Blockchain Governance

and safekeeping

Aggelos Kiayias

Dionysis Zindros, Christos Nasikas

The problem of upgrades

- How can you upgrade a blockchain protocol?
- Blockchain systems inherently *different* from traditional software:
  - **Non-networked software**? Easy:
    Just release a new version of GIMP. Whoever likes it downloads it. Old software works.
  - **Client/server software**? Easy:
    Upgrade server to work with new *and* old protocols. Release new client. Old software works.
    Remove old protocol support from server. Clients forced to upgrade.
  - **p2p software**? Easy:
    Release new software. Old clients communicate only with each other.
    New clients communicate only with each other.
    Old clients forced to upgrade as no peers found.
  - **Blockchain software**? Hard: Consensus relies on honest majority!

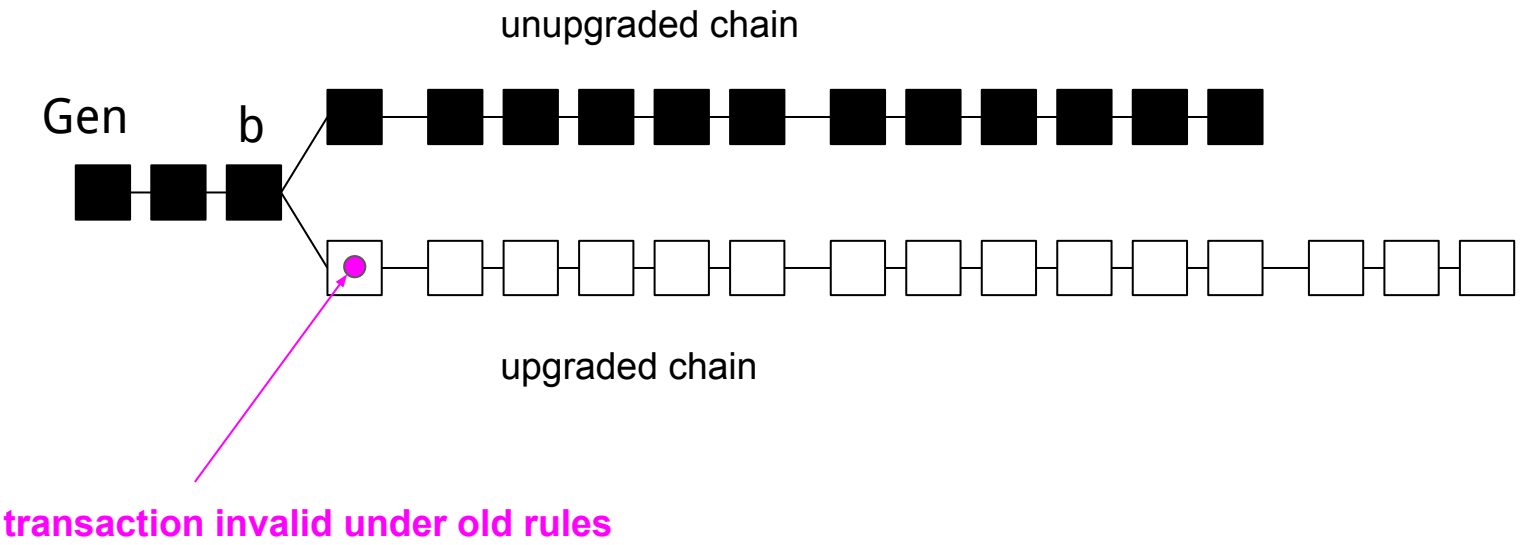
Consensus upgrades

- Some upgrades are client-specific and don’t affect the consensus layer
- Other upgrades affect **which chain is valid** / how valid chains are selected
- Consensus upgrades can be made with a **soft** or **hard** fork

Consensus upgrade?

- Change colors of UI from green to blue
- Fix crash if you put more than 400 BTC in amount textbox
- Introduce new Bitcoin Script operators (e.g. new signature function)
- Introduce new bitcoin address format for multisig
- Change PoW hash function
- Change transactions Merkle tree hash function

Just let people upgrade? Not so fast…
A wild long fork appears!



