

โครงการเลขที่ วศ.คพ. S049-1/2566

เรื่อง

ตรวจสอบประกาศนียบัตรออนไลน์ด้วยบล็อกเชน

โดย

นายคนธกานต์ พุคำ รหัส 630610719

นายคุณาสิน เตชะสีบ รหัส 630610721

โครงการนี้

เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต

ภาควิชาวิศวกรรมคอมพิวเตอร์

คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่

ปีการศึกษา 2566

PROJECT No. CPE S049-1/2566

E-Certificate using Hyperledger Fabric Blockchain

Konthakarn Fukam 630610719

Kunasin Techasueb 630610721

**A Project Submitted in Partial Fulfillment of Requirements
for the Degree of Bachelor of Engineering
Department of Computer Engineering
Faculty of Engineering
Chiang Mai University
2023**

หัวข้อโครงการ : ตรวจสอบประกาศนียบัตรออนไลน์ด้วยบล็อกเชน
: E-Certificate using Hyperledger Fabric Blockchain
โดย : นายคนธกานต์ ฟุ่คำ รหัส 630610719
นายคุณาสิน เตชะสีบ รหัส 630610721
ภาควิชา : วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา : รศ.ดร. ตรัสพงศ์ ไทยอุปถัมภ์
ปริญญา : วิศวกรรมศาสตรบัณฑิต
สาขา : วิศวกรรมคอมพิวเตอร์
ปีการศึกษา : 2566

ภาควิชาวิศวกรรมคอมพิวเตอร์ คณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ ได้อนุมัติให้โครงการนี้เป็นส่วน-
หนึ่งของการศึกษาตามหลักสูตรปริญญาวิศวกรรมศาสตรบัณฑิต (สาขาวิศวกรรมคอมพิวเตอร์)

..... หัวหน้าภาควิชาวิศวกรรมคอมพิวเตอร์
(รศ.ดร. สันติ พิทักษ์กัจจนกุล)

คณะกรรมการสอบโครงการ

..... ประธานกรรมการ
(รศ.ดร. ตรัสพงศ์ ไทยอุปถัมภ์)

..... กรรมการ
(ผศ. โดม โพธิกานนท์)

..... กรรมการ
(ผศ.ดร. กำพล วรดิษฐ์)

หัวข้อโครงการ : ตรวจสอบประกาศนียบัตรออนไลน์ด้วยบล็อกเชน
: E-Certificate using Hyperledger Fabric Blockchain
โดย : นายคนธกานต์ พุ่มคำ รหัส 630610719
นายคุณาสิน เตชะสีบ รหัส 630610721
ภาควิชา : วิศวกรรมคอมพิวเตอร์
อาจารย์ที่ปรึกษา : รศ.ดร. ตรีพงศ์ ไทยอุปถัมภ์
ปริญญา : วิศวกรรมศาสตรบัณฑิต
สาขา : วิศวกรรมคอมพิวเตอร์
ปีการศึกษา : 2566

บทคัดย่อ

ในปัจจุบัน ประกาศนียบัตร (Certificate) จากการศึกษา หรือฝึกอบรม มีแนวโน้มที่จะเป็นรูปแบบกระดาษ (Paper-based) ลดน้อยลง โดยมีการเปลี่ยนไปใช้รูปแบบอิเล็กทรอนิกส์มากขึ้นเรื่อย ๆ ปัญหาของการปลอมแปลงประกาศนียบัตรยังคงมีอยู่ และมีแนวโน้มที่จะรุนแรงมากขึ้นถึงแม้ว่าจะเป็นรูปแบบอิเล็กทรอนิกส์ก็ตาม เราไม่สามารถรู้ได้เลยว่าประกาศนียบัตรนั้นเป็นของจริงหรือของปลอม จากการสำรวจพบว่า มีซอฟต์แวร์ในการปลอมแปลงเอกสารเหล่านี้เกิดขึ้นมาจำนวนมากในโลกออนไลน์ และพบว่าร้อยละ 30 ของทั่วโลกมีการปลอมคุณสมบัติขึ้นที่ตนไม่มีขึ้นมา เราจึงต้องระวังข้อมูลปลอมและหาวิธีการยืนยันเอกสารเหล่านั้นให้ได้ ในโครงการนี้จึงมีแนวคิดในการออกแบบและพัฒนาระบบประกาศนียบัตรอิเล็กทรอนิกส์โดยใช้ไฮเปอร์เลจเจอร์เพบริกบล็อกเชน เพื่อเพิ่มความน่าเชื่อถือ ความถูกต้อง และความปลอดภัยในการรับรอง การยืนยัน และการตรวจสอบประกาศนียบัตร (Certificate) ที่ออกโดยสถานศึกษา ซึ่งเทคโนโลยีบล็อกเชนมีคุณลักษณะพื้นฐานที่สามารถเก็บข้อมูลได้อย่างปลอดภัย มีการใช้ Cryptography ในการป้องกันการแก้ไขข้อมูลในข้อมูลที่เก็บเป็นลักษณะของบล็อกที่เชื่อมต่อกันเป็นเชน โดยโครงการนี้ใช้เทคโนโลยีไฮเปอร์เลจเจอร์เพบริกบล็อกเชน ที่เป็นบล็อกเชนที่ต้องได้รับอนุญาตในการเข้าร่วม (Permissioned Blockchain) มีการใช้ระบบ Digital Signature ในการยืนยันตัวตนในการเข้าถึงข้อมูลผ่าน Smart Contract (Chaincode) เพื่อความปลอดภัย และความน่าเชื่อถือของข้อมูลที่เก็บในบล็อกเชน

Project Title : E-Certificate using Hyperledger Fabric Blockchain
Name : Konthakarn Fukam 630610719
Kunasin Techasueb 630610721
Department : Computer Engineering
Project Advisor : Assoc. Prof. Trasapong Thaiupathump, Ph.D.
Degree : Bachelor of Engineering
Program : Computer Engineering
Academic Year : 2023

ABSTRACT

Currently, there is a trend towards reducing the use of paper-based certificates for education or training, with an increasing shift towards electronic formats. However, the problem of certificate forgery persists, and it is becoming more severe even in electronic formats. We cannot always be certain whether a certificate is genuine or fake.

It has been found that there is a significant amount of software for forging these documents available online, and approximately 30 percent of the global population has experienced the falsification of their credentials. Therefore, we must be cautious about counterfeit information and find ways to verify these documents.

In this project, the idea is to design and develop an electronic certificate system using Hyperledger Fabric blockchain technology to enhance trustworthiness, accuracy, and security in certifying, verifying, and validating certificates issued by educational institutions. Blockchain technology has fundamental features that allow secure data storage, utilizing cryptography to prevent data tampering within interconnected blocks. This project uses a permissioned blockchain, which requires authorization to participate. It also incorporates digital signature systems for identity verification when accessing data through Smart Contracts (Chaincode) to ensure data security and trustworthiness within the blockchain.

