เกี่ยวข้องกับกระบวนการจ่ายเงิน โดยได้รับความสนใจอย่างแพร่หลาย รวมทั้ง

ได้รับการยอมรับจากผู้เชี่ยวชาญทั่วโลกว่าเป็นเทคโนโลยีที่มีศักยภาพ และสามารถ นำมาประยุกต์ใช้ในธุรกิจภาคอื่น ๆ ได้ ไม่จำเพาะเพียงภาคธุรกิจการเงินและการธนาคารเท่านั้น แต่ยังรวมถึงภาครัฐ และหน่วยงานอื่นก็ได้มีการตื่นตัวและศึกษาเกี่ยวกับเทคโนโลยี Blockchain กันอย่างแพร่หลายเช่นกัน

2.1.2.1 Node

อุปกรณ์ในเครือข่าย Blockchain เปรียบได้กับเครื่องคอมพิวเตอร์ โทรศัพท์ หรืออื่น ๆ ที่สามารถเชื่อมต่ออินเทอร์เน็ตและประมวลผลได้ ซึ่งถือว่าเป็นโครงสร้างพื้นฐานที่สำคัญในการกระจายและเชื่อมโยงกันในเครือข่ายเพื่อให้ระบบสามารถทำงานและประมวลผลได้ ทั้งนี้ประเภทของ Node ในเครือข่าย Blockchain สามารถจำแนกได้เป็น

1) Node ที่ทำหน้าที่ในการจัดเก็บสำเนาข้อมูลเท่านั้น ประกอบด้วยFull Node และLight Node
2) Node ที่ทำหน้าที่ตรวจสอบความถูกต้องเท่านั้น หรือที่รู้จักกันในชื่อ Consensus Node

2.1.2.2 Consensus Protocol

ข้อกำหนดในการลงความเห็นร่วมกันระหว่างสมาชิกใน Blockchain โดยสมาชิกต้องยอมรับในกลไกการควบคุมความถูกต้องของข้อมูลผ่านอัลกอริทึมต่าง ๆ เพื่อให้ข้อมูลมีความถูกต้องเที่ยงตรงและข้อมูลบนทุก Node เป็นข้อมูลชุดเดียวกัน รวมทั้งข้อมูลมีการจัดเก็บที่สอดคล้องและมีลำดับการจัดเก็บตรงกัน ทั้งนี้ กระบวนการConsensus มีอยู่ด้วยกันหลายวิธี ยกตัวอย่างเช่น

2.1.2.2.1 Proof-of-Work

กระบวนการทำ Consensus โดยใช้การแก้ปัญหาทางคณิตศาสตร์ซึ่งมีความซับซ้อนมาก ต้องใช้เวลาและทรัพยากรมหาศาลในการแก้ปัญหานั้น ๆ(Mining) เพื่อยืนยันความน่าเชื่อถือของข้อมูลที่จะถูกบันทึกเข้ามาในเครือข่าย

Nodes ต่าง ๆ ที่เข้ามำการ Mining จะถูกเรียกว่า “Miners”โดย Miner จะได้รับค่าตอบแทนจากการทำ Proof-of-Work และด้วยวิธีการดังกล่าว ทำให้การแก้ไขข้อมูลที่ถูกบันทึกลงในระบบ Blockchain แล้วนั้นแทบจะเป็นไปไม่ได้เลย ปัจจุบันมี Public Blockchain ที่ใช้วิธีการยืนยันรายการแบบ Proof-of-Work มากมาย เช่น Bitcoin เป็นต้น

2.1.2.2.2 Proof-of-Stake

กระบวนการทำ Consensus โดยใช้หลักการวาง“หลักทรัพย์” ของผู้ตรวจสอบ (Validator) ในการยืนยันธุรกรรมต่างๆ ผู้ตรวจสอบที่ทำการวางสินทรัพย์จำนวนมากกว่าจะมีโอกาสสูงกว่าที่จะได้รับสิทธิ์ในการเขียนข้อมูลธุรกรรมบน Block ถัดไป โดยผู้ที่ได้รับสิทธิ์ในการเขียนข้อมูลบน Block ถัดไปนั้นจะได้รับค่าธรรมเนียมการดำเนินการเป็นสิ่งตอบแทน ปัจจุบันเริ่มมี Public Blockchain หลาย chain หันมาใช้วิธีการยืนยันรายการแบบ Proof-of-Stake แล้วเพราะไม่ต้องใช้เวลายืนยันธุรกรรมยาวนานเท่า Proof-of-Work และไม่สิ้นเปลืองทรัพยากร

2.1.2.3 Transaction

ธุรกรรม(Transaction) คือการที่เหตุการณ์ใดๆซึ่งถูกกระทำโดยผู้ใช้(ไม่ใช่ตัวระบบเอง) ซึ่งเหตุการณ์นั้นเปลี่ยนแปลงข้อมูลบนบล็อคเชน เช่น A โอนเงินให้ B เงินในบัญชีของ A จะต้องลดลง และ เงินในบัญชีของ B ต้องเพิ่มขึ้น โดยในการทำธุรกรรมนั้น ผู้ทำธุรกรรมจะต้องใช้ Private key เพื่อยืนยันตนในการทำธุรกรรม เพื่อป้องกันไม่ให้ถูกสวมรอยจากผู้ไม่หวังดี ธุรกรรมต่างๆ จะถูก Broadcast ไปในเครือข่ายของบล็อคเชน และจะถูกเพิ่มไปยังบล็อคเชนโดยผ่าน Consensus Protocol ต่อไป

2.1.3 Ethereum

เป็น Platform ของ Blockchain แบบเปิด (Public Blockchain) โดย Ethereum มีความแตกต่างจาก Bitcoin เนื่องจาก Ethereum ถูกออกแบบมาเพื่อให้มีความยืดหยุ่นสูง อีกทั้งยังเป็น Open Source โดยความสามารถของ Ethereum ถือว่าดีใกล้เคียงกับ Bitcoin แต่สิ่งที่เพิ่มขึ้นมา คือ ฟีเจอร์ที่เรียกว่า Smart Contract ซึ่งผู้ใช้ หรือนักพัฒนาโปรแกรมจะสามารถเขียนโปรแกรมลงไปในข้อมูลของสกุลเงิน Ether ได้ เพื่อให้ทำงานอัตโนมัติเมื่อเงื่อนไขเป็นไปตามที่กำหนดไว้ในสัญญาอัจฉริยะ ดังนั้นจึงทำให้สามารถสร้าง Application ต่าง ๆ ขึ้นมาบนเครือข่าย Ethereum อีกชั้นหนึ่งได้ ทำให้เกิดรูปแบบที่หลากหลายในการใช้งานซึ่งแตกต่างจาก Bitcoin ที่เน้นการทำธุรกรรมเพียงอย่างเดียว

2.1.3.1 Smart Contract

สัญญาอัจฉริยะ คือ โปรแกรมคอมพิวเตอร์ที่สามารถดำเนินการตามข้อตกลงโดยอัตโนมัติทันทีที่เกิดเหตุการณ์ตามเงื่อนไขในสัญญาซึ่งได้มีการระบุถึงเงื่อนไข หรือเหตุการณ์ดังกล่าวไว้ล่วงหน้าแล้ว โดยไม่ต้องมีคนกลาง นั่นคือหลักการสำคัญของสัญญาอัจฉริยะ ซึ่งได้ถูกคิดค้นขึ้นในปี 1994 โดย Nick Szabo

การนำสัญญาอัจฉริยะ หรือ Smart Contract มาใช้งานนั้นสามารถช่วยแก้ไขปัญหาความไม่ไว้วางใจกันระหว่างคู่สัญญา การฉ้อโกง และการบิดเบือนสัญญา อีกทั้งยังสามารถช่วย

แก้ปัญหาการตีความเนื้อหาในสัญญา ซึ่งมักจะเป็นข้อพิพาทระหว่างคู่สัญญาเสมอ ๆ เนื่องจากคู่สัญญาทั้งสองฝ่ายต่างตีความสัญญาคนละแบบ โดยในการใช้สัญญาอัจฉริยะบน Ethereum 1 ครั้ง จะต้องเสียค่าธรรมเนียมในการใช้งาน เรียกว่า ค่าธรรมเนียม Gas

2.2 งานที่เกี่ยวข้อง

2.2.1 Proof of Existence Using Blockchain

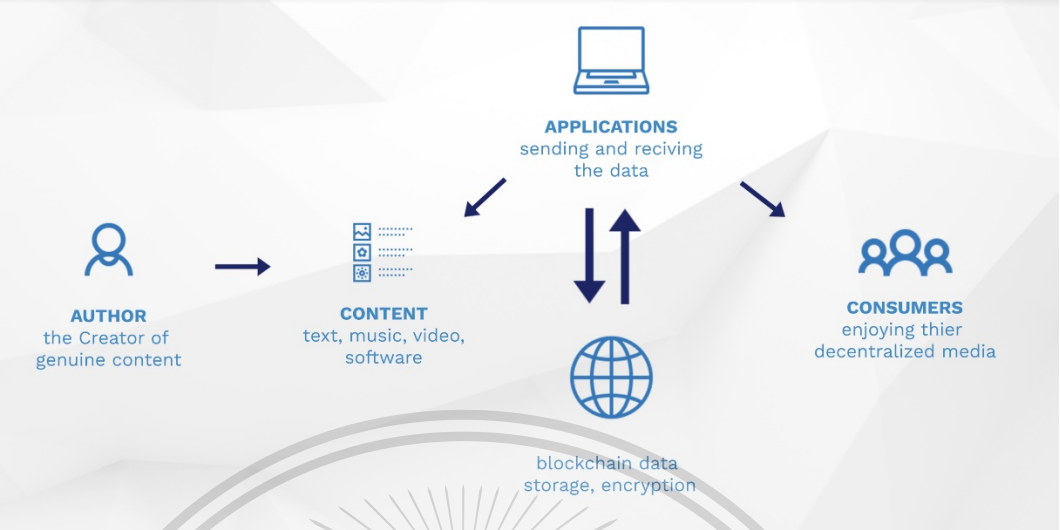
การพิสูจน์ถึงการมีอยู่จริงของเอกสารต่างๆ โดยหลักการคือ การเก็บข้อมูลโดยสรุปของเอกสารที่จะสามารถยืนยันถึงการมีอยู่จริงของเอกสารต้นฉบับได้ หรือที่เรียกว่า Cryptographic Digest รวมไปถึงเวลาที่จัดส่งเอกสาร ไปยังผู้รับซึ่งข้อมูล Cryptographic Digest ดังกล่าวจะถูกจัดเก็บลงใน Blockchain ดังนั้นผู้ใช้งานจะสามารถมั่นใจได้ว่าเอกสารที่ได้รับนั้นเป็นเอกสารที่ถูกต้องและเชื่อถือได้ อีกทั้งไม่จำเป็นต้องกังวลเกี่ยวกับความเป็นส่วนตัวเนื่องจากข้อมูลที่ถูกจัดเก็บลงใน Blockchain เป็นเพียงข้อมูลโดยสรุปของเอกสารที่สามารถยืนยันถึงการมีอยู่จริงของเอกสารต้นฉบับได้ และเวลาที่จัดส่งเอกสารไปยังผู้รับเท่านั้นไม่ใช่เอกสารต้นฉบับ

