

Application for cryptocurrency wallets management

Sławomir Górawski

Agenda

- Thesis overview
 - Goal
 - Challenges
 - Solutions
- Live demo
- Summary

Goal

Goal

Creating an application for cryptocurrency wallets management

- Multiple blockchains
- Unified interface
 - Creating wallets
 - Viewing balances
 - Making transfers
- Simple UX
- Power user friendly

Existing solutions

- Only similar blockchains
- Complex UX
- No customization

E.g.: Copay, MyEtherWallet

Challenges

Creating wallets

- Asymmetric cryptography
- Private key, public key, address
- Different formats

BIP32 and BIP44

Viewing balances

Bitcoin

- Transactions
- Stateless

Harder

Ethereum

- Accounts
- Stateful

Easier

Making transfers

Bitcoin

- UTXOs
- Must spend entire input
- Change transaction
- Multiple recipients

Harder

Ethereum

- Accounts
- Can spend only part of balance
- Only one recipient

Easier

Solutions

Creating wallets

- Unified from the start
- pywallet
- Mnemonic phrase

Viewing balances

- Built-in indexing in Bitcoin
- Call to RPC in Ethereum
- Unified interface
- Charts and values in USD

Making transfers

- UTXO gathering in Bitcoin
- Checking balance in Ethereum
- Signing with private key
- Unified interface - multiple recipients
- Table with info

Live demo