



ข้อเสนอโครงการวิศวกรรมคอมพิวเตอร์  
วิชา 01076014 การเตรียมโครงการวิศวกรรมคอมพิวเตอร์  
ภาคเรียนที่ 2 ปีการศึกษา 2564

1. ชื่อหัวข้อโครงการ (ไทย) ..... กระเป๋าตังค์ฮาร์ดแวร์สำหรับสกุลเงินเข้ารหัส .....
2. ชื่อหัวข้อโครงการ (อังกฤษ) ..... Cryptocurrency Hardware Wallet .....
3. Keyword 3 คำ ..... single-board computer, cryptocurrency, hardware wallet .....
4. ประเภทโครงการ (✓)  
☒ 1. HW+SW      ☐ 2. SW\_Dev      ☐ 3. Research
5. รายชื่อผู้ทำโครงการ  
5.1. นาย ..... ธนพล วงศ์อาษา ..... รหัส ..... 62010356  
5.2. นาย ..... นนทกร จิตร์ชिरานันท์ ..... รหัส ..... 62010452
6. อาจารย์ที่ปรึกษา  
6.1. อาจารย์ที่ปรึกษาหลัก ..... ดร. ปริญญ์ เอกปริญญ์ .....
- 6.2. อาจารย์ที่ปรึกษาร่วม .....

## 1. ที่มาและความสำคัญของปัญหา (Motivation)

Cryptocurrency หรือสกุลเงินเข้ารหัส เป็นสกุลเงินดิจิทัลที่ถูกออกแบบมาเพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนผ่านเครือข่ายคอมพิวเตอร์ ข้อมูลความเป็นเจ้าของเหรียญ Cryptocurrency จะถูกบันทึกไว้ในบัญชีแยกประเภทแบบดิจิทัล หรือที่เรียกว่า Digital Ledger ซึ่งเป็นระบบฐานข้อมูลที่นำเอาวิทยาการเข้ารหัสลับแบบกุญแจสมมาตร (Asymmetric Cryptography หรือ Public-key Cryptography) มาประยุกต์ใช้เพื่อรักษาความปลอดภัยของบันทึกธุรกรรมรายละเอียดจำนวนเงินเข้าและออก ทำให้สามารถตรวจสอบยืนยันความถูกต้องของความเป็นเจ้าของเหรียญ Cryptocurrency ได้

Cryptocurrency Hardware Wallet หรือกระเป๋าตังค์ฮาร์ดแวร์สำหรับสกุลเงินเข้ารหัส เป็นอุปกรณ์ที่ถูกออกแบบมาเพื่อเก็บรักษาข้อมูลกุญแจที่ใช้กับ Digital Ledger อุปกรณ์ Cryptocurrency Hardware Wallet มักถูกใช้งานในกรณีที่มีทรัพย์สินดิจิทัลในกระเป๋าตังค์มีมูลค่าสูง อุปกรณ์ในกลุ่มนี้จึงถูกออกแบบให้ไม่สามารถเชื่อมต่อหรือเชื่อมต่อกับเครือข่ายใดๆ ด้วยเหตุผลด้านความปลอดภัย ทำให้ความสามารถของ Cryptocurrency Hardware Wallet มีจำกัด และมักต้องใช้งานร่วมกับ smart devices อื่น ๆ

โครงการนี้มีเป้าหมายเพื่อศึกษาแนวทางในการพัฒนา Cryptocurrency Hardware Wallet โดยใช้ single-board computer เพื่อรองรับรูปแบบการใช้งาน Cryptocurrency ที่หลากหลาย ในขณะที่ยังคงความสามารถในการจัดเก็บกุญแจให้มีความปลอดภัย เนื่องจากแต่เดิมนั้น Cryptocurrency Hardware Wallet ถูกออกแบบมาเพื่อรองรับรูปแบบการใช้เพื่อเซ็นรับรองธุรกรรมเช่นการโอนเงินเป็นหลัก แต่ในปัจจุบันความนิยมในการใช้งาน Cryptocurrency ไม่ได้จำกัดเพียงการโอนเงิน แต่ยังครอบคลุมการใช้ distributed application และการซื้อขายงานศิลปะผ่าน Non-fungible Token เป็นต้น ซึ่งการเพิ่มความสามารถให้กับ Cryptocurrency Hardware Wallet จะเป็นการลดความจำเป็นที่ต้องพึ่งพา smart devices

## 2. วัตถุประสงค์ (Objectives)

1. เพื่อศึกษาและพัฒนา hardware wallet ซึ่งสามารถลดความจำเป็นในการใช้ร่วมกับอุปกรณ์อื่น
2. เพื่อศึกษาแนวทางการพัฒนาระบบ hardware wallet ด้วย single-board computer และอุปกรณ์ต่อพ่วงที่หาได้ตามท้องตลาด
3. เพื่อศึกษาเพิ่มเติมความสามารถของ hardware wallet ในการจัดการกับ NFTs

## 3. ทฤษฎีที่เกี่ยวข้อง (Theoretical Background)

### 3.1 Blockchain [1]

Blockchain เป็นเทคโนโลยีการจัดเก็บข้อมูลในลักษณะแบบกระจายศูนย์ ซึ่งอยู่ในระบบเครือข่ายคอมพิวเตอร์ โดยที่ตัวระบบมีลักษณะไม่มีศูนย์กลางในลักษณะแบบ Peer-to-peer ระบบเครือข่ายนั้นจะมีข้อกำหนดที่ทำให้แต่ละจุดในเครือข่ายเห็นข้อมูลชุดเดียวกันทั้งหมด

แนวคิดของ Blockchain นั้นได้เริ่มกล่าวถึงในปี ค.ศ. 1991 โดย Stuart Haber และ W. Scott Stornetta โดยทั้งคู่ ได้เสนอแนวทางระบบสำหรับเอกสารที่มีการบันทึกเวลา (Timestamps) เพื่อไม่ให้เกิดการมาดัดแปลงแก้ไข จนกระทั่งปี ค.ศ. 2008 ได้มีเอกสาร Bitcoin ปรากฏตัวขึ้นและ ต่อมาเครือข่ายของมันก็กำเนิดขึ้นในเดือนมกราคม ปี ค.ศ.2009 โดยบุคคลหรือกลุ่มคนผู้ใช้นามแฝงว่า Satoshi Nakamoto ทำให้แนวคิด Blockchain นั้นเป็นจริง Bitcoin คือสกุลเงินเหรียญดิจิทัล ที่ไม่มีสถาบันการเงินเข้ามาควบคุม และใช้ระบบ Blockchain เป็นระบบในการทำธุรกรรม (Transaction) โดยไม่ต้องผ่านบุคคลที่สาม

### 3.1.1. หลักการทำงาน

ลักษณะการเก็บข้อมูลของ Blockchain นั้นจะเป็นการเก็บข้อมูลธุรกรรมสัญญาทั่วไป (Transaction) ลง Block หลายๆ Block และแต่ละ Block จะมีการเชื่อมโยงกันเป็นห่วงโซ่ (Chain) ยาวเป็นสายเดียว ภายใน Block นั้นจะมีค่า Hash Block ก่อนหน้าเพื่ออ้างอิงเป็นลูกโซ่และตรวจสอบความถูกต้อง



