PV204 Security technologies

Bitcoin II.

Petr Švenda *svenda@fi.muni.cz* *@rngsec*
Centre for Research on Cryptography and Security, Masaryk University

Please provide any corrections and comments here (thank you!):
https://drive.google.com/file/d/15z8k8zltcBaxEcF18DGwdoTtUNQFd-9c/view?usp=sharing

CROCS
Centre for Research on
Cryptography and Security

Task: Questions to ask

- Write 1-2 questions you want to discuss about Bitcoin
- https://sli.do #pv204_2024
- We will cover it together towards second half of this lecture
  - (and possibly during seminar)

BLOCKS AND MINING

Problem: Who will include next block into blockchain?

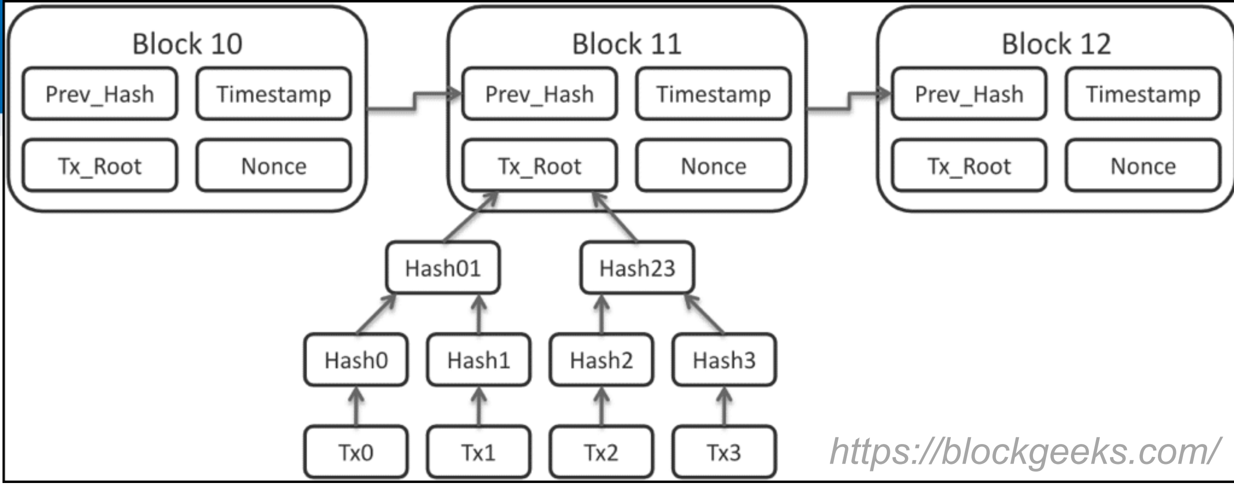
- Transactions (state updates) has to be included somehow into block to be “permanently” valid
- Entity including new block has special position and power
  - Can decide which transactions (state updates) will be included
    - May lead to censorship of certain transactions
    - May lead to transactions reordering impacting the financial value (e.g. MEV)
  - Can decide where new block is appended
    - Shall be last previous block, but can cause malicious forks abandoning part of previously extended blockchain (e.g., 51% attack to rewrite history)
  - Typically receive some reward (motivation for participation)
    - May cause long-term centralized accumulation of underlying token

Who can include next block to blockchain?

