ข้อเสนอโครงงานวิศวกรรมคอมพิวเตอร์
วิชา 01076014 การเตรียมโครงงานวิศวกรรมคอมพิวเตอร์
ภาคเรียนที่ 2 ปีการศึกษา 2564

1. ชื่อหัวข้อโครงงาน (ไทย) กระเป๋าสตางค์ฮาร์ดแวร์สำหรับสกุลเงินเข้ารหัส
2. ชื่อหัวข้อโครงงาน (อังกฤษ) Cryptocurrency Hardware Wallet
3. Keyword 3 คำ single-board computer, cryptocurrency, hardware wallet
4. ประเภทโครงงาน (✓)

   ✓ 1. HW+SW ☐ 2. SW_Dev ☐ 3. Research

5. รายชื่อผู้ทำโครงงาน

   5.1. นาย ธนพล วงศ์อาษา รหัส 62010356

   5.2. นาย นนทกร จิตรชิรานันท์ รหัส 62010452

6. อาจารย์ที่ปรึกษา

   6.1. อาจารย์ที่ปรึกษาหลัก ดร. ปริญญา เอกปริญญา

   6.2. อาจารย์ที่ปรึกษาร่วม

1. ที่มาและความสำคัญของปัญหา (Motivation)

Cryptocurrency หรือสกุลเงินเข้ารหัส เป็นสกุลเงินดิจิทัลถูกออกแบบมาเพื่อใช้เป็นสื่อกลางในการแลกเปลี่ยนผ่านเครือข่ายคอมพิวเตอร์ ข้อมูลความเป็นเจ้าของเหรียญ Cryptocurrency จะถูกบันทึกไว้ในบัญชีแยกประเภทแบบดิจิทัล หรือที่เรียกว่า Digital Ledger ซึ่งเป็นระบบฐานข้อมูลที่นำเอาวิทยาการเข้ารหัสลับแบบกุญแจอสมมาตร (Asymmetric Cryptography หรือ Public-key Cryptography) มาประยุกต์ใช้เพื่อรักษาความปลอดภัยของบันทึกธุรกรรมรายละเอียดจำนวนเงินเข้าและออก ทำให้สามารถตรวจสอบยืนยันความเป็นเจ้าของเหรียญ Cryptocurrency ได้

Cryptocurrency Hardware Wallet หรือกระเป๋าสตางค์ฮาร์ดแวร์สำหรับสกุลเงินเข้ารหัส เป็นอุปกรณ์ที่ถูกออกแบบมาเพื่อเก็บรักษาข้อมูลกุญแจที่ใช้กับ Digital Ledger อุปกรณ์ Cryptocurrency Hardware Wallet มักถูกใช้งานในกรณีที่มีทรัพย์สินดิจิทัลในกระเป๋าสตางค์มีมูลค่าสูง อุปกรณ์ในกลุ่มนี้จึงถูกออกแบบให้ไม่สามารถเชื่อมเชื่อมต่อกับเครือข่ายใดๆ ด้วยเหตุผลด้านความปลอดภัย ทำให้ความสามารถของ Cryptocurrency Hardware Wallet มีจำกัด และมักต้องใช้งานร่วมกับ smart devices อื่น ๆ

โครงงานนี้มุ่งหมายเพื่อศึกษาแนวทางในการพัฒนา 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 จะเป็นการลดความจำเป็นที่ต้องพึงพา 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)

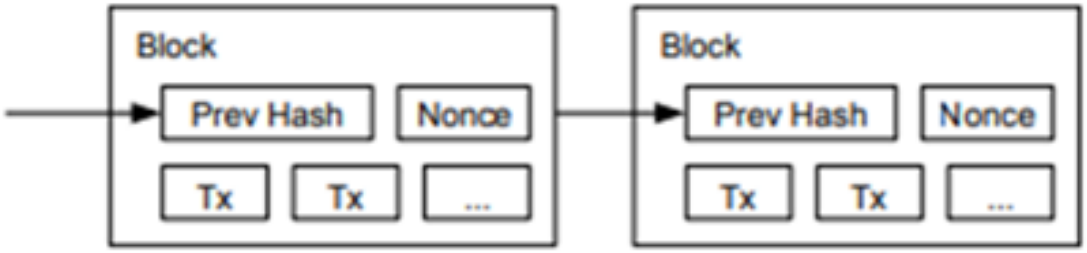
3.1 Blockchain [1]

Blockchain เป็นเทคโนโลยีการจัดเก็บข้อมูลในลักษณะแบบกระจายศูนย์ ซึ่งอยู่ในระบบเครือข่ายคอมพิวเตอร์ โดยที่ตัวระบบมีลักษณะไม่มีศูนย์กลางในลักษณะแบบ Peer-to-peer ระบบเครือข่ายนั้นจะมีข้อกำหนดที่ทำให้ แต่ละจุดในเครือข่ายเห็นข้อมูลชุดเดียวกันทั้งหมด

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

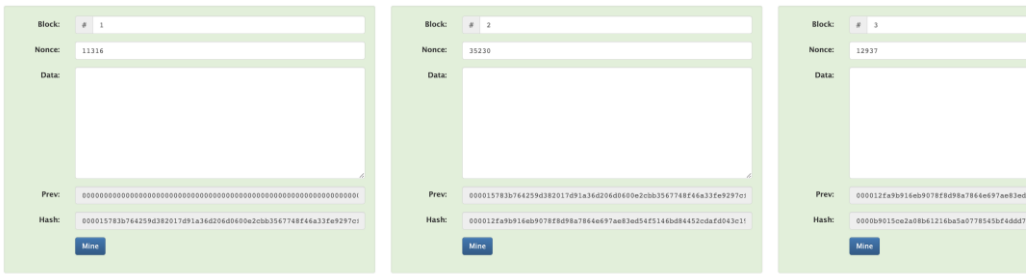
3.1.1. หลักการทำงาน

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



รูปที่ 3.1 การเชื่อมต่อระหว่าง block[1]

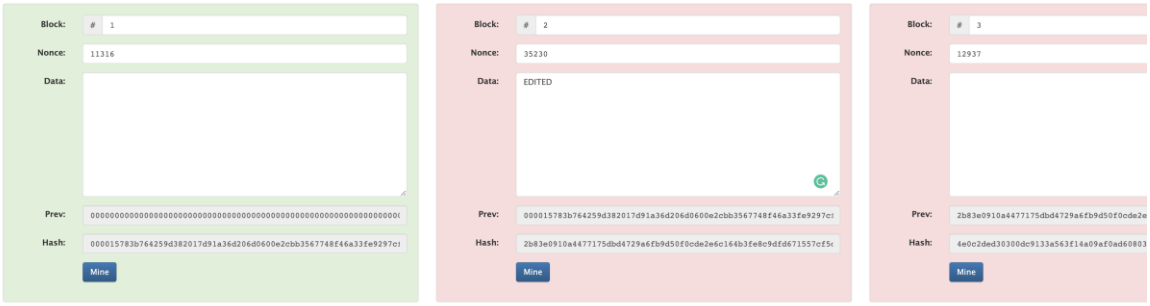
หาก Block มีการเปลี่ยนแปลงข้อมูลจะทำให้ค่า Hash ของ Block นั้นเปลี่ยนตาม ส่งผลให้ Block ที่มีการเชื่อมต่อก่อนหน้านั้นไม่สามารถอ้างอิงถึง Block ที่มีการเปลี่ยนแปลงข้อมูลได้ สามารถดูตัวอย่างการป้องกันการเปลี่ยนแปลงได้ในรูปที่ 3.2, 3.3



รูปที่ 3.2 การเชื่อมต่อระหว่าง block ที่มี Hash เรียงกันถูกต้อง[2]

[1] ที่มาภาพจาก https://bitcoin.org/bitcoin.pdf

[2] ที่มาภาพจาก https://andersbrownworth.com/blockchain/blockchain



รูปที่ 3.3 การเชื่อมต่อระหว่าง block ที่การแก้ไขค่าข้อมูลในบล็อก[3]

เมื่อมีการแก้ไขบล็อกใดบล็อกหนึ่ง บล็อกถัดมาจะไม่สามารถอ้างอิงถึงบล็อกก่อนหน้าได้ และนำไปสู่กระบวนการตรวจสอบความถูกต้องในระบบเครือข่ายภายหลัง เนื่องจากมีการเรียง 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 [4]ให้กับทุก Node เพื่ออัพเดตว่ามี Block ใหม่เกิดขึ้นมา
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 และส่วนแปะหัวกล่องหรือ Header เพื่อใช้บอกให้คนอื่นทราบว่าบรรจุอะไรมา (แต่เปิดดู Item ภายในนั้นไม่ได้)

