BlueWallet: The Secure Bitcoin Wallet

Christian Decker

ETH Zurich – Distributed Computing Group – www.disco.ethz.ch

- Global
- No intermediary
- Instantaneous
- Pseudonymous

- Global
- No intermediary
- Instantaneous
- Pseudonymous
- Secure?

Security

Bitcoin:

- Ledger based on consensus
- ECDSA (secp256k1) signatures
- Auditable

Security

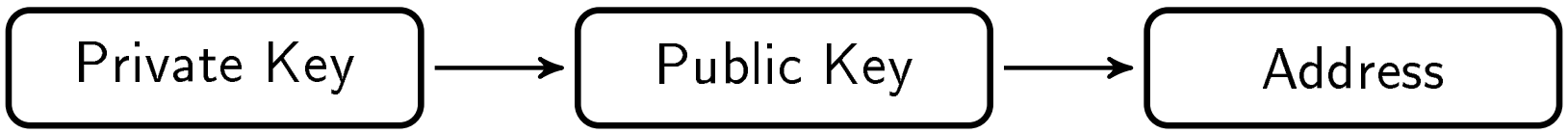
Bitcoin:

- Ledger based on consensus
- ECDSA (secp256k1) signatures
- Auditable

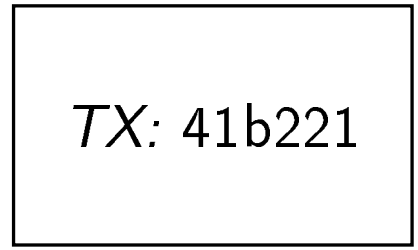
User:

- Theft
- Price instability
- Legal uncertainty
- ...