We will focus mainly on Proof Of Work used in Bitcoin

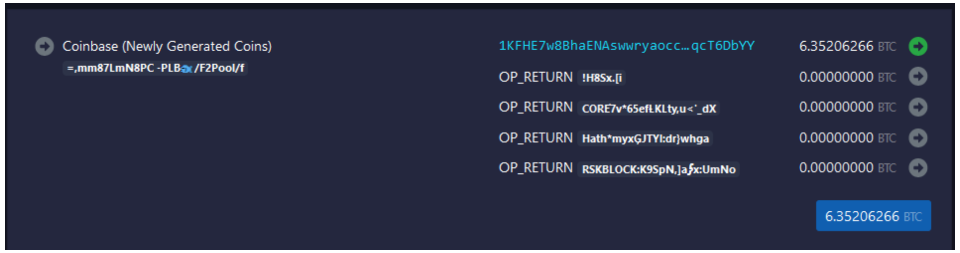
- Proof of Work (PoW, Bitcoin, Ethereum 1.0, Zcash…)
  - Solver of computationally hard puzzle can include new block
- Proof of Stake (PoS, Zcoin, Cardano, BNB, Ethereum 2.0…)
  - More coins you own, higher the probability you will be selected to include next block
  - Various variants, Stake pools…
- Merged Mining (Namecoin…)
  - Hash of block from the chain is included in coinbase tx of other chain (typically Bitcoin)
  - The chain is not performing own mining, Bitcoin miners are getting reward for inclusion of other chains
- Proof of Proof (PoP)
  - Hash of block from other chain is included in Bitcoin transaction (typically OP_RETURN)
  - Security of other chain is improved by security of Bitcoin blockchain
- Proof of Authority (PoA)
  - Small number of trusted actors create new blocks

Bitcoin block



https://blockgeeks.com/

- Header (80 B) + data (up to ~4MB)
  - Version
  - Previous block hash (linking to past blockchain)
  - Merkle root of all included transactions (Coinbase tx + others)
  - Timestamp (unix time)
  - Bits (specification of required mining difficulty)
  - Nonce (variable part for mining, now insufficient)



Coinbase (Newly Generated Coins)
=,mm87LmN8PC -PLB /F2Pool/f

1KFHE7w8BhaENAswwryaocc...qcT6DbYY		6.35206266 BTC
OP_RETURN	!H8Sx.[i	0.00000000 BTC
OP_RETURN	CORE7v*65efŁKLty,u<'_dX	0.00000000 BTC
OP_RETURN	Hath*myxGJTYI:dr}whga	0.00000000 BTC
OP_RETURN	RSKBLOCK:K9SpN,]aʄx:UmNo	0.00000000 BTC

6.35206266 BTC

- Coinbase transaction (reward for miners, emission of new bitcoins)
  - First transaction in every block (only one)
  - Only one input, previous TX ID = 0x0000..00, prev. TX index = 0xffffffff
  - (Typically) equal to block reward + all fees from included transactions

Bitcoin’s Proof of Work (SHA256 function)