Chain คือ หลักการจดจำทุก ๆ ธุรกรรมของทุก ๆ คนในระบบและบันทึกข้อมูลพร้อมจัดทำเป็นสำเนาบัญชี Ledger แจกจ่ายให้กับทุกคนในระบบ

---

[3] ที่มาภาพจาก https://andersbrownworth.com/blockchain/blockchain

[4] บันทึก หรือสมุดบันทึกการเคลื่อนไหวของบัญชี

Consensus คือ ข้อตกลงร่วมกันของแต่ละ Node ในเครือข่าย ในการกระทำต่าง ๆ

Validation คือ การตรวจสอบความถูกต้องแบบทบทวนทั้งระบบและทุก Node

3.2 Smart Contract [2]

Smart Contract เป็นกระบวนการทางดิจิทัล ที่มีการกำหนดขั้นตอนในการปฏิบัติ ไว้ล่วงหน้าก่อน และถูกสร้างขึ้นโดนไม่อาศัยตัวกลาง การใช้งาน Smart Contract คือการใช้งานชุดคำสั่งดังกล่าวนี้ โดยคู่สัญญาจะตกลงถึงขั้นตอนและกลไกก่อนที่จะทำธุรกรรม

แนวคิดของ Smart Contract ที่กล่าวถึงบ่อยในปัจจุบัน เกิดมาจาก Nick Szabo โดยมีการเสนอความคิดไว้ว่า ระบบคอมพิวเตอร์ และเครือข่ายคอมพิวเตอร์ 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 [5]และแพลตฟอร์มการวิเคราะห์ที่ให้รายละเอียดเกี่ยวกับธุรกรรมบล็อคเชน Ethereum ที่กำลังรอดำเนินการ หรือได้รับการยืนยัน

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

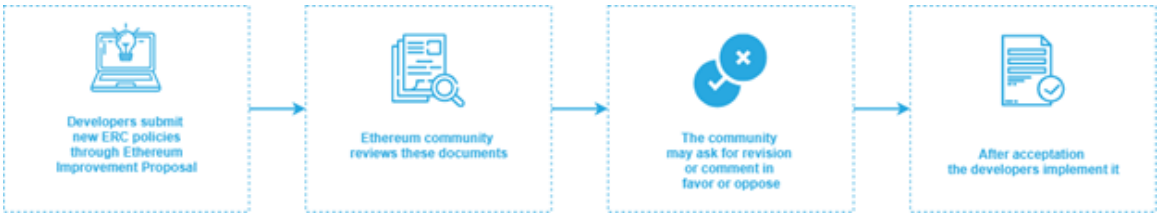
3.3 Tokens [4]

[5] เครื่องมือสำหรับตรวจสอบข้อมูล การเคลื่อนไหวของ Blockchain

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

3.3.1. Ethereum Request for Comment [3]

เรียกโดยชื่อย่อว่า ERC ถือเป็นขั้นตอนในการพัฒนา Ethereum แบบหนึ่ง ซึ่งจะถูกสร้างเพื่อให้สมาชิกผู้พัฒนา Ethereum ให้ความเห็น ทั้งทางเทคนิคและมาตรฐานก่อนที่จะมีการนำไปใช้งานจริงในเครือข่าย Ethereum



รูปที่ 3.4 ขั้นตอนการบัญญัติ ERC[6]

[6] 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[7])

โดยที่ Fungible Token (FT) เป็นทรัพย์สินที่มีคุณสมบัติความสามารถทดแทนกันได้ ยกตัวอย่าง เช่น ธนบัตรชนิดราคา 20 บาทที่ได้รับจากแม่ค้ากับธนบัตรชนิดราคา 20 บาทที่ได้รับจากธนาคาร สามารถใช้ทดแทนกันได้เนื่องด้วยคุณสมบัติความสามารถทดแทนกัน

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 โดยผู้ใช้จำเป็นต้องรักษาไว้ หากสูญหายจะทำให้ไม่สามารถเข้าถึงสินทรัพย์ได้ และหากมีการโจรกรรม โดยมิจฉาชีพก็สามารถก่อให้เกิดการสูญเสียทรัพย์สินในบัญชีได้

กระเป๋าเงินดิจิตอล หรือ crypto wallet จึงเป็นเครื่องมือเพื่ออำนวยความสะดวกในการเก็บ private key เพื่อเพิ่มความปลอดภัยในการใช้งาน cryptocurrency

[7] Initial Coin Offerings หรือเป็นการระดมทุน โดยใช้เหรียญ Token เพื่อเป็นหลักประกันในการระดมนั้น 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 แต่มีข้อเสียเนื่องจากจำเป็นต้องเชื่อมต่อกับระบบเครือข่ายอยู่ตลอดจึงมีความเสี่ยงที่อาจถูกโจมตีจากระบบเครือข่ายได้
2. cold wallet คือกระเป๋าเงินที่ไม่มีการเชื่อมต่อเครือข่ายอินเทอร์เน็ต หากผู้ใช้ต้องการทำธุรกรรม จะต้องดึงข้อมูลออกจาก cold wallet และนำข้อมูลนั้นส่งต่อไปที่อื่นเพื่อทำธุรกรรม จึงจะสามารถทำให้เกิดธุรกรรมขึ้นได้

cold wallet ที่ได้รับความนิยมมี 2 รูปแบบ ได้แก่ paper wallet คือการบันทึก wallet address และ private key ในกระดาษ ทั้งในรูปของการจดหรือ 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

ตัวอย่างของผู้ผลิต 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 การเรียกใช้ทรัพยาก 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]

4. งานวิจัยที่เกี่ยวข้อง (Related Works)

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

งานวิจัยนี้เป็นการทำ Bitcoin wallet บนระบบปฏิบัติการณ์ Android โดยมีการใช้งานแบ่งเป็น 2 ส่วนคือ ส่วนที่เป็น 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 ได้หลายสกุลโดยทำการศึกษาคุณลักษณะในแง่จำนวนสกุล cryptocurrency ที่รองรับ, ภาวะนิรนาม, ราคา, platform ที่รองรับ, การจัดการ key, วิธีการกู้คืน wallet, และการรองรับเงินตราที่ไม่มีทุนสำรอง

5. ขอบเขตของโครงงาน (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. การพัฒนาโครงงาน (Project Development)

6.1 ขั้นตอนการพัฒนา (Methodology)

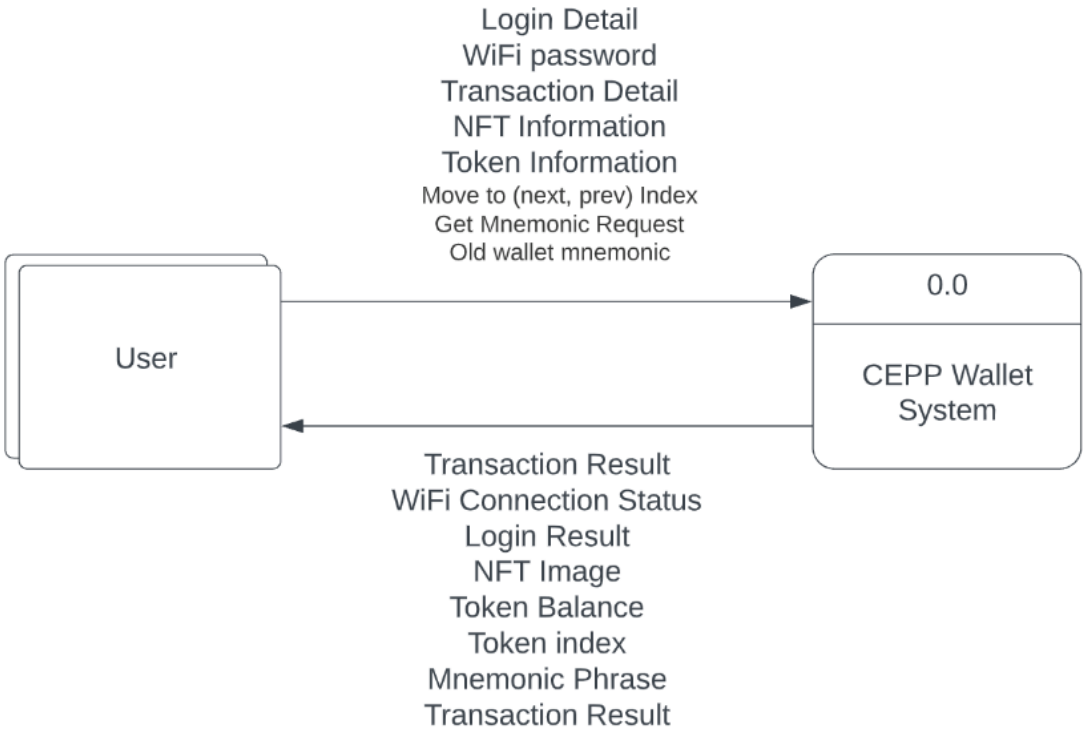
1. กำหนดวัตถุประสงค์ ขอบเขต และเป้าหมายของโครงงาน
2. วางแผนการดำเนินโครงงานและแบ่งการรับผิดชอบแต่ละส่วน
3. สืบค้นและศึกษาเอกสารและงานวิจัยที่เกี่ยวข้อง
4. พัฒนาโครงงาน
    - พัฒนา hardware wallet
    - พัฒนา application (user interface) สำหรับ hardware wallet
    - รวมส่วน hardware wallet เข้ากับ application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

