ECE 443/518 – Computer Cyber Security
Lecture 20 Bitcoin Security

Professor Jia Wang
Department of Electrical and Computer Engineering
Illinois Institute of Technology

October 27, 2025

Outline

Reading Assignment

- This lecture: Bitcoin Security
- Next lecture: Oblivious Transfer, Secure Multi-Party Computation

Outline

Practical Considerations for Cryptocurrency

- Cryptocurrencies that are secure in theory are not necessarily so in practice.
  - Security: compromised hardware and software leak private keys.
  - Usability: complicated operations push people to look for practical solutions that are usually less secure.
  - Privacy: account owners can be targeted if identified physically.
- How to bitcoin is designed to address these threats?
  - Weaknesses are constantly attacked because of the huge value associated with bitcoin.

Bitcoin Custody

- Will you trust someone to manage your bitcoin private keys?
- Yes: third-party custody
  - E.g. exchanges, banks, and brokerage firms.
  - Better usability: access bitcoin the save way as money.
  - No privacy: require physical identity.
  - Security concern: what if they cheat or are compromised?
  - Sometimes this is a must, e.g. to exchange between bitcoin and money, and to store bitcoin in retirement accounts.
- No: self-custody
  - Not your keys, not your coins.
  - Better security and privacy at the cost of usability.
  - Need a better understanding to achieve desired security and privacy, with a focus on managing private keys.
  - A third-party providing custody eventually relies on self-custody to manage bitcoin.

Bitcoin Transactions

- To receive bitcoin
  1. Generate a bitcoin account as a public/private key pair.
  2. Let the other party know the account address (public key) and initiate the transaction as above.
  3. Wait until the transaction to be included in the blockchain.
  4. In theory you can skip 2 and 3 to obtain bitcoin from mining.
- To send bitcoin
  1. Obtain recipient's account address and create a transaction.
  2. Sign the transaction with your private key.
  3. Broadcast the signed transaction to the bitcoin network.
  4. Wait until the transaction to be included in the blockchain.
- What are the threats associated with each step?
  - Clearly you would need to use computers for most of the steps.

Outline

Bitcoin Wallets

- Wallet: a hardware or software implemention of bitcoin protocol that one uses to interact with the bitcoin network.
- Create accounts by generating public/private key pairs.
- Access Internet to obtain the blockchain to check account balances.
- Access private keys to sign transactions.
- Access Internet to broadcast signed transactions.

Hot and Cold Wallets

- Hot wallets: those holding private keys and being able to connect to Internet at the same time.
  - Easy to use and good for learning, e.g. wallet applications installed on your laptop and smartphones.
  - But the private key will leak if the wallet is compromised.
- Cold wallets: those holding private keys but without the capability of network communications.
  - Import transactions and export signed transactions through files that can be inspected to prevent potential leakage.
  - Should cold wallets support Bluetooth or USB connectivities?
- Since cold wallets don't connect to Internet directly, users need to use other software to connect online.
  - To check balance and to broadcast signed transactions.
  - Nither needs access to private key.
  - Usually use a hot wallet without private key.
- Which wallet will you trust?
  - For best protection we should assume both are compromised!

Cold Wallet Threats

- What if adversaries gain physical access to cold wallets?
  - Access its storage to obtain private keys.
- What a compromised cold wallet could do?
  - Not much unless it has means to connect to Internet indirectly.
  - Generate private keys that can be reproduced by adversaries.
  - Replace recipient account addresses with those of adversaries before signing transactions.

Cold Wallet Security

- Use password to control physical access.
  - Private keys are encrypted with password.
  - Counterintuitively, incorrect password should just give different private keys instead of any error message.
- Validate recipients in signed transactions before broadcasting them.
  - E.g. by using the software that broadcasts signed transactions.
  - What if the software colludes with the compromised cold wallet?