กิตติกรรมประกาศ

โครงการนี้จะสำเร็จลุล่วงได้ด้วยความกรุณาจากอาจารย์ รศ.ดร.ตรัสพงศ์ ไทยอุปถัมภ์ อาจารย์ที่ปรึกษาที่ได้เสียสละเวลาอันมีค่าแก่นักศึกษาโครงการนี้ได้รับข้อเสนอแนะและแนวคิดตลอดจนการแก้ไขข้อบกพร่อง รายละเอียดต่างๆตรวจทานแก้ไขด้วยความเอาใจใส่เป็นอย่างยิ่งจนโครงการฉบับนี้สำเร็จสมบูรณ์ลุล่วงไป ได้ด้วยดีขอกราบขอพระคุณเป็นอย่างสูงไว้ ณ ที่นี้จากใจจริงรวมถึง ผศ.โดม โพธิกานนท์ และ ผศ.ดร.กำพล วรดิษฐ์ ที่ให้คำปรึกษา คำแนะนำ จนทำให้โครงการเล่มนี้มีความสมบูรณ์มากที่สุด

ขอบคุณคณะวิศวกรรมศาสตร์ มหาวิทยาลัยเชียงใหม่ ที่ให้สถานที่ในการทำโครงการ ทั้งห้องภาควิชา วิศวกรรมคอมพิวเตอร์ และสถานที่ต่างๆในภาควิชา และยังให้การสนับสนุนทางด้านงบประมาณ อุปกรณ์ต่างๆ ที่จำเป็นต่อการทำโครงการ

ขอขอบพระคุณผู้ปกครอง เพื่อนๆ และรุ่นพี่ทุกคน ที่ให้คำปรึกษา คำแนะนำ และคอยเป็นกำลังใจให้ตลอดมา ซึ่งเป็นแรงผลักดันให้แก่ผู้จัดทำมีความตั้งใจและมุ่งมั่นในการทำงาน จนโครงการนี้มีความสมบูรณ์มากที่สุด

นอกจากนี้ผู้จัดทำขอขอบพระคุณอีกหลายท่านที่ไม่ได้กล่าวถึง ณ ที่นี้ ที่ได้ให้ความช่วยเหลือตลอดมา และสุดท้ายนี้ หากโครงการนี้มีข้อผิดพลาดประการใด ผู้จัดทำขออภัยมา ณ ที่นี้ และพร้อมน้อมรับด้วยความยินดี

นายคนธกานต์ พุคำ
นายคุณาสิน เตชะสีบ
5 ตุลาคม 2566

สารบัญ

| | |
|--|----------|
| บทคัดย่อ | ข |
| Abstract | ค |
| กิตติกรรมประกาศ | ง |
| สารบัญ | จ |
| สารบัญรูป | ช |
| สารบัญตาราง | ซ |
| 1 บทนำ | 1 |
| 1.1 ที่มาของโครงการ | 1 |
| 1.2 วัตถุประสงค์ของโครงการ | 1 |
| 1.3 ขอบเขตของโครงการ | 1 |
| 1.3.1 ขอบเขตด้านฮาร์ดแวร์ | 1 |
| 1.3.2 ขอบเขตด้านซอฟต์แวร์ | 1 |
| 1.4 ประโยชน์ที่ได้รับ | 2 |
| 1.5 เทคโนโลยีและเครื่องมือที่ใช้ | 2 |
| 1.5.1 เทคโนโลยีด้านฮาร์ดแวร์ | 2 |
| 1.5.2 เทคโนโลยีด้านซอฟต์แวร์ | 2 |
| 1.6 แผนการดำเนินงาน | 2 |
| 1.7 บทบาทและความรับผิดชอบ | 3 |
| 1.8 ผลกระทบด้านสังคม สุขภาพ ความปลอดภัย กฎหมาย และวัฒนธรรม | 3 |
| 2 ทฤษฎีที่เกี่ยวข้อง | 4 |
| 2.1 พื้นฐาน Blockchain | 4 |
| 2.1.1 Blockchain คืออะไร | 4 |
| 2.1.2 Blockchain แตกต่างจาก Database ทั่วไปอย่างไร | 4 |
| 2.1.3 Public blockchain คือ | 4 |
| 2.1.4 Private blockchain คือ | 5 |
| 2.1.5 ข้อดีของ Blockchain | 5 |
| 2.2 พื้นฐาน Hyperledger Fabric | 5 |
| 2.2.1 Peers | 5 |
| 2.2.2 Certificate Authorities | 6 |
| 2.2.3 Ordering services | 6 |
| 2.2.4 Channels | 7 |
| 2.2.5 Chaincode หรือ Smart Contracts | 7 |
| 2.3 ความรู้ตามหลักสูตรซึ่งถูกนำมาใช้หรือบูรณาการในโครงการ | 7 |
| 2.3.1 Database Systems (261342) | 7 |
| 2.3.2 NET AND INFO SECURITY (261447) | 7 |
| 2.4 ความรู้นอกหลักสูตรซึ่งถูกนำมาใช้หรือบูรณาการในโครงการ | 8 |
| 2.4.1 ความรู้ทางด้านการทำงานของ Blockchain | 8 |
| 2.4.2 ความรู้การใช้งาน Hyperledger Fabric | 8 |
| 2.4.3 ความรู้ทางด้านการใช้ docker | 8 |

| | | |
|----------|---|-----------|
| 3 | โครงสร้างและขั้นตอนการทำงาน | 9 |
| 3.1 | โครงสร้างของแอปพลิเคชัน | 9 |
| 3.1.1 | Frontend | 9 |
| 3.1.2 | Hyperledger fabric Blockchain | 9 |
| 3.1.3 | Backend | 9 |
| 3.1.4 | Database | 9 |
| 3.2 | ฟีเจอร์ของแอปพลิเคชัน | 9 |
| 3.2.1 | ฟีเจอร์ของ สถานศึกษา | 9 |
| 3.2.2 | ฟีเจอร์ของ นักศึกษา | 10 |
| 3.2.3 | ฟีเจอร์ของ บริษัท | 10 |
| 3.3 | นโยบายความเป็นส่วนตัว | 10 |
| 3.4 | ตัวอย่างการออกแบบ User Interface | 10 |
| 4 | การทดลองและผลลัพธ์ | 15 |
| 4.1 | การเข้าถึงข้อมูลและความถูกต้องของข้อมูล | 15 |
| 4.2 | รู้ว่าข้อมูลถูกแก้ไขเมื่อไหร่ | 15 |
| 4.3 | ข้อมูลมีความปลอดภัย | 15 |
| | บรรณานุกรม | 16 |