รูปที่ 3.1 การเชื่อมต่อระหว่าง block<sup>1</sup>

หาก Block มีการเปลี่ยนแปลงข้อมูลจะทำให้ค่า Hash ของ Block นั้นเปลี่ยนตาม ส่งผลให้ Block ที่มีการเชื่อมต่อก่อนหน้านั้นไม่สามารถอ้างอิงถึง Block ที่มีการเปลี่ยนแปลงข้อมูลได้ และนำไปสู่กระบวนการตรวจสอบความถูกต้องในระบบเครือข่ายภายหลัง เนื่องจากการเรียง Block ไม่ตรงกับ จุดอื่นภายในเครือข่าย หรือหากมีความจำเป็นต้องแก้ไข Block นั้น Block ลำดับถัดไปที่มาต่อหลังจาก Block นี้ต้องแก้ไขค่า Hash ใหม่ตามทั้งหมด การแก้ไขข้อมูลจึงเป็นเรื่องยากและทำให้มีความปลอดภัยสูงหากมี Block ต่อหลังเป็นจำนวนมาก

### 3.1.2. ขั้นตอนการทำงาน

1. CREATE คือ การสร้าง Block ที่บรรจุคำสั่งขอทำรายการธุรกรรม
2. BROADCAST คือ ทำการกระจาย Block ใหม่นี้ให้กับทุก Node ในระบบ และบันทึกรายการธุรกรรมลง Ledger<sup>2</sup> ให้กับทุก Node เพื่ออัปเดตว่ามี Block ใหม่เกิดขึ้นมา

<sup>1</sup> ที่มาภาพจาก <https://bitcoin.org/bitcoin.pdf>

<sup>2</sup> บันทึก หรือสมุดบันทึกการเคลื่อนไหวของบัญชี

3. VALIDATION คือ Node อื่น ๆ ในระบบทำการยืนยันและตรวจสอบข้อมูลของ Block นั้นว่าถูกต้องตามเงื่อนไข Validation โดยกระบวนการทำ Consensus ถือว่าเป็นส่วนหนึ่งของกระบวนการทำ Validation

### 3.1.3. องค์ประกอบ

Block คือ ชุดบรรจุข้อมูลซึ่งมี 2 ส่วนคือส่วนของสิ่งของต่าง ๆ ที่ใส่เข้าไปเรียกว่า Item และส่วนแพะหัวกล่องหรือ Header เพื่อใช้บอกให้คนอื่นทราบว่าบรรจุอะไรมา (แต่เปิดดู Item ภายในนั้นไม่ได้)

Chain คือ หลักการจดจำทุก ๆ ธุรกรรมของทุก ๆ คนในระบบและบันทึกข้อมูลพร้อมจัดทำเป็นสำเนาบัญชี Ledger แจกจ่ายให้กับทุกคนในระบบ

Consensus คือ ข้อตกลงร่วมกัน

Validation คือ การตรวจสอบความถูกต้องแบบทบทวนทั้งระบบและทุก Node

## 3.2 Smart Contract [2]

Smart Contract เป็นกระบวนการทางดิจิทัล ที่มีการกำหนดขั้นตอนในการปฏิบัติ ไว้ล่วงหน้าก่อน และถูกสร้างขึ้นโดยไม่อาศัยตัวกลาง การใช้งาน Smart Contract คือการใช้งานชุดคำสั่งดังกล่าวนี้ โดยคู่สัญญาจะตกลงถึงขั้นตอนและกลไกก่อนที่จะทำธุรกรรม

แนวคิดของ Smart Contract ที่กล่าวถึงบ่อยในปัจจุบัน เกิดมาจาก Nick Szabo โดยมีการเสนอความคิดไว้ว่า Blockchain สามารถนำมาใช้เป็นสื่อกลางในการทำให้เกิดข้อตกลงสัญญาอัจฉริยะ หรือ Smart Contracts ขึ้นมาได้ โดยไม่จำเป็นต้องมีตัวกลางมาตรวจสอบว่าสัญญาเป็นได้จริงหรือไม่

ตัวอย่างการใช้งาน Smart Contract จะยกตัวอย่างการซื้อขายรถยนต์ และเป็นการทำสัญญาระหว่างสองฝ่าย อลิซ และ บ๊อบ โดยทั่วไปหากใช้งานสัญญาปกติ จำเป็นจะต้องมีตัวกลางเป็นบุคคลที่สามที่เชื่อถือได้ เพื่อยืนยันความถูกต้องของสัญญาก่อน ซึ่งเป็นกระบวนการซับซ้อน ใช้เวลานานและต้องเสียค่าธรรมเนียมจำนวนมาก แต่หากใช้งาน Smart Contract อลิซ และ บ๊อบสามารถออกแบบขั้นตอนที่สัญญาจะทำ จากนั้นจึงใช้ระบบ Blockchain ในการยืนยันความถูกต้องของสัญญา

### 3.2.1. เครื่องมือที่ใช้พัฒนา [3]

#### 3.2.1.1. Solidity

เป็นภาษาโปรแกรมเชิงวัตถุที่มุ่งเน้นในการเขียนด้าน Smart Contract มีไวยากรณ์คล้ายกับ JavaScript, C ++ หรือ Java

#### 3.2.1.2. Etherscan

Etherscan เป็น Blockchain Explorer <sup>3</sup>และแพลตฟอร์มการวิเคราะห์ที่ให้รายละเอียดเกี่ยวกับธุรกรรมบล็อกเชน Ethereum ที่กำลังรอดำเนินการ หรือได้รับการยืนยัน

Etherscan เป็นเครื่องมือสำหรับค้น และตรวจสอบข้อมูลสาธารณะทั้งหมดบนบล็อกเชน Ethereum และบางครั้งเรียกว่า “Ethplorer” ข้อมูลนี้รวมถึงข้อมูลธุรกรรม ที่อยู่กระเป๋าเงิน Smart Contract และอื่นๆ อีกมากมาย

### 3.3 Tokens [4]

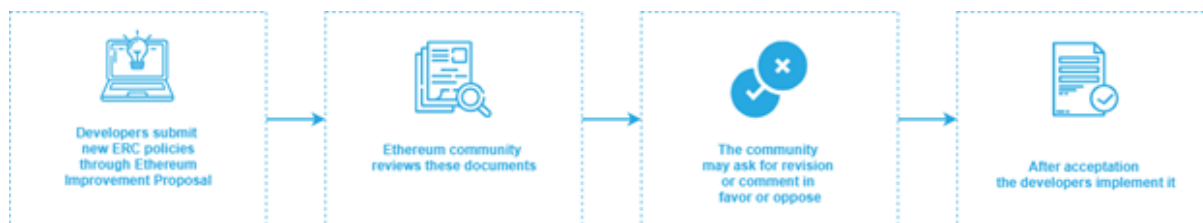
tokens คือเหรียญ cryptocurrency ที่ถูกสร้างขึ้น โดยไม่ได้มี blockchain เป็นของตัวเอง โดยสร้างอยู่บน Blockchain ของเหรียญอื่น เช่น เหรียญ UNI ถูกสร้างขึ้นบน Blockchain ของ Ethereum โดยอาจจะถูกสร้างโดย smart contract เพื่อใช้ในวัตถุประสงค์ที่เจาะจง เพื่อใช้ในระบบนิเวศน์บางอย่าง