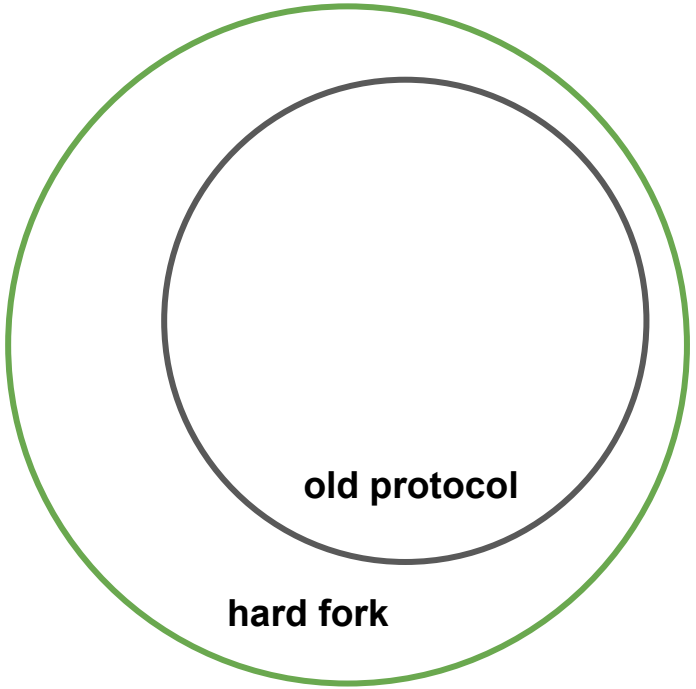
Common Prefix violated

Hard and soft forks

Mechanisms to propose changes in the consensus mechanism

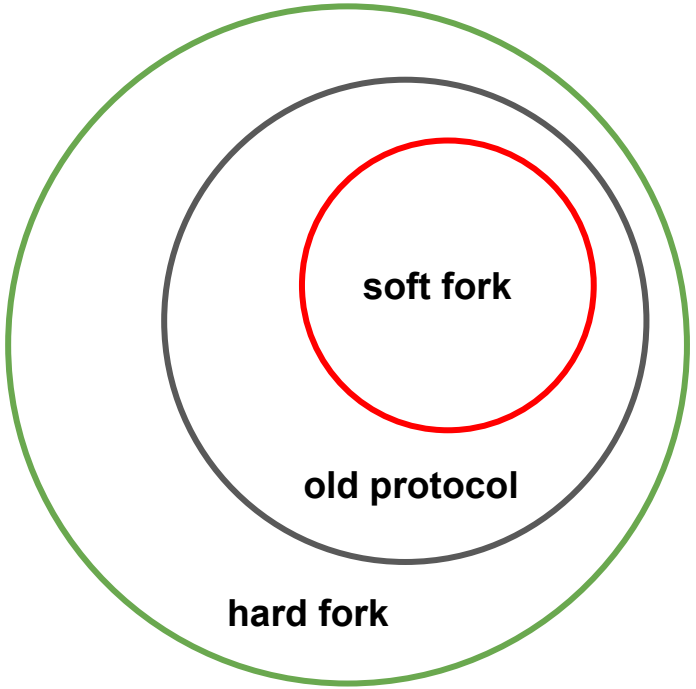
Hard fork

- **Increases** the validity language
- txs / blocks that were invalid are now valid
- All old valid txs / blocks are still valid
- Old miners **reject** some new-style txs / blocks
- New miners **accept** old-style txs / blocks
- New miners would switch back to old protocol chain if it ever becomes longer