สารบัญรูป

| | | |
|-----|--|----|
| 2.1 | Peer | 5 |
| 2.2 | Certificate Authorities | 6 |
| 2.3 | Peers Diagram 5 | 7 |
| 3.1 | หน้า Login | 11 |
| 3.2 | หน้า Register | 11 |
| 3.3 | หน้า Add course สำหรับสำนักทะเบียน | 12 |
| 3.4 | หน้า Add course Success | 12 |
| 3.5 | หน้าตรวจสอบ Transaction แต่ละบล็อก | 13 |
| 3.6 | หน้าหลังจากบริษัท login สำเร็จ | 13 |
| 3.7 | หน้าหลังจากบริษัท getข้อมูล | 14 |
| 3.8 | หน้าหลังจากนักศึกษา login สำเร็จ | 14 |

สารบัญตาราง

บทที่ 1

บทนำ

1.1 ที่มาของโครงการ

เกมเป็นสื่อบันเทิงประเภทหนึ่งที่มีการแพร่หลายเป็นอย่างมากในปัจจุบัน ไม่ว่าจะเป็นเกมบนมือถือ บนเว็บไซต์ เกมบนเครื่องเล่นเกมต่างๆที่ออกแบบมาเพื่อเกมใดเกมหนึ่งโดยเฉพาะ และรวมไปถึงเกมบนคอมพิวเตอร์ ซึ่งบางเกมได้มีการจัดการแข่งขันกันขึ้น เพื่อชิงรางวัลต่างๆมากมายภายในงานแข่ง ส่งผลให้ผู้คนให้ความสนใจกับเกมมากขึ้น และส่งผลให้อุตสาหกรรมเกมมีการเติบโตอย่างรวดเร็ว จนเกิดอาชีพใหม่ๆมากมายที่เกี่ยวกับเกม เช่น Streamer, นักกีฬา E-sport, นักพากย์เกม เป็นต้น

โดยโครงการนี้ได้เริ่มต้นมาจากการที่ผู้พัฒนาชื่นชอบในการเล่นเกมน และมีความสนใจที่จะสร้างเกมขึ้นมาหนึ่งเกม ซึ่งผู้พัฒนาได้ลองทำการศึกษาพื้นฐานต่างๆเกี่ยวกับการสร้างเกม และตัดสินใจเสนอความสนใจเหล่านี้พร้อมกับอธิบายเหตุผลให้กับอาจารย์ฟัง จนสุดท้ายได้ทำการตกลงกับอาจารย์ว่าจะสร้างเกม 3D แนว RPG action ขึ้นมา ซึ่งก็คือ เกม Miracle from sky นั่นเอง

สำหรับเกม Miracle from sky เป็นเกมแนว Action RPG OpenWorld แบบ Single-player ที่มีมุมมองเป็น มุมมองของบุคคลที่สาม ซึ่งผู้พัฒนาให้มีความสนใจ และอยากนำมาเป็นต้นแบบในการทำเกมคือ Genshin impact และ Diablo ซึ่งทางระบบ gameplay จะเน้นไปทาง Genshin impact ส่วนระบบสกิลจะเน้นไปทาง Diablo ซึ่งในเกม ผู้เล่นจะได้รับบทเป็นเด็กสาวที่ต้องผจญภัยในโลกกว้าง และฝึกฝนตัวเองให้เก่งขึ้น เพื่อที่จะไปปราบจอมมาร โดยระหว่างการเดินทางผู้เล่นจะได้พบศัตรูหลากหลายรูปแบบ ซึ่งต้องใช้วิธีรับมือที่แตกต่างกัน ได้สำรวจโลกแฟนตาซีกว้างใหญ่ และได้พบเจอกับปริศนาต่างๆที่รอให้ผู้เล่นได้เข้าไปแก้ไขหาคำตอบ

1.2 วัตถุประสงค์ของโครงการ

1. เพื่อตอบสนองความสนใจ ความต้องการของผู้พัฒนาที่อยากจะทำเกมของตัวเองขึ้นมาซักหนึ่งเกม
2. เพื่อสร้างประสบการณ์ต่างๆที่น่าตื่นเต้น สนุกสนาน และน่าติดตามให้กับผู้เล่น ผ่านทางตัวเกม ทั้งด้านเนื้อเรื่อง gameplay และสิ่งต่างๆภายในเกม
3. เพื่อสร้างความบันเทิงให้กับผู้เล่น และช่วยทำให้ผู้เล่นรู้สึกผ่อนคลายเวลาเล่นเกม
4. เพื่อเป็นแบบอย่าง และแรงบันดาลใจให้กับหลายๆคนที่อยากจะลองสร้างเกมของตัวเองขึ้นมา

1.3 ขอบเขตของโครงการ

1.3.1 ขอบเขตด้านฮาร์ดแวร์

1. เกมสามารถเล่นได้ผ่านทางคอมพิวเตอร์ ซึ่งได้แก่ PC, laptop
2. เกมจะใช้เมาส์ แป้นพิมพ์ ในการควบคุม

1.3.2 ขอบเขตด้านซอฟต์แวร์

1. เกมจะรองรับแค่ระบบปฏิบัติการ Windows

2. เกมถูกออกแบบมาสำหรับผู้เล่นคนเดียว
3. เกมมีมุมมองเป็นแบบมุมมองบุคคลที่สาม เท่านั้น ไม่สามารถเปลี่ยนมุมมองอื่นๆได้

1.4 ประโยชน์ที่ได้รับ

1. ผู้เล่นจะได้รับความสนุกสนาน ความบันเทิงต่างๆภายในเกม
2. ผู้เล่นจะได้รับประสบการณ์ใหม่ๆมากมายจากการเกม
3. ผู้พัฒนาได้รับประสบการณ์ใหม่ๆในการทำงานเป็นทีม และประสบการณ์ต่างๆในการสร้างเกม ซึ่งเป็นผลดีต่อการทำงานในอนาคต

1.5 เทคโนโลยีและเครื่องมือที่ใช้

1.5.1 เทคโนโลยีด้านฮาร์ดแวร์

1. คอมพิวเตอร์รุ่น Lenovo legion y540, core i5 ใช้ในการออกแบบ และพัฒนา
2. คอมพิวเตอร์รุ่น Asus Rog, core i7 ใช้ในการออกแบบ และพัฒนา

1.5.2 เทคโนโลยีด้านซอฟต์แวร์

1. Github ใช้ในการ พัฒนาและอัปเดต source code
2. Figma ใช้ในการออกแบบหน้าตาของเว็บไซต์
3. Visual studio ใช้ในการเขียน code
4. Docker ใช้ในการจำลองการสร้างserver
5. Javascript ภาษาที่ใช้ในการเขียน chaincode
6. Photoshop ใช้ในการออกแบบ
7. React ใช้สำหรับสร้าง user interface