---

<sup>3</sup> เครื่องมือสำหรับตรวจสอบข้อมูล การเคลื่อนไหวของ Blockchain

### 3.3.1. Ethereum Request for Comment [3]

เรียกโดยชื่อย่อว่า ERC ถือเป็นขั้นตอนในการพัฒนา Ethereum แบบหนึ่ง ซึ่งจะถูกสร้างเพื่อให้สมาชิกผู้พัฒนา Ethereum ให้ความเห็น ทั้งทางเทคนิคและมาตรฐานก่อนที่จะมีการนำไปใช้งานจริงในเครือข่าย Ethereum



รูปที่ 3.2 ขั้นตอนการบัญญัติ ERC<sup>4</sup>

<sup>4</sup> ที่มาภาพจาก <https://articles.devsight.me/smart-contract-%E0%B8%9A%E0%B8%99-ethereum-public-blockchain-permissionless-blockchain-%E0%B8%94%E0%B9%89%E0%B8%A7%E0%B8%A2-solidity-path-3-95eb4a3c9cae>

### 3.3.1.1. ERC20

เป็นมาตรฐานในการพัฒนาที่นิยมใช้ใน token รูปแบบ Fungible Token และอนุญาตให้ใช้รูปแบบ Application Programming Interface (API) ภายใน smart contract (ส่วนใหญ่ใช้ใน ICOs<sup>5</sup>)

โดยที่ Fungible Token (FT) เป็นทรัพย์สินที่มีคุณสมบัติความสามารถทดแทนกันได้ ยกตัวอย่างเช่น ธนบัตรชนิดราคา 20 บาทที่ได้รับจากแม่ค้ากับธนบัตรชนิดราคา 20 บาทที่ได้รับจากธนาคาร สามารถใช้ทดแทนกันได้เนื่องจากคุณสมบัติความสามารถทดแทนกัน

### 3.3.1.2. ERC721

เป็นมาตรฐานในการพัฒนาที่นิยมใช้ใน token รูปแบบ Non-Fungible Token และอนุญาตให้ใช้รูปแบบ Application Programming Interface (API) ภายใน smart contract นอกจากนั้นยังมีฟังก์ชันการถ่ายโอนและติดตาม Non-Fungible Tokens

โดยที่ Non-Fungible Token (NFT) เป็นทรัพย์สินที่มีคุณสมบัติแตกต่างกันและไม่สามารถทดแทนกันได้ ยกตัวอย่างเช่น ที่ดินบ้านของครอบครัวกับที่ดินบ้านของเพื่อนไม่สามารถทดแทนกันได้ หรือ แมวของครอบครัวกับแมวของเพื่อนไม่สามารถทดแทนกันได้

## 3.4 Crypto Wallet [5]

การใช้งาน cryptocurrency จำเป็นต้องใช้ private key ซึ่งเป็นกุญแจสำหรับใช้ทำธุรกรรมบน blockchain โดยผู้ใช้งานจำเป็นต้องรักษาไว้ หากสูญหายจะทำให้ไม่สามารถเข้าถึงสินทรัพย์ได้ และหากมีการโจรกรรม โดยมีจาชิปก็สามารถก่อให้เกิดการสูญเสียทรัพย์สินในบัญชีได้

กระเป๋าดิจิทัล หรือ crypto wallet จึงเป็นเครื่องมือเพื่ออำนวยความสะดวกในการเก็บ private key เพื่อเพิ่มความปลอดภัยในการใช้งาน cryptocurrency

---

<sup>5</sup> Initial Coin Offerings หรือเป็นการระดมทุน โดยใช้เหรียญ Token เพื่อเป็นหลักประกันในการระดมทุนนั้น ๆ



### 3.4.1. ประเภทของ Wallet

crypto wallet สามารถแบ่งออกได้หลายลักษณะ ตามลักษณะการใช้งาน โดยรูปแบบที่นิยมแบ่งสามารถแบ่งออกได้ 2 ประเภท ดังนี้

1. hot wallet คือกระเป๋าที่สร้างโดยใช้ระบบดิจิทัล และเชื่อมต่อกับเครือข่ายอยู่ตลอดเวลา ซึ่งโดยทั่วไปมักจะถูกสร้างโดยใช้ software อย่างเดียว  
จุดเด่นของ hot wallet คือใช้งานง่าย สะดวกเหมือนระบบการเงินโดยทั่วไป สามารถเข้าถึงได้ง่าย ถ่ายโอนสินทรัพย์ รวมถึงสร้างธุรกรรมได้สะดวก แต่มีข้อเสียเนื่องจากจำเป็นต้องเชื่อมต่อกับระบบเครือข่ายอยู่ตลอดเวลาจึงมีความเสี่ยงที่อาจถูกโจมตีจากระบบเครือข่ายได้
2. cold wallet คือกระเป๋าเงินที่ไม่มีการเชื่อมต่อเครือข่ายอินเทอร์เน็ต หากผู้ใช้งานต้องการทำธุรกรรมจะต้องดึงข้อมูลออกจาก cold wallet และนำข้อมูลนั้นส่งต่อไปที่อื่นเพื่อทำธุรกรรม จึงจะสามารถทำให้เกิดธุรกรรมขึ้นได้

cold wallet ที่ได้รับความนิยมมี 2 รูปแบบ ได้แก่ paper wallet คือการบันทึก wallet address และ private key ในกระดาษ ทั้งในรูปของการจุดหรือ pattern ที่สามารถแปลงเป็น wallet address และ private key ได้ อีกรูปแบบหนึ่งคือ hardware wallet ซึ่งเป็นอุปกรณ์เก็บรหัส มักออกแบบด้วยรูปแบบบัตรหรือ thumb drive

จุดแข็งของ cold wallet คือด้านความปลอดภัย เนื่องจากการจะเข้าถึง private key นั้นต้องเข้าถึงตัว wallet โดยตรง ซึ่งลดโอกาสการโดนโจมตีทางดิจิทัลได้อย่างมาก ขณะเดียวกัน จุดด้อยของ cold wallet คือหากสูญหาย ก็ยากที่จะเข้าถึงการใช้งานใน private key ได้

จากคุณสมบัติข้างต้นของทั้ง 2 ประเภท สามารถระบุได้ว่า hot wallet เหมาะกับผู้ใช้งาน cryptocurrency ทั่วไปหรือผู้ที่ต้องใช้งานรายวัน เก็บจำนวนเหรียญไว้ไม่สูง เพื่อความคล่องตัวในการใช้งาน ขณะที่ cold wallet เหมาะกับผู้ที่ต้องการเก็บ cryptocurrency จำนวนหรือมีมูลค่ามาก เพื่อการเก็บรักษามากกว่าโอนถ่ายใช้งานเหรียญ

