Blockchain Wallets and Security

Paul Puey, CEO

edge

edgesecure.co

Topics

- Private Keys
- Types of Wallets
- Security Issues
- Tools

edge

@paullinator

Private Keys

3a1076bf45ab87712ad64ccb3b10217737f7faacbf2872e88fdd9a537d8fe266

S6c56bnXQiBjk9mqSYE7ykVQ7NzrRy

order public pelican party amount judge empty expand razor next sheriff modify about

edge

@paullinator

Types of Wallets

- Hot Wallet 
- Cold Wallet 
- Multisig 
- Custodial 

edge

@paullinator

Biggest Security Issues

Custodial Services (Exchanges)

User Error

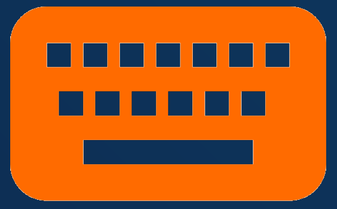
Device Hack

edge

@paullinator

Device Security Issues

Key Logger



Screen Grabber

Disk Reader

edge

@paullinator

Device Security

- Encrypt keys at rest
- Do not display keys to user
- Do not let user enter keys via keyboard
- Browser issues

edge

@paullinator

Encryption

- Password derivation
- Salts
- Random size headers

edge

@paullinator

Encryption

- Password derivation
  - SHA256
  - PBKDF2
  - Scrypt (N, r, p parameters)

edge

@paullinator

Encryption

- Salts
  - hashfunction(password + salt) => encryption key
  - Store salt with encrypted data

edge

@paullinator

Encryption

- Password strength
  - Favor 3-4 random words vs 8-10 characters
  - https://github.com/dropbox/zxcvbn

edge

@paullinator

Encryption

- Random size headers
  - AES256 requires 256 bit blocks
  - [header][data][padding]

edge

@paullinator

Tools

- Keythereum
  - https://github.com/ethereumjs/keythereum
- Edge SDK
  - https://github.com/Airbitz/edge-login-ui

edge

@paullinator

Edge SDK

```
_abcUi = abcui.makeABCUIContext({
  apiKey : 'api-key-here',
  appId : 'com.mydomain.myapp',
  assetsPath : '/path-to-assets/',
  vendorName : 'My Awesome Project',
  vendorImageUrl : 'https://mydomain.com/mylogo.png'
});
```

edge

@paullinator

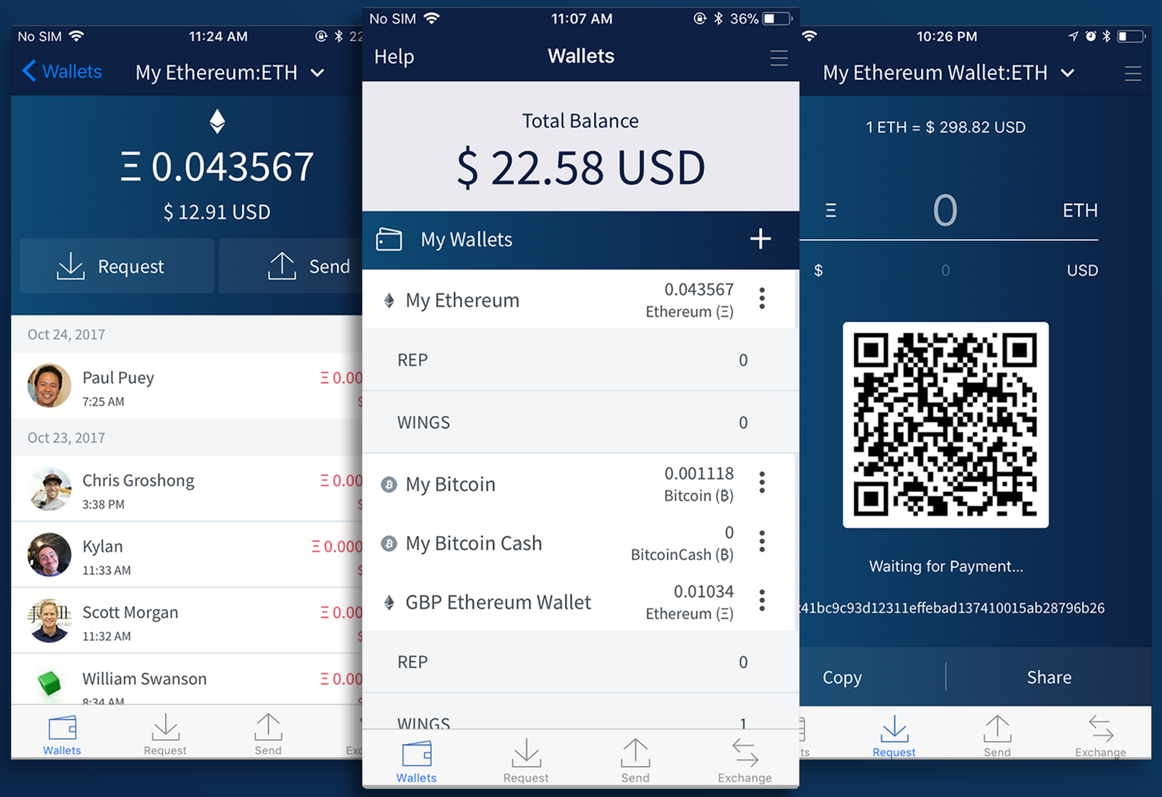
Edge SDK

```
_abcUi.openLoginWindow(function(error, account) {
  _account = account;
});
```

edge

@paullinator

Edge Wallet



- Bitcoin
- Bitcoin Cash
- Litecoin
- Dash
- Ethereum
- ERC20 Tokens

edgesecure.co

@paullinator

Blockchain Wallets and Security

Paul Puey, CEO

edge

edgesecure.co