1.6 แผนการดำเนินงาน

| ขั้นตอนการดำเนินงาน | ต.ค. 2566 | พ.ย. 2566 | ธ.ค. 2566 | ม.ค. 2567 | ก.พ. 2567 | มี.ค. 2567 |
|---|-----------|-----------|-----------|-----------|-----------|------------|
| ศึกษาค้นคว้าการใช้งาน hyperledger fabric Blockchain | | | | | | |
| วางแผนออกแบบระบบต่างๆ | | | | | | |
| พัฒนาฐานข้อมูลเข้าสู่ระบบ | | | | | | |
| สร้างหน้า login registerและหน้าต่างๆ | | | | | | |
| ทดลองtestระบบnetwork | | | | | | |

| ขั้นตอนการดำเนินงาน | ต.ค. 2566 | พ.ย. 2566 | ธ.ค. 2566 | ม.ค. 2567 | ก.พ. 2567 | มี.ค. 2567 |
|---------------------|-----------|-----------|-----------|-----------|-----------|------------|
| เขียน chaincode | | | | | | |
| เขียน api ต่างๆ | | | | | | |
| ทดสอบระบบและแก้ไข | | | | | | |

1.7 บทบาทและความรับผิดชอบ

1.การออกแบบโดยรวม: ในส่วนนี้จะช่วยกันทำ โดยการระดมความคิด ข้อเสนอต่างๆ มารวมกันแล้วเลือกเอาในสิ่งที่ สามารถทำได้และ สิ่งเห็นตรงกันว่าอยากจะให้มี

1.8 ผลกระทบด้านสังคม สุขภาพ ความปลอดภัย กฎหมาย และวัฒนธรรม

โครงการของเราได้ใช้ระบบprivate blockchain ที่มีความปลอดภัยสูงและมีความน่าเชื่อถือมากทำให้ระบบของเราสามารถตรวจสอบป้องกันการปลอมแปลงเอกสารซึ่งเป็นการกระทำที่ผิดกฎหมายช่วยให้การอยู่ร่วมกันในสังคมน่าอยู่และยังมีความปลอดภัยทางด้านข้อมูลสูงไม่มีการเปิดเผยข้อมูลก่อนไต่ถามไต่ถามไปและสามารถรักษาความเป็นส่วนตัวของผู้ใช้งานได้ทำให้ผู้ใช้งานได้ใช้เว็บไซต์ของเราได้โดยไม่มีกังวลใดๆ

บทที่ 2

ทฤษฎีที่เกี่ยวข้อง

ในการตรวจสอบประกาศนียบัตรออนไลน์ด้วยบล็อกเชนก่อนที่จะลงมือสร้างนั้นผู้พัฒนาจำเป็นต้องไปศึกษาเกี่ยวกับ Blockchain ก่อนสำหรับสร้างซึ่งจะไปศึกษาจาก Hyperledger Fabric และใช้ Blockchain แบบ private โดยเนื้อหาในบทนี้จะอธิบายในส่วนของความรู้ ทฤษฎีที่เกี่ยวข้อง และหลักการต่างๆที่ผู้พัฒนาได้ศึกษา และนำไปใช้ในการสร้าง Blockchain เพื่อให้ผู้ที่เข้ามาอ่านได้เข้าใจหลักการต่างๆในเบื้องต้น และเพื่อให้เข้าใจเนื้อหาในบทถัดๆไปได้ง่ายมากยิ่งขึ้น

2.1 พื้นฐาน Blockchain

2.1.1 Blockchain คืออะไร

[2] Blockchain คือเทคโนโลยีว่าด้วยระบบการเก็บข้อมูล Data Structure ซึ่งไม่มีตัวกลาง แต่ข้อมูลที่ได้รับการปกป้องจะถูกแชร์และจัดเก็บเป็นสำเนาไว้ในเครื่องของทุกคนที่ใช้ฐานข้อมูลเดียวกันเสมือนห่วงโซ่ Chain โดยทุกคนจะรับทราบร่วมกัน ว่าใครเป็นเจ้าของและมีสิทธิในข้อมูลตัวจริง เมื่อมีการอัปเดตข้อมูลใด ๆ สำเนาข้อมูลในฐานเดียวกันก็จะอัปเดตตามไปด้วยทันที ทำให้การปลอมแปลงข้อมูลไม่ใช่เรื่องง่าย เพราะทุกคนต้องรับทราบและตรวจสอบความถูกต้องของข้อมูลร่วมกันได้ อีกทั้งไม่มีระบบล่ม และภัยใด ๆ ก็ไม่อาจทำลายอุปกรณ์ในระบบได้พร้อมกัน เช่นเดียวกับการถูกแฮ็กข้อมูล ซึ่งต้องทำการแฮ็กทุกเครื่องในฐานเดียวกันพร้อม ๆ กัน หรืออย่างน้อยต้องแฮ็กเครื่องที่ถือสำเนาให้ได้มากกว่าร้อยละ 51 จึงจะแฮ็กได้สำเร็จ เทคโนโลยี Blockchain จึงนับว่ายอดเยี่ยมในแง่ของเครดิตและความปลอดภัย นอกจากนี้ ยังเป็นเทคโนโลยีที่เข้ามารองรับการซื้อขายสกุลเงินดิจิทัล เช่น บิทคอยน์ Bitcoin ฯลฯ ให้มีความปลอดภัยด้านข้อมูลมากยิ่งขึ้นด้วย

2.1.2 Blockchain แตกต่างจาก Database ทั่วไปอย่างไร

[1] คือ Blockchain จะมีการเก็บข้อมูลไว้เป็นกลุ่มๆ ไว้ใน block ซึ่งมักรวมข้อมูลไว้ด้วยกัน ซึ่งมีการเก็บข้อมูลจะในมาต่อกับ block ก่อนหน้ามีลักษณะเป็นโซ่ ซึ่งถ้าข้อมูลก่อนหน้าผิดพลาดหรือถูกแก้ไขจะทำให้รู้ได้เพราะเหมือนโซ่ที่ขาดออกจากกัน แต่ในส่วนของ database ทั่วไปจะเก็บในรูปแบบของตารางซึ่งถ้าถูกแก้ไขจะทำให้เราไม่รู้ตัวได้ว่าถูกแก้ไขเมื่อใด แต่ถ้า Blockchain

2.1.3 Public blockchain คือ

[5] คือ เป็น Blockchain ที่ทุกคนสามารถเข้าถึงและมีส่วนร่วมได้ เนื่องจากเป็น Open Network ทั้งหมด โดยลักษณะของการใช้งานพื้นฐานของ Blockchain ประเภทนี้ คือ การแลกเปลี่ยน Cryptocurrency และการขุด รวมถึงความสามารถในการรักษาความไว้วางใจระหว่าง Community ของผู้ใช้ทั้งหมด เนื่องจากทุกคนในเครือข่ายรู้สึกมีแรงจูงใจที่จะทำงานเพื่อพัฒนาเครือข่าย แต่ข้อเสียของ Blockchain ประเภทนี้ คือ ต้องใช้พลังงานจำนวนมากในการประมวลผลธุรกรรมเพราะใช้ระบบ Proof of work ในการตรวจสอบธุรกรรม และปัญหาอีกอย่างที่พบเจอคือ การเปิดกว้างเกินไป จึงทำให้ไม่มีความเป็นส่วนตัวในการทำธุรกรรม