2.2.2 Provenance

ระบบที่ใช้ตรวจสอบรายละเอียดของสินค้าต่างๆว่าตรงกับที่ระบุไว้บนฉลากหรือไม่ เช่น ส่งมาจากที่ใด เพื่อให้ผู้บริโภคสามารถมั่นใจในสินค้าที่ตนเองซื้อมาได้ โดย Provenance นำคุณสมบัติของเทคโนโลยี Blockchain ที่เป็น Decentralized มาใช้ให้เกิดประโยชน์ นั่นคือ ข้อมูลจาก Provenance จะเป็นข้อมูลที่เชื่อถือได้ เพราะการจะแก้ไขข้อมูลใน Blockchain จากผู้ไม่หวังดี เป็นสิ่งที่แทบจะเป็นไปไม่ได้เลย

2.2.3 GoChain Intellectual Property

ระบบที่ใช้เก็บข้อมูลต่างๆของทรัพย์สินทางปัญญา เช่น เจ้าของผลงาน สังกัด วันเวลาที่วางขายผลงาน เพื่อใช้เป็นหลักฐานยืนยันความเป็นเจ้าของของผลงานต่างๆ และสามารถนำไปใช้เป็นหลักฐานในชั้นศาลหากมีข้อพิพาทเกี่ยวกับทรัพย์สินทางปัญญาเกิดขึ้น



รูป 2.5 ลำดับการทำงานของ GoChain Intellectual Property

2.3 เครื่องมือที่ใช้งานในการพัฒนาระบบ

2.3.1 React

คือ Javascript library ที่ถูกพัฒนาโดย Facebook ซึ่งออกแบบมาเพื่อสร้าง UI ให้กับ web application ซึ่งจะทำงานส่วนใหญ่เกี่ยวกับ view layer หัวใจหลักของ React นั้นคือ component การที่สร้าง component ขึ้นมาสามารถทำให้ reuse การใช้งานได้ และเมื่อประกอบกันหลาย component กลายเป็น UI ของ Web Application

React ใช้หลักการ Virtual DOM ในการทำงาน ทำให้มีประสิทธิภาพมากขึ้น เพราะหน้าเว็บที่เป็นแบบเก่านั้นจะใช้หลักการของ DOM ธรรมดาซึ่งจะเก็บข้อมูลในรูปแบบของ Tree ซึ่งหากมีข้อมูลจำนวนมาก จะทำให้จำนวนชั้น และ กิ่งมีจำนวนมาก หากต้องการอัพเดตข้อมูลในกิ่งใดจะทำได้ช้า แต่ Virtual DOM แทนที่จะเก็บข้อมูล โครงการ tag html แบบ DOM นั้นก็จะเก็บเป็น reference ของข้อมูลแทนทำให้สามารถอ้างอิงและ update ข้อมูลได้เร็วกว่า เหมือน tag div ที่ซ้อนกันหลายๆชั้น แทนที่จะเก็บข้อมูล div tag ทั้งหมดก็เก็บเพียงว่า มี div แบบใดซ้อนกันอย่างไร เมื่อจะ update ทำได้โดยอ้างอิง tag ที่ต้องการเปลี่ยน แล้วทำการ render มาเท่านั้นทำให้ประสิทธิภาพของ Virtual DOM เร็วกว่า DOM มาก

2.3.2 Express.js

Web framework ที่พัฒนาจาก NodeJs ที่มีขนาดเล็ก และมีความยืดหยุ่นมาพร้อมกับคุณลักษณะเด่นและความสามารถที่หลากหลาย สำหรับใช้ในการพัฒนาเว็บไซต์ หรือ Mobile app

ด้วยเครื่องมือสำหรับ HTTP method ที่มากมาย และ ฟังก์ชันมิดเดิลแวร์ที่ใช้งานง่ายทำให้สามารถสร้าง API ที่สมบูรณ์ได้สะดวกและรวดเร็ว

2.3.3 Web3.js

ชุดของ library ที่ใช้ติดต่อ node ใน Ethereum ด้วย HTTP, IPC, Web socket ซึ่งเป็น Javascript API ที่พัฒนาขึ้นโดย Ethereum เอง

2.3.4 Truffle

Environment สำหรับพัฒนาและทดสอบแอพพลิเคชั่นบน Ethereum Virtual Machine (EVM) โดย Truffle จะช่วยอำนวยความสะดวกในด้านต่างๆ เช่น

-Compile Smart contract

-Deploy Smart Contract

-Test Smart contract

ถือได้ว่าเป็นเครื่องมือพัฒนาแอพพลิเคชั่นบน Smart contract ที่ครอบคลุมทุกการใช้งานเลยทีเดียว

2.3.5 Ganache

Ganache เป็น Ethereum Blockchain บนเครื่องเราเอง ใช้สำหรับ deploy contract แบบ local โดย Ganache จะทำงานแบบ 1 Block / 1 Transaction ทำให้สามารถพัฒนา ทดสอบ Smart contract ได้รวดเร็วมาก ๆ เนื่องจากบางครั้งไม่จำเป็นต้อง Deploy ไปบน Test Network เพราะจะใช้เวลานาน และต้องใช้เงิน ETH ในการดำเนินการ

2.3.6 MetaMask

MetaMask เป็น Extension ที่สามารถทำงานร่วมกับ Web browser ต่าง ๆ ได้ เช่น Chrome, Firefox หรือ Brave เป็นต้น โดย MetaMask เป็น Ethereum wallet ใช้สำหรับบริหารจัดการ Ethereum และ Token บน Ethereum โดย MetaMask จะทำงานร่วมกับ Web3.js เพื่อติดต่อกับ Blockchain

เราสามารถเพิ่ม หรือสร้าง Ethereum Account บน MetaMask ได้ และเมื่อ DApp ต้องการจะทำธุรกรรมบน Account นั้นๆ ผู้ใช้งานจะต้องกดยืนยันในหน้าต่างของ MetaMask ก่อน เพื่อยืนยันการทำธุรกรรมนั้น อีกทั้ง MetaMask ยังถูกใช้เก็บ Key สำหรับใช้ในการ Deploy Smart Contract ไปบน Network ต่าง ๆ ได้อีกด้วย

บทที่ 3

การออกแบบและพัฒนา

3.1 ความต้องการของระบบ

3.1.1 Functional

1) สถานศึกษาสามารถเพิ่มใบประกาศนียบัตรออนไลน์เข้าในระบบได้
2) สามารถตรวจสอบได้ว่าใบประกาศนียบัตรออนไลน์ เป็นของจริงและมีความถูกต้องหรือไม่
3) สามารถเพิกถอนใบประกาศนียบัตรออนไลน์ได้
4) Third party Application สามารถใช้งานระบบ ภายใต้ข้อกำหนดของระบบหลัก

3.1.2 Non-Functional

1) ข้อมูลมีความปลอดภัย
2) ข้อมูลของใบประกาศนียบัตรจะไม่ถูกเก็บในระบบ เพื่อความเป็นส่วนตัวของข้อมูล

3.2 ภาพรวมของระบบ

ในการพัฒนาปริญญานิพนธ์นี้ ประกอบไปด้วยงานส่วนหลัก 3 ส่วน คือส่วนเว็บแอพพลิเคชั่นส่วน Front-end, เว็บแอพพลิเคชั่นส่วน API และ ส่วนของบล็อคเชน

3.2.1 เว็บแอพพลิเคชั่นส่วน Front-end

เป็นส่วนที่ใช้ติดต่อกับผู้ใช้งาน โดยจะแบ่งได้เป็น 4 ส่วนด้วยกัน คือ ส่วนเพิ่มใบประกาศนียบัตร, ส่วนตรวจสอบใบประกาศนียบัตร, ส่วนจับคู่ชื่อผู้ใช้งานกับ public key ของผู้ใช้งาน ,ส่วนเปลี่ยนสถานะใบประกาศนียบัตร โดยในส่วนนี้ ผู้จัดทำจะสร้าง Official App ของระบบ และเปิดโอกาสให้ผู้พัฒนาอื่นพัฒนา Third-party App เพื่อมาใช้ระบบได้ด้วย เนื่องจากปริญญานิพนธ์นี้เป็น Open source

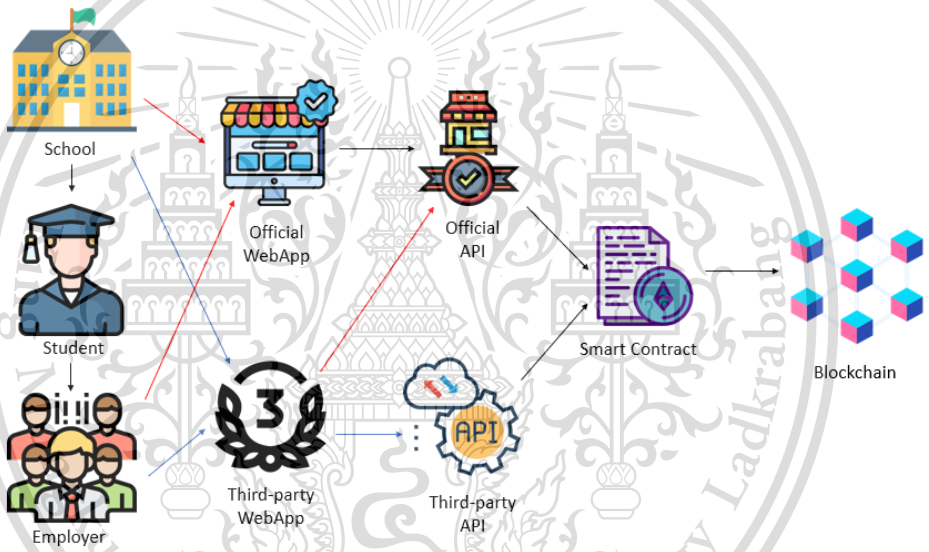
3.2.2 เว็บแอพพลิเคชั่นส่วน API

เป็นส่วนที่ใช้ติดต่อระหว่างส่วน Front-end และ Smart contract โดยจะแปลงข้อมูลที่ได้จากส่วน Front-end ให้เป็นข้อมูลที่พร้อมใช้งานบน Smart contract แล้วส่งไปยัง Smart contract โดย

ในส่วนนี้ ผู้จัดทำจะสร้าง Official App ของระบบ และเปิดโอกาสให้ผู้พัฒนาอื่นพัฒนา Third-party API เพื่อมาใช้ระบบได้ด้วย เนื่องจากปริญญานิพนธ์นี้เป็น Open source