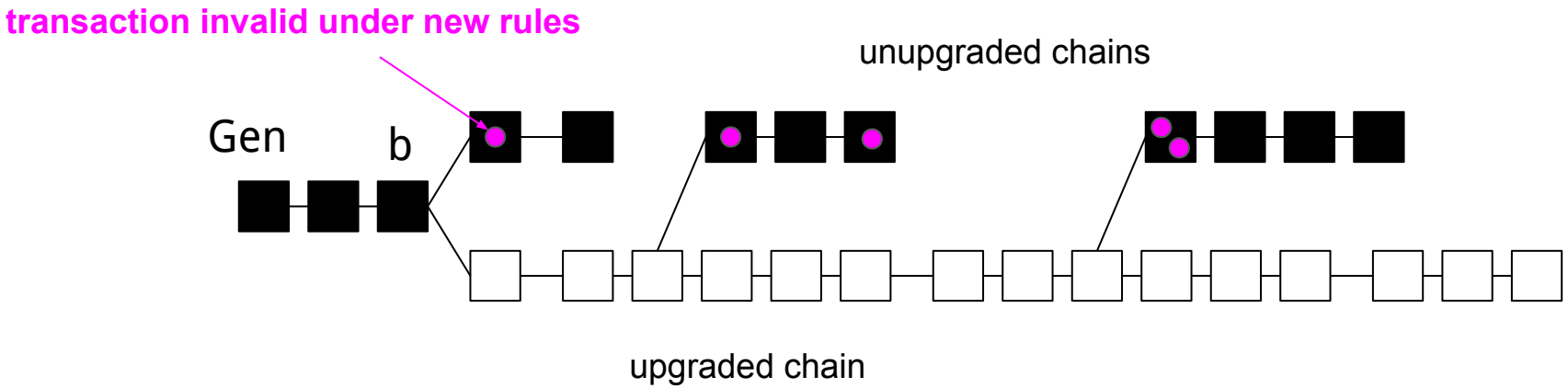


Soft forks

- **Reduces** the validity language
- txs / blocks that were valid are now invalid
- All old invalid txs / blocks are still invalid
- Old miners **accept** new-style txs / blocks
- New miners **reject** some old-style txs / blocks
- Most miners upgrade
- Old miners adopt new chain!
- Old blocks abandoned
- Old miners **forced** to upgrade



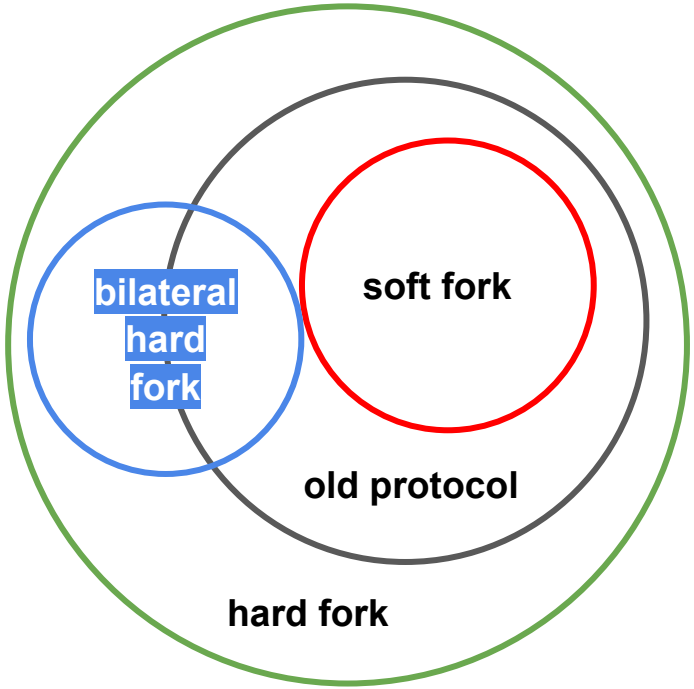
A soft fork execution



Common Prefix OK!

Bilateral hard forks

- **Special type of hard fork**
- **Modifies** the validity language
- Some txs / blocks that were valid are now invalid
- Some txs / blocks that were invalid are now valid
- New miners reject some old-style txs / blocks
- Old miners reject some new-style txs / blocks
- Old/new chain incompatible
  New miners can never switch back to
  old protocol chain



Bitcoin block sizes

- Bitcoin block sizes are limited to 1MB
  i.e., the sum of all the transaction sizes in the Merkle tree must be < 1MB
- Each (p2pkh) transaction is ~250 bytes
- We can fit 4000 transactions in each block
- Each block is produced every 10 mins
- Bitcoin’s bandwidth is limited to 7 tx / s

Why is the Bitcoin block small?