6.2 การออกแบบ (Design)

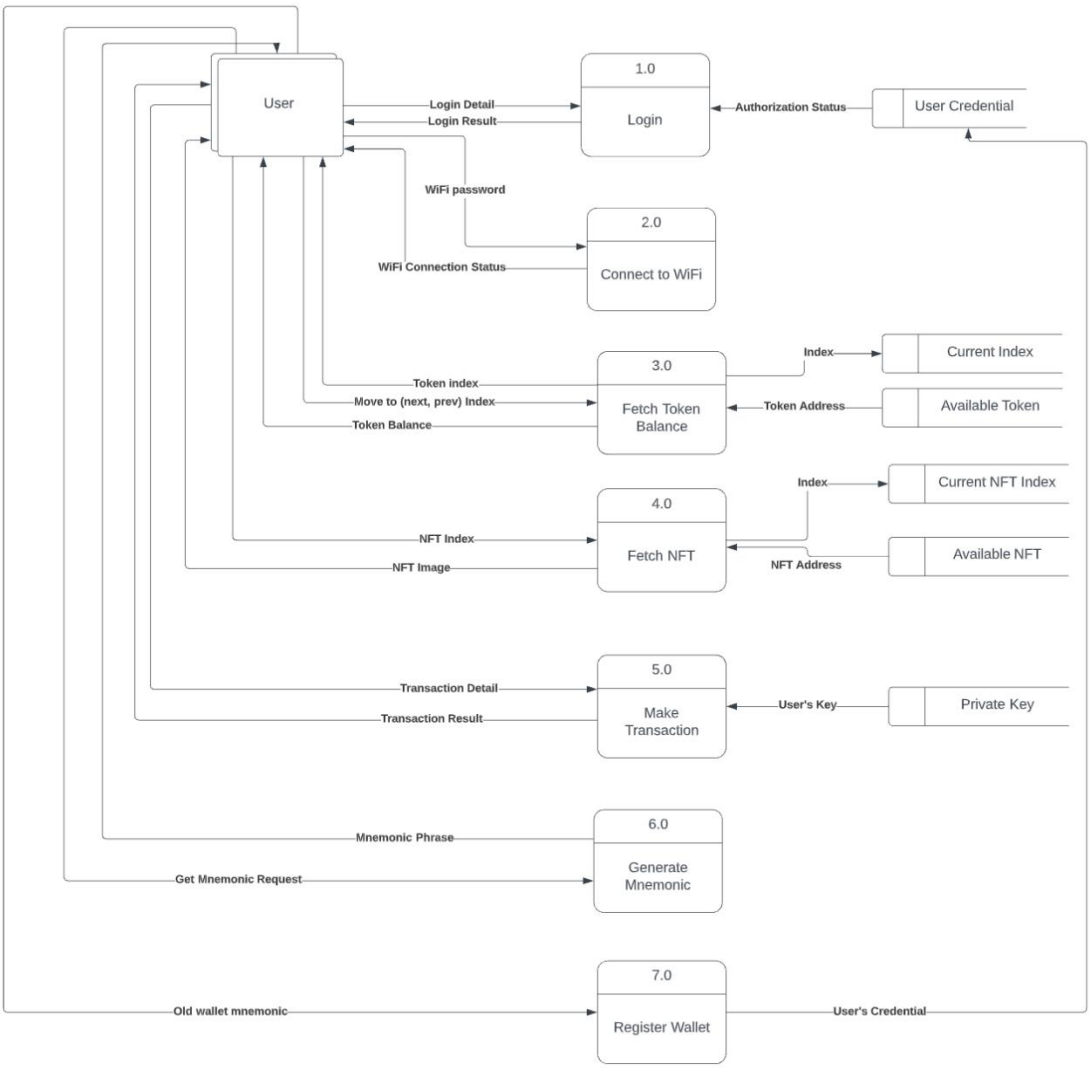
การออกแบบที่ทำมาจะเป็น Dataflow Diagram ที่แสดงถึงการแลกเปลี่ยนข้อมูลต่าง ๆ ในระบบและส่วนที่เป็น User Interface Design โดยเลือกใช้ Figma ในการออกแบบ

6.2.1. Dataflow Diagram

Dataflow Diagram นี้ใช้ในการแสดงการส่งผ่านข้อมูลระหว่างส่วนประกอบต่าง ๆ ในระบบ hardware wallet โดยจะแบ่งความสามารถเป็นส่วนที่เป็น wallet และส่วนความสามารถเพิ่มเติมได้แก่การทำงานกับ NFTs, การแลกเปลี่ยนเหรียญ, และการโอนเหรียญ



รูปที่ 6.1 Context Diagram



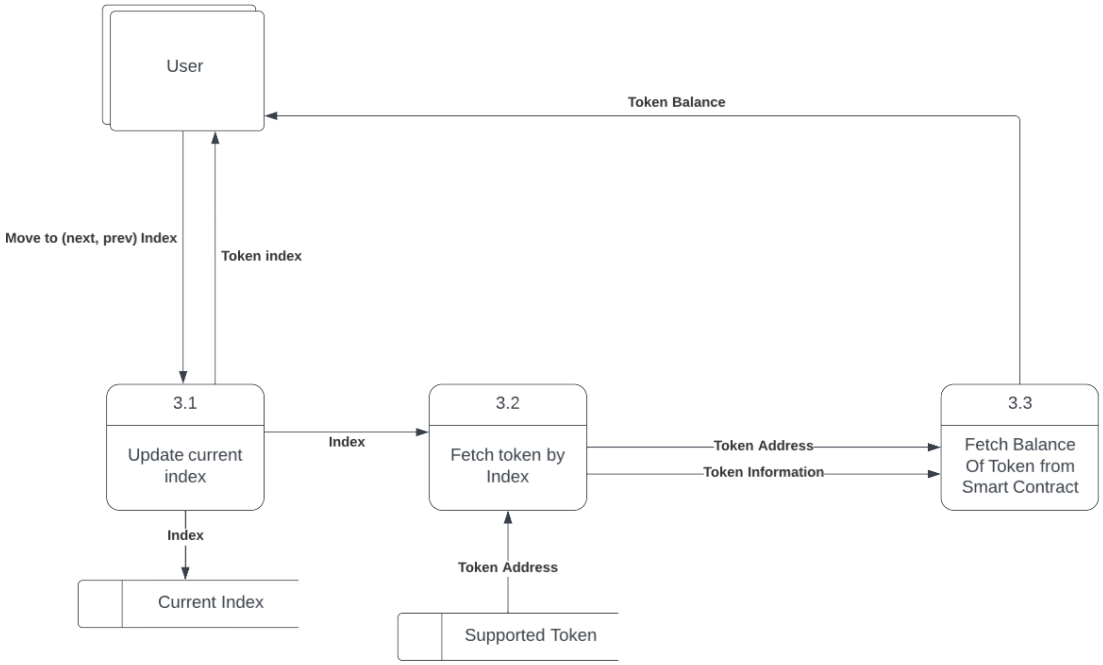
รูปที่ 6.2 Diagram 0

ใน diagram นี้ (รูปที่ 6.2) จะมอง functionality ต่าง ๆ ของตัว wallet และโปรแกรมเป็น 7 process หลัก ๆ ได้แก่