### 3.4.2. Hardware Wallet [6]

เป็นอุปกรณ์ที่ทำหน้าที่เป็น Cryptocurrency wallet ประเภทหนึ่งซึ่งมีหน้าที่ในการเก็บ Private Key ของผู้ใช้ไว้เพื่อใช้ในการทำธุรกรรม ข้อดีของ hardware wallet คือ

1. พกพาได้สะดวก
2. มีความปลอดภัยสูง

ตัวอย่าง hardware wallet ที่วางขายในท้องตลาดได้แก่ Ledger, Trezor, SafePal เป็นต้น อุปกรณ์เหล่านี้มีความปลอดภัยสูงและมีความสามารถแตกต่างกันไป ให้เลือกใช้ได้ตามที่ผู้ใช้ หรือสามารถสร้างด้วยตนเองได้ โดยมีรูปแบบหนึ่งเป็นที่นิยมซึ่งสร้างโดยใช้บอร์ด Raspberry Pi เรียกว่า PiTrezor

## 3.5 Web Application

web application เป็นซอฟต์แวร์ที่รันอยู่บน web server และส่วนใหญ่สามารถเข้าถึงได้ผ่าน web browser มีการทำงานเป็นสถาปัตยกรรมแบบ client-server [7]

### 3.5.1. การพัฒนา Web Application ในปัจจุบัน

web application ส่วนใหญ่สามารถแบ่งส่วนการทำงานได้เป็น 2 ส่วนคือ front-end และ back-end โดยการพัฒนาแอปพลิเคชันในฝั่ง front-end จะเป็นส่วนของการติดต่อกับผู้ใช้และส่วน back-end จะเป็นส่วนติดต่อกับ database, API, และการทำกิจกรรมอื่น ๆ เบื้องหลังเช่นการเก็บ log การเรียกใช้ทรัพยากร เป็นต้น [8]

ในปัจจุบันการพัฒนาแอปพลิเคชันทั้ง 2 ฝั่งมีการนำ framework และ library มาใช้งานเพื่อให้ผู้พัฒนาสามารถทำงานได้ง่ายขึ้น

ข้อดีของการพัฒนาแอปพลิเคชันด้วย framework/library คือ ซอฟต์แวร์มีเสถียรภาพมากขึ้น, ผู้พัฒนาสามารถพัฒนาซอฟต์แวร์ได้เร็วยิ่งขึ้น, รูปแบบโค้ดมีความเป็นมาตรฐานและสม่ำเสมอ, และประสบการณ์การใช้งานของผู้ใช้ที่ดีขึ้น

ข้อเสียของการพัฒนาแอปพลิเคชันด้วย framework/library คือ ซอฟต์แวร์อาจมีความซับซ้อนมากขึ้นโดยไม่จำเป็น, การดัดแปลงซอฟต์แวร์เดิมให้เข้ากับ framework/library ทำได้ยาก, แนวทางพัฒนาถูกจำกัด, การเปลี่ยน version ของ framework/ library อาจทำให้เกิดบัค, และผู้พัฒนาต้องใช้เวลาในการศึกษาใช้งาน [9]

### 3.5.2. React JS (ย้ายไปส่วนผลการศึกษา)

React เป็น front-end JavaScript library สำหรับการทำ website ที่เป็น single-page application นอกจากนี้ยังสามารถใช้งานได้ฟรีและเป็น open source โดยมีจุดเด่นที่การมองส่วนประกอบของ user interface เป็น component [10]

จุดเด่นของ React [11] คือ

1. การโค้ดเน้นที่ให้โปรแกรม “ทำอะไร” ไม่ใช่ “ทำอะไร” จึง debug ได้ง่ายและผลลัพธ์มีความแน่นอนสม่ำเสมอ

2. มองส่วนของโปรแกรมเป็นชิ้นส่วนย่อยที่ไม่ขึ้นต่อกัน (Component) การใช้งานเพียงนำแต่ละส่วนมาประกอบต่อกันจะสามารถทำเป็น user interface ได้โดยง่าย นอกจากนี้ยังสามารถใช้ JavaScript ในการควบคุมการทำงานของแต่ละชิ้นส่วนได้โดยตรงโดยอยู่ในรูปของ JSX
3. ไม่มีข้อจำกัดทางด้าน tech stack และหากต้องการทำโปรแกรมในรูปแบบอื่นเช่น mobile application ก็สามารถเลือกใช้ React Native ซึ่งมีความคล้ายคลึงกันในการพัฒนาได้เช่นกัน

การพัฒนา front-end ด้วย React ซึ่งในปัจจุบันมีความซับซ้อนมากขึ้น จึงมีการพัฒนาเป็น package ขึ้นมาเพื่อให้พัฒนาได้ง่ายขึ้น สำหรับ package ที่นิยมใช้งานกันเช่น

1. React Router เป็น package สำหรับทำการ routing ทั้งฝั่ง client-side และ server-side [12]
2. Redux เป็น state management package สำหรับแอปพลิเคชัน JavaScript ในปัจจุบันแนะนำให้ใช้งาน Redux Toolkit ซึ่งเป็น library เสริมที่พัฒนาโดยใช้ Redux เป็นแกนหลัก และสำหรับการใช้งานกับ React แนะนำให้ใช้ package React Redux ควบคู่กันด้วย [13]
3. Tailwind CSS เป็น utility CSS framework ที่ช่วยให้สามารถตกแต่ง UI โดยอาศัยการเรียกใช้งาน utility class ต่าง ๆ ที่ตัว package มีมาให้ นอกจากนี้ยังสามารถทำการปรับแต่งหรือเพิ่มเติม class ได้ตามความต้องการอีกด้วย [14]

#### 4. งานวิจัยที่เกี่ยวข้อง (Related Works)

##### 4.1 Security Of Cryptocurrency Using Hardware Wallet and QR Code [15]

งานวิจัยนี้เป็นการทำ Bitcoin wallet บนระบบปฏิบัติการ Android โดยมีการใช้งานแบ่งเป็น 2 ส่วนคือส่วนที่เป็น QR code-based application ซึ่งจะทำหน้าที่เป็น hot wallet และส่วนที่เป็น cold wallet ซึ่งทำหน้าที่เก็บรักษา private key

cold wallet จะถูกใช้งานในรูปแบบ offline เพื่อทำหน้าที่ในการ generate และเก็บ private key สำหรับผู้ใช้งาน

hot wallet ที่ได้ทำการพัฒนานี้มีความสามารถในการโอน Bitcoin และช่วยให้ผู้ใช้สามารถติดตามประวัติการทำธุรกรรมกับ Bitcoin รวมถึงการ sign transaction ได้อีกด้วยโดยอาศัยการสแกน QR code เพื่อทำการระบุตัวตน ยืนยันตัวตน และตรวจสอบตัวตนของผู้ใช้ เพื่อให้มีความปลอดภัย

##### 4.2 Cryptocurrency Wallet: A Review [16]

งานวิจัยนี้ศึกษาเกี่ยวกับชนิดของ wallet ที่ใช้ในการเก็บ public key และ private key สำหรับการทำธุรกรรมบน blockchain ซึ่งสามารถแบ่งได้ 3 ประเภทคือ software, hardware, และ paper ซึ่ง software wallet จะอยู่ในรูปแบบ website, โทรศัพท์เคลื่อนที่, หรือบน Desktop

