**Cryptocurrency**
- At the core, cryptocurrency is an open ledger keeping track of transactions.
- Copy of ledger maintained across the nodes in the network.
- Authenticity:
  - Elliptic curve cryptography to authenticate transactions.
  - Private key to sign the transaction.
  - Public key to verify the transaction.
- Validity:
  - Blockchain to validate transactions.
  - Inputs: Previous unspent transaction.
  - Outputs: New addresses with unspent funds.

**Hierarchical Deterministic Wallet**
- Hierarchical deterministic wallets help to decrease the risk of online storage and improve the security by just publishing the public keys and keeping private keys offline.
- Separate the generation of public and private key.
- Cold storage decrease the risk of online storage.

**Wallet Implementation**
- Wallet divided into offline wallet and networked wallet.
- Offline wallet:
  - Capable of generating private and public keys.
  - Sign the unsigned transaction.
- Networked wallet:
  - Capable to monitor for outputs on public keys.
  - Hardened wallet capable of performing transaction.

**Wallet**
- Cryptocurrency wallets are the software which bridges the gap between users and cryptocurrencies.
- Provide an easy way to transact.
- Key management:
  - Private key generation.
  - Public key derivation.
  - Secure key storage.

**Key Generation**
- Public key derivation:
  \[ P(x, y) = k \cdot G(x, y) \]
  where:
  - \( k \): Private key (large random integer).
  - \( G \): Base point on the curve.
  - \( P \): Public key (point on the curve).
- Child private key generation:
  - \( k_{child} = k_1 \cdot k_2 \).
  - \( P_{child} = k_{child} \cdot G \).
- Child public key generation:
  - \( P_{child} = k \cdot P \).
- 

**Problems**
- Simple device wallets prioritized convenience over security.
- Secure wallets are inconvenient.
- Wallets become a central point of failure which needs frequent backups.
- Storing private and public keys together create security risks.

**Future Work:**
- Bitcoin Improvement Proposal 39 to generate mnemonics phrase which is a part of seed generation process.
- Shamir Secret Sharing Scheme can be used to split the secret between two or more individuals, and M out of N confirmation needed to authenticate.
- A multisignature transaction requires M out of N signatures to authorize a transaction. Feature to create multisignature transaction will be an improvement in the security of the wallet.

**Conclusion:**
- In cryptocurrency wallets, there is a trade-off between security and convenience.
- Hierarchical deterministic wallet helps improve security as well as convenience.

**Contact**
Ankush Arun Kawanpure
Rochester Institute of Technology
aak3988@rit.edu
Phone: 585-747-0326

**References**

**Design and Analysis of Wallets for Selected Cryptocurrencies**
Ankush Arun Kawanpure
Advisor: Prof. Stanislaw P. Radziszowski