1. Login ซึ่งทาหน้าที่ในการเข้าถึง wallet และเริ่มใช้งานตั้งแต่การทา transaction และการเลือกแสดงผล NFT ทั้งนี้วิธีในการเข้าใช้งานอาจเป็นการใช้ PIN Code, Mnemonic Phrase, Password/Passphrase หรือวิธีอื่น ๆ ตามความเหมาะสม
2. Connect to WiFi เนื่องจาก wallet นี้จะสามารถทา transaction ในตัวได้ (Hot Wallet) จึงจาเป็นต้องมีการเชื่อมต่อกับ internet ซึ่งในที่นี้ทางผู้จัดทาเลือกเป็นการเชื่อมต่อด้วย WiFi
3. Fetch token balance มีไว้ใช้สาหรับการตรวจสอบว่ามูลค่า token ที่เก็บอยู่ มีเหลืออยู่เท่าไร
4. Fetch NFT มีหน้าที่ในการดึงรูปภาพ NFT มาแสดงผลในอุปกรณ์
5. Make Transaction มีหน้าที่ในการโอน token ต่าง ๆ ที่ผู้ใช้มี ไปสู่ wallet อื่น ๆ

6. Generate Mnemonic มีหน้าที่ในการสร้าง Mnemonic Phrase เพื่อทาการรักษาความปลอดภัยตัว wallet โดย process นี้จะถูกทาครั้งแรกครั้งเดียวเมื่อเปิดใช้งาน wallet ใหม่เท่านั้น

7. Register Wallet จะใช้เมื่อผู้ใช้เคยมี wallet เดิมมาอยู่ก่อนแล้ว และต้องการนา token หรือข้อมูลจาก wallet เดิมมาใช้ในอุปกรณ์ชิ้นนี้ต่อ



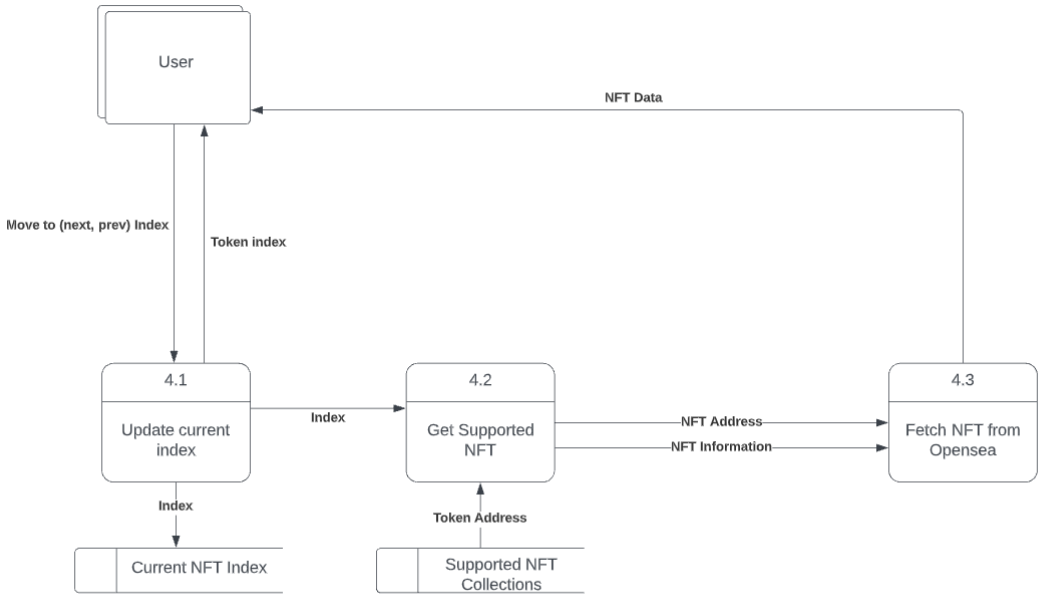
รูปที่ 6.3 Diagram 1: Process 3.0 Fetch Token Balance

รายละเอียดเพิ่มเติมสาหรับ Process 3.0 (รูปที่ 6.3) มีดังนี้

3.1 Update Current Index เนื่องจาก token ที่รองรับมีหลากหลายสกุลให้เลือกใช้ ผู้ใช้จึงสามารถทาการเลื่อนเปลี่ยนสกุลของ token ที่ต้องการตรวจสอบได้

3.2 Fetch Token by Index มีหน้าที่ในการตรวจสอบ token ที่ตัว wallet สามารถรองรับได้และเลือกส่งต่อข้อมูลให้ process 3.3

3.3 Fetch balance of Token from smart contract ทาหน้าที่ในการนาข้อมูลของ token ไปค้นหาใน smart contract และดึงค่ามาเพื่อแสดงผลบนตัว wallet



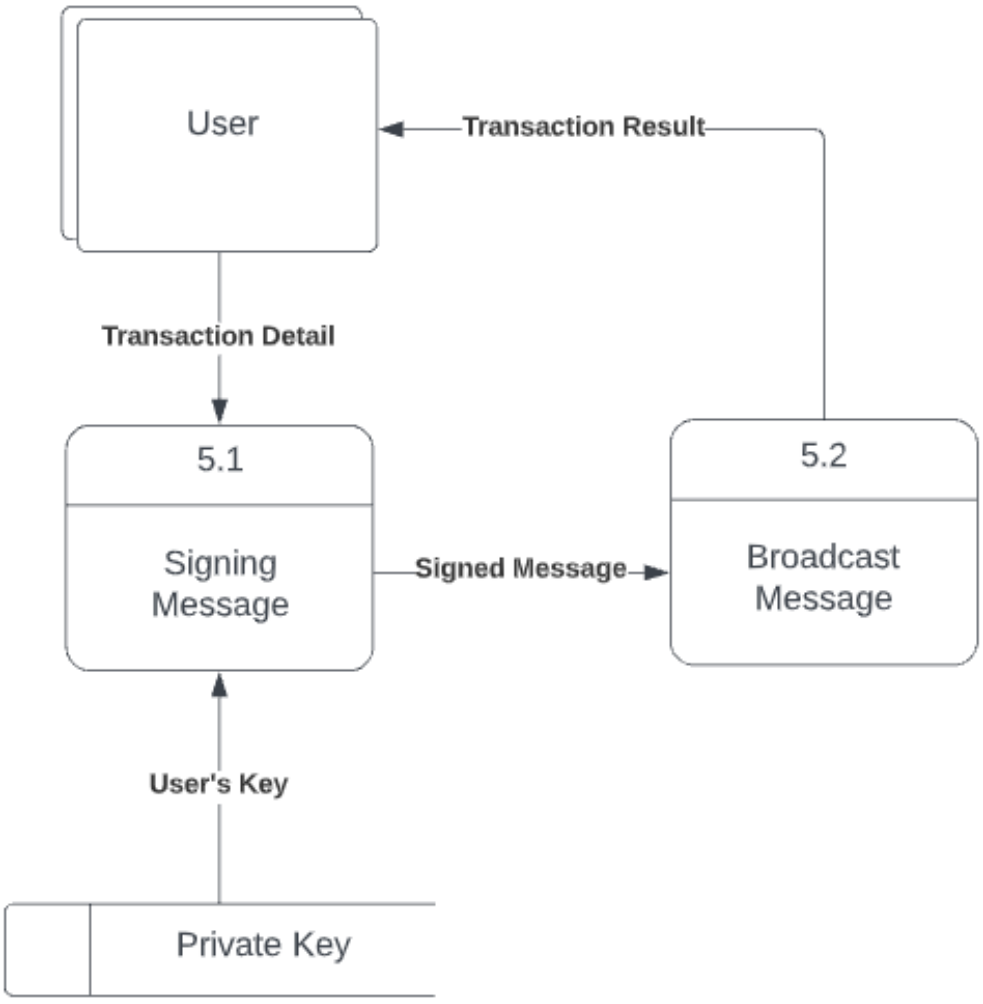
รูปที่ 6.4 Diagram 1: Process 4.0 Fetch NFT

รายละเอียดเพิ่มเติมสาหรับ Process 4.0 (รูปที่ 6.4) มีดังนี้

4.1 Update Current Index เนื่องจาก NFT ของผู้ใช้มีได้จานวนมาก ผู้ใช้จึงสามารถทาการเลื่อน NFT ที่ต้องการแสดงผลได้

4.2 Get supported NFT มีหน้าที่ในการตรวจสอบว่า NFT collection ที่ผู้ใช้มี สามารถนามาแสดงผลบนตัวอุปกรณ์ได้หรือไม่และเลือกส่งต่อข้อมูลดังกล่าวให้ process 4.3

4.3 Fetch NFT from OpenSea ทาหน้าที่ในการนาข้อมูล NFT ไปค้นหาบน OpenSea และนามาแสดงผลบนตัวอุปกรณ์ (ทั้งนี้ NFT ที่ได้มาอาจมีการ resize หรือลด resolution เพื่อให้สามารถแสดงผลบนอุปกรณ์ได้)