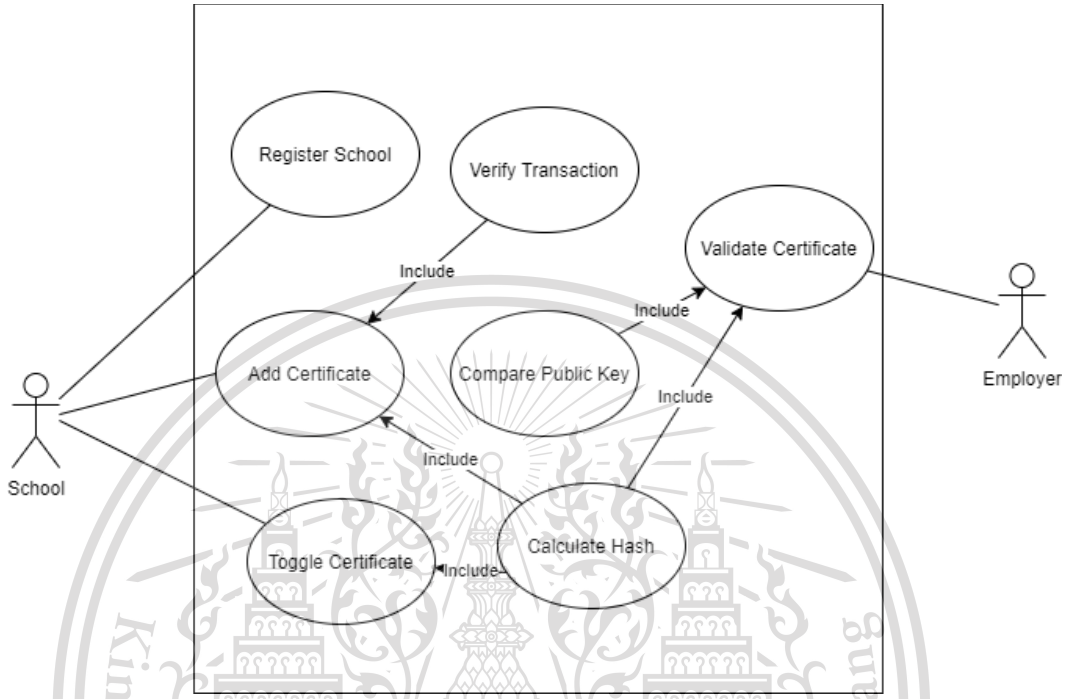
3.2.3 บล็อคเชนและ Smart contract

เป็นส่วนที่เก็บข้อมูล Hash ของใบประกาศนียบัตร วันที่เพิ่ม และเป็นส่วนที่ควบคุมกลไกในการตรวจสอบประกาศนียบัตรออนไลน์ทั้งหมด ประกอบด้วยฟังก์ชั่นหลักๆ 4 ฟังก์ชั่น คือ ส่วนเพิ่มใบประกาศนียบัตร, ส่วนตรวจสอบใบประกาศนียบัตร, ส่วนจับคู่ชื่อผู้ใช้งานกับ Public key ของผู้ใช้งาน, ส่วนเปลี่ยนสถานะใบประกาศนียบัตรโดยส่วนนี้จะเป็น Open source เพื่อให้ผู้พัฒนาอื่นสามารถพัฒนาแอพพลิเคชั่นมาใช้งานระบบได้



รูป 3.1 ภาพรวมของระบบ

3.3 Use case diagram



รูป 3.2 Use case diagram

ตาราง 3.1 Use case Add Certificate

Use case ID	UC-1
Use case Name	Add Certificate
Primary Actor	School
Description	เพิ่มไฟล์ประกาศนียบัตรออนไลน์
Pre-condition	นักเรียนจบคอร์สออนไลน์
Flow	1. สถาบัน Upload ไฟล์ประกาศนียบัตร 2. ระบบทำการคำนวณหา Hash 3. ระบบทำการตรวจสอบว่าข้อมูลนั้นถูกต้องหรือไม่
Post-condition	เพิ่ม Hash ของไฟล์ประกาศนียบัตรลงใน Blockchain

ตาราง 3.2 Use case Verify Transaction

Use case ID	UC-2
Use case Name	Verify Transaction
Primary Actor	-
Description	ตรวจสอบความถูกต้องของข้อมูล
Pre-condition	สถาบันเพิ่มไฟล์ประกาศนียบัตรออนไลน์
Flow	1. ทำการตรวจสอบว่า Private key นั้นอยู่ในรูปแบบที่ถูกต้องหรือไม่ 2. ตรวจสอบว่าไฟล์ประกาศนียบัตรมีขนาดไม่เล็กเกินไป และไม่ใหญ่เกินไป
Post-condition	-

ตาราง 3.3 Use case Calculate Hash

Use case ID	UC-3
Use case Name	Calculate Hash
Primary Actor	-
Description	คำนวณเลข Hash ของไฟลประกาศนียบัตร
Pre-condition	ไฟล์ประกาศนียบัตรถูก Upload
Flow	1. คำนวณ Hash ของไฟล์ประกาศนียบัตรด้วย Algorithm ที่กำหนด
Post-condition	-

ตาราง 3.4 Use case Compare Public key

Use case ID	UC-4
Use case Name	Compare Public key
Primary Actor	-
Description	เปรียบเทียบ Public key ที่ user ป้อนว่าตรงกับ Public key ที่ Blockchain ส่งมาหรือไม่
Pre-condition	Public key ถูกป้อนเข้าระบบ
Flow	1. เปรียบเทียบ Public key ที่ user ป้อนว่าตรงกับ Public key ที่ Blockchain ส่งมาหรือไม่
Post-condition	-

ตาราง 3.5 Use case Validate Certificate

Use case ID	UC-5
Use case Name	Validate Certificate
Primary Actor	Employer
Description	ตรวจสอบความถูกต้องและเป็นของจริงหรือไม่
Pre-condition	ต้องการตรวจสอบว่าใบประกาศนียบัตรนั้นถูกต้องและเป็นของจริง
Flow	1. สถานประกอบการ Upload ไฟล์ใบประกาศนียบัตร และแนบ Public key ของสถาบันการศึกษา 2. ระบบทำการคำนวณหา Hash 3. ส่งไปตรวจสอบว่ามีอยู่บน Blockchain หรือไม่ 4. หากมี ตรวจสอบว่า Address ของผู้ที่เพิ่มใบลงบน Blockchain ตรงกับ Address ที่แนบมาหรือไม่

ตาราง 3.6 Use case Validate Certificate(ต่อ)

Post-condition	รายงานผลการตรวจสอบไฟล์ใบประกาศนียบัตรออนไลน์

ตาราง 3.7 Use case Register School

Use case ID	UC-6
Use case Name	Register School
Primary Actor	School
Description	เพิ่ม Link ของหน้าสถาบันการศึกษาในการเข้าใช้งานครั้งแรก
Pre-condition	Login เข้าสู่ระบบ
Flow	1. โรงเรียน Login เข้าใช้งานเป็นครั้งแรก 2. โรงเรียนเพิ่ม Link ไปยังสถาบันของตนเอง 3. โรงเรียนสามารถเพิ่มใบประกาศนียบัตรได้
Post-condition	ปลดล็อกฟังก์ชั่นการเพิ่มใบประกาศนียบัตร

ตาราง 3.8 Use case Toggle Certificate

Use case ID	UC-7
Use case Name	Toggle Certificate
Primary Actor	School
Description	เปลี่ยนสถานะของใบประกาศนียบัตร (เพิกถอน หรือยกเลิกการเพิกถอน)
Pre-condition	Login เข้าสู่ระบบ
Flow	1. โรงเรียน Login เข้าใช้งาน 2. เลือกใช้ฟังก์ชั่นเพิกถอน/ยกเลิกการเพิกถอนใบประกาศนียบัตร 3. ใส่ confirmation text

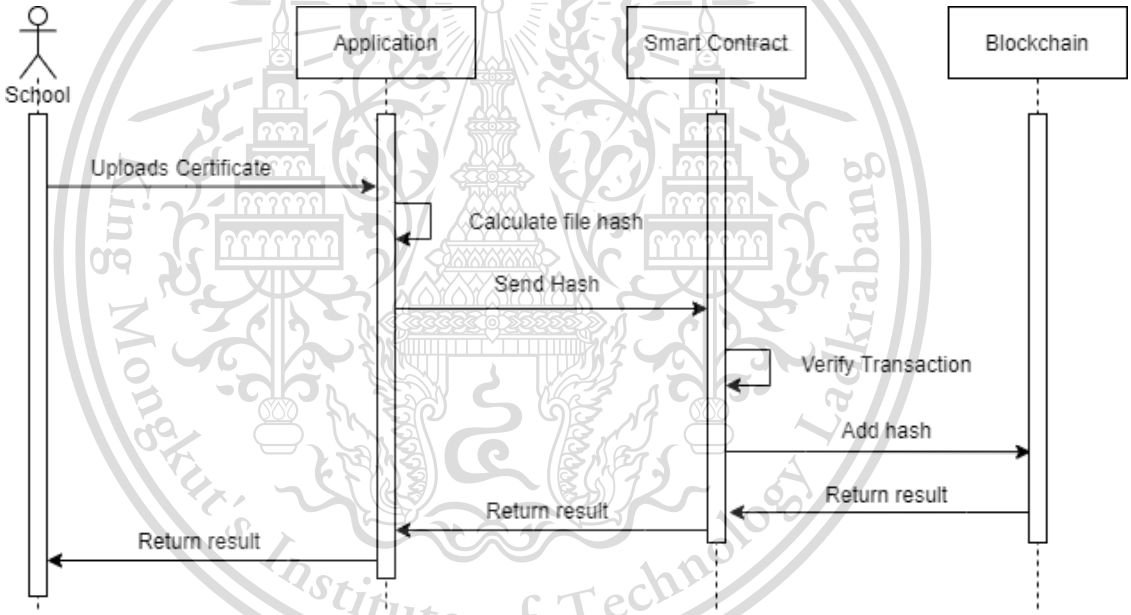
ตาราง 3.9 Use case Toggle Certificate(ต่อ)

Post-condition	ใบประกาศนียบัตรถูกเปลี่ยนสถานะ

3.4 กลไกการทำงาน

3.4.1 กลไกการทำงานของการเพิ่มใบประกาศนียบัตรออนไลน์

ในการเพิ่มใบประกาศนียบัตรลงในระบบนั้น ผู้ใช้ (สถาบันการศึกษาผู้ออกใบประกาศนียบัตร) จะต้อง Upload ใบประกาศนียบัตรไปยัง Web Application (ไม่ว่าจะเป็น Official App หรือ Third-party App ก็ตาม) แล้ว Web Application จะทำการคำนวณ Hash แล้วส่งค่า Hash ไปยัง Smart contract และ Blockchain เพื่อเพิ่มใบประกาศนียบัตรลงใน Blockchain ต่อไป

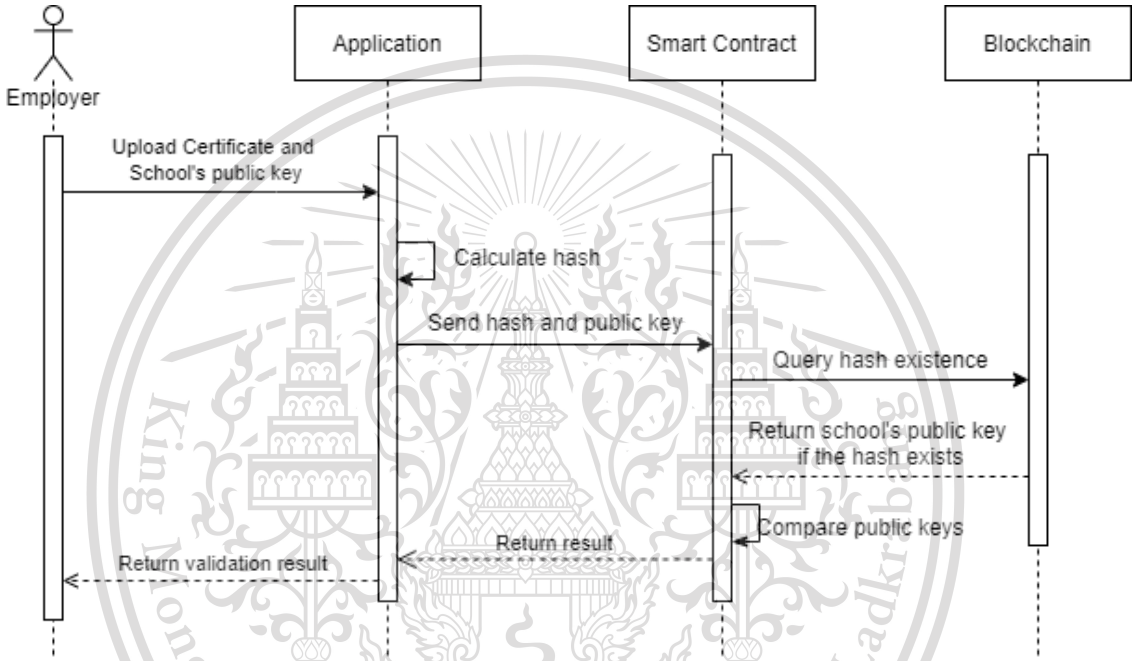


รูป 3.3 Sequence diagram ของการเพิ่มใบประกาศนียบัตรใหม่

3.4.2 กลไกการทำงานของการตรวจสอบใบประกาศนียบัตรออนไลน์

ในการตรวจสอบใบประกาศนียบัตร ผู้ใช้จะต้อง Upload ใบประกาศนียบัตร ที่ต้องการจะตรวจสอบ และกรอก Public key ของผู้เพิ่มใบประกาศนียบัตร(ผู้เพิ่ม จะต้องประกาศ Public key ของตัวเองให้ทราบโดยทั่วกัน) ไปยัง Web Application จากนั้น Web Application จะทำการคำนวณ Hash ของไฟล์ที่ Upload ไป แล้วส่ง Hash และ Public key ไปยัง Smart contract