งานวิจัยนี้เน้นการศึกษาไปที่ wallet ซึ่งสามารถรองรับ cryptocurrency ได้หลายสกุลโดยทำการศึกษาคูณลักษณะในแง่จำนวนสกุล cryptocurrency ที่รองรับ, ภาวะนิรนาม, ราคา, platform ที่รองรับ, การจัดการ key, วิธีการกู้คืน wallet, และการรองรับเงินตราที่ไม่มีทุนสำรอง

## 5. ขอบเขตของโครงการ (Scope)

- 5.1 hardware wallet สามารถเก็บ cryptocurrency สกุลที่ทำงานอยู่บน Ethereum เท่านั้น
- 5.2 hardware wallet สามารถแสดงข้อมูลของ NFTs ที่มาจาก OpenSea ได้เท่านั้น
- 5.3 NFTs ที่สามารถ trade ได้จะต้องอยู่บน OpenSea เท่านั้น
- 5.4 การโอน cryptocurrency สามารถทำได้เฉพาะกับสกุลที่ทำงานอยู่บน Ethereum เท่านั้น

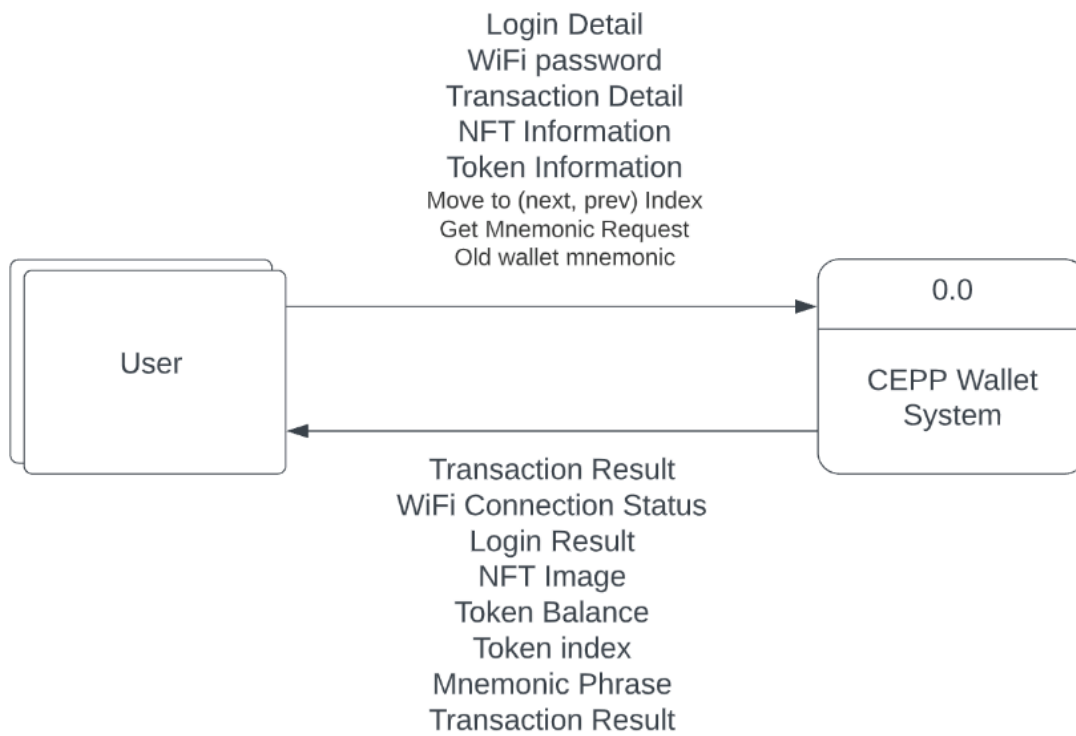
## 6. การพัฒนาโครงการ (Project Development)

### 6.1 ขั้นตอนการพัฒนา (Methodology)

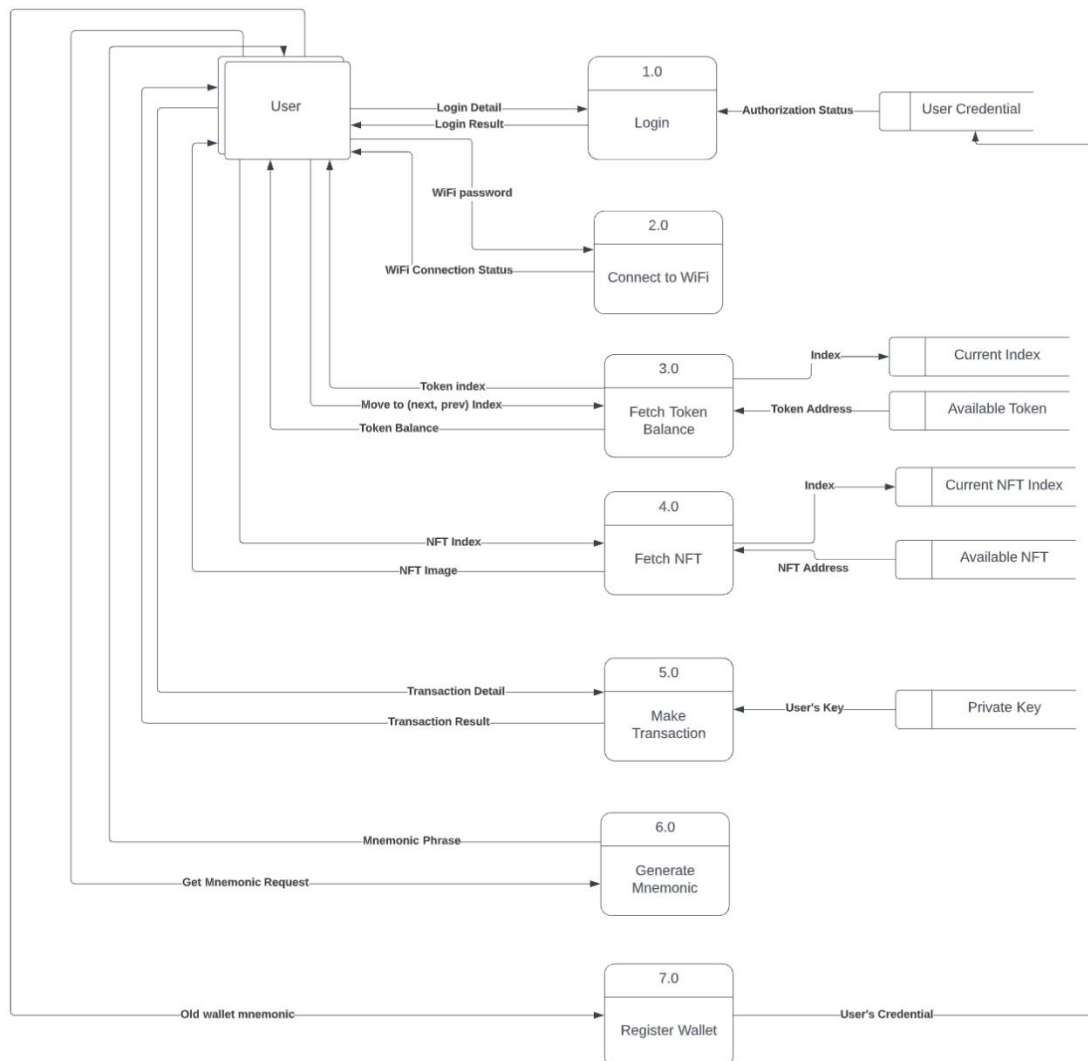
1. กำหนดวัตถุประสงค์ ขอบเขต และเป้าหมายของโครงการ
2. วางแผนการดำเนินโครงการและแบ่งการรับผิดชอบแต่ละส่วน
3. สืบค้นและศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง
4. พัฒนาโครงการ
  - พัฒนา hardware wallet
  - พัฒนา application (user interface) สำหรับ hardware wallet
  - รวมส่วน hardware wallet เข้ากับ application
5. ทดสอบความสามารถของ hardware wallet และทำการปรับปรุงแก้ไข
6. นำ hardware wallet ที่ได้พัฒนาไปทดสอบกับผู้ใช้งานจริง และปรับปรุงแก้ไขตามข้อติชมที่ได้รับ
7. สรุปผลการดำเนินงานและจัดทำเอกสาร