เท่าไรนัก ตัวอย่างของ Public blockchain network เช่น Bitcoin , Ethereum , BNB Chain ซึ่งต่างเป็น Blockchain ยอดนิยมที่ทุกคนสามารถเข้าถึงได้ง่าย

2.1.4 Private blockchain คือ

[5] คือ Blockchain ที่ทำงานในเครือข่ายแบบปิด ซึ่งสามารถเข้าร่วมได้เฉพาะบุคคลที่ได้รับอนุญาตหรือคำเชิญเท่านั้น โดย Blockchain ประเภทนี้เหมาะที่สุดสำหรับองค์กรและธุรกิจที่ต้องการใช้ Blockchain สำหรับการใช้งานภายใน ขณะที่การทำธุรกรรมใน Private blockchain นั้นเร็วและง่ายเมื่อเทียบกับ Public blockchain แต่ข้อเสีย คือ ไม่มีการกระจายอำนาจ เนื่องจากมีผู้มีอำนาจเพียงคนเดียวที่ดูแลเครือข่าย

2.1.5 ข้อดีของ Blockchain

[1] คือ ช่วยเพิ่มความปลอดภัยของข้อมูลและสามารถรู้ได้ว่าข้อมูลของเราถูกแก้ไขหรือดัดแปลงไหม

2.2 พื้นฐาน Hyperledger Fabric

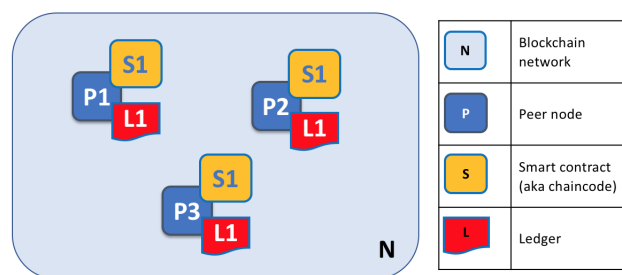
[3] Hyperledger Fabric เป็น private blockchain ซึ่งหมายความว่า ใครก็ตามที่ต้องการเข้าร่วมและใช้งานข้อมูลบน chain ในระบบ จะต้องได้รับสิทธิ์ก่อน จึงสามารถมองเห็นและใช้งานข้อมูลที่อยู่ใน chain นั้นๆได้ ซึ่งจะแตกต่างจาก public blockchain ที่ไม่ว่าจะเป็นใครก็สามารถมีสิทธิ์เข้าถึงข้อมูลบน ledger ได้นั่นเอง

Hyperledger Fabric เป็น Distributed Ledger ถูกออกแบบมาเพื่อใช้งานเกี่ยวกับการทำ transaction ระหว่างองค์กร โดยแต่ละองค์กรจะมีช่องทางที่ใช้สำหรับ communicate ซึ่งกันและกัน โดยที่องค์กรหนึ่งๆสามารถอยู่ได้หลายช่องทาง และแต่ละช่องทางนั้นข้อมูลจะถูกแยกจากกันอย่างชัดเจน

ด้วยพื้นฐานของโครงการที่ต้องการให้ Architecture ของ Hyperledger Fabric มีลักษณะเป็น Modular ตัว Hyperledger Fabric จึงประกอบด้วย Component สำคัญๆดังต่อไปนี้

2.2.1 Peers

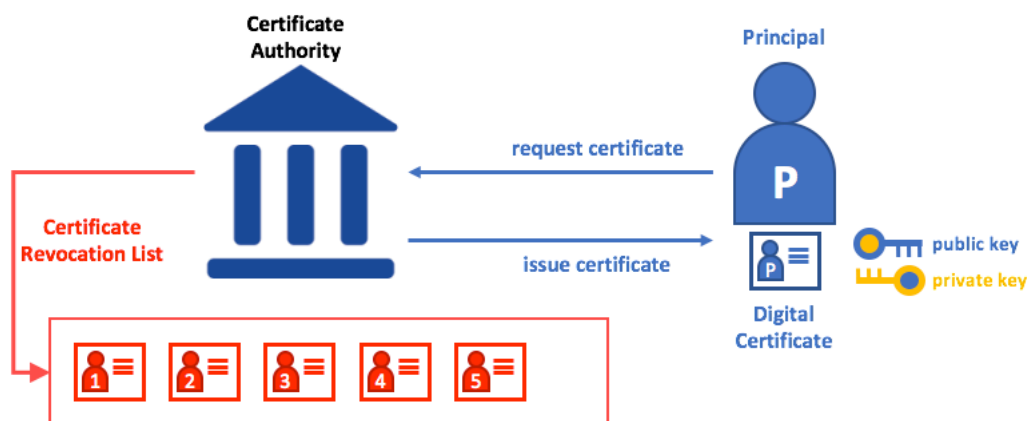
[4] โดยส่วนตัวหากจะให้จินตนาการว่า Peers คืออะไร ก็ให้นึกถึง Network แบบ Peer-to-Peer โดย Peer ในที่นี้ก็คือ Node แต่ละ Node ภายใต Network ของ Blockchain นั้นๆ นั่นเอง



รูปที่ 2.1: ตัวอย่างของpeer ที่มา: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html>

2.2.2 Certificate Authorities

[4] หากพูดถึง Blockchain ก็ต้องบอกว่ามันเป็นกลุ่มของ Network ที่ทำหน้าที่ประมวลผลข้อมูลร่วมกัน โดยเฉพาะใน Permissioned Blockchain อย่าง Hyperledger Fabric ที่เราจำเป็นต้องรู้ว่าคนที่เข้ามาเป็นใคร ตัวจริงหรือไม่ มีสิทธิ์ในการเข้าถึง Network ในรูปแบบใดบ้าง



รูปที่ 2.2: Certificate Authorities ที่มา:<https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html>

Certificate Authorities มีหน้าที่ Generate Identity ของทุกๆ Actor ที่ต้องการใช้งาน Network ของ Blockchain โดย Certificate Authorities จะสร้าง Digital Certificate ที่ระบุตัวตนของ Actor ตามมาตรฐาน X.509