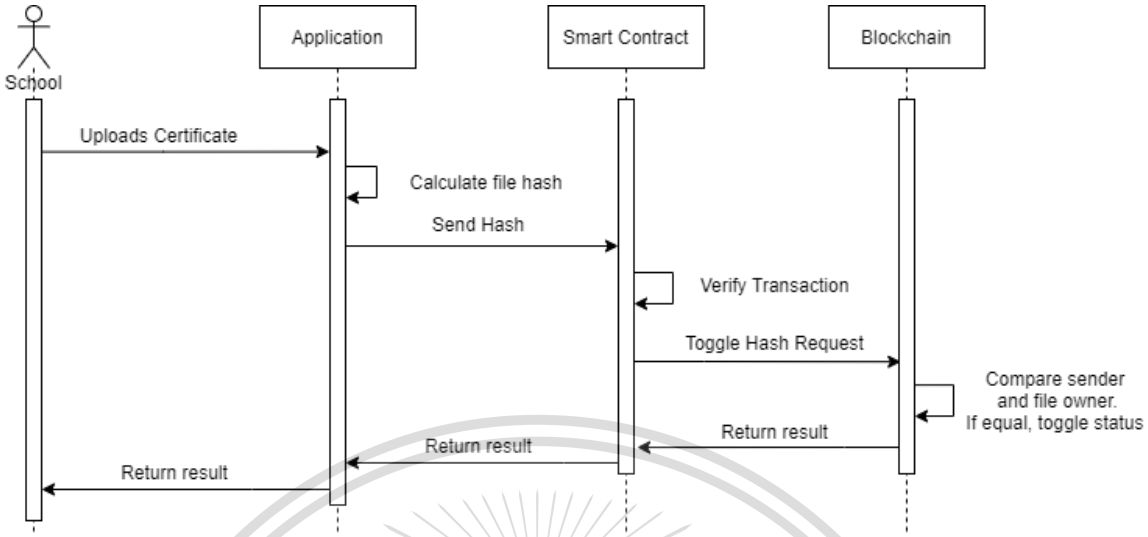
Smart contract จะทำการสอบถามไปยัง Blockchain ว่ามี Hash นั้นอยู่ใน Blockchain หรือไม่ หากมี Blockchain จะทำการส่งเลข Public key ของผู้เพิ่มไฟล์ กลับมายัง Smart contract จากนั้น Smart contract จะทำการเปรียบเทียบ Public key ที่ผู้ใช้กรอกเข้ามากับ Public key ที่ได้จาก Blockchain หากตรงกันจึงจะถือว่าใบประกาศนียบัตรออนไลน์ใบนั้นถูกต้อง และ ออกโดยผู้ที่ถูกกล่าวอ้างว่าเป็นผู้ออก ใบประกาศนียบัตรใบนั้นจริงๆ



รูป 3.4 Sequence diagram ของการตรวจสอบใบประกาศนียบัตรออนไลน์

3.4.3 กลไกการทำงานของการเปลี่ยนสถานะใบประกาศนียบัตร

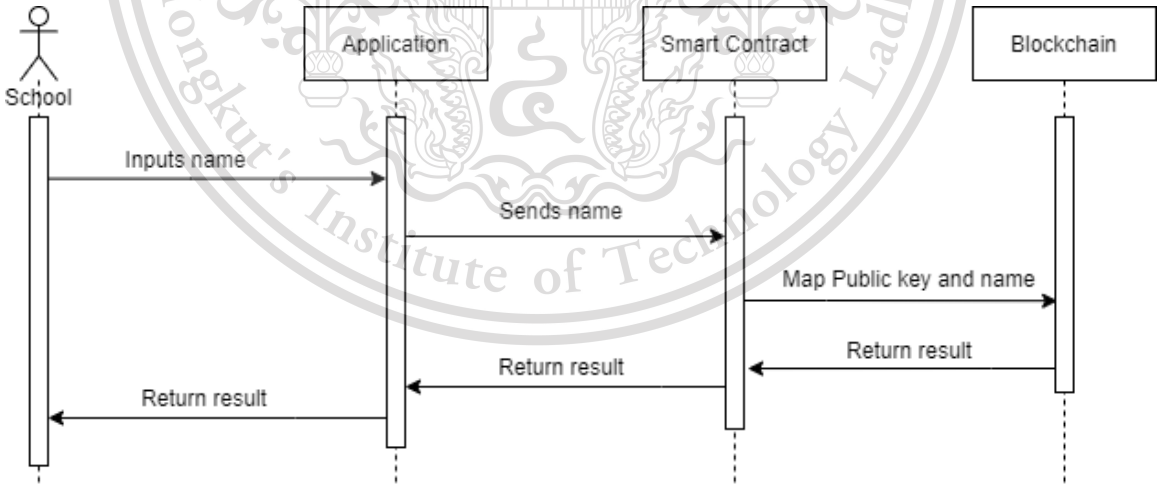
ในการเปลี่ยนสถานะใบประกาศนียบัตร ผู้ใช้จะต้องทำการ upload ไฟล์ใบประกาศนียบัตร และ Confirmation text(ชื่อไฟล์ที่ upload เข้ามา) หาก Confirmation text ตรงกับชื่อไฟล์ ระบบจะทำการคำนวณ hash ของไฟล์ แล้วทำการส่งไปยัง Smart Contract เพื่อ query public key ของผู้เพิ่มใน Blockchain หากตรงกับ Public key ของผู้ที่เป็นคนทำการเรียกใช้ฟังก์ชั่นเปลี่ยนสถานะใบประกาศนียบัตร ระบบจะทำการเปลี่ยนสถานะของใบประกาศนียบัตรบน Blockchain



รูป 3.5 Sequence diagram ของการเปลี่ยนสถานะใบประกาศนียบัตรออนไลน์

3.4.4 กลไกการทำงานของการจับคู่ชื่อผู้ใช้งานกับ Public key ของผู้ใช้งาน

เมื่อผู้ใช้ทำการเรียกใช้ฟังก์ชั่นจับคู่ชื่อผู้ใช้งานกับ Public key ของผู้ใช้งาน ส่วน Web Application จะทำการส่ง Public key และชื่อที่ผู้ใช้งานกรอกเข้ามาไปยัง Blockchain เพื่อเปลี่ยนข้อมูลส่วนชื่อผู้ใช้



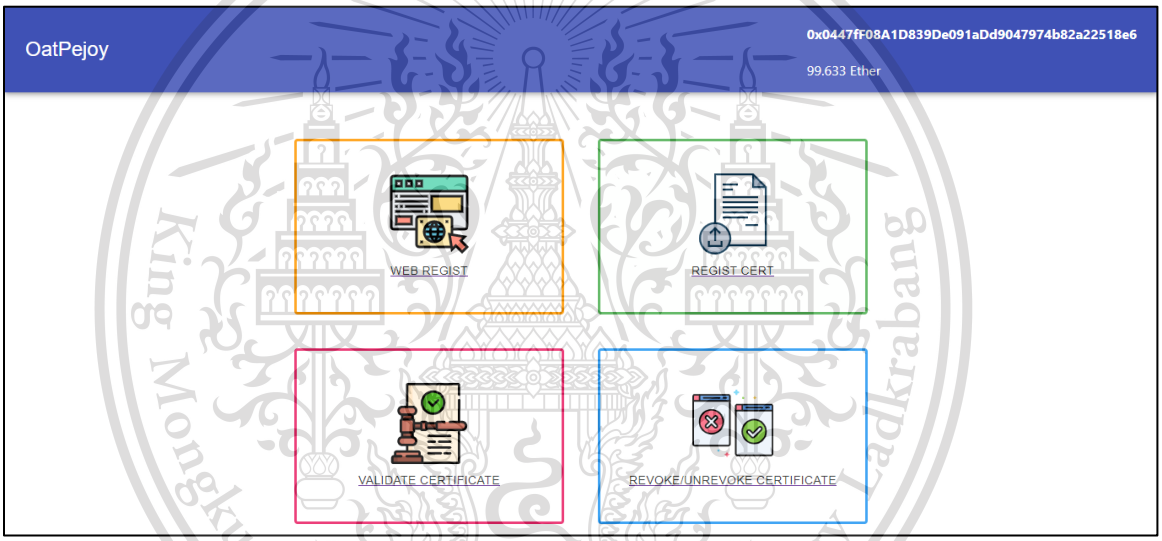
รูป 3.6 Sequence diagram ของการจับคู่ชื่อผู้ใช้งานกับ Public key ของผู้ใช้งาน

3.5 ส่วนติดต่อผู้ใช้งาน

ระบบรับรองใบประกาศนียบัตรออนไลน์นี้ เป็น Open source ซึ่งผู้พัฒนาอื่นสามารถพัฒนาหน้า Web Application ขึ้นเองได้เช่นกัน ในที่นี่จะพูดถึง Official Applicationที่ผู้ทำปริญญานิพนธ์เป็นผู้พัฒนาขึ้นเอง โดยสามารถแบ่งได้เป็น 5 ส่วน ดังนี้

3.5.1 เมนูหลัก

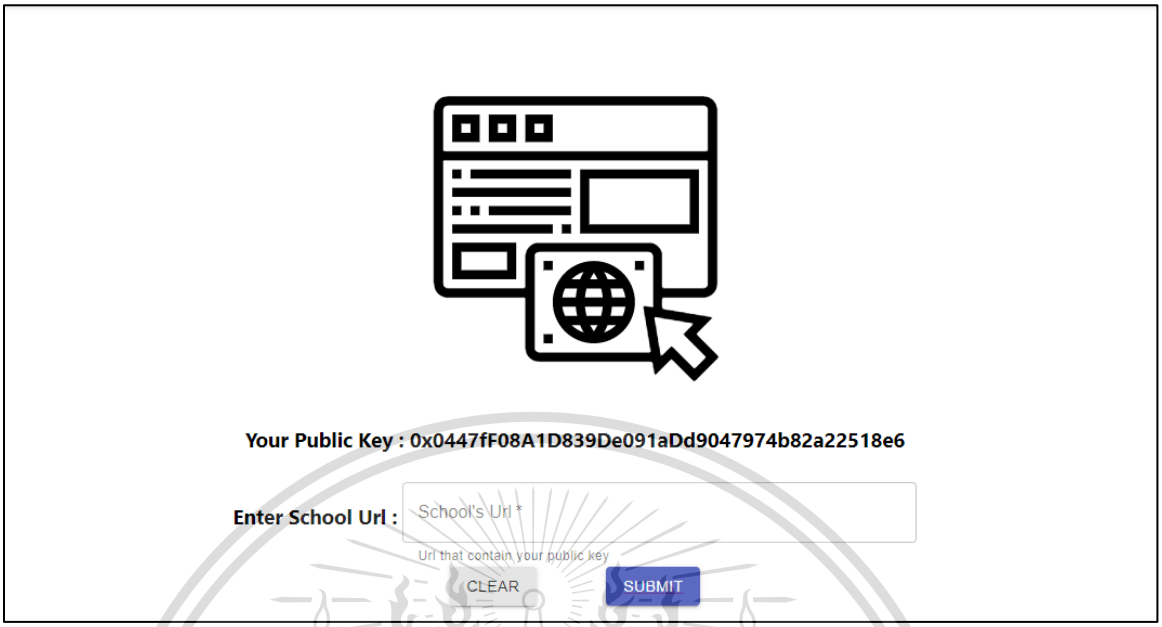
หน้าหลักที่มีปุ่มเชื่อมโยงไปหน้าการทำงานต่างๆ อันประกอบไปด้วยลงทะเบียนชื่อสถานศึกษา เพิ่มใบประกาศนียบัตร ตรวจสอบใบประกาศนียบัตร และ เปลี่ยนสถานะใบประกาศนียบัตร