### 6.2 การออกแบบ (Design)

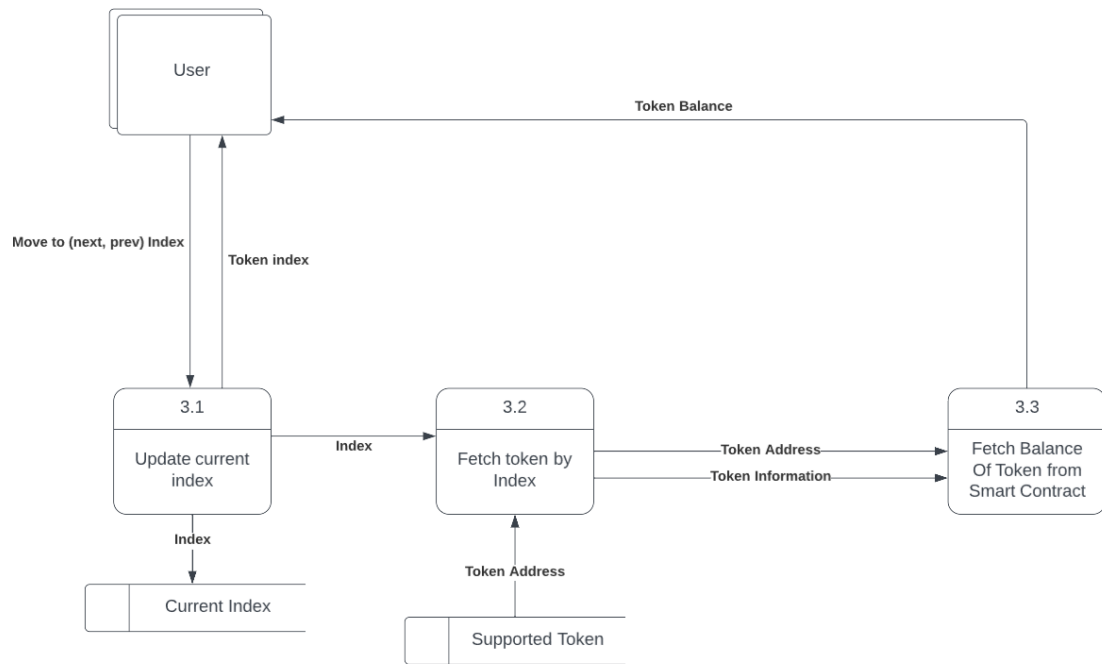
#### 6.2.1. Dataflow Diagram



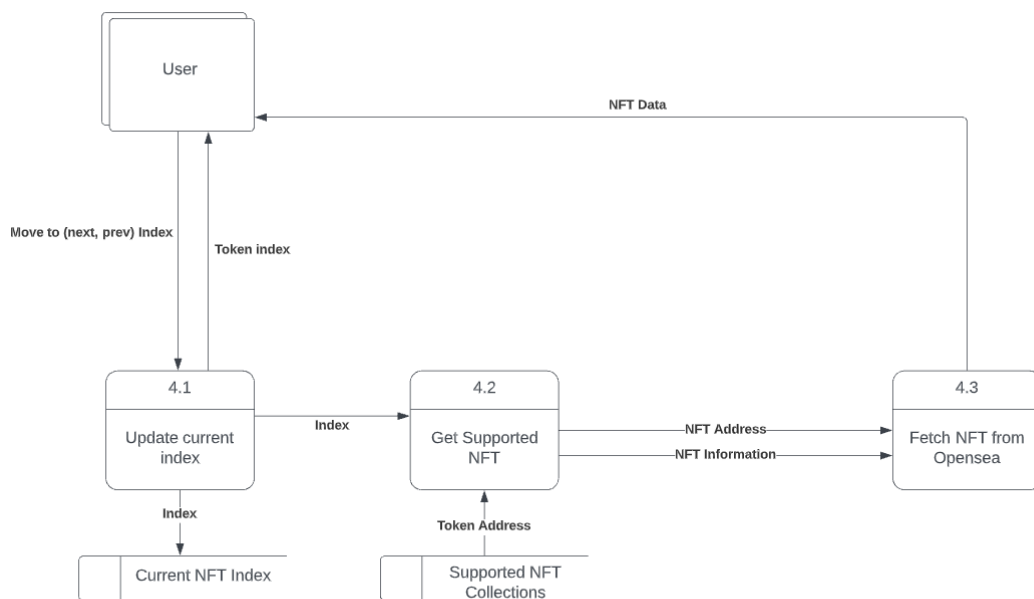
รูปที่ 6.1 Context diagram



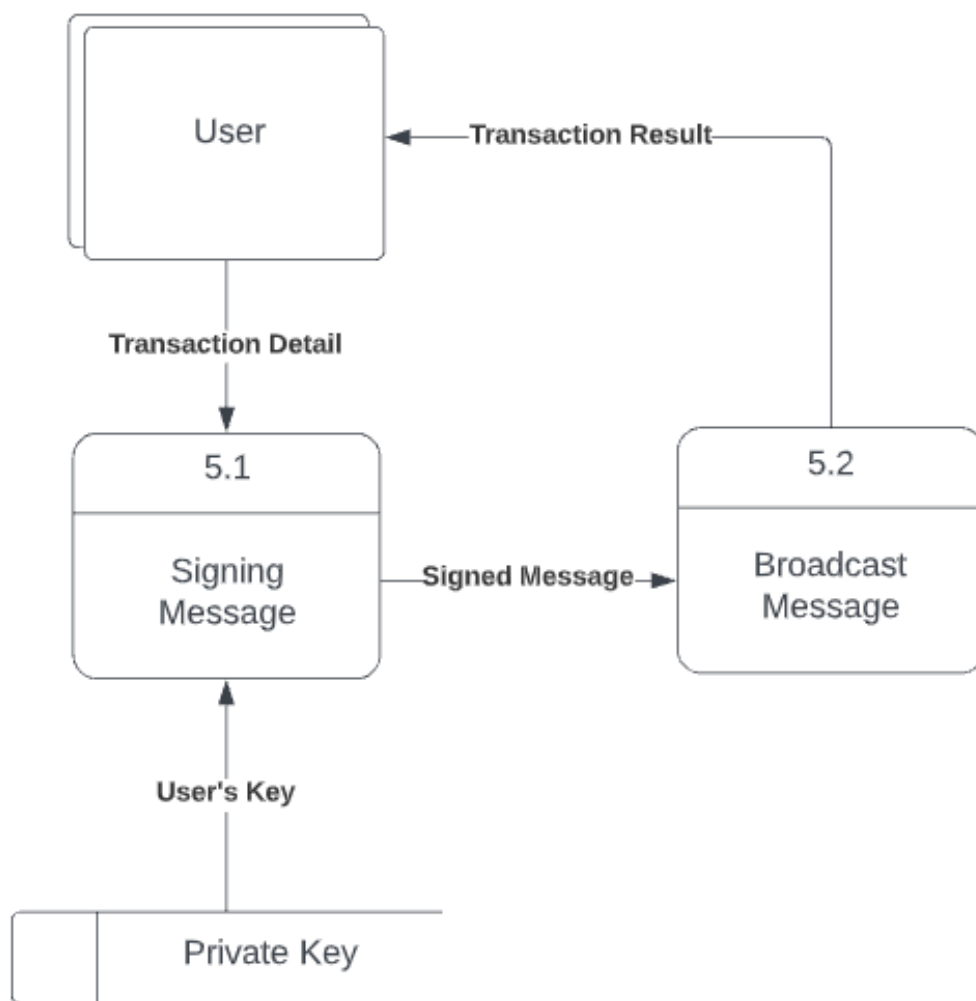
รูปที่ 6.2 Diagram 0



รูปที่ 6.3 Diagram 1: Process 3.0 Fetch Token Balance



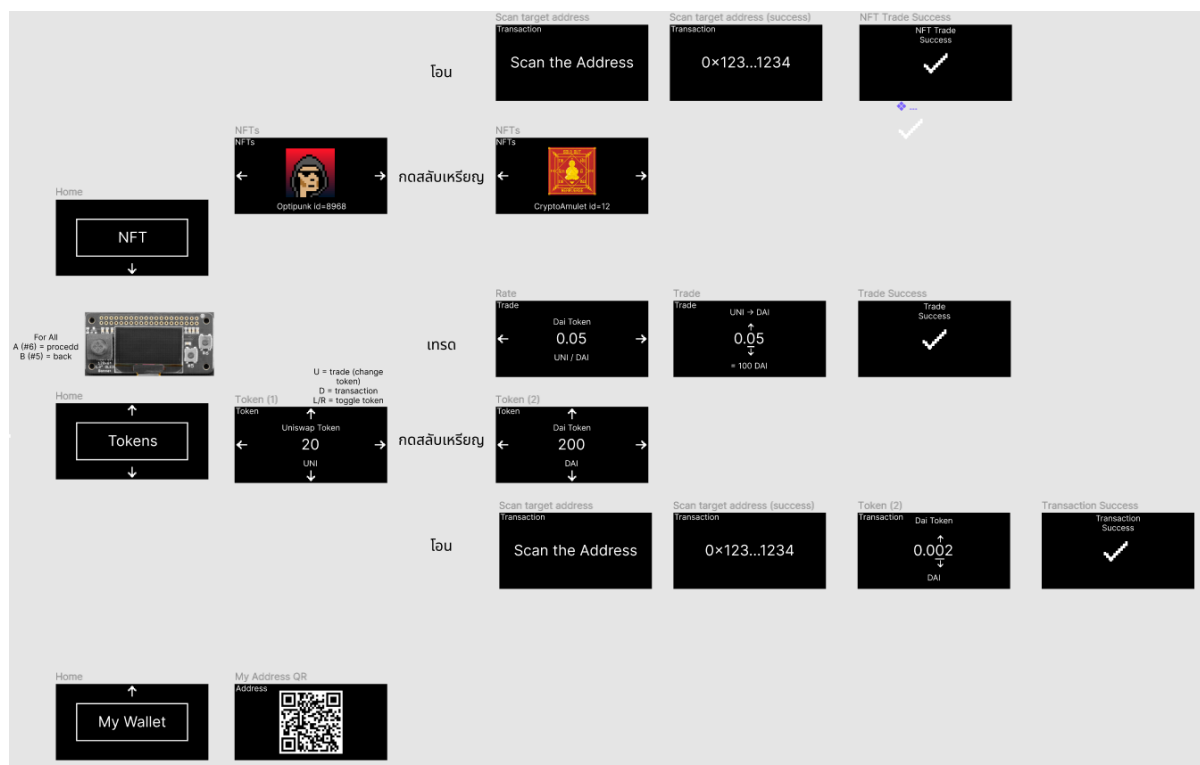