- We want miners and non-miners alike to be able to run **full nodes**
- Full nodes validate every transaction
- That way I can check the application layer history
- If I’m receiving some money, I know it was produced according to Bitcoin’s macroeconomics
- Even if dishonest majority appears, the **history of execution** is correct
- Some parties have limited bandwidth (< 1 MB / 10 mins), e.g. China
- Some parties have limited CPU for tx sig validation
- For safety, we want a part of the network (~90%) to keep up with blocks

Should the Bitcoin block size be increased?

- Probably yes. Transaction bandwidth limits are significant bottleneck!
- Transaction fees **very high** when blocks are full (Dec 2017): 40$ / tx
- We can have full nodes for 90% with > 4MB blocks
- But probably not much bigger…
- The bandwidth problem remains even if blocks are somewhat bigger
- We need Layer 2 solutions
    - This is beyond the scope this course
    - Read about “Lightning Network” if interested

The Bitcoin Civil War

- In 2017, Bitcoin was hard forked into Bitcoin (BTC) and Bitcoin Cash (BCH)
- Bitcoin Cash supports blocks up to 8MB
- Bitcoin still has the block size limit at 1MB
    - Bitcoin miners cannot accept Bitcoin cash blocks, as Bitcoin validation mandates < 1MB

Ethereum Classic

- TheDAO was a Decentralized Autonomous Organization on Ethereum
- Decentralized Autonomous Organization are organizations which are governed pseudonymously by pks using Smart Contracts
- TheDAO was a venture capital fund
- In June 2016, it was hacked using a *re-entrancy* bug (More on that next week!)
- $50M were stolen
- Ethereum was hard forked to recover the funds
- Some people decided not to fork -- creating Ethereum Classic

Bitcoin history

1983: David Chaum, “e-cash”: Centrally controlled electronic money

1998: Wei Dai, “bmoney”: First decentralized ideas

2005: Nick Szabo, “bit gold”: First idea to use PoW for money

2008: Satoshi Nakamoto, “Bitcoin: A peer-to-peer electronic cash system”

2009: Bitcoin software published

Who is Satoshi Nakamoto?

- Bitcoin’s anonymous author
- Team or individual?
- Wrote the bitcoin **paper**
- Made the first bitcoin **implementation**
- Participated in **IRC discussions** about bitcoin
- Wrote in **bitcointalk forum**
- Led bitcoin to be what it is today
- Claimed he was Japanese
    - ...never wrote a word of Japanese
- Suddenly disappeared in Dec 2010

Who could Satoshi be?

- Nick Szabo? Wei Dai?
- Dr Vili Lehdonvirta & Michael Clear?
- Neal King, Vladimir Oksman & Charles Bry?
- Shinichi Mochizuki, Jed McCaleb?
- Dread Pirate Roberts who ran the Silk Road drug store?
- Dorian Nakamoto?
- Craig Steven Wright?


LEAVE SATOSHI
ALONE!

