Security

Keeping Private Keys to Yourself

Leonhard A. Weese
President, Bitcoin Association of Hong Kong
leo@bitcoin.org.hk

Genesis Block, March 27, 2018

Convenience vs Security

- Hold your bitcoins yourself
- Trust your device
- Secure your accounts
- Learn your threat model
- Choose from your options
  - Multisig
  - Cold Storage
  - Hardware key

Move Bitcoins Off Exchanges

- Exchanges:
  Theft, fraud, loss, ransom, seizure, DDoS
- Bitcoins held by exchanges are IOUs
- If you actively trade, know about the risks:
- Can there be adequate compensation?

Trust Your Device

- Don't root or jailbrake
- Keep your device up to date
- Beware of programs from bittorrent
- Beware of macros, java
- Read warning messages
- Make backups

Secure Your Accounts

- Email and social is most vulnerable
- Unique, memorable passwords
- Password managers
- Two-factor authentication
  - SMS
  - Apps (Google Auth, Authy)
  - Hardware (FIDO U2F)

Learn your threat model

- Hackers
- Governments
- Fires
- Thieves
- Illness

Bitcoin wallets

- Hot wallets
- Cold wallets
- Hardware wallets
- Multi-signature solutions

	few transactions	many transactions
small value	Online Wallet	Mobile Wallet
large value	Paper Wallet	Hardware Wallet

Hot Wallets

- Phone OR Computer
- Multisig wallet (phone AND computer)
- Online wallet

- Backup solutions similar to cold wallets

Cold Wallets

- Paper seed in safe
- Encrypted in password manager
- Multisig wallet (family, lawyer, bank vault, safe)

- Watch-only wallets to receive funds

Hardware Wallets

- Ledger
- Trezor

- Backup solution similar to cold wallet

TAILS

- The Amnesic Incognito Live System
- Boots from a USB stick
- Drastically reduces risk of attacks
- Forgets everything at shutdown

- Ideal to create various styles of cold wallets

Leonhard A. Weese

President, Bitcoin Association of Hong Kong

leo@bitcoin.org.hk

@LeoAW

https://www.bitcoin.org.hk

PGP: 9185 B1FD 625A 1AD0 CCFE F451 C073 56F5 BB4D D1B7

Genesis Block, March 27, 2018