รูปที่ 6.5 Diagram 1: Process 5.0 Make Transaction

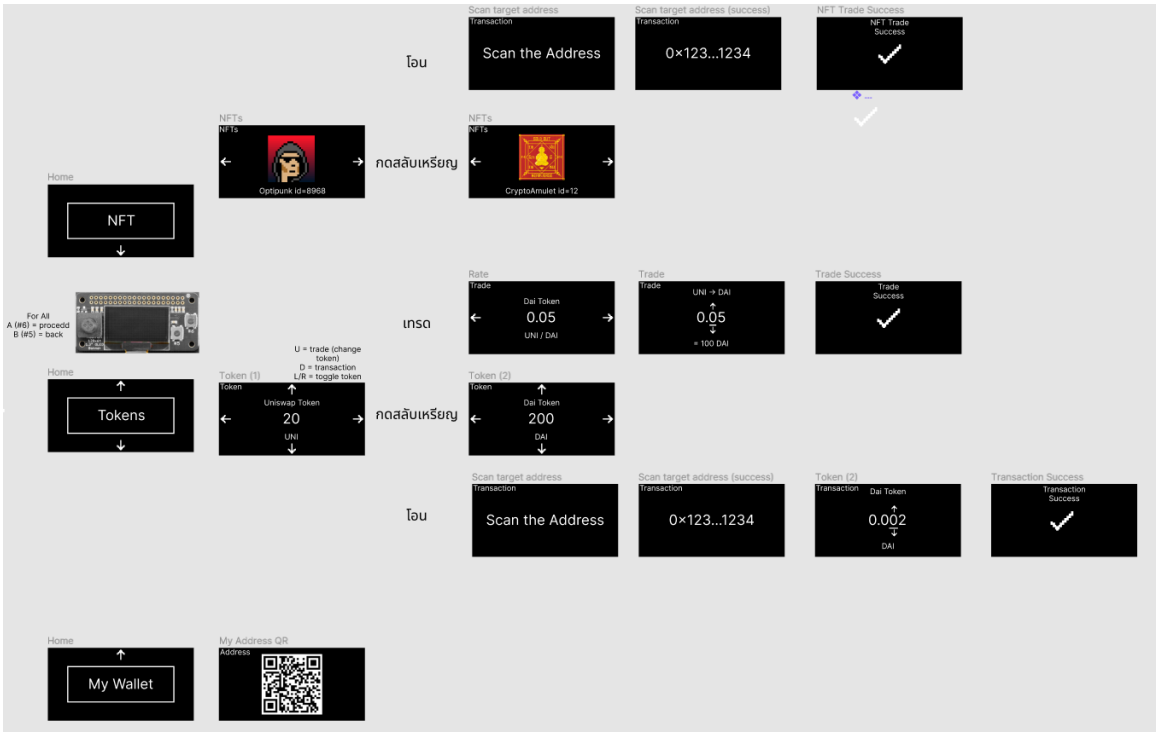
รายละเอียดเพิ่มเติมสาหรับ Process 5.0 มีดังนี้

5.1 Signing Message ทาการนาข้อมูลการทา transaction มา sign ด้วย private key ของผู้ใช้และส่งต่อให้ process 5.2

5.2 Broadcast Message ทาการส่งข้อมูล transaction ที่ผ่านการ sign จาก process 5.1 มาแล้วออกสู่ blockchain

6.2.2. User Interface Design

สำหรับการออกแบบ User Interface ผู้จัดทำได้เลือกใช้ขนาดหน้าจอแสดงผลขนาด 128 x 64 pixels (อ้างอิงตามขนาดของ Adafruit OLED 128x64 pixels) โดยแบ่งส่วนการทำงานเป็น 3 ส่วนคือการทำงานกับ NFTs, การแลกเปลี่ยนและโอนเหรียญ, และ wallet address



รูปที่ 6.6 User interface design

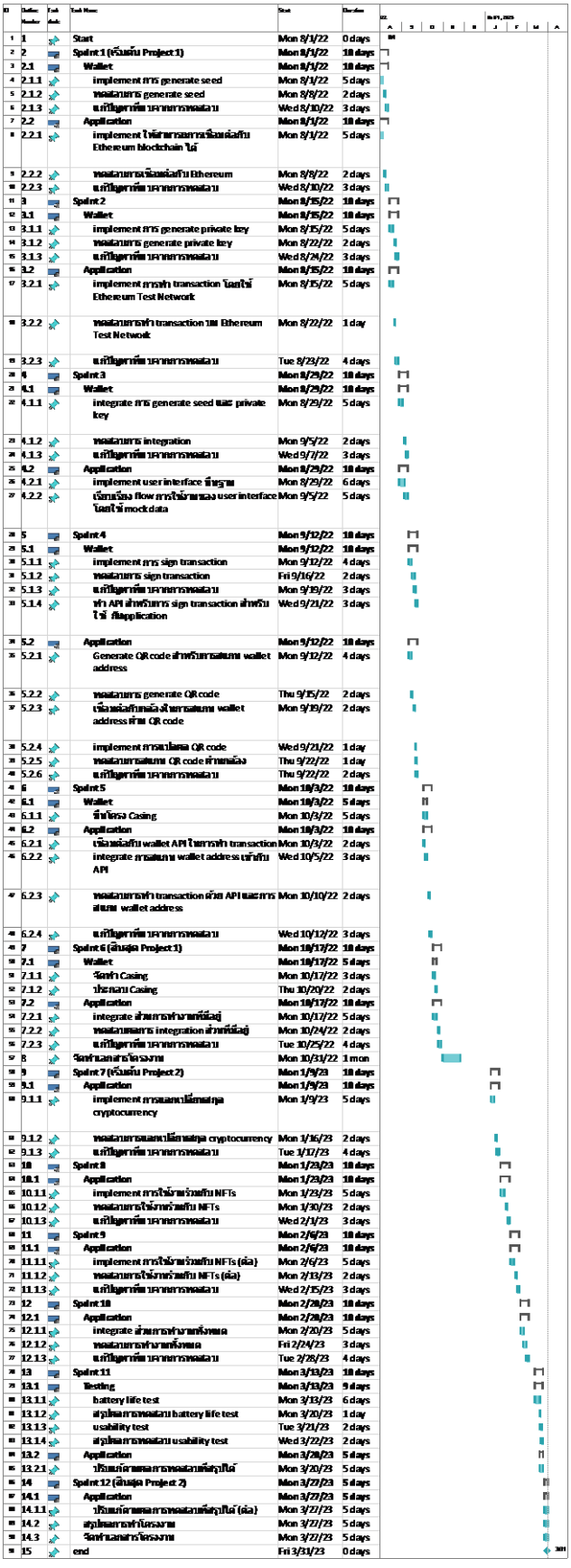
6.3 แนวทางการทดสอบและการวัดประสิทธิภาพ (Test and Performance Evaluation Approaches)

6.3.1. ทดสอบ unit test สำหรับ application โดยใช้ Jest framework

6.3.2. ทดสอบอายุการใช้งาน (battery life) ว่าอุปกรณ์ที่พัฒนาสามารถใช้งานได้กี่นาทีโดยทดสอบในสถานการณ์ที่เป็น idle (stand by) และเปิดหน้าเมนูหลักไว้ตลอดเวลา โดยทดสอบอย่างละ 3 รอบ และหาค่าเฉลี่ยเวลาที่ใช้งานได้

6.3.3. ทดสอบ Usability Test โดยใช้อาสาสมัครที่มีความสนใจด้าน cryptocurrency เป็นผู้เข้าร่วมทดสอบอุปกรณ์ที่ได้พัฒนา

7. แผนการดำเนินโครงงาน (Gantt Chart)



