Internship

13 July 2020

Offline transaction for IoT devices

1st stage

- Use ESP8266 as an IoT device that directly send data to blockchain
    - save power -wifi scheduler (trigger by RTC and input data)
        - power is measured using usb power meter
    - save memory – shrink the code (i.e, split web application from the skeleton code)
    - Offline transaction – save data in a textfile, and send all data in one transaction when the wifi is on
        - security (use cryptography to protect private key)

- 2^{nd} stage
  - implement using a low power device (flash memory:256 kB)

Lead by Shen Yik

Dapp for Supply Chain

1st stage:

- Integrate blockchain with IPFS

- Elliptic-curve cryptography(encrypt using public key, decrypt using private key)

- upload encrypted file to IPFS

    - download from IPFS and decrypt the encrypted file

- Create smart contract for a supply chain node

- 2nd stage

  - create a complete DAPP for all supply chain node

  - ensure ownership transfer is successful

Lead by Aathira

Anonymous Blockchain (1)

1st stage

- create a blockchain
- integrate with stealth address, ring signature, and RingCT (monero)
- integrate with Faster Dual-Key Stealth Address Protocol (paper: Faster Dual-Key Stealth Address for Blockchain-Based Internet of Things Systems)

- 2nd stage

  - integrate with a new anonymous blockchain algorithm

  - analyze the performance of these algorithms

Lead by Hank

Anonymous Blockchain (2)

1st stage

- Anonymous device identity on blockchain

  - implement zk-SNARK in Ethereum (using ZoKrates)

  - create a smart contract as a verifier

  - generate a proof and convince the verifier regarding identity of the device

2nd stage

- implement Zokrate using IoT devices
- analyze minimum resource requirement for IoT devices

Lead by Nathan