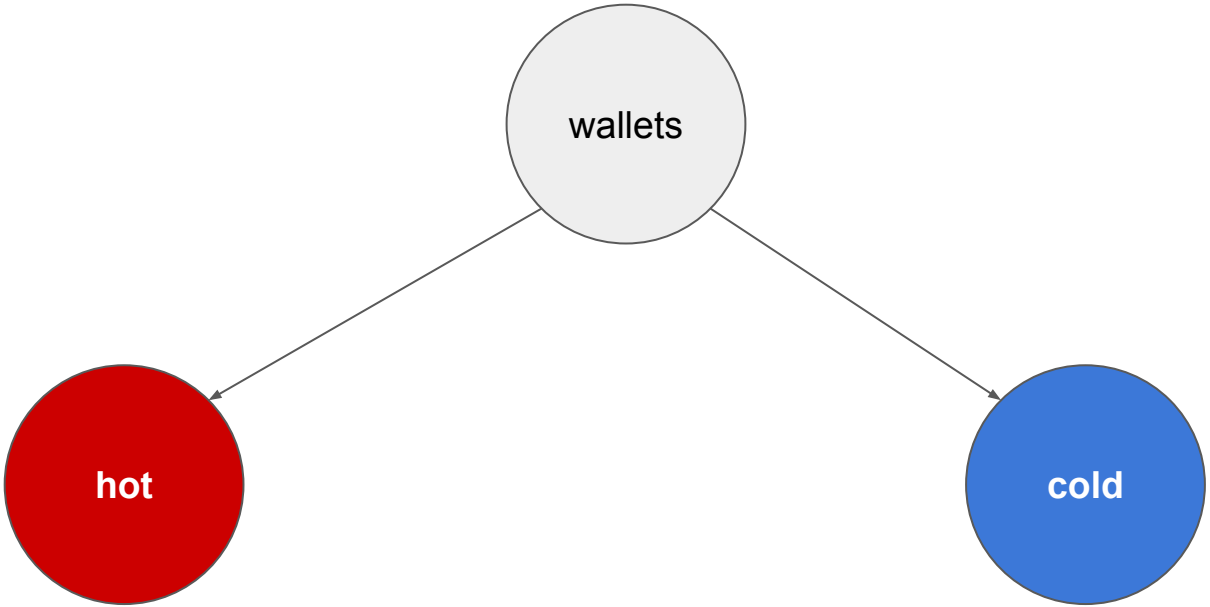
Wallet seeds and HD wallets

- An infinite sequence of wallet private keys can be generated from a single “master private key” (BIP 0032) -- an **HD wallet**
- A private key can be encoded in the form of a human-readable *seed*
- This seed is sufficient to recover *all* the private keys of a wallet
- Typically backed up on paper and optionally encrypted with password

Example:

```
deal smooth awful edit virtual monitor term sign start home shrimp
wrestle
```

Wallet classification



Hot and cold wallets

- I can have my keys on an Internet-connected computer
  - “**Hot** wallet”
  - Easy to use
  - I can always spend my money immediately
- I can keep my private keys offline
  - “**Cold** wallet”
  - Kept on a computer not connected to the Internet or a hard drive
  - My keys cannot easily be stolen
  - I can move my keys to a hot wallet when I need to spend it
  - I can see how much money I have using my public keys which can be kept safely online!

Other ways to store cold wallets

Paper wallet

- Private key is printed on a piece of paper
- Can be kept in a physical safe or a real bank vault
- Can optionally be encrypted with a secret password (which is remembered)