ID	Task Name	Start	Duration
1	Start	Mon 8/1/22	0 days
2	Sprint 1 (เริ่มนับ Project 1)	Mon 8/1/22	10 days
3	2.1 Wallet	Mon 8/1/22	10 days
4	2.1.1 implement การ generate seed	Mon 8/1/22	5 days
5	2.1.2 ทดสอบการ generate seed	Mon 8/8/22	2 days
6	2.1.3 แก้ไขตามที่ อาจารย์แนะนำ	Wed 8/10/22	3 days
7	2.2 Application	Mon 8/1/22	10 days
8	2.2.1 implement ให้สามารถสร้างเชื่อมต่อกับ Ethereum blockchain ได้	Mon 8/1/22	5 days
9	2.2.2 ทดสอบการเชื่อมต่อกับ Ethereum	Mon 8/8/22	2 days
10	2.2.3 แก้ไขตามที่ อาจารย์แนะนำ	Wed 8/10/22	3 days
11	3 Sprint 2	Mon 8/15/22	10 days
12	3.1 Wallet	Mon 8/15/22	10 days
13	3.1.1 implement การ generate private key	Mon 8/15/22	5 days
14	3.1.2 ทดสอบการ generate private key	Mon 8/22/22	2 days
15	3.1.3 แก้ไขตามที่ อาจารย์แนะนำ	Wed 8/24/22	3 days
16	3.2 Application	Mon 8/15/22	10 days
17	3.2.1 implement การทำ transaction โดยใช้ Ethereum Test Network	Mon 8/15/22	5 days
18	3.2.2 ทดสอบการทำ transaction ใน Ethereum Test Network	Mon 8/22/22	1 day
19	3.2.3 แก้ไขตามที่ อาจารย์แนะนำ	Tue 8/23/22	4 days
20	4 Sprint 3	Mon 8/29/22	10 days
21	4.1 Wallet	Mon 8/29/22	10 days
22	4.1.1 integrate การ generate seed และ private key	Mon 8/29/22	5 days
23	4.1.2 ทดสอบการ integration	Mon 9/5/22	2 days
24	4.1.3 แก้ไขตามที่ อาจารย์แนะนำ	Wed 9/7/22	3 days
25	4.2 Application	Mon 8/29/22	10 days
26	4.2.1 implement user interface ขึ้นมาใหม่	Mon 8/29/22	6 days
27	4.2.2 เขียนเรื่อง flow การใช้งานของ user interface โดยใช้ mock data	Mon 9/5/22	5 days
28	5 Sprint 4	Mon 9/12/22	10 days
29	5.1 Wallet	Mon 9/12/22	10 days
30	5.1.1 implement การ sign transaction	Mon 9/12/22	4 days
31	5.1.2 ทดสอบการ sign transaction	Fri 9/16/22	2 days
32	5.1.3 แก้ไขตามที่ อาจารย์แนะนำ	Mon 9/19/22	3 days
33	5.1.4 ทำ API สำหรับการ sign transaction สำหรับใช้ กับapplication	Wed 9/21/22	3 days
34	5.2 Application	Mon 9/12/22	10 days
35	5.2.1 Generate QR code สำหรับการแสดง wallet address	Mon 9/12/22	4 days
36	5.2.2 ทดสอบการ generate QR code	Thu 9/15/22	2 days
37	5.2.3 เพิ่มเหล่งที่มาหลัง สำหรการแสดง wallet address ด้วย QR code	Mon 9/19/22	2 days
38	5.2.4 implement การสแกน QR code	Wed 9/21/22	1 day
39	5.2.5 ทดสอบการแสดง QR code ด้านหลัง	Thu 9/22/22	1 day
40	5.2.6 แก้ไขตามที่ อาจารย์แนะนำ	Thu 9/22/22	2 days
41	6 Sprint 5	Mon 10/3/22	10 days
42	6.1 Wallet	Mon 10/3/22	5 days
43	6.1.1 ปรับโครง Casing	Mon 10/3/22	5 days
44	6.2 Application	Mon 10/3/22	10 days
45	6.2.1 เพิ่มเหล่งที่มา wallet API ในการทำ transaction	Mon 10/3/22	2 days
46	6.2.2 integrate การแสดง wallet address เข้ากับ API	Wed 10/5/22	3 days
47	6.2.3 ทดสอบการทำ transaction ด้วย API และการแสดง wallet address	Mon 10/10/22	2 days
48	6.2.4 แก้ไขตามที่ อาจารย์แนะนำ	Wed 10/12/22	3 days
49	7 Sprint 6 (สิ้นสุด Project 1)	Mon 10/17/22	10 days
50	7.1 Wallet	Mon 10/17/22	5 days
51	7.1.1 จัดทำ Casing	Mon 10/17/22	3 days
52	7.1.2 ประกอบ Casing	Thu 10/20/22	2 days
53	7.2 Application	Mon 10/17/22	10 days
54	7.2.1 integrate ส่วนการทำงานที่เหลือ	Mon 10/17/22	5 days
55	7.2.2 ทดสอบผลการ integration ส่วนที่เหลือ	Mon 10/24/22	2 days
56	7.2.3 แก้ไขตามที่ อาจารย์แนะนำ	Tue 10/25/22	4 days
57	8 จัดทำเอกสารโครงงาน	Mon 10/31/22	1 mon
58	9 Sprint 7 (เริ่มนับ Project 2)	Mon 1/9/23	10 days
59	9.1 Application	Mon 1/9/23	10 days
60	9.1.1 implement การแลกเปลี่ยนสกุล cryptocurrency	Mon 1/9/23	5 days
61	9.1.2 ทดสอบการแลกเปลี่ยนสกุล cryptocurrency	Mon 1/16/23	2 days
62	9.1.3 แก้ไขตามที่ อาจารย์แนะนำ	Tue 1/17/23	4 days
63	10 Sprint 8	Mon 1/23/23	10 days
64	10.1 Application	Mon 1/23/23	10 days
65	10.1.1 implement การใช้งานร่วมกับ NFTs	Mon 1/23/23	5 days
66	10.1.2 ทดสอบการใช้งานร่วมกับ NFTs	Mon 1/30/23	2 days
67	10.1.3 แก้ไขตามที่ อาจารย์แนะนำ	Wed 2/1/23	3 days
68	11 Sprint 9	Mon 2/6/23	10 days
69	11.1 Application	Mon 2/6/23	10 days
70	11.1.1 implement การใช้งานร่วมกับ NFTs (ต่อ)	Mon 2/6/23	5 days
71	11.1.2 ทดสอบการใช้งานร่วมกับ NFTs (ต่อ)	Mon 2/13/23	2 days
72	11.1.3 แก้ไขตามที่ อาจารย์แนะนำ	Wed 2/15/23	3 days
73	12 Sprint 10	Mon 2/20/23	10 days
74	12.1 Application	Mon 2/20/23	10 days
75	12.1.1 integrate ส่วนการทำงานทั้งหมด	Mon 2/20/23	5 days
76	12.1.2 ทดสอบการทำงานทั้งหมด	Fri 2/24/23	3 days
77	12.1.3 แก้ไขตามที่ อาจารย์แนะนำ	Tue 2/28/23	4 days
78	13 Sprint 11	Mon 3/13/23	10 days
79	13.1 Testing	Mon 3/13/23	9 days
80	13.1.1 battery life test	Mon 3/13/23	6 days
81	13.1.2 สรุปผลการทดสอบ battery life test	Mon 3/20/23	1 day
82	13.1.3 usability test	Tue 3/21/23	2 days
83	13.1.4 สรุปผลการทดสอบ usability test	Wed 3/22/23	2 days
84	13.2 Application	Mon 3/20/23	5 days
85	13.2.1 ปรับแก้ตามผลการทดสอบที่สรุปได้	Mon 3/20/23	5 days
86	14 Sprint 12 (สิ้นสุด Project 2)	Mon 3/27/23	5 days
87	14.1 Application	Mon 3/27/23	5 days
88	14.1.1 ปรับแก้ตามผลการทดสอบที่สรุปได้ (ต่อ)	Mon 3/27/23	5 days
89	14.2 สรุปผลการทำโครงงาน	Mon 3/27/23	5 days
90	14.3 จัดทำเอกสารโครงงาน	Mon 3/27/23	5 days
91	15 end	Fri 3/31/23	0 days

รูปที่ 7.1 Gantt chart

8. ประโยชน์ที่คาดว่าจะได้รับ (Expected Benefits)

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

9. ผลการศึกษาเทคโนโลยีที่ใช้พัฒนา

9.1 React

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

จุดเด่นของ React คือการโค้ดดิ้งที่เน้นเขียนให้โปรแกรม “ทำอะไร” เป็นหลัก การใช้งานส่วนต่าง ๆ เป็น component ที่เป็นอิสระต่อกัน และข้อจำกัดในการเลือกใช้ tech stack ที่น้อย [11]

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-first CSS framework ที่ช่วยให้สามารถตกแต่ง UI โดยอาศัยการเรียกใช้งาน utility class ต่าง ๆ ที่ตัว package มีมาไว้ให้ นอกจากนี้ยังสามารถทำการปรับแต่งหรือเพิ่มเติม class ได้ตามความต้องการอีกด้วย [14]

9.2 Tailwind CSS

เป็น utility-first CSS framework ซึ่งเน้นไปที่การเขียน CSS ผ่านการเลือกใช้ class ในไฟล์ HTML แทนการเขียนแยกไปอีกไฟล์ นอกจากนี้ยังสามารถปรับแต่งค่าตั้งต้นต่าง ๆ ให้เปลี่ยนไปตามความต้องการของผู้พัฒนาด้วยก็ได้จึงเหมาะกับการพัฒนาที่ต้องใช้ความรวดเร็วและมีความยืดหยุ่น นอกจากนี้ความสามารถในการลบ CSS class ที่ไม่ได้ใช้งานออกจาก production build (purging) ยังทำให้ไฟล์ CSS มีขนาดเล็กลงอีกด้วย

9.3 Docker

เป็น Container Tool ที่ช่วยในงานแยก Process การทำงานของ Applications หลาย ๆ ส่วนให้ทำงานไม่ทับซ้อนกัน Docker จะช่วยให้การทำงานแต่ละ Module ไม่ทับซ้อนกัน และไม่เข้ามาสร้างผลกระทบต่อถึงกันได้

9.4 Python

เป็นภาษาที่มีความเป็นที่นิยมสูง เป็นภาษาที่มีโครงสร้างคำสั่งที่ไม่ซับซ้อน เข้าใจง่าย อีกทั้งยังมีชุดคำสั่งสำเร็จรูป (Library) ให้เลือกใช้งานมากมาย เช่น ติดต่อฐานข้อมูลต่าง ๆ , ระบบเครือข่าย ทำให้เขียนโปรแกรมใหม่ได้รวดเร็วมากขึ้น

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] N. Szabo, “Formalizing and Securing Relationships on Public Networks” First Monday. https://firstmonday.org/ojs/index.php/fm/article/download/548/469 (accessed May 17, 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

[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

[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.