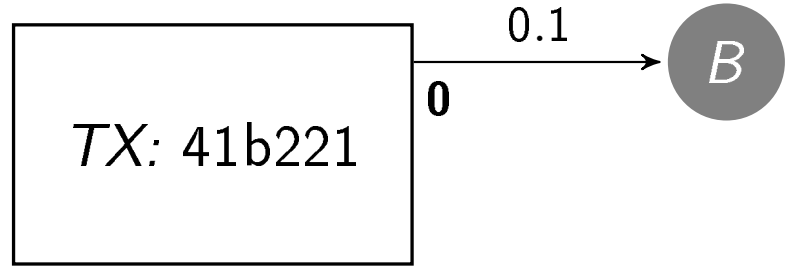
Opening an account in Bitcoin



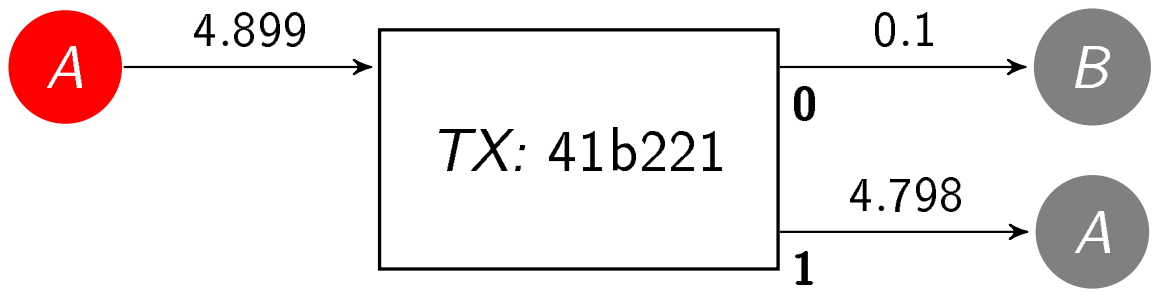
Transferring bitcoins



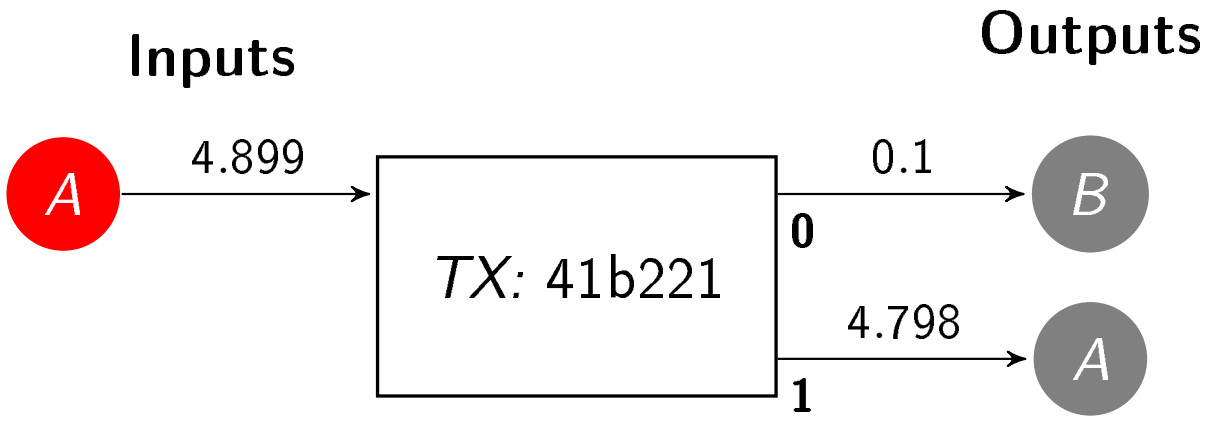
Transferring bitcoins



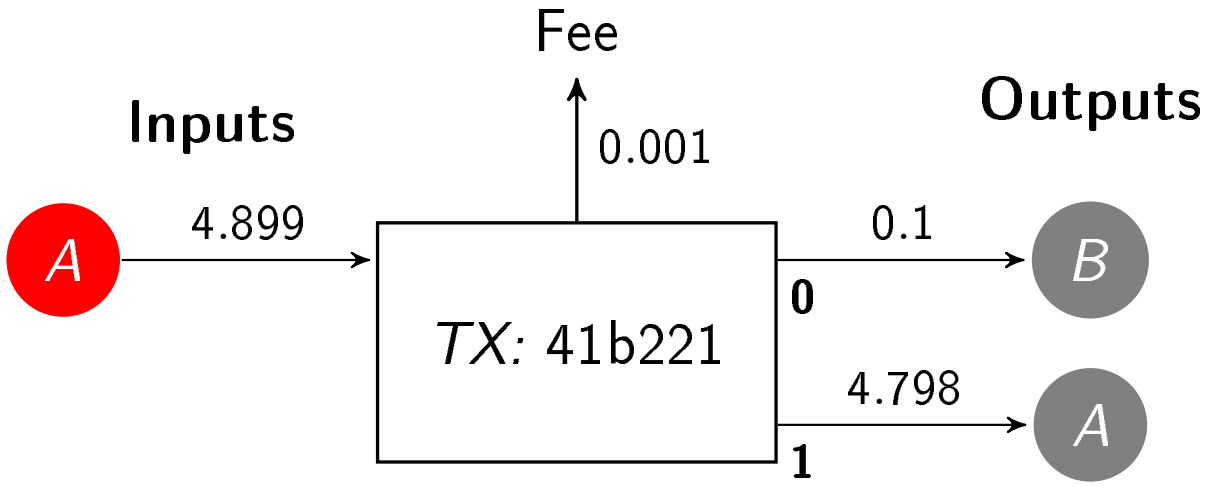
Transferring bitcoins



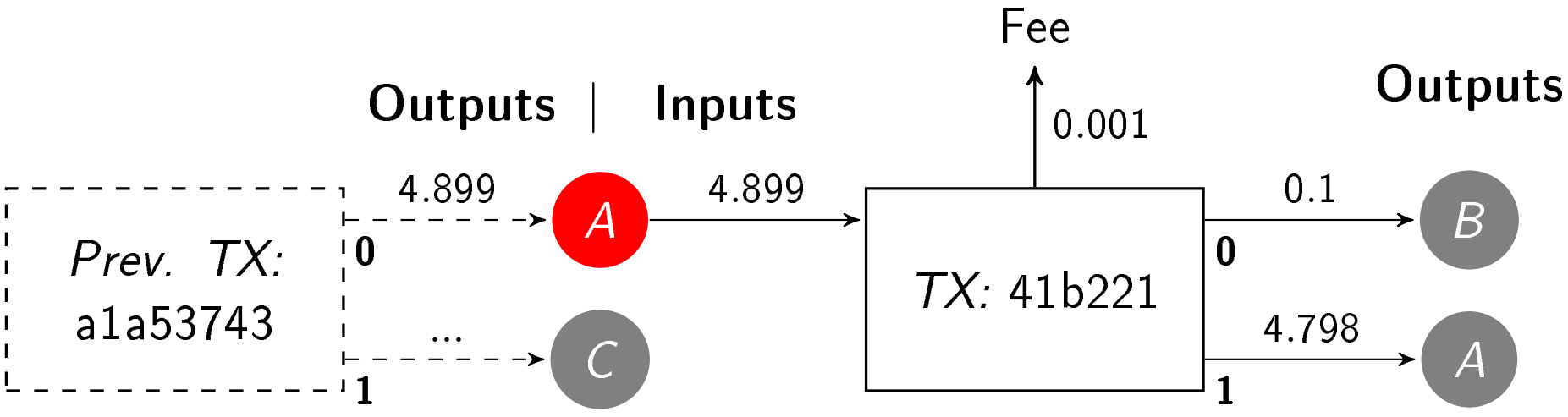
Transferring bitcoins



Transferring bitcoins

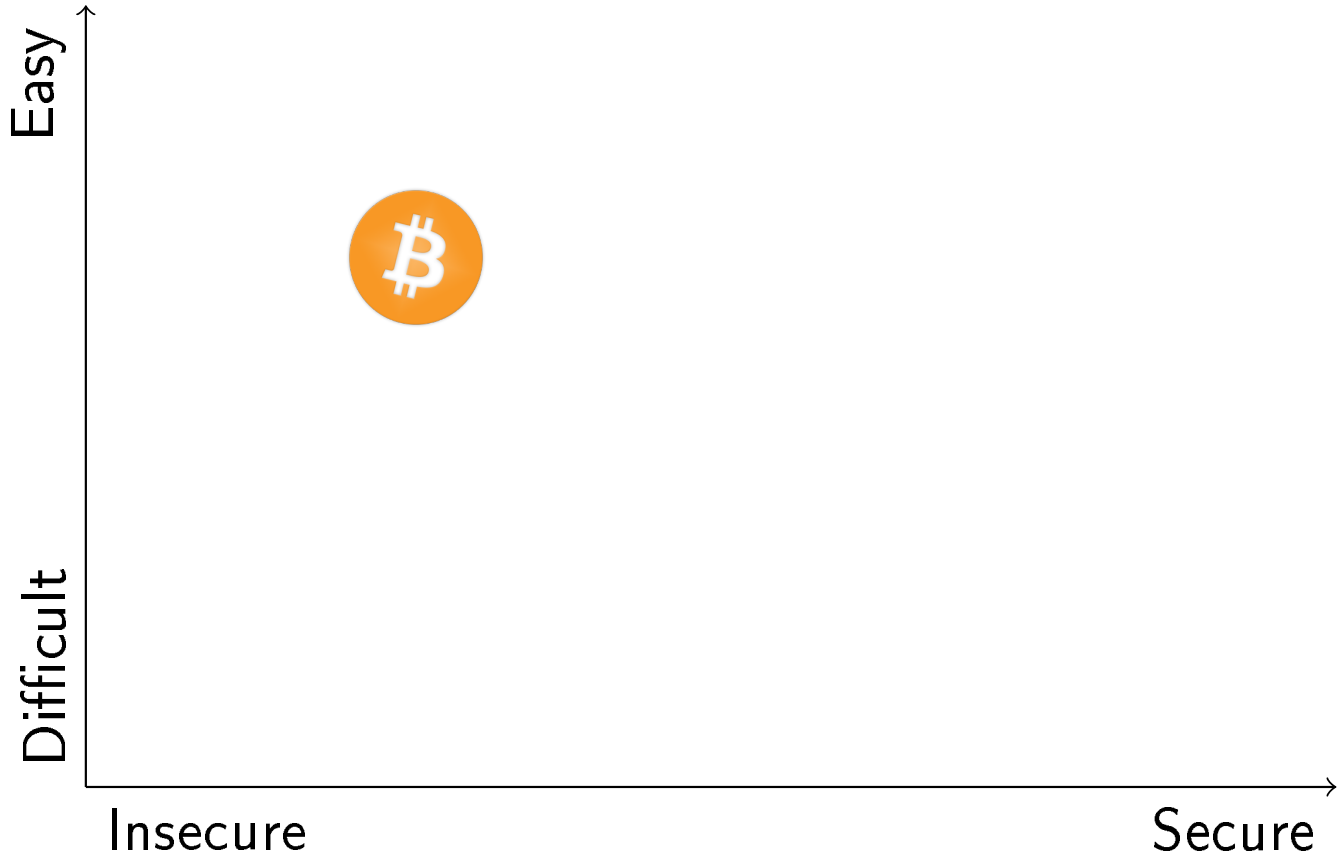


Transferring bitcoins



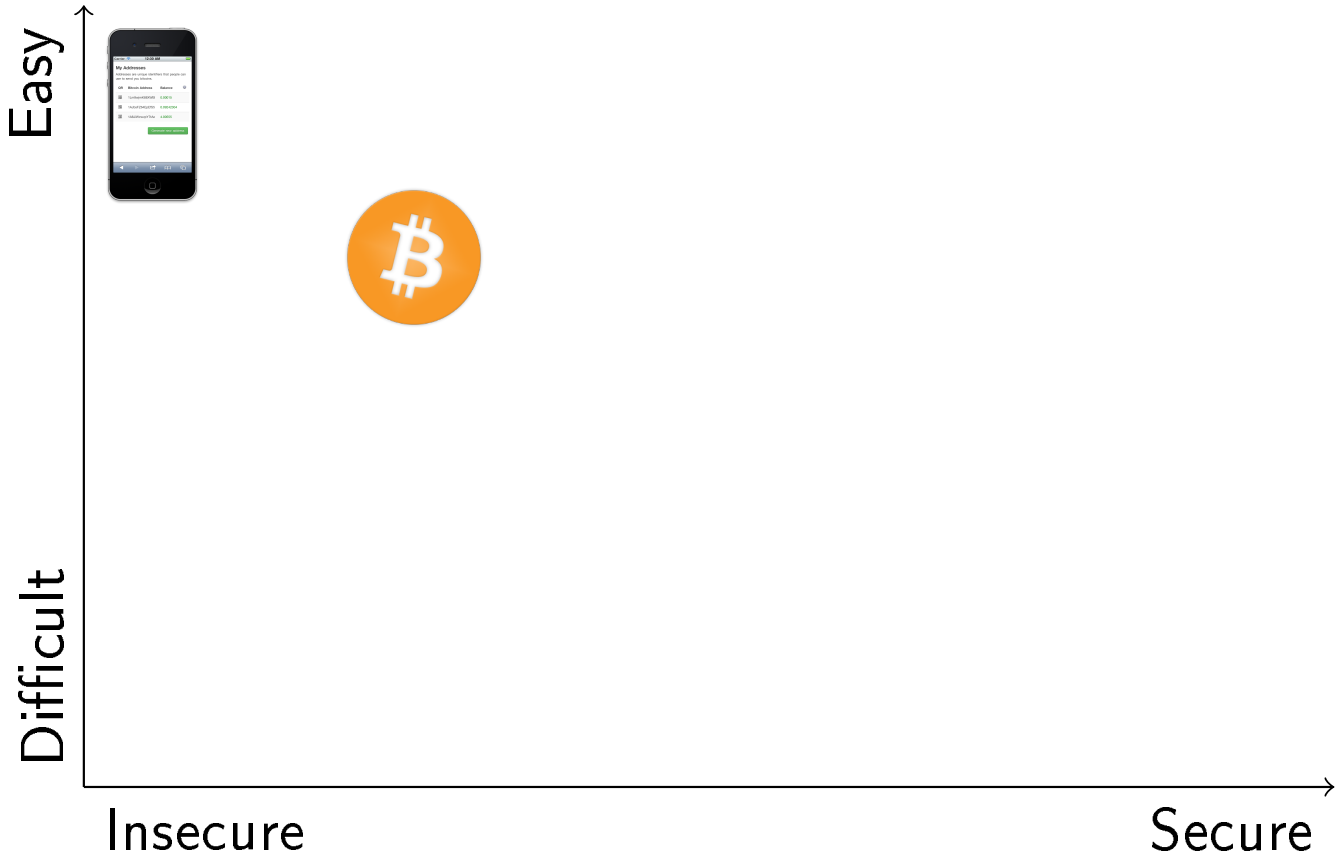
Securing User Wallets

Protecting private keys is paramount.