2.2.3 Ordering services

[4] ในโลกของ Hyperledger Fabric Ordering Service จะทำหน้าที่หลักๆ 2 ส่วน คือ

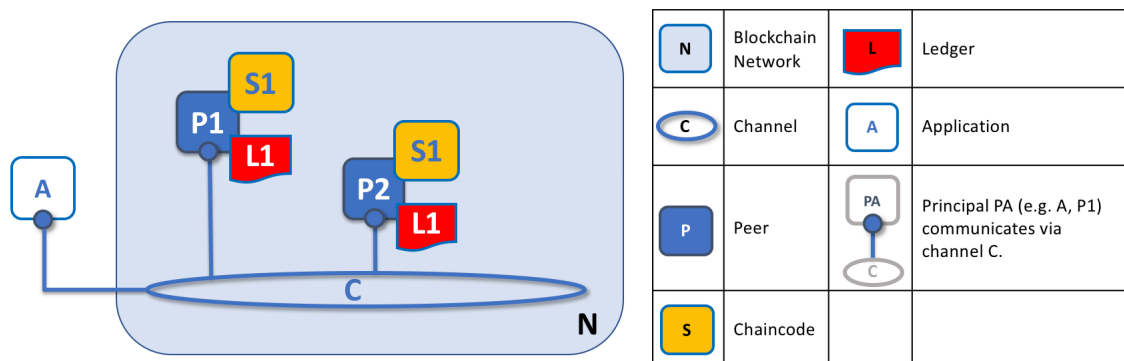
1. Pack ตัว Transaction ที่ต้องการแก้ไข Ledger ที่ส่งเข้ามาจาก Application แต่ละตัว
2. กระจาย Pack ของ Transaction ที่สร้างขึ้นนั้น ไปยังแต่ละ Peer ที่อยู่ใน Network

โดยในแต่ละ Transaction ของการจัดการกับข้อมูลที่อยู่ใน Ledger จะประกอบไปด้วย 3 ระยะ คือ

1. Proposal เป็นระยะที่เกิดขึ้นหลังจากที่ Application ปลายทางส่ง Request เข้ายัง Endorser เพื่อสร้าง Proposal สำหรับ Update ข้อมูล ขั้นตอนนี้เสร็จสิ้น Endorser จะส่ง Response กลับไปที่ Application
2. Proposal เป็นระยะที่เกิดขึ้นหลังจากที่ Application ปลายทางส่ง Request เข้ายัง Endorser เพื่อสร้าง Proposal สำหรับ Update ข้อมูล ขั้นตอนนี้เสร็จสิ้น Endorser จะส่ง Response กลับไปที่ Application
3. Validation and commit เมื่อ Peers ได้รับข้อมูล Transaction จาก Ordering Services หากข้อมูลมีความถูกต้องก็จะ Commit เข้าไปใน Ledger ของตัวเอง

2.2.4 Channels

[4] หากจะเปรียบเทียบว่า Channel ใน Hyperledger Fabric คืออะไร ก็ให้นึกถึงช่องทางที่เปิดให้เข้าถึงในแต่ละ Peer ของ Network นั้นๆ



รูปที่ 2.3: peers diagram 5 ที่มา: <https://hyperledger-fabric.readthedocs.io/en/release-2.2/peers/peers.html>

ยกตัวอย่างในรูป การจะเข้าที่ Peer P1 และ P2 ได้ ก็จำเป็นที่จะต้องเข้าผ่าน Channel C ที่ถูกสร้างขึ้น แต่ถ้าหากใน Network นี้มี Peer P3 อยู่ในภายใน Network Application A ก็จะไม่สามารถเข้าถึงได้ เนื่องจาก Channel C ที่ถูกสร้างขึ้น ไม่ได้เชื่อมต่อกับ Peer P3 ที่ถูกสร้างขึ้นนั่นเอง

2.2.5 Chaincode หรือ Smart Contracts

[4] หากใครใช้งาน Eterium ก็คงจะรู้จัก Smart Contract ที่เขียนด้วย Solidity ของ Eterium มาบ้างเช่นกัน โดย Concept อาจจะไม่ต่างกัน โดย Chaincode จะมีลักษณะเหมือนโปรแกรมขนาดเล็ก ที่เปิดให้ Application ส่งคำสั่งเข้ามาประมวลผลข้อมูลที่อยู่ภายใน Ledger ได้ สำหรับ Hyperledger Fabric เปิดให้นักพัฒนาสามารถพัฒนา Chaincode ผ่านทาง Fabric SDK ได้ด้วยภาษาที่ค่อนข้างหลากหลาย ได้แก่ Go, Javascript หรือ Java

2.3 ความรู้ตามหลักสูตรซึ่งถูกนำมาใช้หรือบูรณาการในโครงงาน

ในการทำโครงงานนี้กลุ่มของพวกเราได้นำความรู้ตามหลักสูตรต่างๆ มาประยุกต์ใช้ ซึ่งได้แก่

2.3.1 Database Systems (261342)

ในการออกแบบ database เราจะใช้ความรู้ในการออกแบบการเก็บข้อมูลแบบ offchain ว่าออกแบบยังไงให้เก็บข้อมูลครบถ้วนและไม่มากเกินไป

2.3.2 NET AND INFO SECURITY (261447)

ใช้ความรู้ในการออกแบบ Smart Contracts ว่าออกแบบยังไงให้ปลอดภัยไม่ถูกโจมตีและรับมือกับการโจมตีอย่างไรหรือทำให้สามารถรู้ตัวได้ไวว่าโดนโจมตี

2.4 ความรู้นอกหลักสูตรซึ่งถูกนำมาใช้หรือบูรณาการในโครงการ

ในการทำโครงการนี้กลุ่มของพวกเราได้นำความรู้นอกหลักสูตรต่างๆ มาประยุกต์ใช้ ซึ่งได้แก่

2.4.1 ความรู้ทางด้านการทำงานของ Blockchain

เนื่องจากกลุ่มของเราไม่มีความรู้ด้าน Blockchain จึงต้องไปศึกษา Blockchain ดังที่กล่าวไว้ในข้อ 2.1 พื้นฐาน Blockchain ว่า Blockchain มีการทำงานอย่างไร

2.4.2 ความรู้การใช้งาน Hyperledger Fabric

เนื่องจากพวกเรามีการใช้ Blockchain แบบ Private Blockchain จึงเลือกใช้ Hyperledger Fabric ในการพัฒนา กลุ่มของพวกเราจึงได้ทำการศึกษาเพิ่มเติมกันเอง โดยอาศัยสื่อต่างๆทางอินเทอร์เน็ต เช่น youtube, google เป็นต้น ดังที่กล่าวไว้ในข้อ 2.2 พื้นฐาน Hyperledger Fabric

2.4.3 ความรู้ทางด้านการใช้ docker

เนื่องจากเราต้องใช้ docker ในการจำลองการเปิดเซิร์ฟเวอร์ในการส่งข้อมูลจากหลายๆที่เราจึงต้องไปศึกษาการใช้ dockerเบื้องต้น