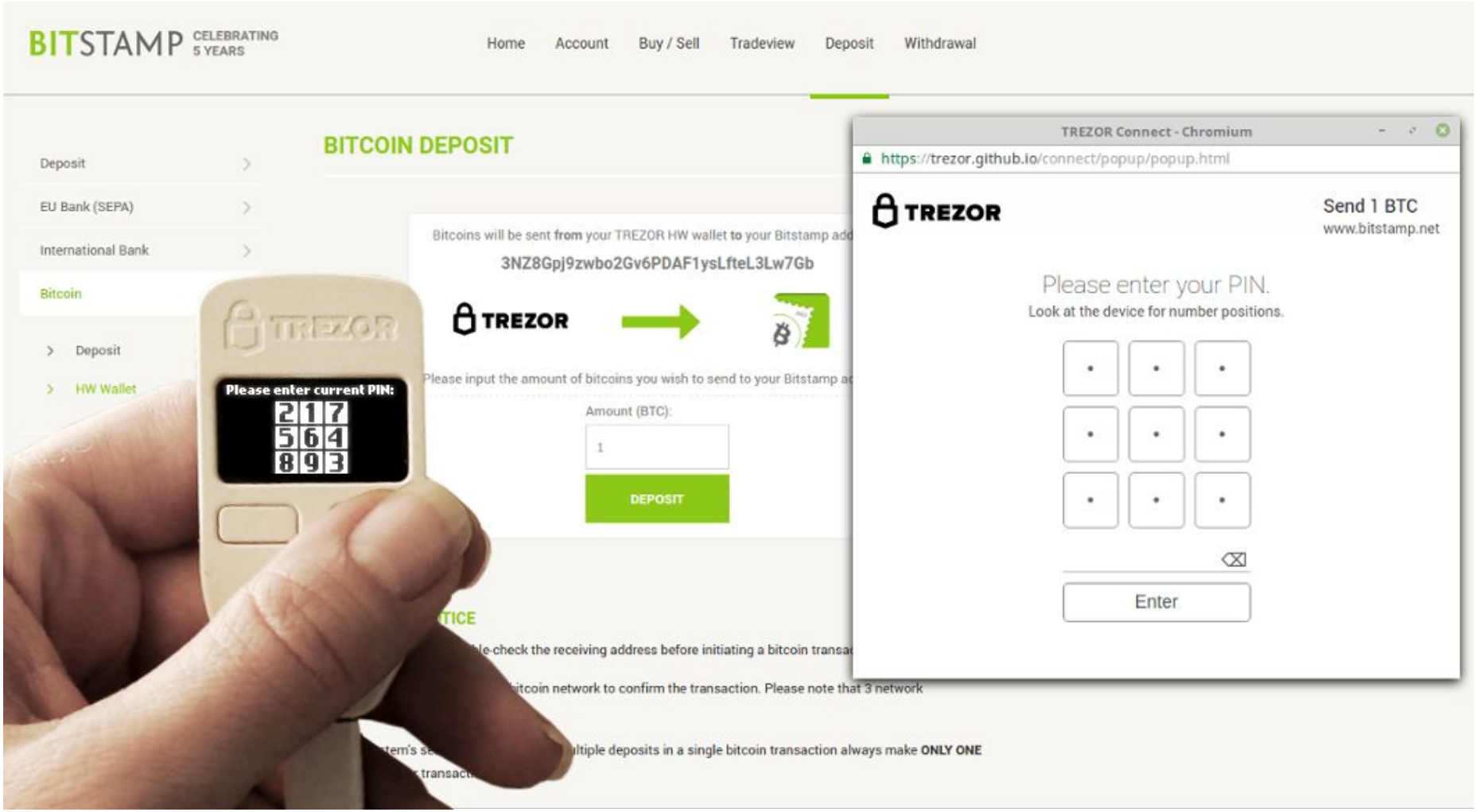
Brain wallet

- Private key is literally SHA256(“my dog’s name is Barbie”)
  or some other passphrase
- Full private key can be recovered by memory
- Extremely unsafe! (More than $100,000 stolen due to low entropy passwords)