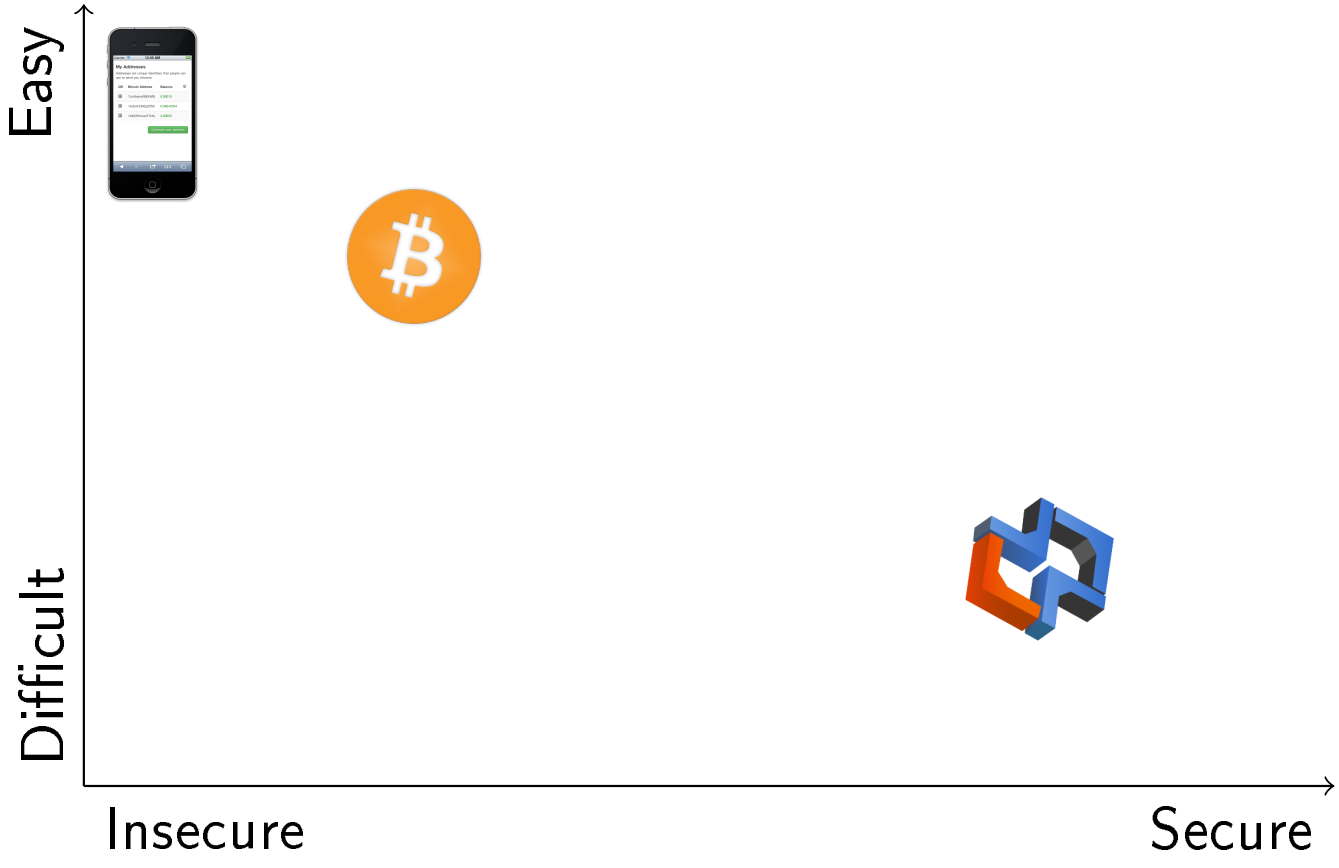
Securing User Wallets

Protecting private keys is paramount.



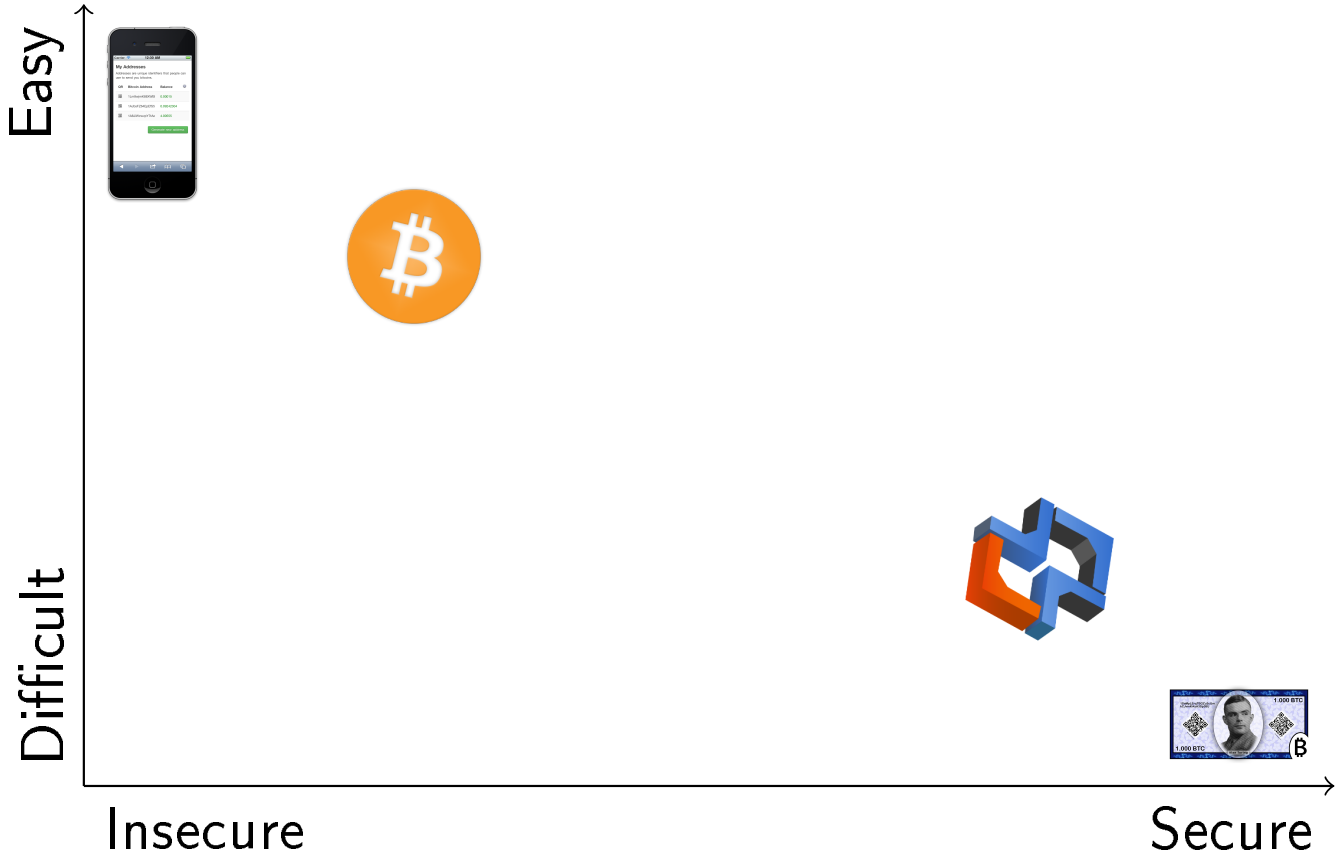
Securing User Wallets

Protecting private keys is paramount.