รูป 3.7 เมนูหลัก

3.5.2 หน้าลงทะเบียนชื่อสถานศึกษา

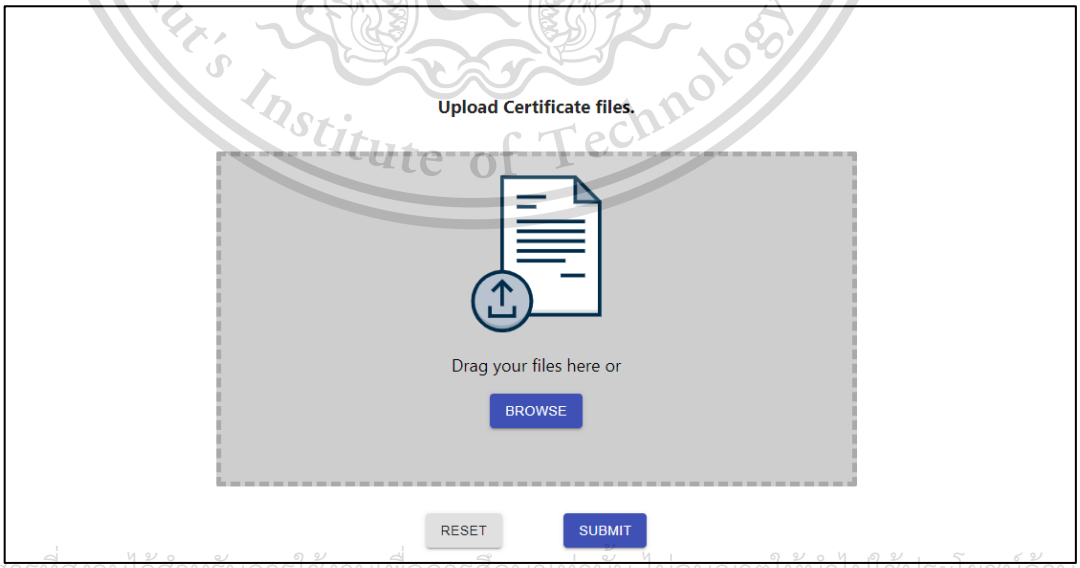
ก่อนที่จะสามารถเพิ่มใบประกาศนียบัตรไปยังระบบ สถานศึกษาจำเป็นจะต้องลงทะเบียนสถานศึกษาก่อน โดยกรอก URL ของสถานศึกษาตนเอง ฟังก์ชั่นนี้จะช่วยอำนวยความสะดวกให้แก่ผู้ที่มาตรวจสอบใบประกาศนียบัตร โดย เมื่อตรวจสอบใบประกาศนียบัตรแล้วผ่าน ระบบจะแสดง URL ของสถานศึกษาให้ผู้ใช้งานทราบด้วย



รูป 3.8 หน้าลงทะเบียนชื่อสถานศึกษา

3.5.3 หน้าเพิ่มใบประกาศนียบัตรออนไลน์

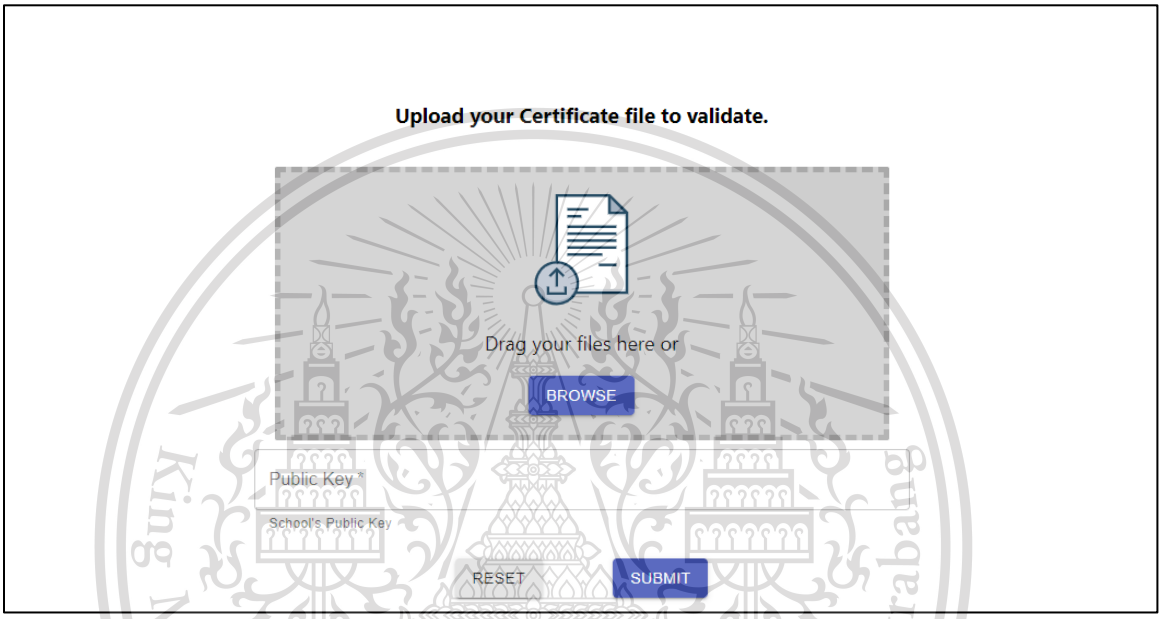
จะใช้หน้านี้ได้ก็ต่อเมื่อลงทะเบียนสถานศึกษาเรียบร้อยแล้ว หน้านี้จะเป็นหน้าที่ใช้สำหรับเพิ่มใบประกาศนียบัตรลงในระบบ โดยสามารถทำได้ทั้งแบบ Drag and drop และแบบกดปุ่ม Upload เมื่อเพิ่มใบประกาศนียบัตรเรียบร้อยแล้ว จะมีข้อความแจ้งผู้ใช้งานว่าเพิ่มสำเร็จ



รูป 3.9 หน้าเพิ่มใบประกาศนียบัตรออนไลน์

3.5.4 หน้าตรวจสอบใบประกาศนียบัตรออนไลน์

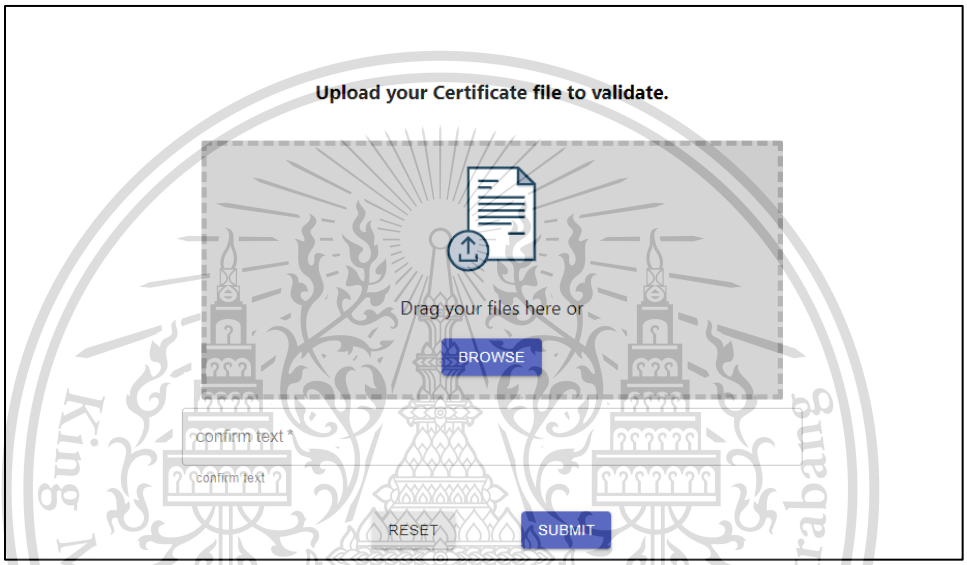
หน้านี้จะเป็นหน้าที่ใช้สำหรับตรวจสอบใบประกาศนียบัตร โดยผู้ใช้จะต้องกรอก Public key ของสถานศึกษา และ Upload ไฟล์ใบประกาศนียบัตรซึ่งสามารถทำได้ทั้งแบบ Drag and drop และแบบกดปุ่ม Upload เมื่อผู้ใช้กดปุ่ม Submit หน้าเว็บจะแจ้งผลการตรวจสอบ



รูป 3.10 หน้าตรวจสอบใบประกาศนียบัตรออนไลน์

3.5.5 หน้าเปลี่ยนสถานะใบประกาศนียบัตร

หน้านี้จะใช้สำหรับเพิกถอนใบประกาศนียบัตร หรือ ยกเลิกการเพิกถอนใบประกาศนียบัตร โดยจะต้องใส่ Confirm text เพื่อยืนยันการทำรายการ ผู้ที่จะทำการเปลี่ยนสถานะของใบประกาศนียบัตรได้ จะต้องใช้ account เดียวกันกับ account ที่เพิ่มใบประกาศนียบัตรใบนั้นๆเข้ามาเท่านั้น



รูป 3.11 หน้าดูประวัติการเพิ่มใบประกาศนียบัตรออนไลน์

บทที่ 4

การทดลองและผลการทดลอง

ในการพัฒนาระบบรับรองและตรวจสอบใบประกาศนียบัตรออนไลน์ด้วยเทคโนโลยีบล็อคเชนนั้น มีอยู่ 3 ส่วนที่ทางผู้พัฒนาได้ดำเนินการไปแล้วและมีผลการทดลอง ดังนี้