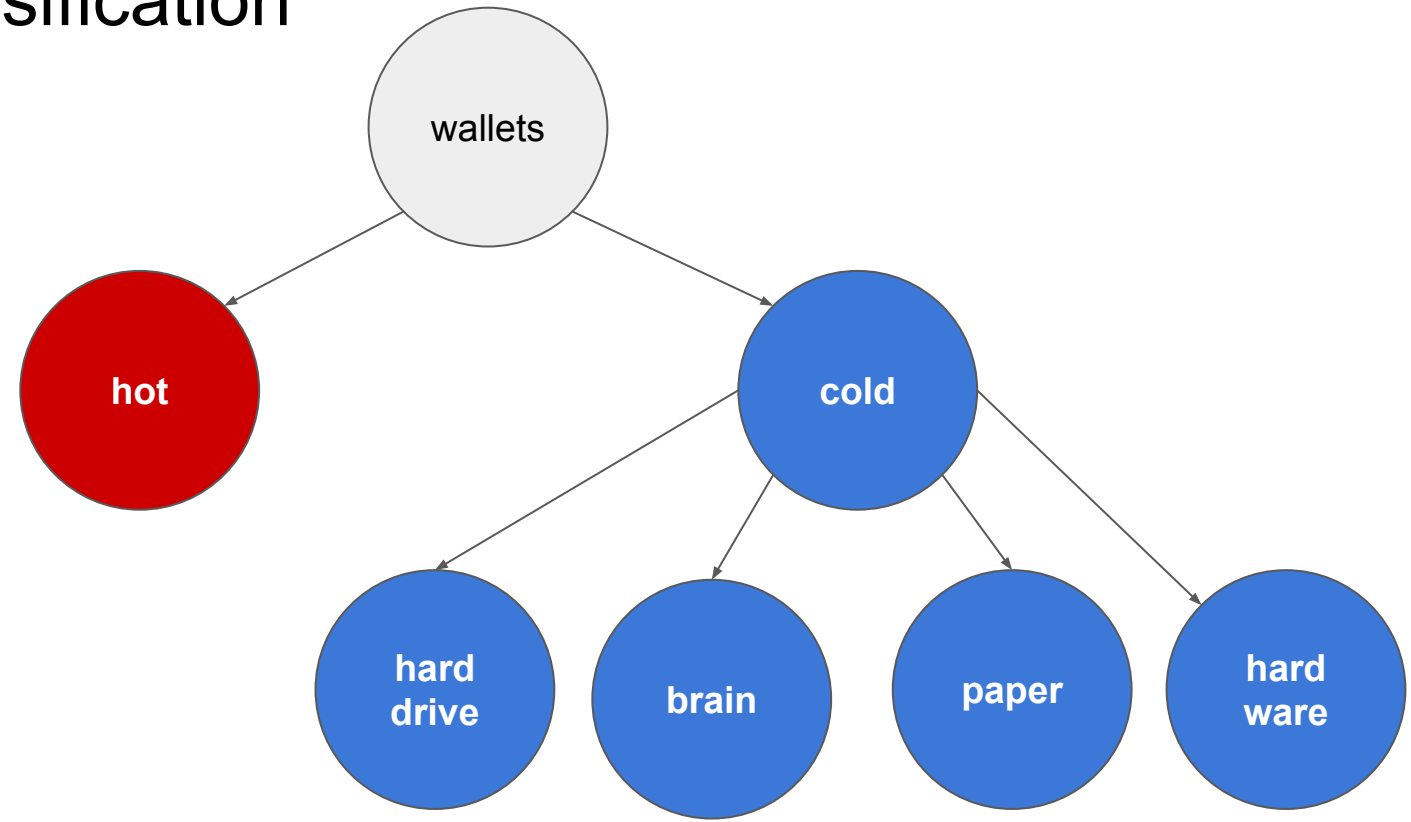
Hardware wallet

- Special hardware device used to store private keys
- Cold wallet
- Most popular ones: **Trezor** and **Ledger**
- Connects to a computer via USB
- Keys never leave the device
- Device produces signed transaction, sends transaction to computer
- Addresses you sent to are verified by looking at the screen
- As hardware/software is specialized, much harder to “hack” or have bugs
- Works safely even if host computer is compromised
- Protected by a pin in case of theft
- Can be backed up into paper and/or other hardware wallets


TREZOR
Confirm sending
0.0469 BTC
to
1Nuu2753n7h3ZnCQJ
CT2HVKTFfQjhpXhcw
Confirm
Cancel


BITSTAMP CELEBRATING 5 YEARS
Home
Account
Buy / Sell
Tradeview
Deposit
Withdrawal
BITCOIN DEPOSIT
Deposit
EU Bank (SEPA)
International Bank
Bitcoin
Deposit
HW Wallet
Bitcoins will be sent from your TREZOR HW wallet to your Bitstamp add
3NZ8Gpj9zwbo2Gv6PDAF1ysLfteL3Lw7Gb
TREZOR
Please input the amount of bitcoins you wish to send to your Bitstamp a
Amount (BTC):
1
DEPOSIT
TICE
le-check the receiving address before initiating a bitcoin transa
itcoin network to confirm the transaction. Please note that 3 network
ltiple deposits in a single bitcoin transaction always make ONLY ONE
TREZOR
Please enter current PIN:
2 1 7
5 6 4
8 9 3
TREZOR Connect - Chromium
https://trezor.github.io/connect/popup/popup.html
TREZOR
Send 1 BTC
www.bitstamp.net
Please enter your PIN.
Look at the device for number positions.
Enter

Wallet classification



Hardware wallet demo

Thank you!