ภาคผนวก

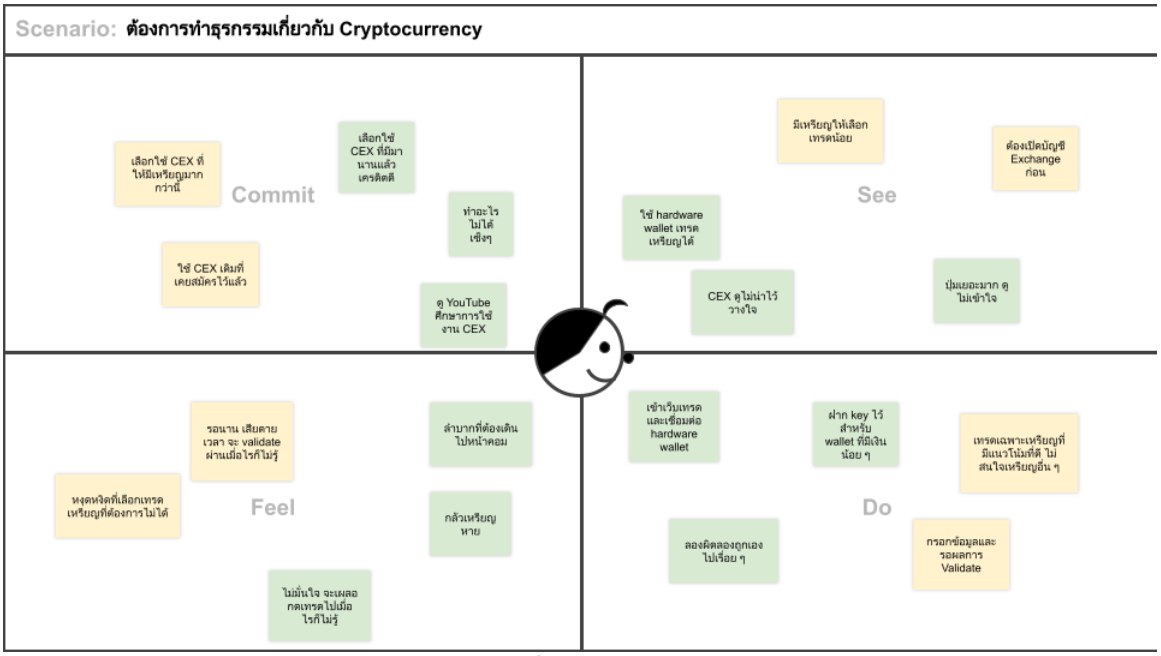
ภาคผนวก

1. UX Process

รูปที่ 1 การสรุปปัญหาของ User จากการสัมภาษณ์

จากการทำ User Interview จะสรุปปัญหาของผู้ใช้ได้ดังรูปที่ 1 ข้างต้น กลุ่มผู้จัดทำเลือกปัญหาข้อที่ 3 คือ Hardware Wallet ที่ใช้มักจะไม่ฉลาด และเมื่อรีบทำธุรกรรมจะต้องใช้คอมพิวเตอร์เสมอ เหตุผลที่เลือกเนื่องมาจากว่าเป็นปัญหาที่ Hardware Wallet ส่วนใหญ่เลือกไม่แก้ อาจด้วยเพราะไม่ต้องการ Compromise ความปลอดภัยของอุปกรณ์

ทางผู้จัดทำจึงเห็นชัดเจนขึ้นว่าสามารถสร้าง Hardware Wallet ที่ฉลาดมากขึ้น สามารถทำ Transaction ได้หลายอย่างมากขึ้นในตัวมันเอง ทั้งนี้อาจจะถูกลดทอนเรื่องความปลอดภัยไปบ้าง แต่จะทำให้ Surface of attack แคบลง เพราะไม่จำเป็นต้องเชื่อมต่ออุปกรณ์อื่นเหมือน Hardware Wallet และ Software Wallet ที่มีอยู่ก่อน

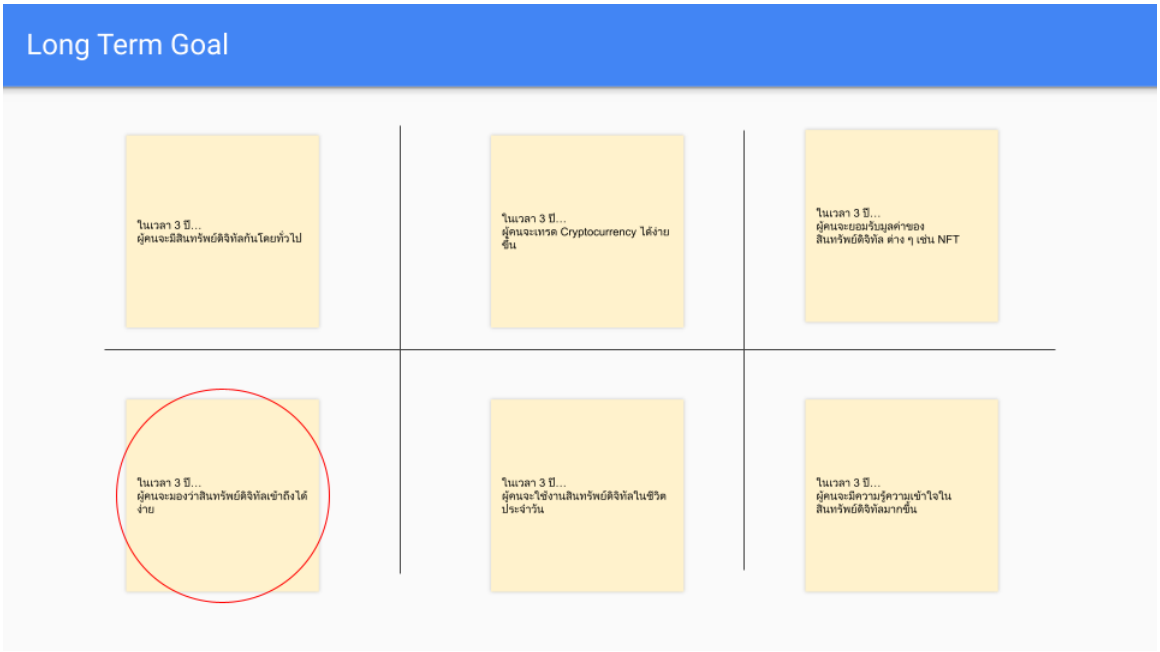


รูปที่ 2 Empathy Map

ผู้จัดทำได้นำข้อมูลดังกล่าวมาสร้างเป็น Scenario เพื่อจำลองสถาณการณ์ที่เกิดขึ้นเมื่อ User ต้องการจะทำธุรกรรมเกี่ยวกับ Cryptocurrency และทำเป็น Empathy Map ตามรูปที่ 2