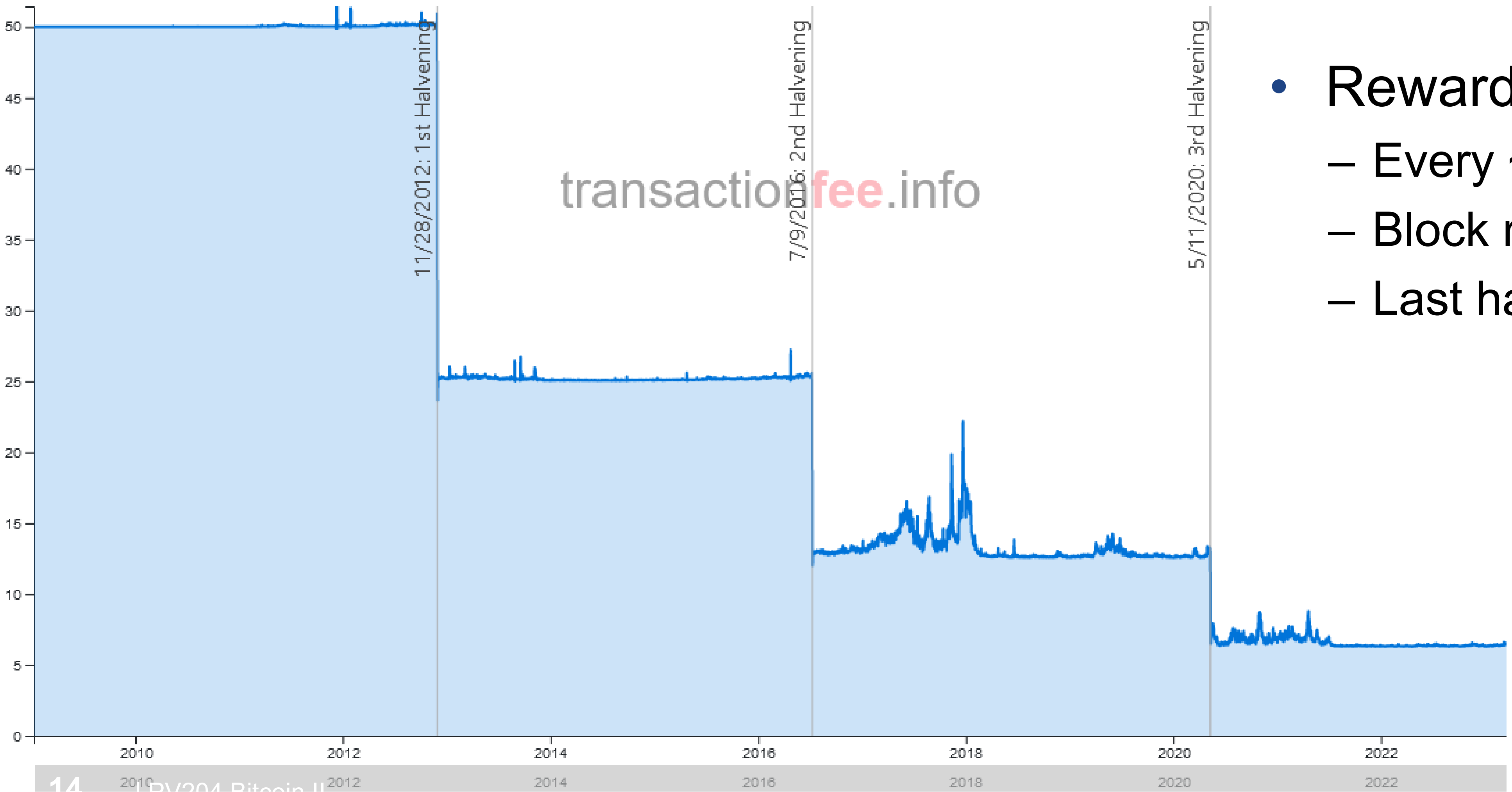
- Crucial for security of blockchain (no rewrite of history)
- Initially on CPU (Satoshi: “Everyone can participate 1 CPU 1 vote”`)
- CPU→GPU →FPGA →ASIC
- Initially solo mining, later collaborative mining (too little chance alone)
- First mining pool: SlushPool in Prague (now Braiins Pool)
  - Miners join their hashrate, fraction of reward based on number of partial solutions
- Cambridge university centre for alternative finance (CBECI)
  - Where are the miners? https://cbeci.org/mining_map/
  - More mining details: https://cbeci.org/cbeci/methodology

https://transactionfee.info/charts/block-coinbase-amount/?start=2009-01-09

DEMO: SHOW EVOLUTION OF REWARDS

Miner reward – coinbase output: block + fees

Shows the average coinbase transaction output amount.