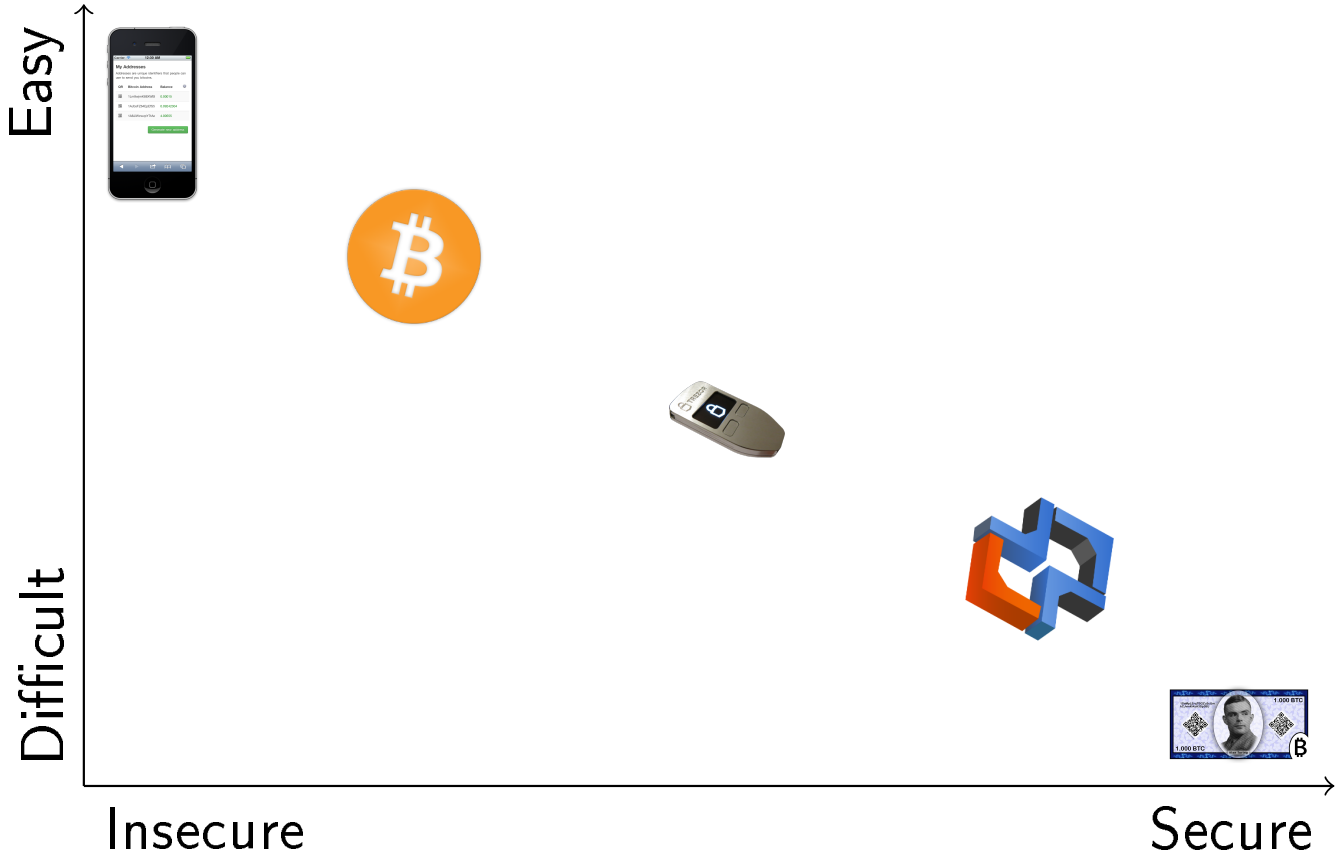
Securing User Wallets

Protecting private keys is paramount.



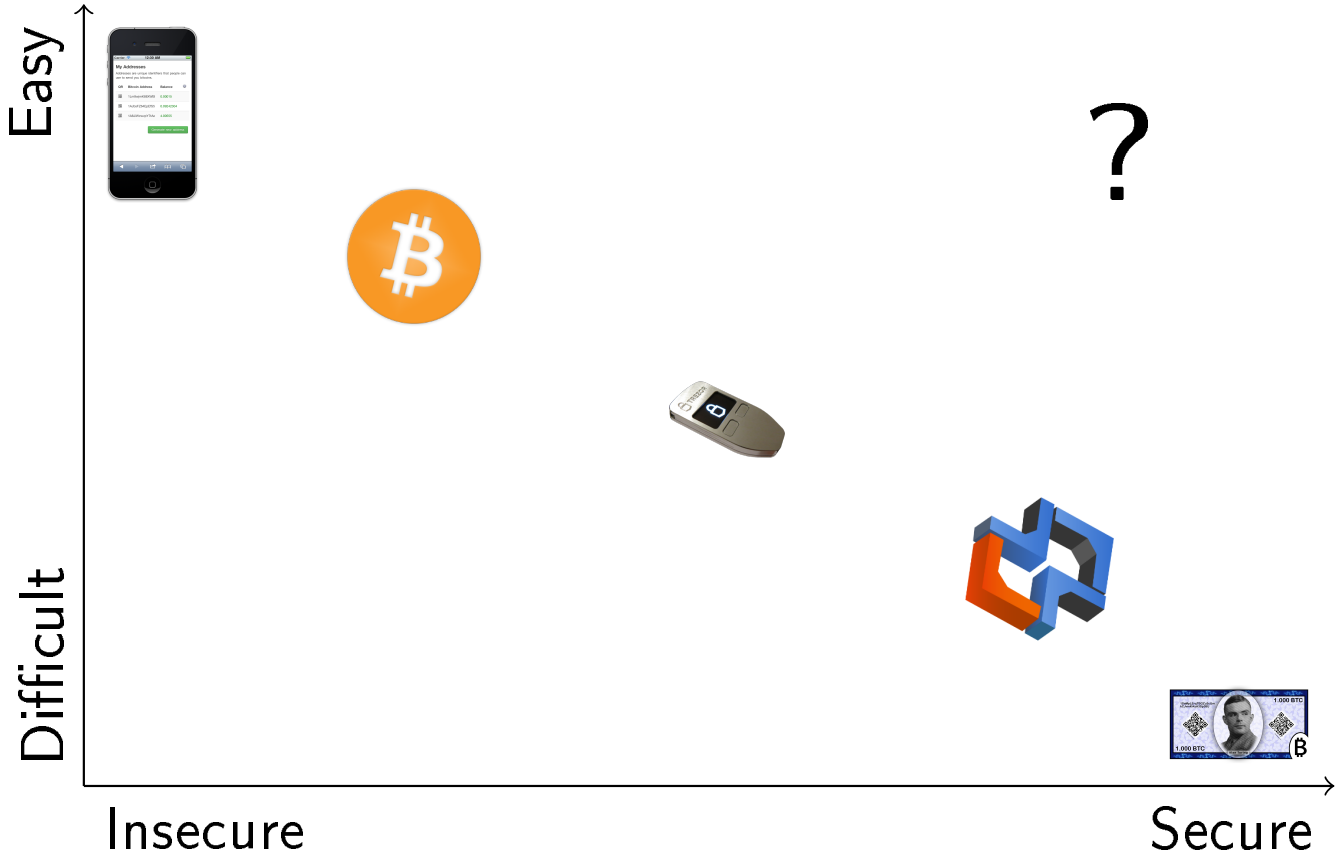
Securing User Wallets

Protecting private keys is paramount.



Securing User Wallets

Protecting private keys is paramount.