บทที่ 3

โครงสร้างและขั้นตอนการทำงาน

ในบทนี้จะกล่าวถึงการออกแบบและฟีเจอร์ของแอปพลิเคชัน นโยบายความเป็นส่วนตัวของผู้ใช้ User interface และการออกแบบฐานข้อมูลของแอปพลิเคชัน

3.1 โครงสร้างของแอปพลิเคชัน

แอปพลิเคชันนี้แบ่งออกเป็น ดังนี้ frontend Backend hyperledger fabric blockchain และ database ซึ่งทำงานร่วมกัน

3.1.1 Frontend

เป็นส่วนแสดงผลหน้าจอของเว็บไซต์ เป็นส่วนที่เชื่อมต่อผู้ใช้กับ application โดยจะใช้ react ในการแสดงผล

3.1.2 Hyperledger fabric Blockchain

เป็นส่วนของ Private blockchain ที่แอปพลิเคชันนี้ใช้เก็บ transaction log ที่เก็บข้อมูลที่มีการเปลี่ยนแปลงใน worldstate

3.1.3 Backend

เป็นส่วนประมวลผลของแอปพลิเคชัน เป็นส่วนประมวลผลการทำงานคำสั่งต่างๆเป็นตัวกลางในการรับส่งข้อมูลระหว่าง frontend กับ database โดยจะใช้เป็น ภาษา javascript

3.1.4 Database

เป็นฐานข้อมูลที่ใช้เก็บข้อมูลใน worldstate เพื่อนำข้อมูลไปประมวลผลโดยจะใช้เป็น mongoDB

3.2 ฟีเจอร์ของแอปพลิเคชัน

ในแอปพลิเคชันจะมี User 3 แบบ คือ สถานศึกษา นักศึกษา บริษัทต่างๆ

3.2.1 ฟีเจอร์ของ สถานศึกษา

ฝั่งสถานศึกษา คือฝั่งของผู้ใช้ที่ต้องทำการส่งข้อมูลเข้า blockchain เพื่อไปอัปเดตข้อมูลใน world-state และรับรองความถูกต้องของข้อมูล โดยมีฟีเจอร์ในการทำงานโดยต่อไปนี้

1. การลงทะเบียนและยืนยัน ฝั่งสถานศึกษาต้องลงทะเบียนกับทางระบบแล้วจะได้ตัว key เพื่อมาใช้ในการยืนยันตัวตน
2. การจัดการข้อมูล สถานศึกษาสามารถจัดการข้อมูลต่างๆเข้า blockchain ได้ เช่นการเพิ่มข้อมูล แก้ไขข้อมูล

3.2.2 ฟังก์ชันของ นักศึกษา

ฝั่งนักศึกษาสามารถเข้ามาดูข้อมูลต่างๆของตัวเองได้และสามารถ export one time key ส่งให้บริษัท ตรวจสอบข้อมูลของตนเองได้ โดยมีฟังก์ชันในการทำงานโดยต่อไปนี้

1. การดูข้อมูลของตน นักศึกษาจะlogin เข้าไปด้วย key และสามารถตรวจสอบข้อมูลรายวิชาต่างๆ ที่ได้ลงทะเบียนไป และสามารถตรวจสอบ transaction log ได้ ว่ามีบริษัทไหนได้เข้ามาดูบ้าง
2. การ export public-key นักศึกษาสามารถ export Key ของตัวเองและนำไปให้บริษัทที่อยากตรวจสอบความถูกต้องของตนเองเพื่อเพิ่มความน่าเชื่อถือ

3.2.3 ฟังก์ชันของ บริษัท

ในฝั่งของบริษัทจะสามารถนำ key ของนักศึกษามาตรวจสอบข้อมูลในระบบได้

1. ระบบลงทะเบียน ก่อนที่บริษัทจะเข้ามาดูข้อมูลของนักศึกษานั้นต้องลงทะเบียนยืนยันตัวตนกับระบบ เสียก่อน
2. การตรวจสอบข้อมูลของนักศึกษา บริษัทสามารถตรวจสอบข้อมูลของนักศึกษาที่ตนเองได้รับ key มา และสามารถตรวจสอบ transaction log เพื่อดูความน่าเชื่อถือของข้อมูลได้

3.3 นโยบายความเป็นส่วนตัว




1. ข้อมูลของนักศึกษาต้องได้รับการยินยอมจากเจ้าตัวเสียก่อนถึงจะสามารถเปิดเผยได้
2. การตรวจสอบข้อมูลของนักศึกษารันสามารถตรวจสอบได้แค่ วิชาที่เรียนมา วัตถุประสงค์ของวิชานั้น และสามารถยืนยันได้ว่านักศึกษามาจากมหาวิทยาลัยนั้นจริงๆ

เป็นส่วนแสดงผลหน้าจอของเว็บไซต์ เป็นส่วนที่เชื่อมต่อผู้ใช้กับ application

3.4 ตัวอย่างการออกแบบ User Interface

ออกแบบโดยใช้ Figma ซึ่งเป็นเครื่องมือสำหรับการออกแบบ User Interface ที่ได้รับความนิยมสูงสุดในปัจจุบัน

E-Certificate



Log In

Username

Password




Key

Log In Button

[Sign Up](#)

รูปที่ 3.1: หน้า Login

E-Certificate



Register

Username

Password

Email

company

Register

รูปที่ 3.2: หน้า Register

E-Certificate

Frame 4

addcourse

Course No

Course Name

Add Course

Add Course

enrollment detail

Get Course

Block detail

Number Of Block :3

Block 1

Block 2

รูปที่ 3.3: หน้า Add course สำหรับสำนักทะเบียน

E-Certificate

Frame 6

addcourse

Course No

Course Name

addcourse success

Transaction id
239dc8cx023214k3m3kl12mlldsm213ed;scxlpdsp[cdsf:2lwe;wlwplelwdlscx[lad[pl]24-p=-4p=3-3