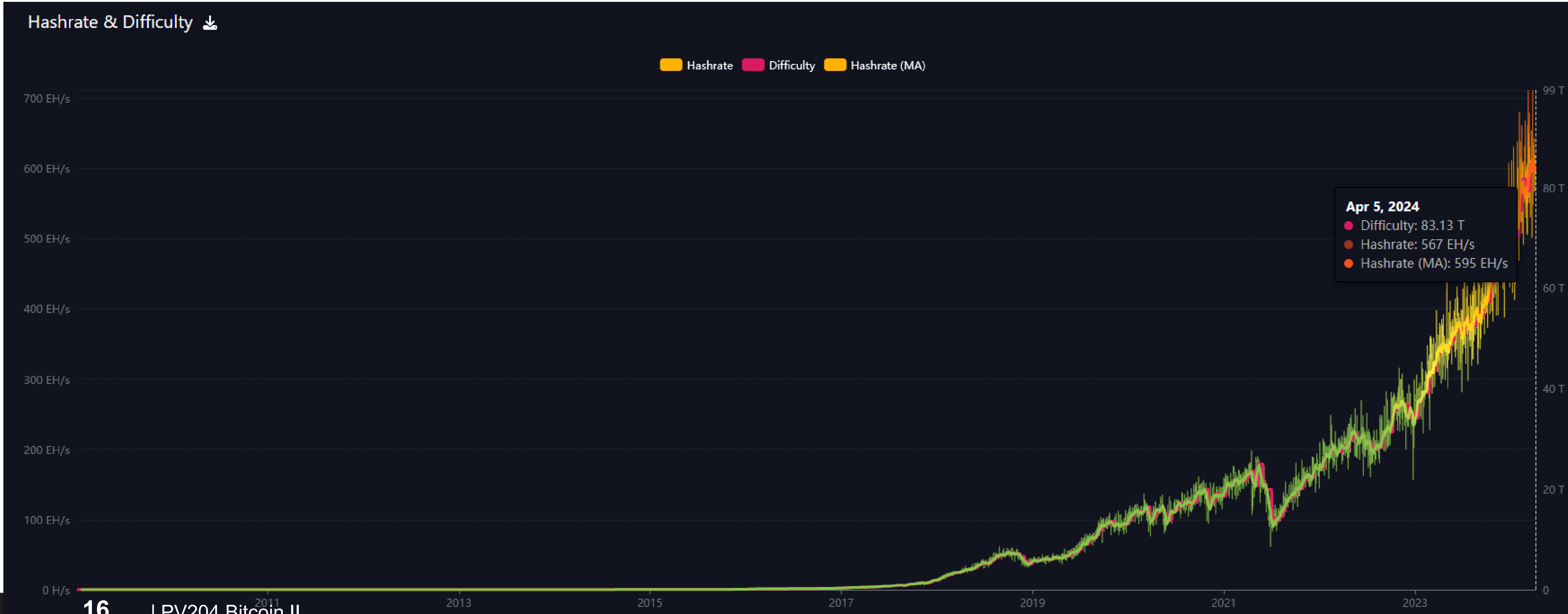
- Reward halving
  - Every ~4 years
  - Block reward drops to ½
  - Last halving in year 2140

Difficulty adjustment

- Bitcoin shall have one block every ten minutes (on average)
- Block must have overall hash with specific number of leading zeroes (March 2024 ~84 binary 0s)
  - Miners change part of block header to try different hashes until required found
- How to specify the number of leading zeroes for decades in future?
  - Speed of new blocks found depends on the overall speed of hashing
  - Overall speed of hashing depends on technology advancements (single chip) and number of chips deployed
  - Impossible to predict technology and interest into distant future
  - If # zeroes is too low => blocks are found too fast (and vice versa)
- Idea of difficulty adjustment (part of consensus protocol), https://en.bitcoin.it/wiki/Difficulty
  - Check number of actually mined blocks every 2016 blocks (shall be ~14 days)
    - Increase/decrease difficulty for next period based on actual number of mined blocks
  - Every full node can deterministically compute expected difficulty (lower # zeroes rejected)
- Block hash must be below the “Target” number (computed to avg keep 1 block / ~10 min)
  - “Target” is transformed to “Bits” (condensed 4 bytes number – coefficient (3B) + exponent (1B))
  - Current difficulty is relative number of current Target with respect to Target of Genesis block

https://mempool.space/graphs/mining/hashrate-difficulty#all

Hashrate in time (>595EH/s = 5.9*10^{20} hash/sec = 2^{66} /sec) 595,000,000,000,000,000,000x SHA256 computations per second