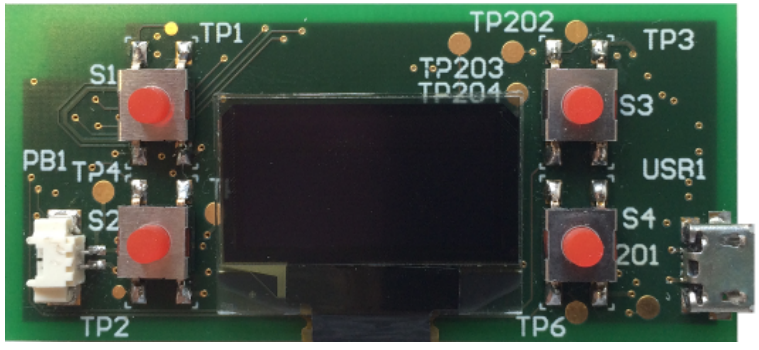


Goals

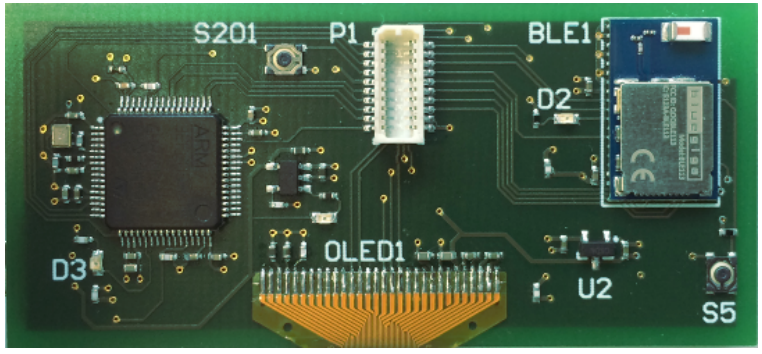
- Mobile (Point-of-Sale payments)
- Easy to use
- Real-time payments
- Secure

Result

Front



Back



Technical Details

Communication Chip

- Bluegiga BLE113 (8 bit)
- 8 kB RAM
- Always on
- Handles communication
- Handles user interaction

Technical Details

Communication Chip

- Bluegiga BLE113 (8 bit)
- 8 kB RAM
- Always on
- Handles communication
- Handles user interaction

Crypto Chip

- STM32 F20RE (32 bit)
- 512 kB RAM
- On demand
- Performs crypto operations
- Stores private keys

Technical Details

Communication Chip

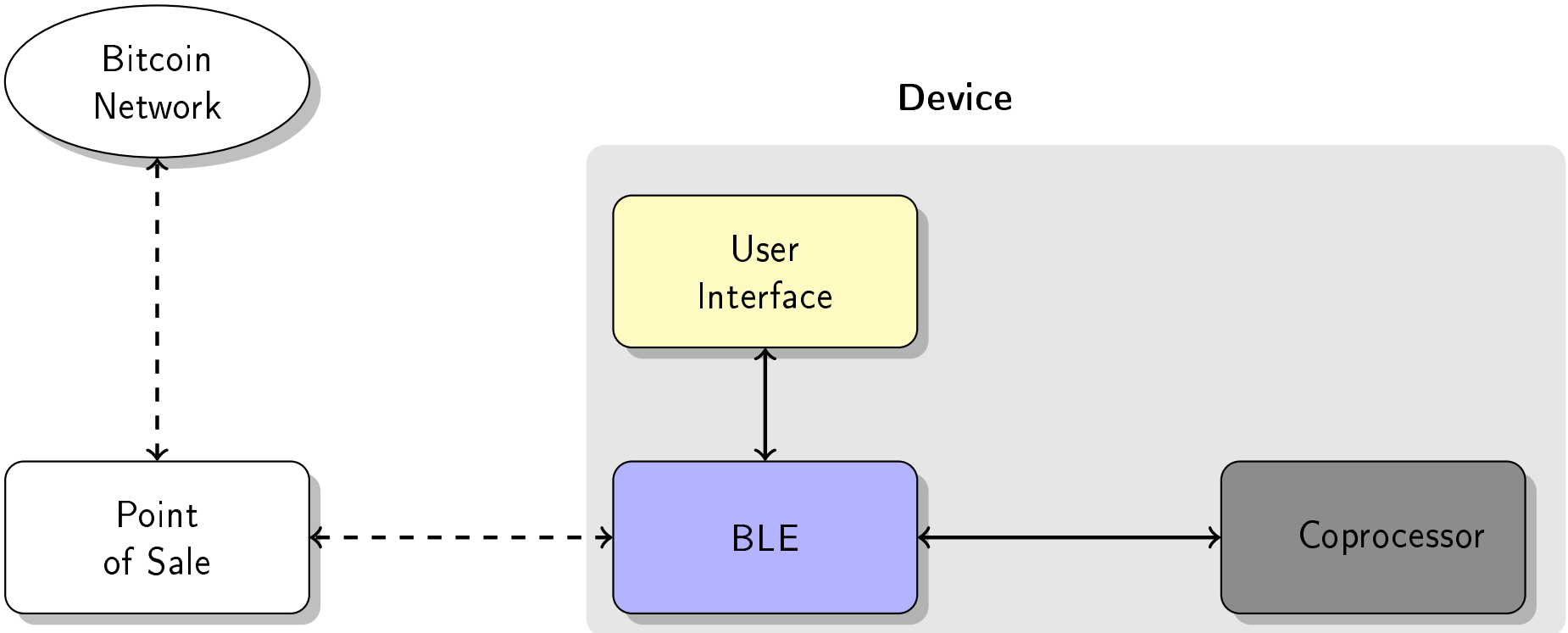
- Bluegiga BLE113 (8 bit)
- 8 kB RAM
- Always on
- Handles communication
- Handles user interaction

Crypto Chip

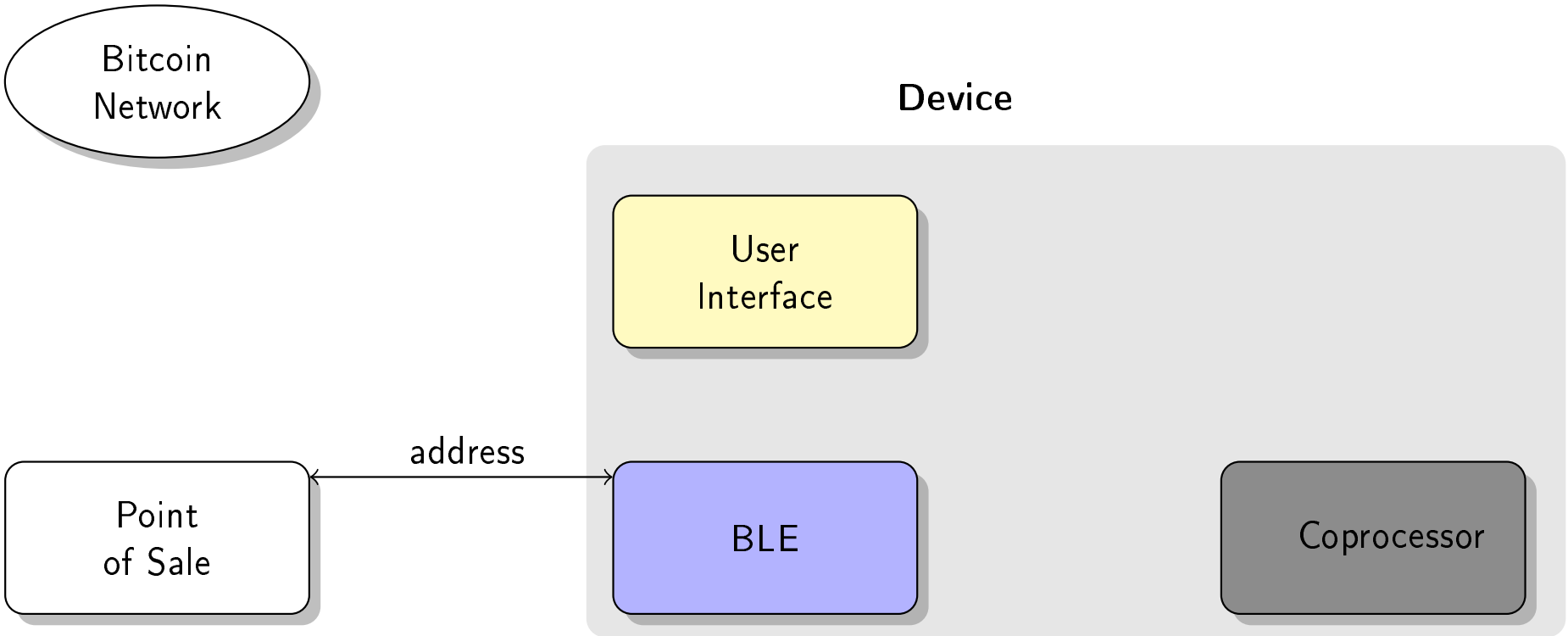
- STM32 F20RE (32 bit)
- 512 kB RAM
- On demand
- Performs crypto operations
- Stores private keys

There are currently no secure cryptocoprocessors with ECDSA secp256k1.