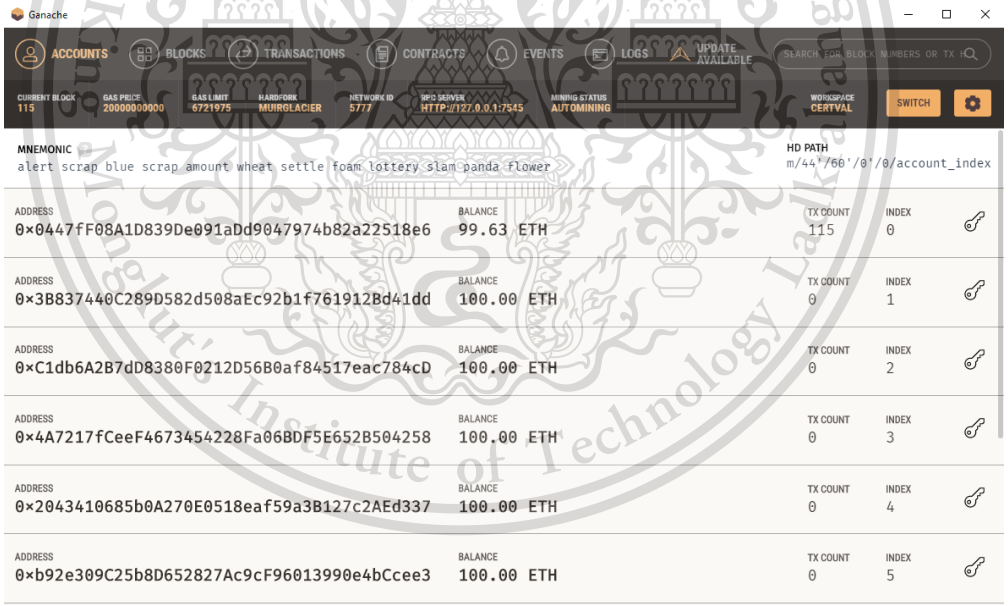
4.1 การสร้าง Blockchain สำหรับทดสอบ(Test Network)

4.1.1 วัตถุประสงค์

สร้างระบบ Blockchain แบบ Testnet เพื่อใช้ในการพัฒนาและทดสอบ Smart Contract

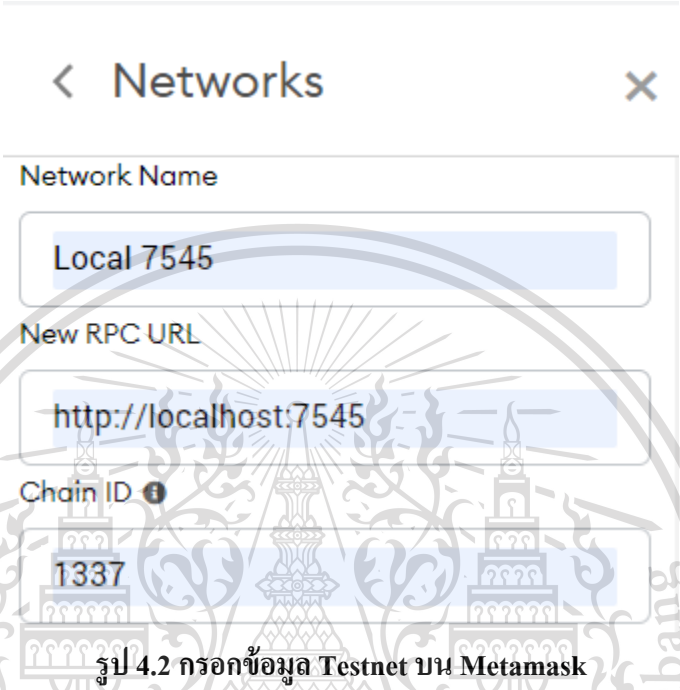
4.1.2 วิธีการทดลอง

1) สร้าง Testnet ด้วยโปรแกรม Ganache



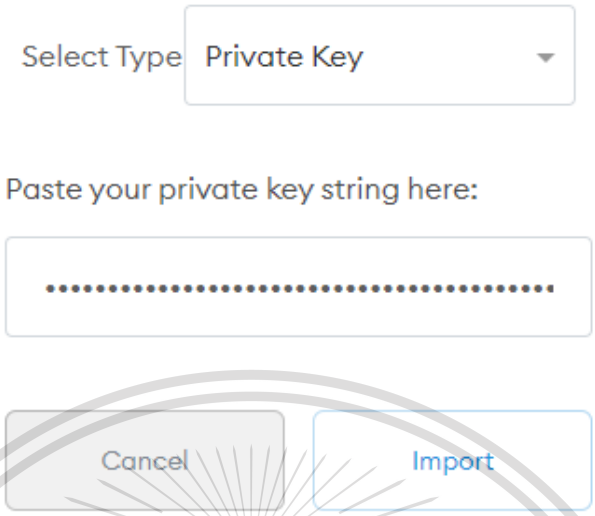
รูป 4.1 หน้าโปรแกรม Ganache

2) ทดสอบการเชื่อมต่อไปยัง Testnet ด้วย Metamask โดยการกรอกข้อมูลของ Testnet ให้ครบถ้วน รวมถึงกรอกข้อมูล Private key ของ Account



รูป 4.2 กรอกข้อมูล Testnet บน Metamask

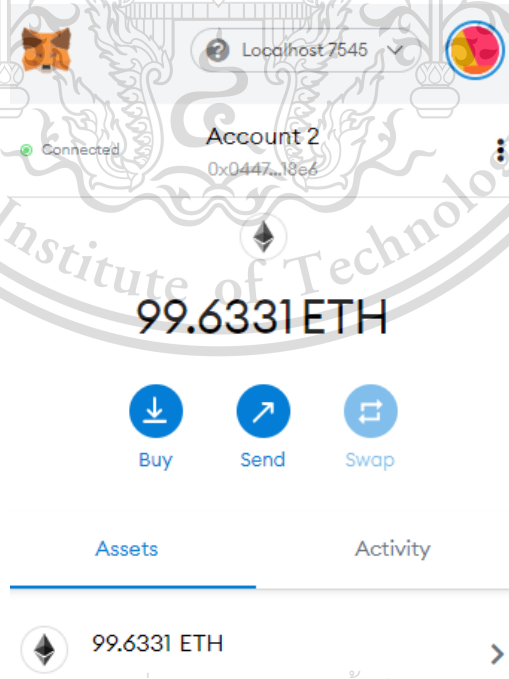
รูป 4.3 หน้าข้อมูล account บน Ganache



รูป 4.4 หน้าเพิ่ม account บน Metamask

4.1.3 ผลการทดลอง

เชื่อมต่อไปยัง Testnet สำเร็จ เห็นได้จากข้อมูลของ account ที่ปรากฏขึ้นบนโปรแกรม Metamask



รูป 4.5 ข้อมูล account บน Metamask

4.2 การ Deploy Smart Contract บน Testnet

4.2.1 วัตถุประสงค์

Deploy Smart Contract ที่พัฒนาแล้วไปยัง Testnet เพื่อเรียกใช้งานต่อไป

4.2.2 วิธีการทดลอง

1) คอมไพล์ Smart Contract ด้วยคำสั่ง truffle compile
2) Deploy Smart Contract

4.2.3 ผลการทดลอง

รูป 4.6 Deploy Smart Contract ลงใน Account ที่สร้างโดยโปรแกรม Ganache

4.3 ทดลองใช้ API

4.3.1 วัตถุประสงค์

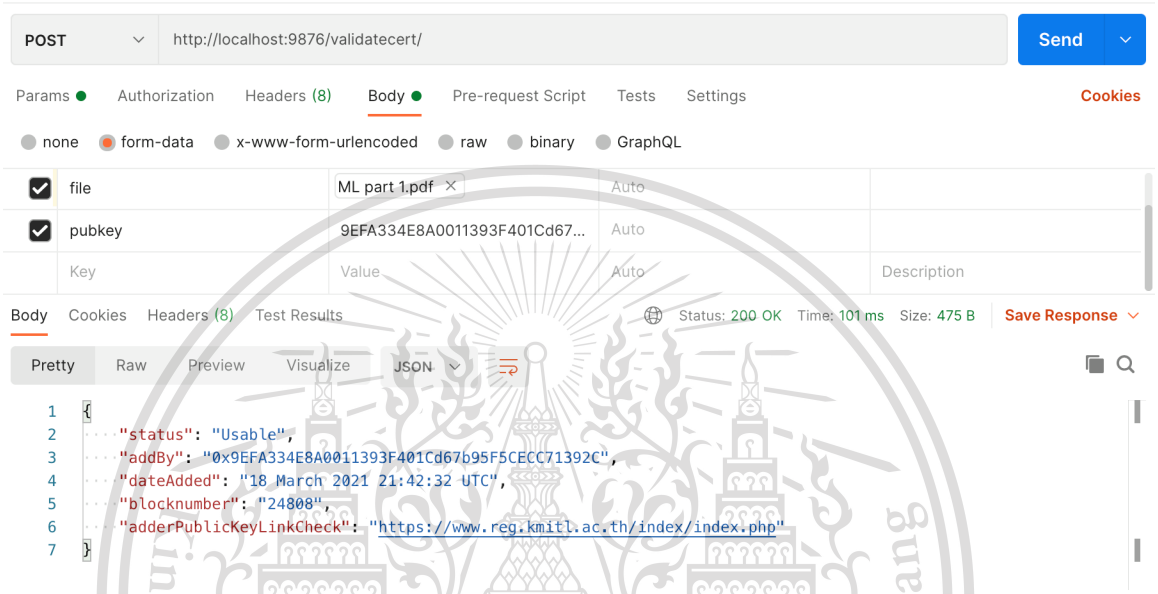
ทดลองใช้ API ผ่านโปรแกรม POSTMAN

4.3.2 วิธีการทดลอง

1) Run API ด้วยคำสั่ง nodemon app.js
2) เรียกใช้ฟังก์ชั่นต่างๆบน API ผ่านโปรแกรม POSTMAN

4.3.3 ผลการทดลอง

เมื่อทดลองเรียกใช้ฟังก์ชั่น validatecert โดยมี Request Parameter เป็นไฟล์ และ Public key จะได้ผลลัพท์เป็นข้อมูลการตรวจสอบใบประกาศนียบัตร



รูป 4.7 การเรียกใช้และผลลัพธ์การเรียกใช้ฟังก์ชัน validatecert ของ API

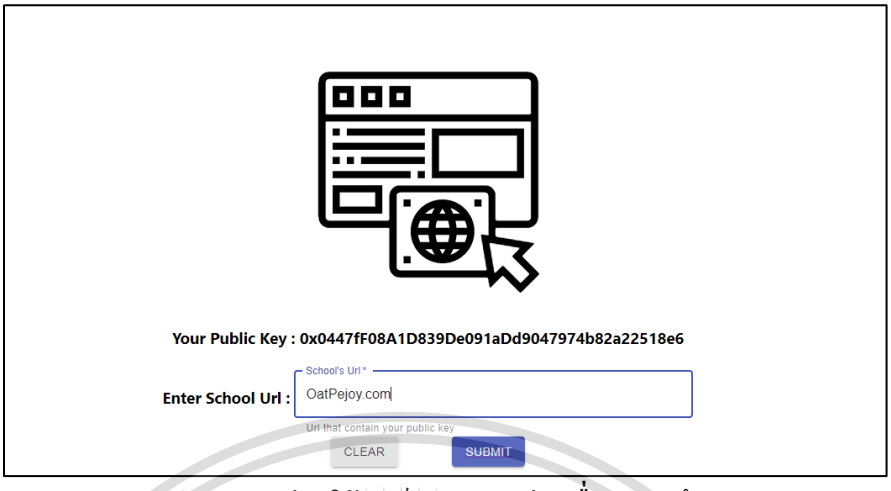
4.4 ทดลองใช้ Official Web Application

4.4.1 วัตถุประสงค์

ทดลองใช้ Official Web Application ที่ใช้งานผ่าน Front-end โดยมี API และ Blockchain ทำงานอยู่เบื้องหลัง

4.4.2 วิธีการทดลอง

1) Run Web Application ส่วน Client ด้วยคำสั่ง npm start
2) ทดลองใช้ฟังก์ชั่นลงทะเบียนชื่อสถานศึกษา