รูปที่ 6.4 Diagram 1: Process 4.0 Fetch NFT



รูปที่ 6.5 Diagram 1: Process 5.0 Make Transaction

### 6.2.2. User Interface Design





รูปที่ 6.6 User interface design

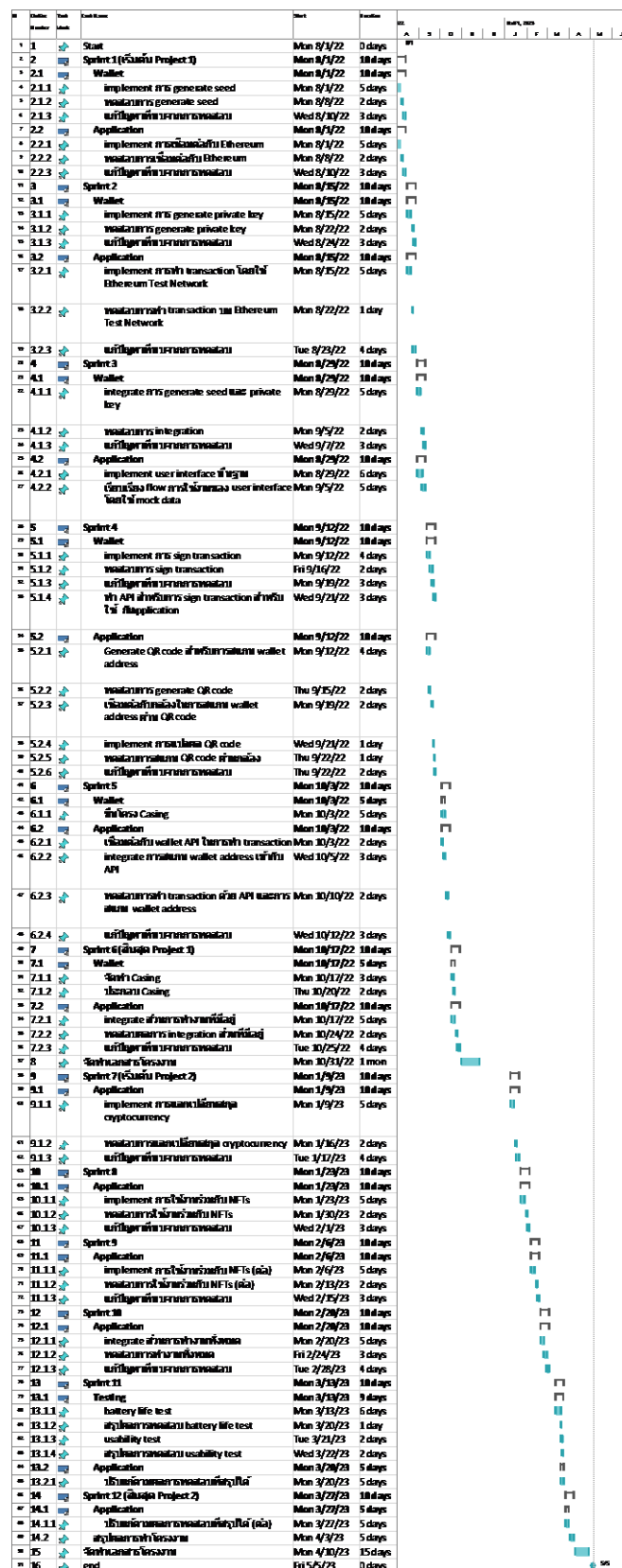
### 6.3 แนวทางการทดสอบและการวัดประสิทธิภาพ (Test and Performance Evaluation Approaches)