Apr 5, 2024
● Difficulty: 83.13 T
● Hashrate: 567 EH/s
● Hashrate (MA): 595 EH/s

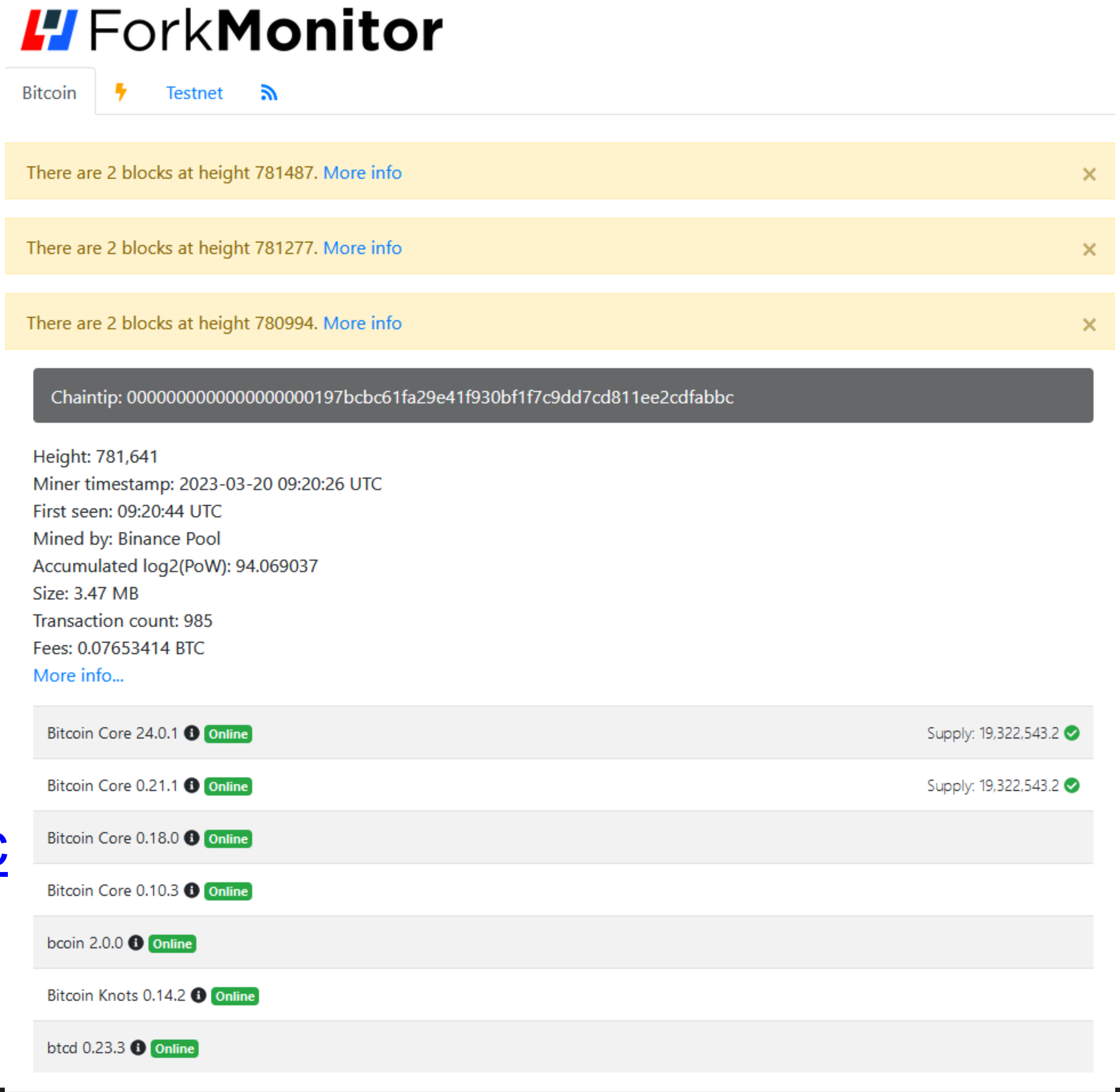
https://mempool.space/

https://mempool.space/graphs/mining/hashrate-difficulty#all

DEMO: SHOW DIFFICULTY ADJUSTMENT, HASHRATE

Blockchain forks

- Occasional natural forks happen
  - (not to be confused with softforks)
- Quickly resolved
  - usually, next block
- Sometimes temporary double-spent can occur
  - Same input used in different txs
- https://forkmonitor.info/nodes/btc



There are 2 blocks at height 781487. More info ×

There are 2 blocks at height 781277. More info ×

There are 2 blocks at height 780994. More info ×

Chaintip: 0000000000000000000197bcbc61fa29e41f930bf1f7c9dd7cd811ee2cdfabbc

Height: 781,641
Miner timestamp: 2023-03-20 09:20:26 UTC
First seen: 09:20:44 UTC
Mined by: Binance Pool
Accumulated log2(PoW): 94.069037
Size: 3.47 MB
Transaction count: 985
Fees: 0.07653414 BTC
More info...