Number Of Block :3

Block 1

Block 2

รูปที่ 3.4: หน้า Add course Success

E-Certificate

f
in
github

Frame 8

Course No

Course Name

Add Course

enrollment detail

Get Course

Block detail

Number Of Block :3

Block 1

data about transaction

รูปที่ 3.5: หน้าตรวจสอบ Transaction แต่ละบล็อก

E-Certificate

f
in
github

enrollment detail

Get Course

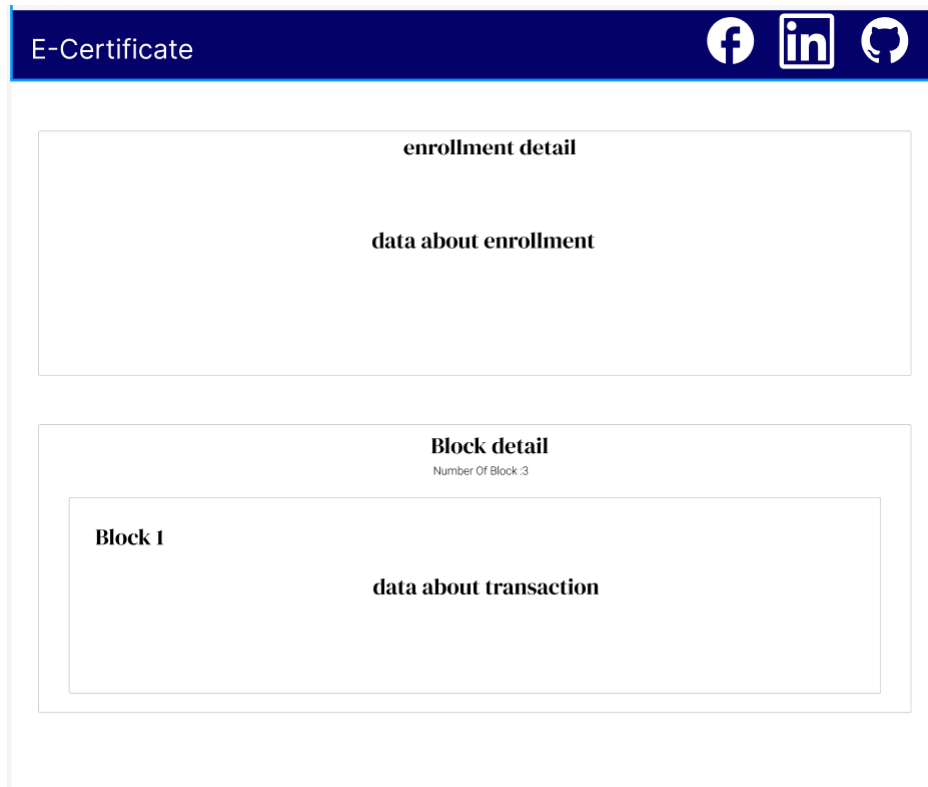
Block detail

Number Of Block :3

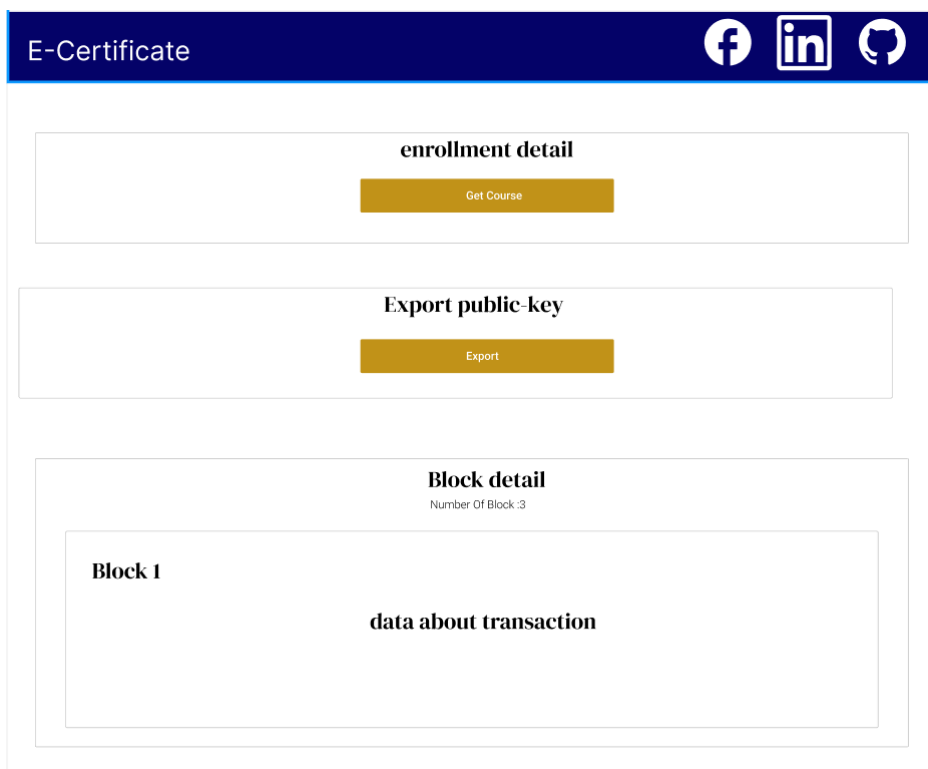
Block 1

data about transaction

รูปที่ 3.6: หน้าหลังจากบริษัท login สำเร็จ



รูปที่ 3.7: หน้าหลังจากบริษัท getข้อมูล



รูปที่ 3.8: หน้าหลังจากนักศึกษา login สำเร็จ

บทที่ 4

การทดลองและผลลัพธ์

ในบทนี้จะเป็นการทดสอบการทำงานของระบบ

4.1 การเข้าถึงข้อมูลและความถูกต้องของข้อมูล

โดยจะทำการทดสอบทั้ง3ฝั่งของUser

1. ฝั่งสำนักทะเบียน สามารถแก้ไขข้อมูลของนักศึกษาได้
2. ฝั่งนักศึกษา สามารถดูข้อมูลของตนเองได้และสามารถสร้าง one time key ซึ่งสามารถใช้ได้1ครั้ง เพื่อให้บริษัทเข้ามาดูได้ สามารถเห็นได้ว่าบริษัทไหนเข้ามาดูข้อมูลของเราได้บ้าง
3. ฝั่งบริษัท เข้าไปดูข้อมูลนักศึกษาตาม key ที่ได้รับมา

4.2 รู้ว่าข้อมูลถูกแก้ไขเมื่อไหร่

ถ้าข้อมูลถูกแก้ไขจะต้องรู้ว่าข้อมูลถูกแก้ไขตรงไหนเมื่อไหร่อย่างไร

4.3 ข้อมูลมีความปลอดภัย

มีแค่สำนักทะเบียนเท่านั้นที่สามารถแก้ไขข้อมูลได้ ซึ่งคนอื่นสามารถทำได้แค่ดู

บรรณานุกรม

- [1] *Blockchain* คืออะไร มีหลักการทำงานอย่างไร. <https://blog.cloudhm.co.th/what-is-blockchain/>.
- [2] นวัตกรรมโอนเงินระหว่างประเทศยุคใหม่ฉบับไว. <https://thirakc.medium.com/>
- [3] มาทำความรู้จัก*HyperledgerFabric* กันเถอะ. <https://thirakc.medium.com/>
- [4] มารู้จัก*Blockchain* ในฉบับของ*HyperledgerFabric* กัน. <https://sutthirak.dev/>
- [5] รู้จัก3ประเภทของ*Blockchain* พร้อมตัวอย่างการนำไปใช้งานเบื้องต้นในแวดวงต่างๆ. <https://tech-sauce.co/tech-and-biz/three-different-types-of-blockchain>.