รายงานความก้าวหน้าวิชา Computer Engineering Project Preparation

ครั้งที่ 1

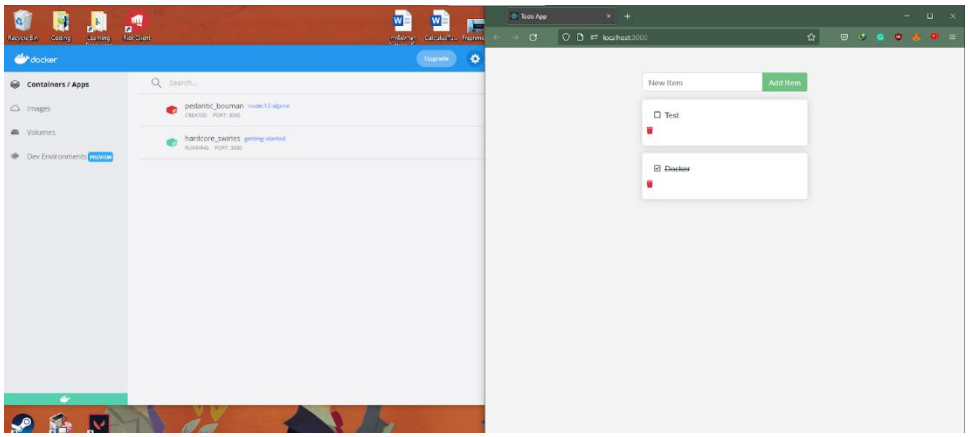
1. ชื่อโครงงาน (อังกฤษ) Cryptocurrency Hardware Wallet

2. การดำเนินงานมีความก้าวหน้า 28%

3. ความก้าวหน้าระหว่างวันที่ 14 ก.พ. 65 ถึงวันที่ 04 มี.ค. 65

4. รายละเอียดความก้าวหน้า

- จัดให้มีการพูดคุยงานกับอาจารย์ที่ปรึกษาโครงงาน และได้รับแนวทางในการเริ่มต้นศึกษาโดยเน้นการศึกษาไปที่เรื่องพื้นฐานของ crypto wallet และจุดประสงค์การใช้งาน รวมถึงเรื่องของการรักษาความปลอดภัยของ Private Key ที่เก็บไว้ใน crypto wallet นอกจากนี้ยังมีการถกถึงปัญหาต่าง ๆ ที่เกี่ยวข้องกับแนวคิดของตัวโครงงานเช่น ความเป็นไปได้ของโครงงาน ความสะดวกในการใช้งานของผู้ใช้ ความปลอดภัยในการจัดเก็บ Private Key\
- ศึกษาการใช้งาน Docker ขั้นต้น ได้แก่ การติดตั้ง, การทำ Dockerfile, การใช้ Volume, การใช้ Compose, การสร้างและใช้งาน docker image