Bitcoin Core 24.0.1 Online	Supply: 19,322,543.2 ✓
Bitcoin Core 0.21.1 Online	Supply: 19,322,543.2 ✓
Bitcoin Core 0.18.0 Online	
Bitcoin Core 0.10.3 Online	
bcoin 2.0.0 Online	
Bitcoin Knots 0.14.2 Online	
btcd 0.23.3 Online	

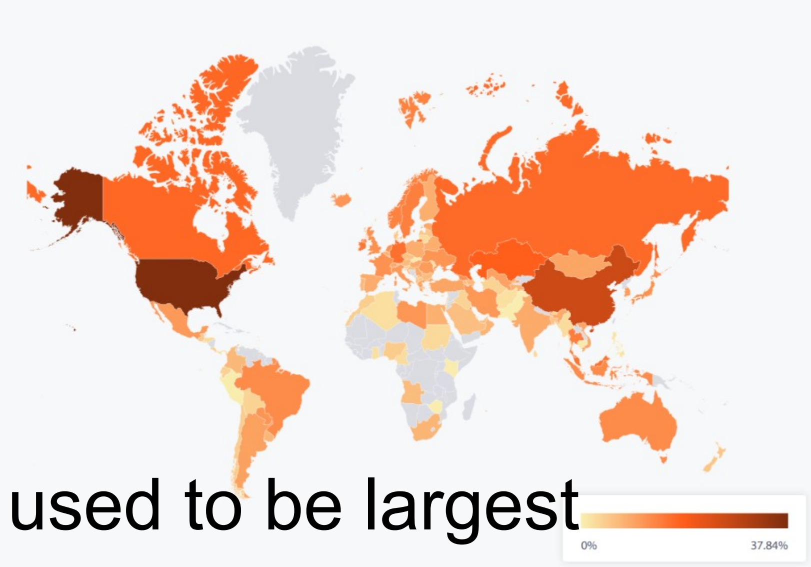
https://forkmonitor.info/nodes/btc

Double spent tx https://forkmonitor.info/stale/btc/782129

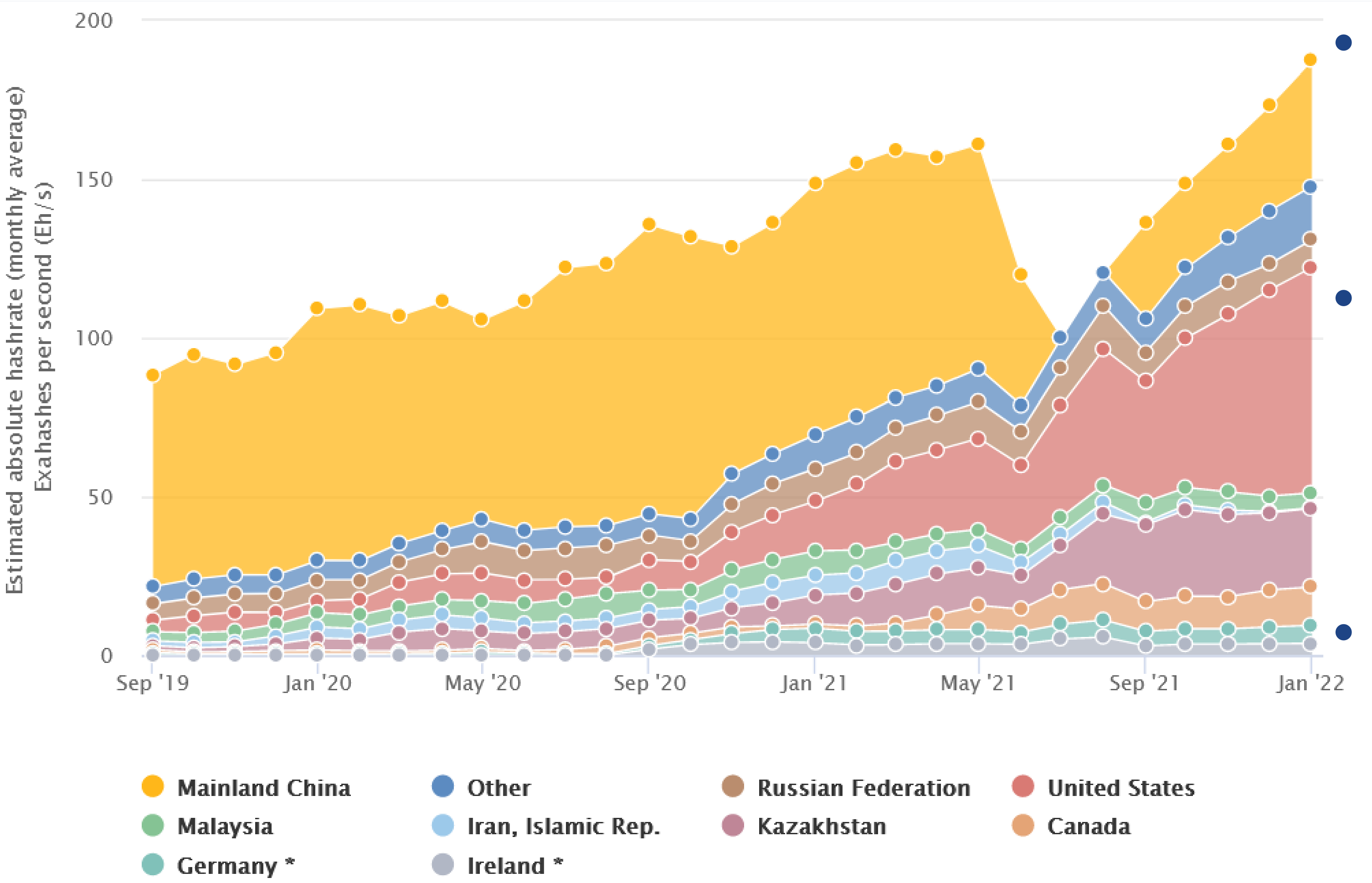
DEMO: SHOW NATURAL FORKS

https://cbeci.org/mining_map/

Bitcoin mining map (January 2022)



Evolution of network hashrate



- China used to be largest
  - >80% (till 2018, slow decrease)
  - Mining ASICS made in China
- China evicted "all" miners in May 2021
  - Officially 0% (unofficially still active
  - Now coming back 21.11%
- Resulted in strong increase in:
  - US 37.84%, Kazakhstan 13.22%
  - Canada 6.48%, other 9% …

Demo – Bitmain Antminer S9 mining

- Efficiency: 80-100 J/TH per second (= 80-100W/TH), from 2017
- Connected to mining pool using Stratum v2 protocol