6.3.1. ทดสอบ unit test สำหรับ application โดยใช้ Jest framework

6.3.2. ทดสอบอายุการใช้งาน (battery life) ว่าอุปกรณ์ที่พัฒนาสามารถใช้งานได้กี่นาทีโดยทดสอบในสถานการณ์ที่เป็น idle (stand by) และเปิดหน้าจอหลักไว้ตลอดเวลา โดยทดสอบอย่างละ 3 รอบและหาค่าเฉลี่ยเวลาที่ใช้งานได้

6.3.3. ทดสอบ Usability Test โดยใช้อาสาสมัครที่มีความสนใจด้าน cryptocurrency เป็นผู้เข้าร่วมทดสอบอุปกรณ์ที่ได้พัฒนา

## 7. แผนการดำเนินงานโครงการ (Gantt Chart)



รูปที่ 7.1 Gantt chart

## 8. ประโยชน์ที่คาดว่าจะได้รับ (Expected Benefits)

1. ผู้จัดทำได้รับความรู้พื้นฐานเกี่ยวกับบล็อกเชนและการจัดเก็บกุญแจด้วยกระเป๋าฮาร์ดแวร์
2. ผู้จัดทำได้รับความรู้พื้นฐานในพัฒนาโปรแกรมประยุกต์เพื่อทำงานบน single-board computer
3. แนวทางการพัฒนาระบบฮาร์ดแวร์และซอฟต์แวร์สำหรับ cryptocurrency hardware wallet
4. ผู้ใช้ wallet มีช่องทางเพิ่มเติมในการแสดงความเป็นเจ้าของ NFTs และสามารถแลกเปลี่ยน NFTs ได้สะดวกมากขึ้น

## 9. ผลการศึกษาเทคโนโลยีที่ใช้พัฒนา (หากไม่มั่นใจ tech ไหนอย่าเอาลง)

9.1 React

9.2 Redux

9.3 Tailwind CSS

9.4 Docker

9.5 Python

## 10. เอกสารอ้างอิง (Reference)

- [1] “Why is Blockchain Important and Why Does it Matters [2022 Edition],” Simplilearn.com.<https://www.simplilearn.com/tutorials/blockchain-tutorial/why-is-blockchain-important> (accessed May 05, 2022).
- [2] “SMART CONTRACT คืออะไร?,” ETDA. <https://www.etda.or.th/th/Useful-Resource/knowledge-sharing/articles/What-is-Smart-Contract.aspx> (accessed May 05, 2022).
- [3] P. Nakarin, “Smart Contract บน Ethereum Public Blockchain/Permissionless Blockchain ด้วย Solidity Path 3...,” Medium, Dec. 31, 2020. <https://articles.devsight.me/smart-contract-%E0%B8%9A%E0%B8%99-ethereum-public-blockchain-permissionless-blockchain-%E0%B8%94%E0%B9%89%E0%B8%A7%E0%B8%A2-solidity-path-3-95eb4a3c9cae> (accessed May 05, 2022).
- [4] “Coin และ Token แตกต่างกันอย่างไร?” <https://zipmex.com/th/learn/difference-between-coin-token/> (accessed May 05, 2022).
- [5] “มารู้จัก Crypto Wallet เมื่อ Cryptocurrency ก็ต้องใช้กระเป๋าเงิน.” <https://www.scb10x.com/blog/getto-know-cryptowallet> (accessed May 05, 2022).
- [6] W. Suknantee, “Hardware Wallet คืออะไร?,” Bitkub.com, Dec. 14, 2020. <https://medium.com/bitkub/hardware-wallet-acf1868a9558> (accessed May 05, 2022).
- [7] “Web application,” Wikipedia. Apr. 27, 2022. Accessed: May 05, 2022. [Online]. Available: [https://en.wikipedia.org/w/index.php?title=Web\\_application&oldid=1084972116](https://en.wikipedia.org/w/index.php?title=Web_application&oldid=1084972116)

- [8] “Web App Development in 2022: Everything You Need to Know.” <https://trio.dev/blog/web-app-development> (accessed May 05, 2022).
- [9] “Pros and Cons of Using a Front-End Library (Or Framework).” <https://bluemodus.com/articles/pros-and-cons-of-using-a-front-end-library-or-framework> (accessed May 05, 2022).
- [10] “React (JavaScript library),” Wikipedia. May 02, 2022. Accessed: May 05, 2022. [Online]. Available: [https://en.wikipedia.org/w/index.php?title=React\\_\(JavaScript\\_library\)&oldid=1085724690](https://en.wikipedia.org/w/index.php?title=React_(JavaScript_library)&oldid=1085724690)
- [11] “React – A JavaScript library for building user interfaces.” <https://reactjs.org/> (accessed May 05, 2022).
- [12] “React Router | Tutorial.” <https://reactrouter.com/docs/en/v6/getting-started/tutorial> (accessed May 05, 2022).
- [13] “Getting Started with Redux | Redux.” <https://redux.js.org/introduction/getting-started> (accessed May 05, 2022).
- [14] “Tailwind CSS - Rapidly build modern websites without ever leaving your HTML.” <https://tailwindcss.com/> (accessed May 05, 2022).
- [15] A. G. Khan, A. H. Zahid, M. Hussain, and U. Riaz, “Security Of Cryptocurrency Using Hardware Wallet And QR Code,” in 2019 International Conference on Innovative Computing (ICIC), Lahore, Pakistan, Nov. 2019, pp. 1–10. doi: 10.1109/ICIC48496.2019.8966739.
- [16] S. Suratkar, M. Shirole, and S. Bhirud, “Cryptocurrency Wallet: A Review,” in 2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP), Chennai, India, Sep. 2020, pp. 1–7. doi: 10.1109/ICCCSP49186.2020.9315193.