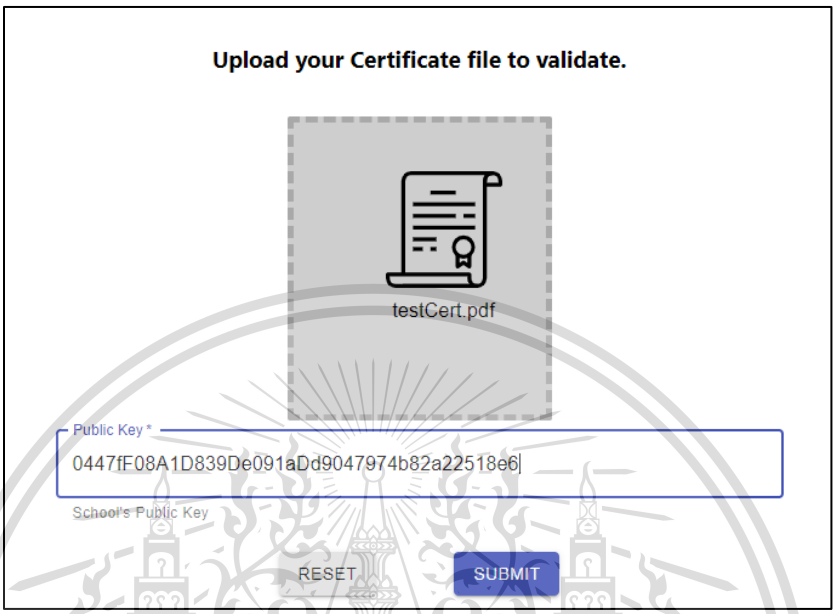


รูป 4.8 การเรียกใช้ฟังก์ชันลงทะเบียนชื่อสถานศึกษา

3) ทดลองใช้ฟังก์ชั่นเพิ่มใบประกาศนียบัตร

รูป 4.9 การเรียกใช้ฟังก์ชันเพิ่มใบประกาศนียบัตร

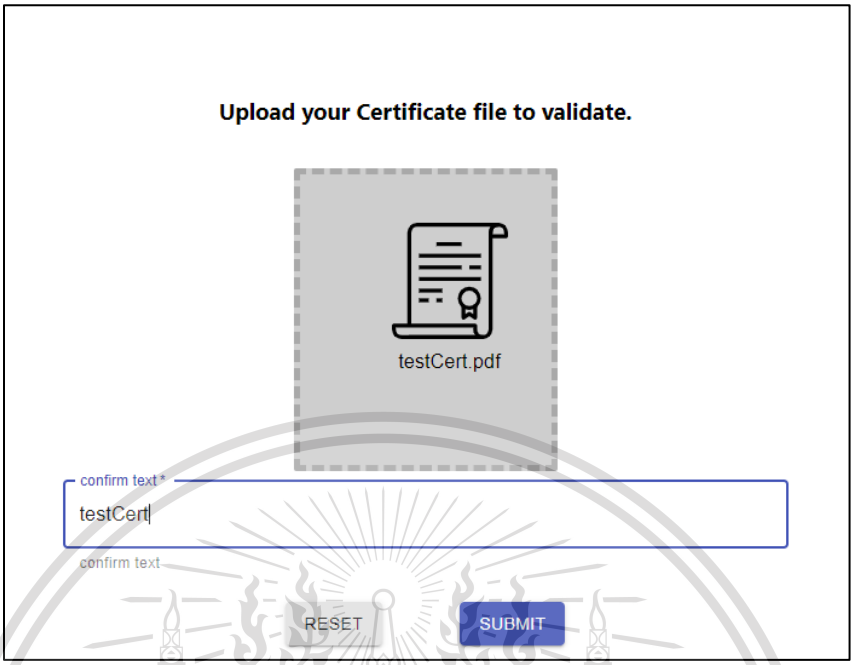
4) ทดลองใช้ฟังก์ชั่นตรวจสอบใบประกาศนียบัตร



รูป 4.10 การเรียกใช้ฟังก์ชันตรวจสอบใบประกาศนียบัตร

5) ทดลองตรวจสอบใบประกาศนียบัตรที่ไม่เคยถูกเพิ่มเข้าในระบบ

6) ทดลองใช้ฟังก์ชั่นเพิกถอนใบประกาศนียบัตร

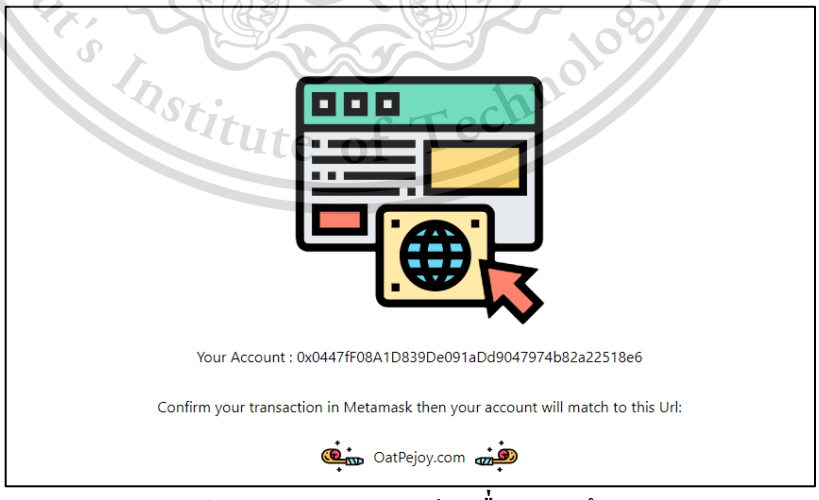


รูป 4.11 การเรียกใช้ฟังก์ชันเพิกถอนใบประกาศนียบัตร

7) เรียกใช้ฟังก์ชั่นตรวจสอบใบประกาศนียบัตรเพื่อตรวจสอบใบประกาศนียบัตรที่ถูกเพิกถอนอีกครั้ง

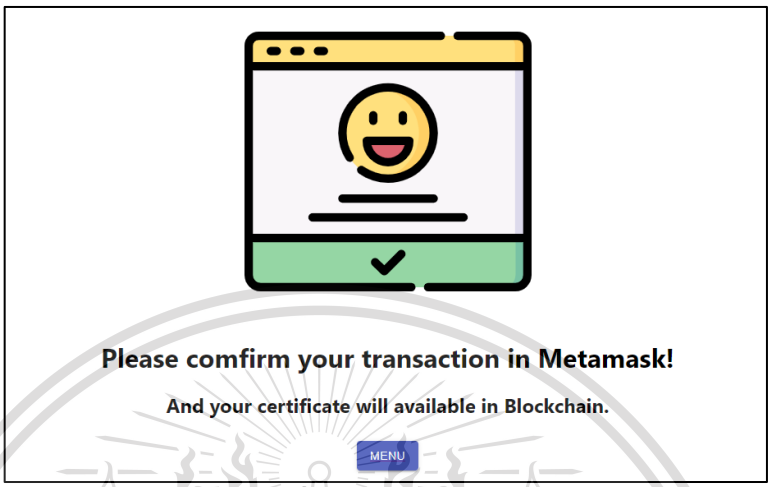
4.4.3 ผลการทดลอง

1) เมื่อลงทะเบียนชื่อสถานศึกษาสำเร็จ จะแสดงหน้าเว็บแสดงผลสำเร็จ



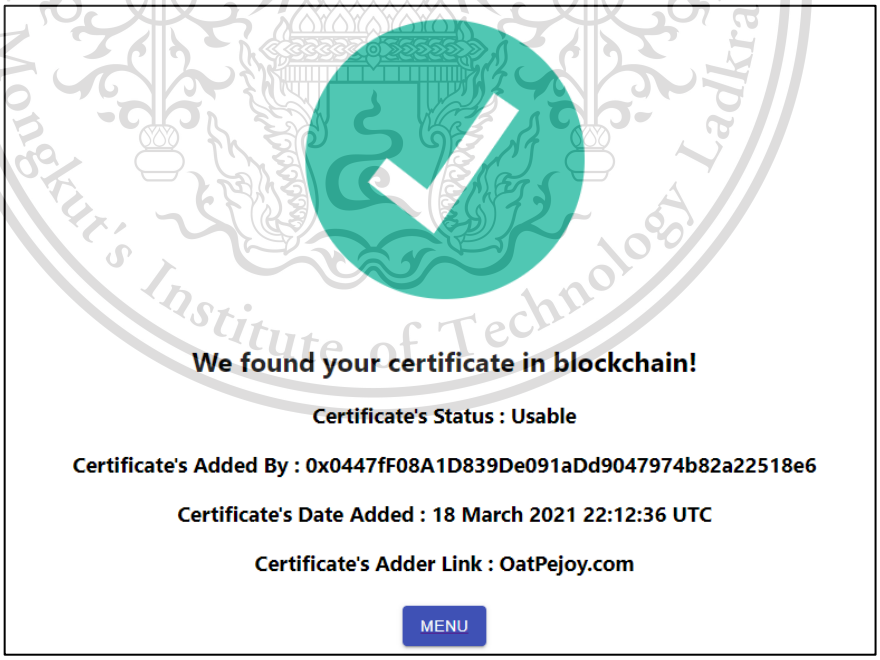
รูป 4.12 ผลการลงทะเบียนชื่อสถานศึกษา

2) เมื่อเพิ่มใบประกาศนียบัตรสำเร็จ จะแสดงหน้าเว็บแสดงผลสำเร็จ

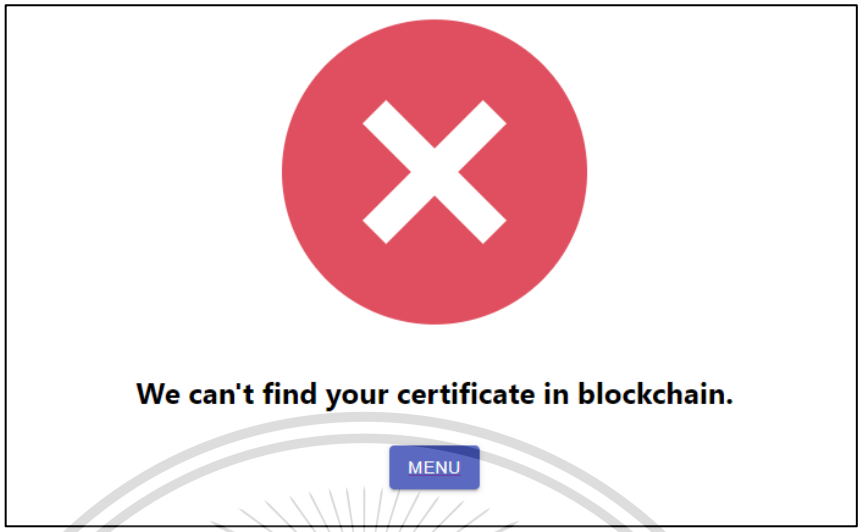


รูป 4.13 ผลการเพิ่มใบประกาศนียบัตรลงในระบบ

3) แสดงผลตรวจสอบไฟล์ใบประกาศนียบัตร

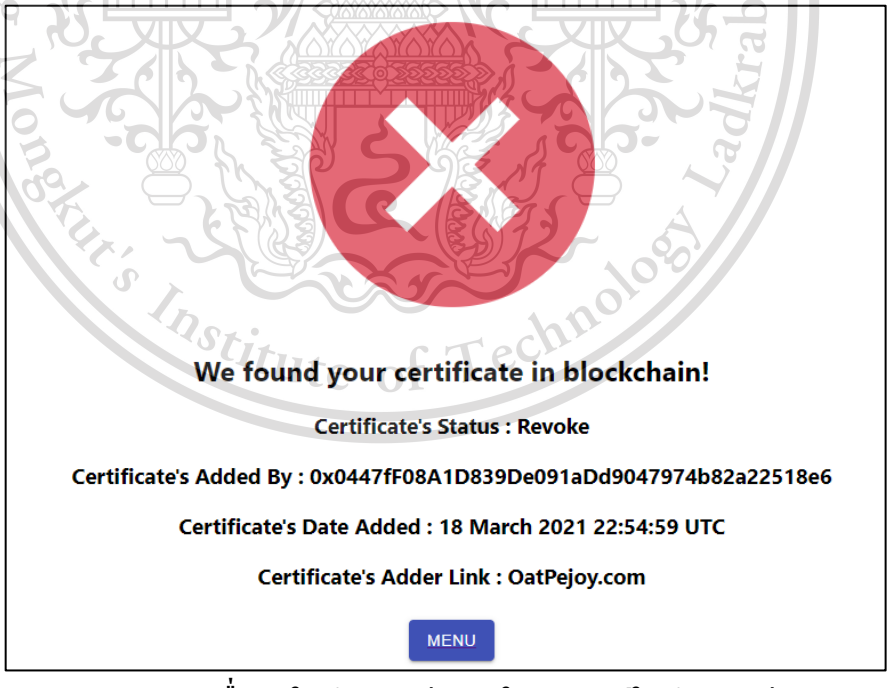


รูป 4.14 ผลการตรวจสอบเมื่อพบใบประกาศนียบัตรในระบบ



รูป 4.15 ผลการตรวจสอบเมื่อไม่พบใบประกาศนียบัตรในระบบ

4) หากใบประกาศนียบัตรถูกเพิกถอน เมื่อตรวจสอบจะพบใบประกาศนียบัตร แต่สถานะจะแจ้งว่าถูกเพิกถอน