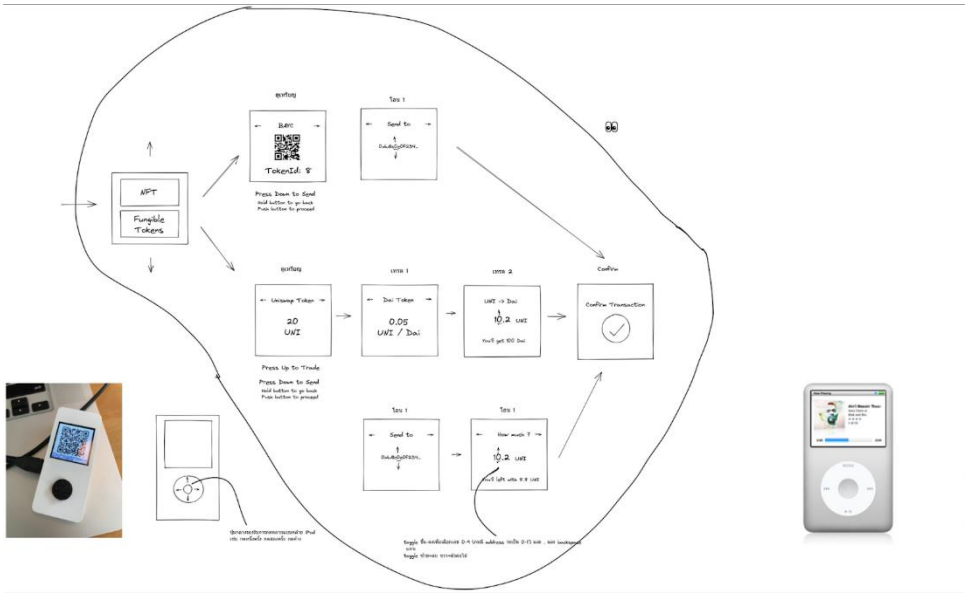
รูปที่ 1 การศึกษาใช้งาน Docker

- ศึกษาการใช้งาน Frontend Library คือ React with TypeScript รวมถึงการใช้งาน State Management
- ศึกษาความสามารถขั้นพื้นฐานและข้อจำกัดของ Pitrezor ซึ่งเป็น Hardware Wallet DIY ที่ใช้งานได้บน Raspberry P
- ศึกษาเรื่องการเข้ารหัสแบบ Elliptic Curve
- ศึกษาความสามารถและข้อจำกัดของ Hardware Wallet ที่เป็นที่นิยมในตลาดปัจจุบันได้แก่ Ledger และ Trezor
- ศึกษาเบื้องต้นเรื่องการสร้าง Crypto Wallet ภายใต้มาตรฐาน BIP39, BIP44
- ศึกษาการ generate mnemonic keys ตามมาตรฐาน BIP39
- ศึกษาการทำงานเบื้องต้นของการใช้งาน Library ethers.js, web3.js เพื่อติดต่อกับ blockchain ของ Ethereum

```
async function main() {
  const [provider] = await hre.ethers.getSigners();
  const abiCoder = hre.ethers.utils.defaultAbiCoder;
  let result;

  // const sighash = "0xacb394b1";
  const sighash2 = "0x5e88bc14";
  const sighash3 = "0x0c62a991";
  const padding = "000000000000000000000000";
  const address = "0x5FbDB2315678afecb367f032d93F642f64180aa3";
  // const params = "0x0000000000000000000000000000000000000000000000000000000000000080000000000000000000000000";

  // await hre.network.provider.send("hardhat_setBalance", [
  //  '0xbE5539dCE374c2Dfa009c3fb39229578E71BBb9B',
  //  "0xffffffffffffffff",
  // ]);

  // Sign the transaction
  result = await provider.sendTransaction({
    to: "0x5FbDB2315678afecb367f032d93F642f64180aa3",
    data: `${sighash2}${padding}${address.split("0x")[1]}`
  })

  // Sign the transaction
  result = await provider.sendTransaction({
    to: "0x5FbDB2315678afecb367f032d93F642f64180aa3",
    data: `${sighash3}${abiCoder.encode(["uint256"], [4]).split("0x")[1]}`
  })
  console.log('result', result);

  // Call the contract
  result = await provider.call({
    to: "0x5FbDB2315678afecb367f032d93F642f64180aa3",
    // data: `${sighash}${params.split("0x")[1]}`
    data: '0xacb394b1000000000000000000000000000000000000000000000000000000000000008000000000000000000000000000000000000000'
  });
  console.log('result', abiCoder.decode(["string"], result));
  console.log('result', result);
}
```

- รูปที่ 2 การศึกษาใช้งาน ethers.JS

- ออกแบบ User Interface โดยเบื้องต้น



รูปที่ 3 การออกแบบ Casing และ User Interface โดยเบื้องต้น

5. ปัญหาที่เกิดขึ้นและแนวทางการแก้ไข

Problem No. 1

สถานะ ☒ กำลังดำเนินการ ☐ แก้ไขสำเร็จ

รายละเอียดปัญหา

รูปแบบการโอนเงิน / NFT ผ่านอุปกรณ์โดยตรงยากเกินไป เนื่องจากอุปกรณ์มีขนาดจำกัด จึงสามารถที่จะปฏิสัมพันธ์กับอุปกรณ์ได้ค่อนข้างลำบาก

แนวทางแก้ไข/การแก้ไข

ศึกษาวิธีการโอนของอุปกรณ์อื่นๆที่มีลักษณะคล้ายคลึงกัน เช่น เครื่องเล่นเกม, โทรศัพท์ปุ่มกด และอื่น ๆ

6. สิ่งที่จะดำเนินการต่อไป

- ศึกษาความสามารถของ Pitrezor เพิ่มเติม และทดลองใช้หากมีอุปกรณ์ให้ทดลองจริงได้
- ออกแบบ User Experience
- ออกแบบ User Interface ในรูปแบบ Web Application โดยทำการ Prototype ผ่านโปรแกรม Figma และรูปแบบปุ่มกดบนตัว Wallet
- ออกแบบตัว casing และปุ่มกดเพื่อทำ interaction กับ Wallet
- ออกแบบ Software Architecture ในส่วนของ Web Application และออกแบบการปฏิสัมพันธ์ระหว่าง application ที่รันบน wallet โดยเบื้องต้น
- เริ่มจัดทำเอกสารในส่วนของที่มาและความสำคัญ และส่วนของวัตถุประสงค์การทำโครงงาน
- เสนอแนวทางพัฒนา Crypto Wallet โดยอ้างอิงจากความสามารถของ Wallet ที่มีอยู่เดิม
- ศึกษาและเลือกแนวทางในการรักษาความปลอดภัยของ Private Key ที่เก็บไว้บน Hardware Wallet โดยวิธีการต่าง ๆ เช่นการใช้ PIN