รูปที่ 3 Persona

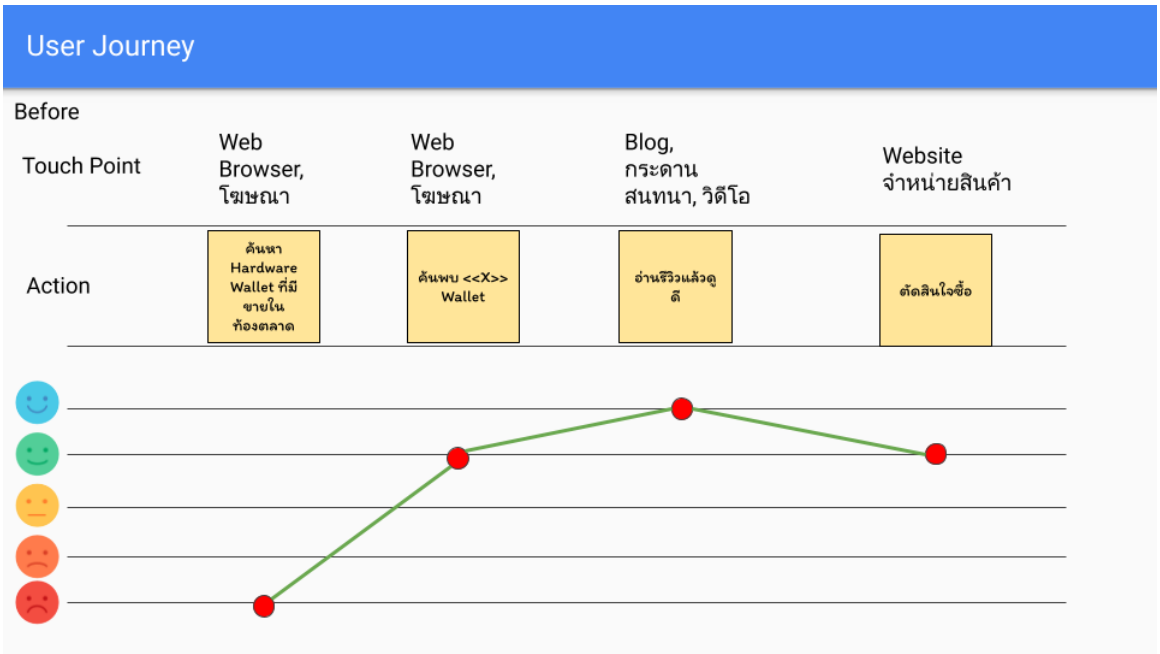
จาก User Interview ที่ทำมา สามารถนำมารวมเป็น Persona ได้ดังรูปที่ 3 โดยเป็น Personality กลาง ๆ ระหว่างนักลงทุนที่พร้อมรับความเสี่ยงจากราคาที่ผันผวนในระยะสั้นได้ แต่มีความระมัดระวังในเรื่องทางเทคนิค เช่น การขโมย Private Key เป็นต้น



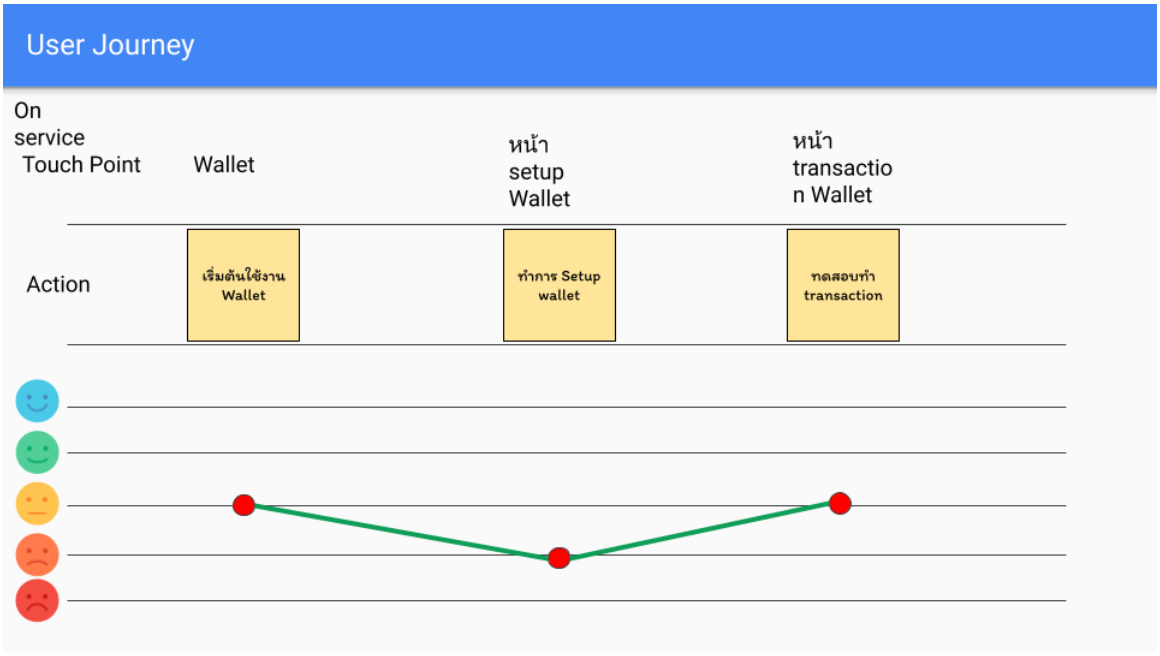
รูปที่ 4 Long Term Goal

เหตุผลที่เลือก Long Term Goal “ในเวลา 3 ปี... ผู้คนจะมองว่าสินทรัพย์ดิจิทัลเข้าถึงได้ง่าย” เพราะว่าในปัจจุบันจะเห็นว่าผู้ที่ให้การสัมภาษณ์ส่วนใหญ่ไม่มีความสนใจในตัว NFTs หรือแม้มีความสนใจก็ไม่ได้อยากมีในครอบครองเนื่องจากข้อจำกัดด้านการจัดแสดงผลงาน NFTs ต่าง ๆ ผู้จัดทำจึงมีความคิดเห็นว่าการที่จะทำให้ผู้คนมีความสนใจ NFTs ได้มากขึ้นอย่างหนึ่งคือการทำให้สามารถจัดแสดง NFTs ได้สะดวกมากขึ้น

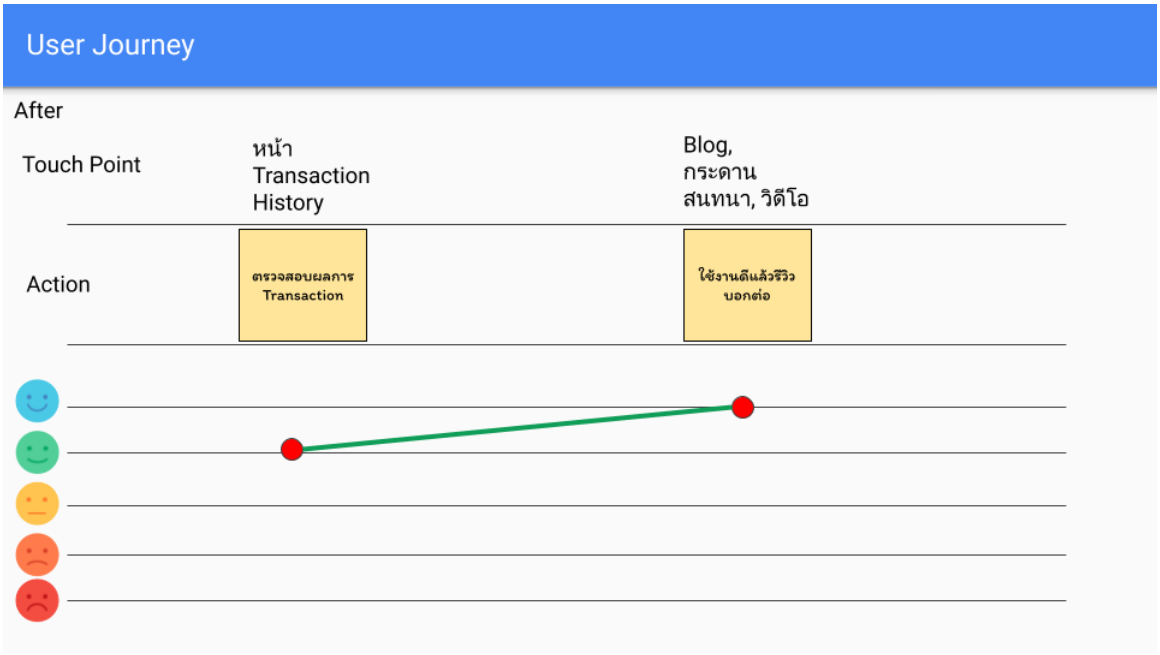
จากผลการวิเคราะห์ทั้งหมด จึงสามารถนำมาจัดทำเป็น User Journey ตั้งแต่การค้นพบอุปกรณ์ไปจนถึงการใช้งานได้ดังนี้



รูปที่ 5 User Journey: การค้นพบ



รูปที่ 6 User Journey: การใช้งาน



รูปที่ 7 User Journey: หลังการใช้งานและบอกต่อ