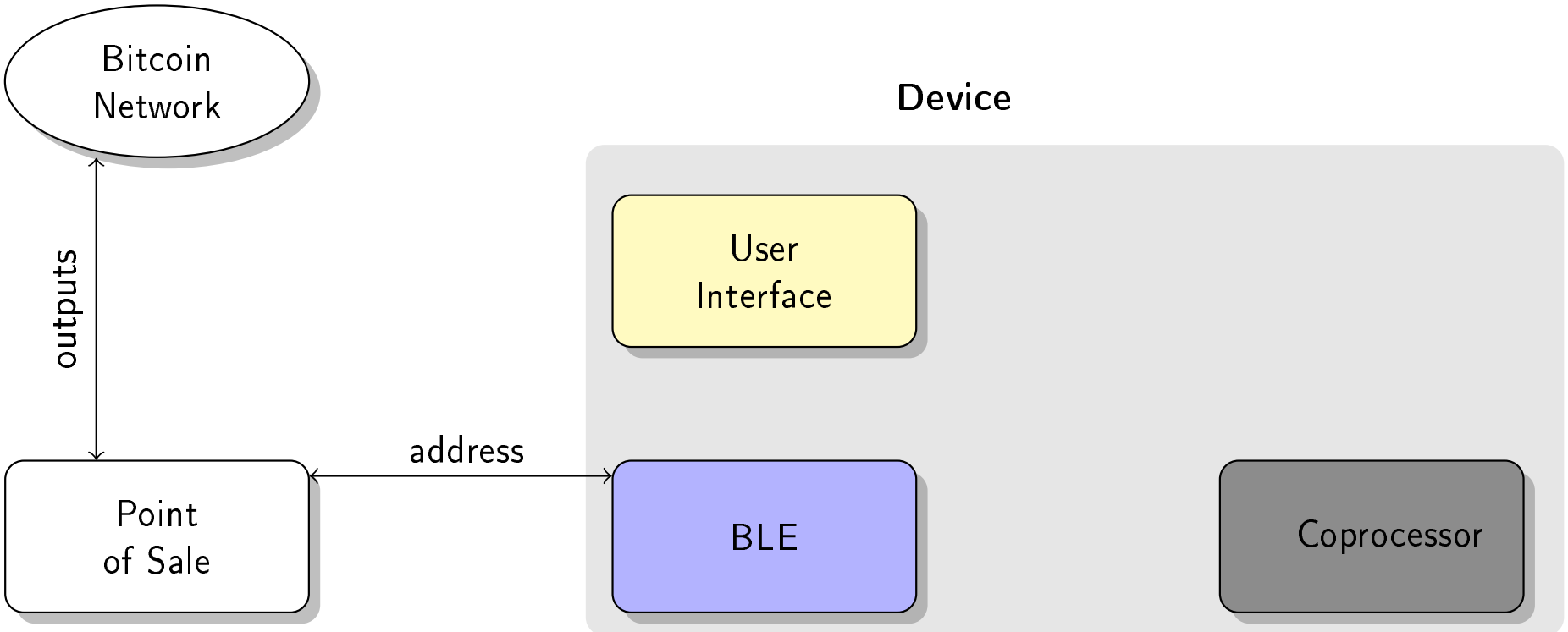
Walkthrough



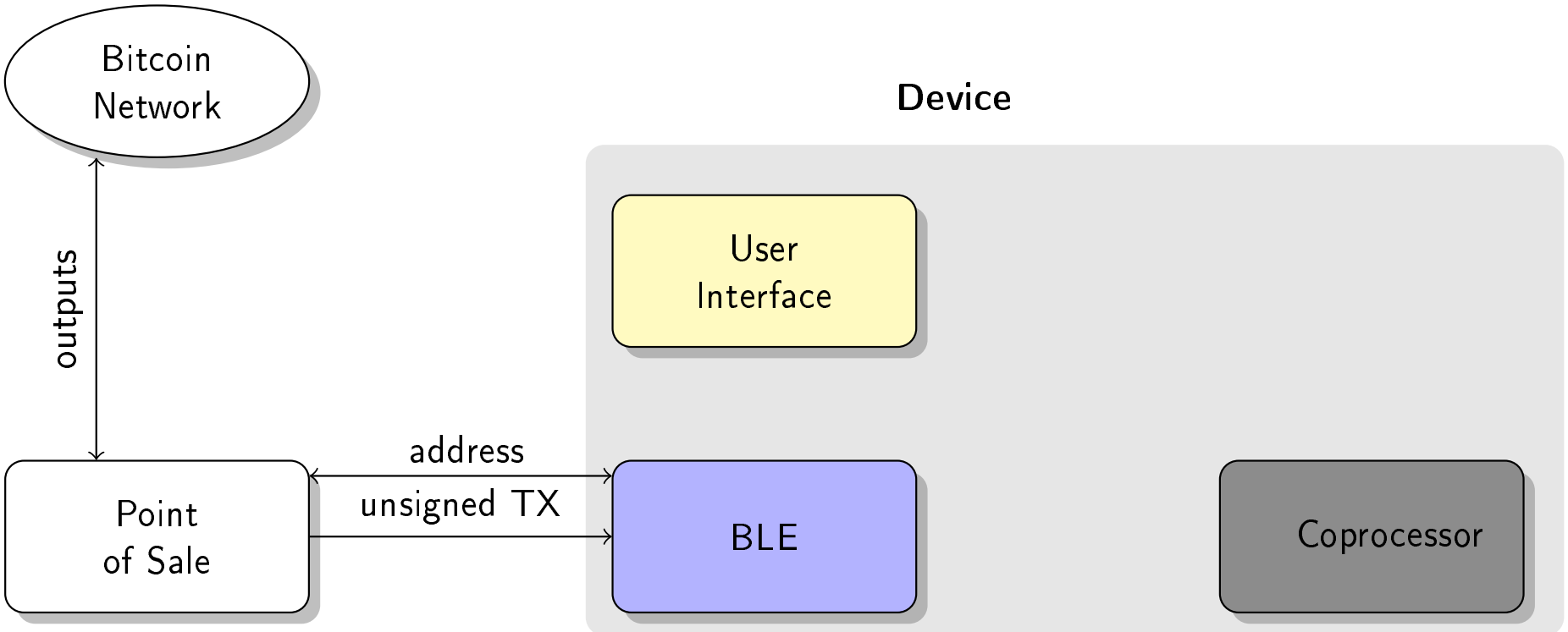
Walkthrough



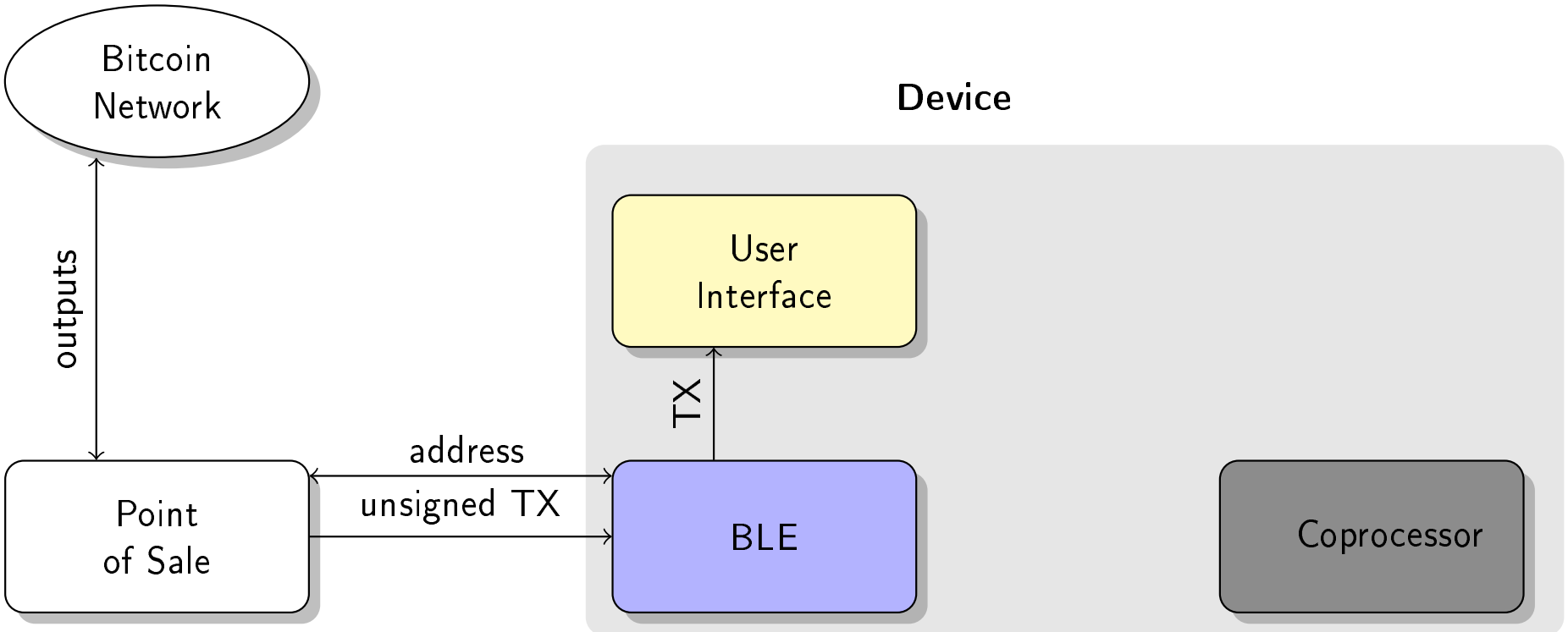
Walkthrough



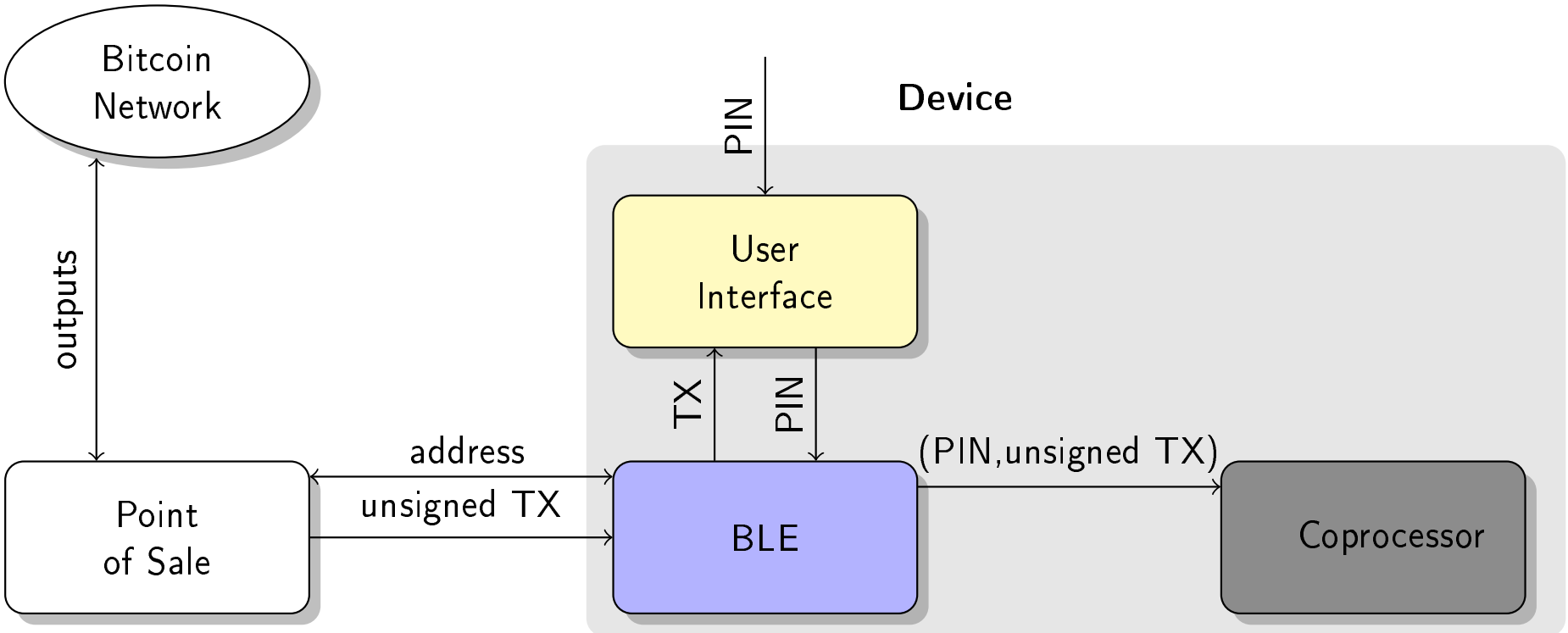
Walkthrough



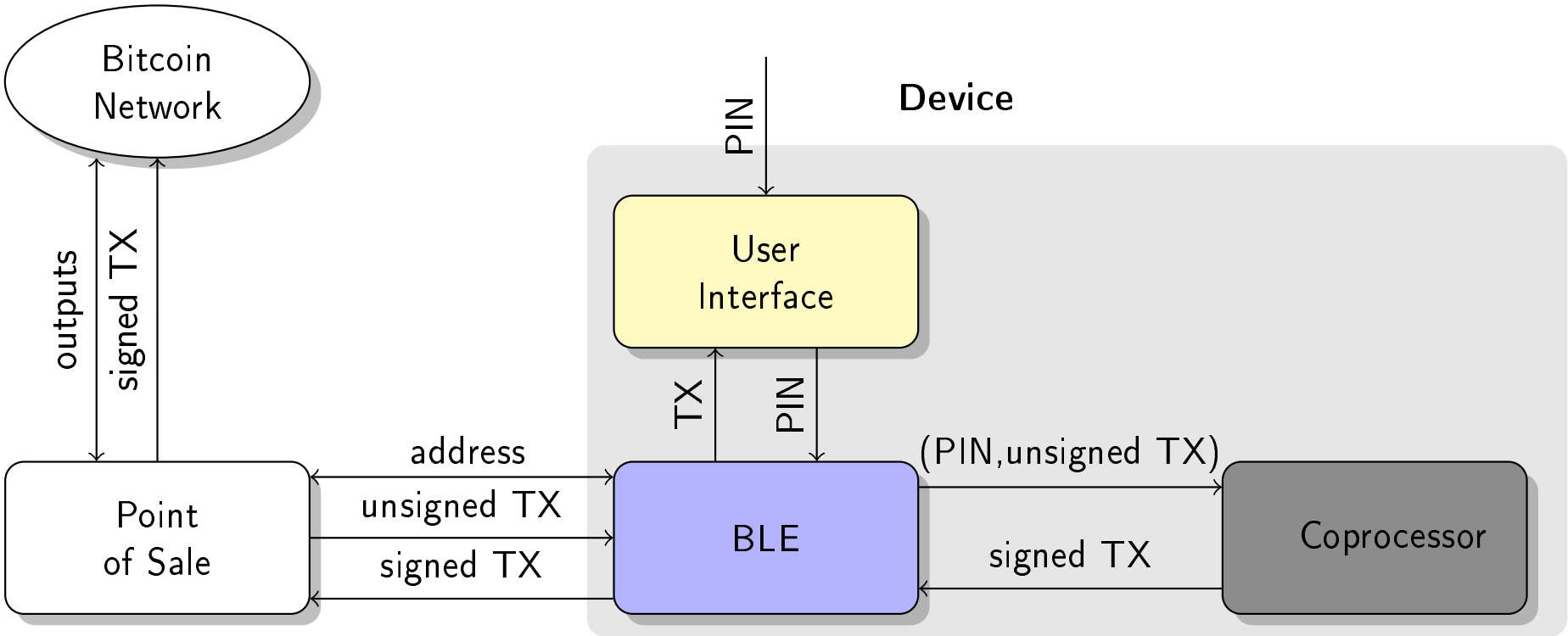
Walkthrough



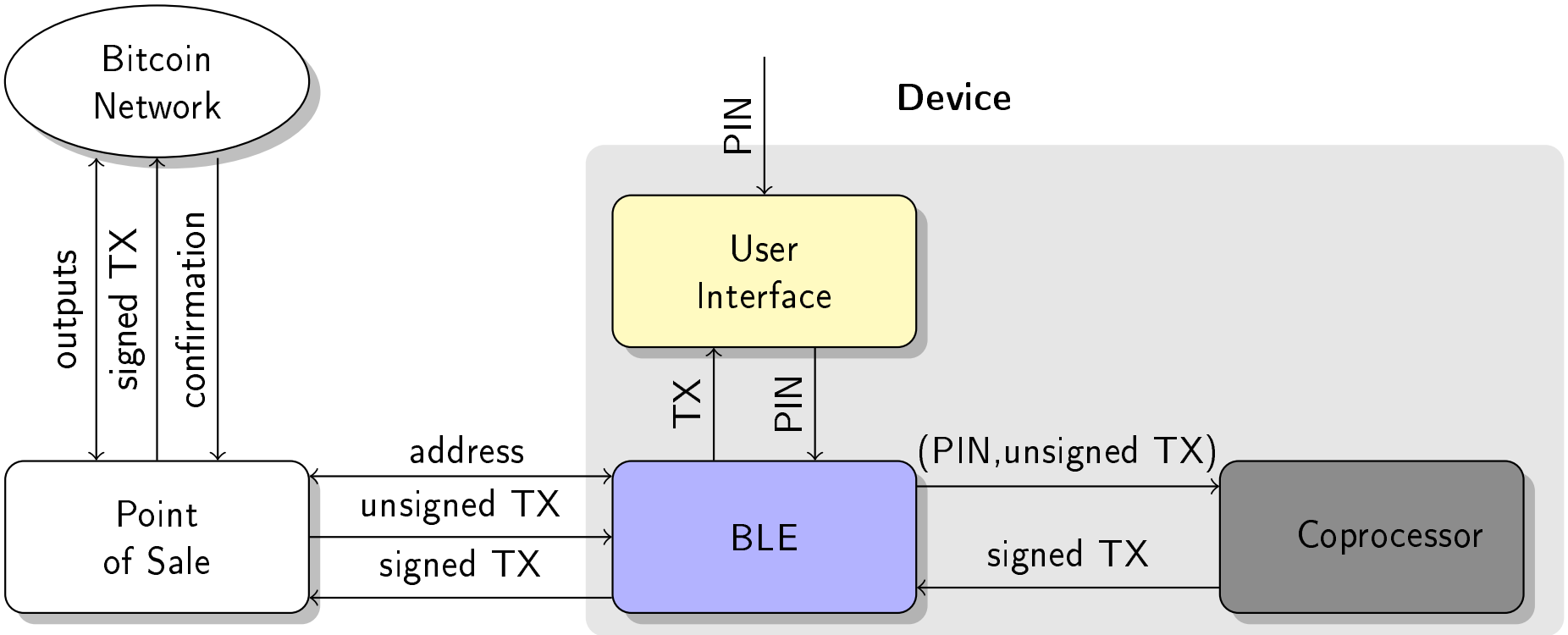
Walkthrough



Walkthrough