รูป 4.16 ผลการตรวจสอบเมื่อพบใบประกาศนียบัตรในระบบแต่ใบประกาศนียบัตรถูกเพิกถอน

บทที่ 5
สรุปผลการทดลอง

5.1 บทสรุป

จากการที่ได้ทำการพัฒนาระบบรับรองและยืนยันใบประกาศนียบัตรออนไลน์ด้วยเทคโนโลยีบล็อคเชนโดยการทำงานติดต่อกันระหว่างเว็บแอปพลิเคชันแบบทางการที่ทางผู้พัฒนาได้จัดทำขึ้นมาเองกับ Smart Contract นั้นสามารถทำการติดต่อกันได้เป็นอย่างดี สามารถตอบกลับผลลัพธ์การทำงานต่าง ๆได้ครบถ้วนทุกฟังก์ชันที่ออกแบบไว้ได้ ทั้งนี้จะสามารถใช้งานได้ผ่าน Web Browser ที่สามารถติดตั้งส่วนขยาย Crypto Wallet เช่น Metamask ได้เท่านั้น

ในส่วนของ API จากที่ได้ทำการทดลองใช้งานผ่าน Postman ก็สามารถตอบกลับผลลัพธ์ได้ถูกต้องเช่นเดียวกันกับผลลัพธ์ที่เรียกผ่านเว็บแอปพลิเคชั่นแบบทางการที่ทางผู้พัฒนาได้จัดทำขึ้นมาเอง หากมีผู้ที่ต้องการจะพัฒนาหน้าเว็บไซต์ส่วนแสดงผลเองแล้วต้องการที่ใช้งานส่วน API สำหรับทำ Transaction กับ Smart Contract นั้นก็จำเป็นจะต้องส่งข้อมูลตามรูปแบบและข้อมูลที่จำเป็นสำหรับการเรียกใช้งานในแต่ละฟังชันก์นั้นๆมาเอง เนื่องจากไม่ได้ใช้งาน Wallet แบบเป็นส่วนขยายเหมือนกับเว็บแอปพลิเคชันแบบทางการที่ทางผู้พัฒนาได้จัดทำขึ้นมา ซึ่งจำเป็นต้องมีการส่งข้อมูลที่เป็นความลับ และสร้างความเสียหาย หากขั้นตอนการติดต่อมาเกิดรั่วไหลหรือถูกดักขโมยข้อมูลจากผู้ไม่ประสงค์ดีได้ ทั้งนี้ทางผู้ใช้ที่จะพัฒนาส่วนหน้าเว็บแอปพลิเคชั่นจะต้องทำการป้องกันในส่วนนี้เอง

5.2 ปัญหาและอุปสรรค

1) ในส่วนของเว็บแอปพลิเคชันแบบทางการที่ทางผู้พัฒนาได้จัดทำขึ้นมาเองนั้นจะมีการแสดงผลเมื่อผู้ใช้งานดำเนินการที่หน้าเว็บสำเร็จแต่ไม่สามารถยืนยันได้ว่าการดำเนินการส่วน Smart Contract จะสำเร็จเนื่องจากได้ใช้ Metamask เป็น Wallet ดังนั้นส่วนที่ดำเนินการกับ Smart Contract จึงไปอยู่ที่ Metamask ซึ่งผู้จัดทำไม่สามารถจัดการผลการทำงานของ Metamask ได้ หากผู้ใช้งานยกเลิกการทำ Transaction ที่ Metamask การดำเนินการนั้น ๆก็จะไม่สำเร็จเช่นกัน
2) ในส่วนของ API ปัญหาจะอยู่ที่ความปลอดภัยในการส่งข้อมูลเข้ามาติดต่อกับ API ซึ่ง ในบางฟังก์ชันนั้นจะต้องส่ง Private Key เข้ามาทำงานเพื่อยืนยัน Transaction ดังนั้นหากมีการรั่วไหลหรือถูกดักขโมยข้อมูลโดยผู้ไม่ประสงค์ดีในระหว่างการส่ง จะเป็นผลเสียต่อทางโรงเรียนหรือสถาบันหรือหน่วยงานใดๆที่เป็นเจ้าของบัญชีนั้นอย่างร้ายแรง ทั้งนี้การป้องกันนี้ทางผู้ใช้งาน

จะต้องทำการรับมือเอง โดยอาจใช้งาน https กับเว็บแอปพลิเคชันของโรงเรียนหรือสถาบันหรือหน่วยงานนั้นๆเพื่อทำการเข้ารหัสข้อมูลก่อนจะติดต่อเข้ามาใช้งาน API

5.3 แนวทางในการพัฒนาต่อ

1) เทคนิคในการพัฒนาส่วนหน้าการแสดงผลในการแสดงตามเงื่อนไขต่างๆให้ดีกว่านี้ ซึ่งทางผู้พัฒนาไม่มีความชำนาญมากพอในการจัดทำ
2) การพัฒนา Smart Contract นั้นอาจสามารถเพิ่มเงื่อนไขในการทำงานเพื่อเพิ่มความปลอดภัยในการใช้งานได้
3) ปริญญานิพนธ์ชิ้นนี้ได้ลองประยุกต์ใช้งานกับใบประกาศนียบัตรออนไลน์เท่านั้น แต่สามารถนำไปต่อยอดกับเอกสารใดๆที่เก็บเป็นแบบดิจิตัลมาใช้ประยุกต์ใช้งานเข้าด้วยได้

บรรณานุกรม

ดร.มณฑา ชยากรวิกรม,เกียรติศักดิ์ วงศ์ประเสริฐ,สมมนัส เกตุผ่อง,ชฎิล อินทระนก และสถาพน พัฒนะคูหา. 2562. **Blockchain For Government Services การใช้เทคโนโลยีบล็อกเชนสำหรับภาครัฐ.** กรุงเทพฯ : สำนักงานพัฒนารัฐบาลดิจิทัล (องค์การมหาชน).

Provenance. 2015. **Provenance White Paper.** [online].
Available : https://www.provenance.org/whitepaper

Chulapat Amatachaya. 2020. **Cryptography 101.** [online].
Available : https://p3j0y.medium.com/cryptography-101-c8606c0b2f58

PoEx Co., Ltd. 2020. **Proof of existence.** [online].
Available : http://docs.proofofexistence.com

Marie Gonzalez. 2019. **Using Blockchain to Protect Artists and Manage Intellectual Property Law.** [online].
Available:https://medium.com/gochain/using-blockchain-to-protect-artists-and-manage-intellectual-property-law-124b5774ea8f

Margaret Rouse. 2020. **Digital Signature.** [online].
Available : https://searchsecurity.techtarget.com/definition/digital-signature

ภาคผนวก ก

สัญญาอัจฉริยะ

สัญญาอัจฉริยะ(Smart Contract) ถูกพัฒนาด้วยภาษา Solidity และถูก Deploy บนเครือข่ายทดลอง Infura Rinkeby

ก.1 ซอร์สโค้ดสัญญาอัจฉริยะ

สามารถเข้าถึงซอร์สโค้ดสัญญาอัจฉริยะได้ที่

https://github.com/Krow18D/DigitalCertValidate/blob/main/contracts/Poe.sol

ก.2 ที่อยู่ของสัญญาอัจฉริยะ

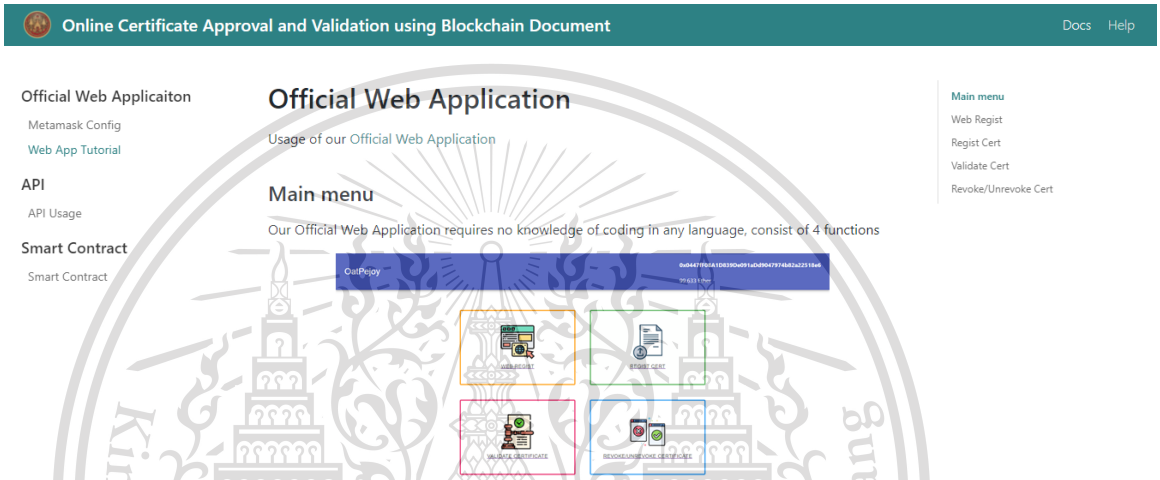
ผู้ใช้สามารถนำซอร์สโค้ดสัญญาอัจฉริยะจาก URL ในข้อ ก.1 ไปทำการ Deploy เองได้ หรือสามารถเรียกใช้สัญญาอัจฉริยะที่ผู้พัฒนาได้ Deploy บนเครือข่ายทดลอง Infura Rinkeby ได้ที่

`https://rinkeby.infura.io/v3/b7a05df5e4ff4c05b767ad142933054e`

ภาคผนวก ข

หน้าเว็บเอกสารประกอบการใช้งาน

เว็บไซต์เอกสารประกอบการใช้งานของส่วน Official Web Application ส่วน Official API และส่วน Smart Contract สามารถเข้าถึงได้จาก https://op-digitalcertval-docu.netlify.app/



รูป ข.1 หน้าเว็บเอกสารประกอบการใช้งาน