Private Key Generation

- Bitcoin accounts are identified by ECDSA.
  - For simplicity, let's just write a bitcoin private key as $k_{pri} = a$ and the corresponding address as $k_{pub} = \alpha^a$.
- $k_{pri} = a$ has a length of 256 bits and should be generated from a true random number generator (TRNG).
- Could we use an online random number generator?
  - No, we should assume all such websites are compromised – adversaries will record all random number generated and watch for the corresponding bitcoin address.
- Cold wallets may take TRNG outputs manually to protect against attacks on key generation.
  - Rolling a die gives 1 out 6 possibilities. Rolling 100 dice will generate enough randomness for a 256-bit random number.
  - Clearly, you should not use a virtual dice roller from online.

Private Key Recovery

- What if the cold wallet (or other device for private key storage) is broken or lost?
  - Lost private keys cannot be recovered – all funds are lost.
- BIP-39 Mnemonic Code
  - Avoid human errors in handling bytes and binary strings.
  - A list of 2048 (2^{11}) easy-to-remember words.
  - Derive and reproduce a private key from 24 words.
  - Potentially with a password.
- Still, a reliable way to backup the words is required.
  - Clearly, you should not store them in your emails or any devices that connect to Internet.
  - Prevent lost of backups and leakage from backups – not a good idea to write them down on a piece of paper.
  - What about using multiple cold wallets?
  - Consider using multi-signature (multisig) for more effective use of multiple cold wallets.

Outline

Transactions and Privacy

- Privacy concern: multiple transactions on a single bitcoin account may reveal a lot of information about its owner.
  - Multiple accounts could and should be used for a single owner to protect owner's identity.
- Ideally one account should be used twice.
  - Once for receiving bitcoin.
  - The other should spend all – if there is any remaining balance, it should be sent to a new account in the same transaction.

Unspent transaction output (UTXO)

- A transaction consumes ALL bitcoin from a set of addresses, and then deposits them into a set of NEW addresses.
- In practice, this implies bitcoin doesn't maintain a single account with a running balance.
  - Sometimes we simply say "bitcoin doesn't have accounts".
- Instead, since each address receives its only deposit from a transaction, we identify it within the transaction as a UTXO.
  - Owner owns UTXOs.
  - Each UTXO is spent entirely in a future transaction.
- What about usability?
  - The owner need to generate and maintain a private key for each UTXO.

Hierarchical Deterministic Wallets

- BIP-32: derive normal or hardened child private keys from the parent private key $k_{pri} = a$, each for a usable address for UTXOs.
- Normal child private keys make it easier to derive addresses
  - For simplicty, consider ith child private key as $k_{pri,i} = a + i$.
  - Then the ith address is $k_{pub,i} = \alpha^{a+i} = k_{pub} \times \alpha^{i}$.
  - The owner can derive the addresses without accessing the child private keys or the parent private key – less chance of leaking them.
- However, leaking a normal child private key cause all normal child private keys and the parent private key to be leaked.
  - Use hardened child private keys if that's a concern.
  - To derive addresses, the owner needs to access the hardened child private keys and the parent private key – more chance of leaking them.

Network Traffic and Privacy

- The bitcoin network consists of bitcoin (full) nodes that are connected as a peer-to-peer network.
  - Store and validate current blockchain.
  - Resolve fork by proof-of-work consensus.
  - Forward blockchain to other nodes.
  - Forward transactions to other nodes.
- One needs to connect to a bitcoin node to check account balances and to broadcast signed transactions.
- Privacy concern: nodes may identify owners by the IP addresses that their wallets use to connect to nodes.
  - Use of virtual private networks (VPNs) may hide IP addresses from nodes but will expose the same to the owner of VPNs.
- Run your own node and connect your wallets to it.
  - It is much more difficult to decide which node a signed transaction reaches first since nodes will relay transactions but not their origins.

Summary

- A lot of efforts to make bitcoin more usable in practice, improving its security and privacy.