Walkthrough



Goals

- Mobile
- Easy to use
- Real-time payments
- Secure

Goals

- Mobile ✓
- Easy to use
- Real-time payments
- Secure

Goals

- Mobile ✓
- Easy to use ✓
- Real-time payments
- Secure

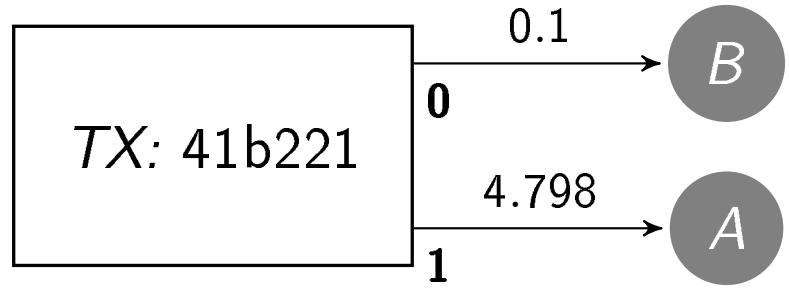
Goals

- Mobile ✓
- Easy to use ✓
- Real-time payments ✓
- Secure

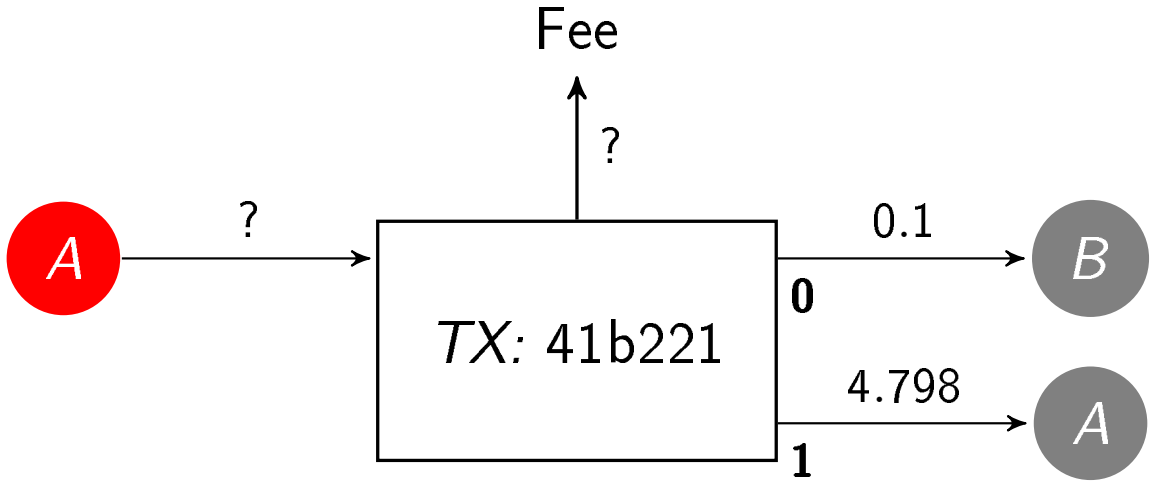
Goals

- Mobile ✓
- Easy to use ✓
- Real-time payments ✓
- Secure ?

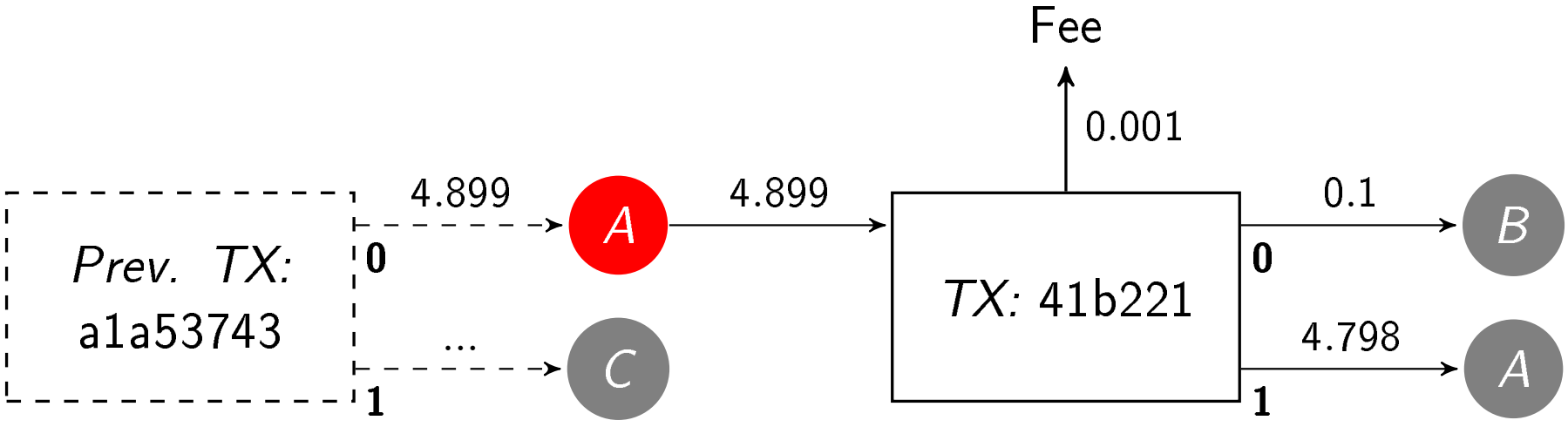
Security



Security



Security



Send previous transactions to BlueWallet

Conclusion

- Mobile ✓
- Easy to use ✓
- Real-time payments ✓
- Secure ✓

Thank you, questions?

Authors:
Tobias Bamert
Christian Decker
Roger Wattenhofer
Samuel Welten