https://ccaf.io/cbnsi/cbeci/methodology

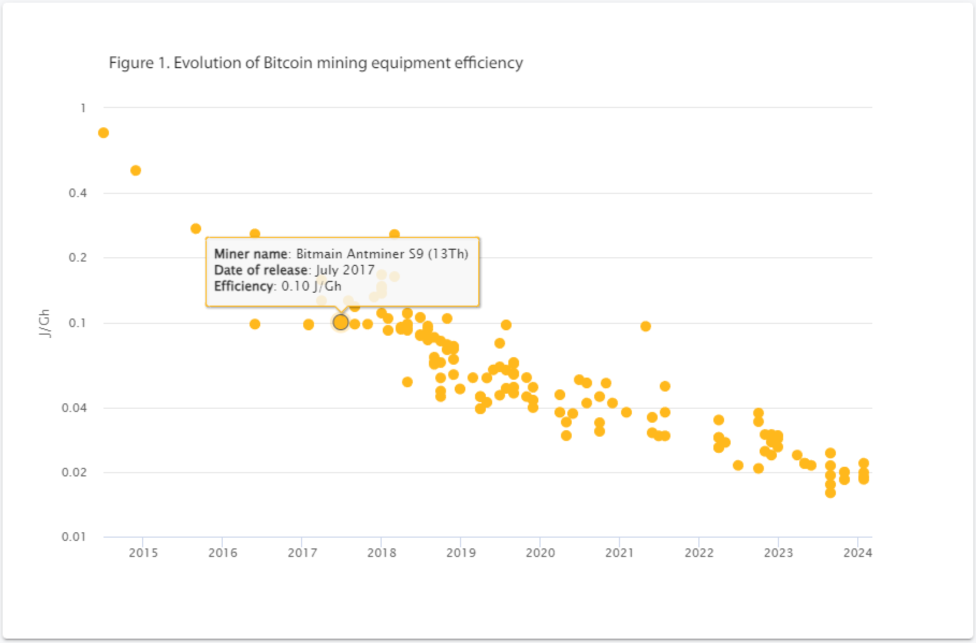
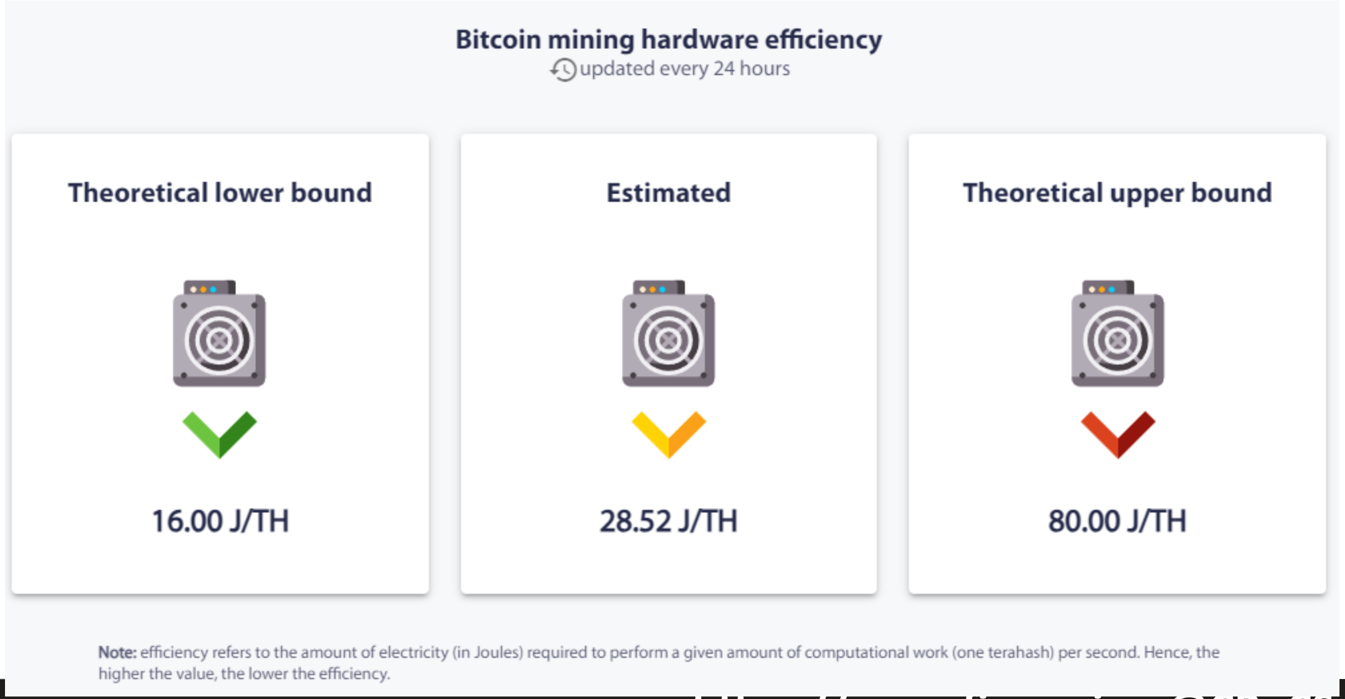


Figure 1. Evolution of Bitcoin mining equipment efficiency



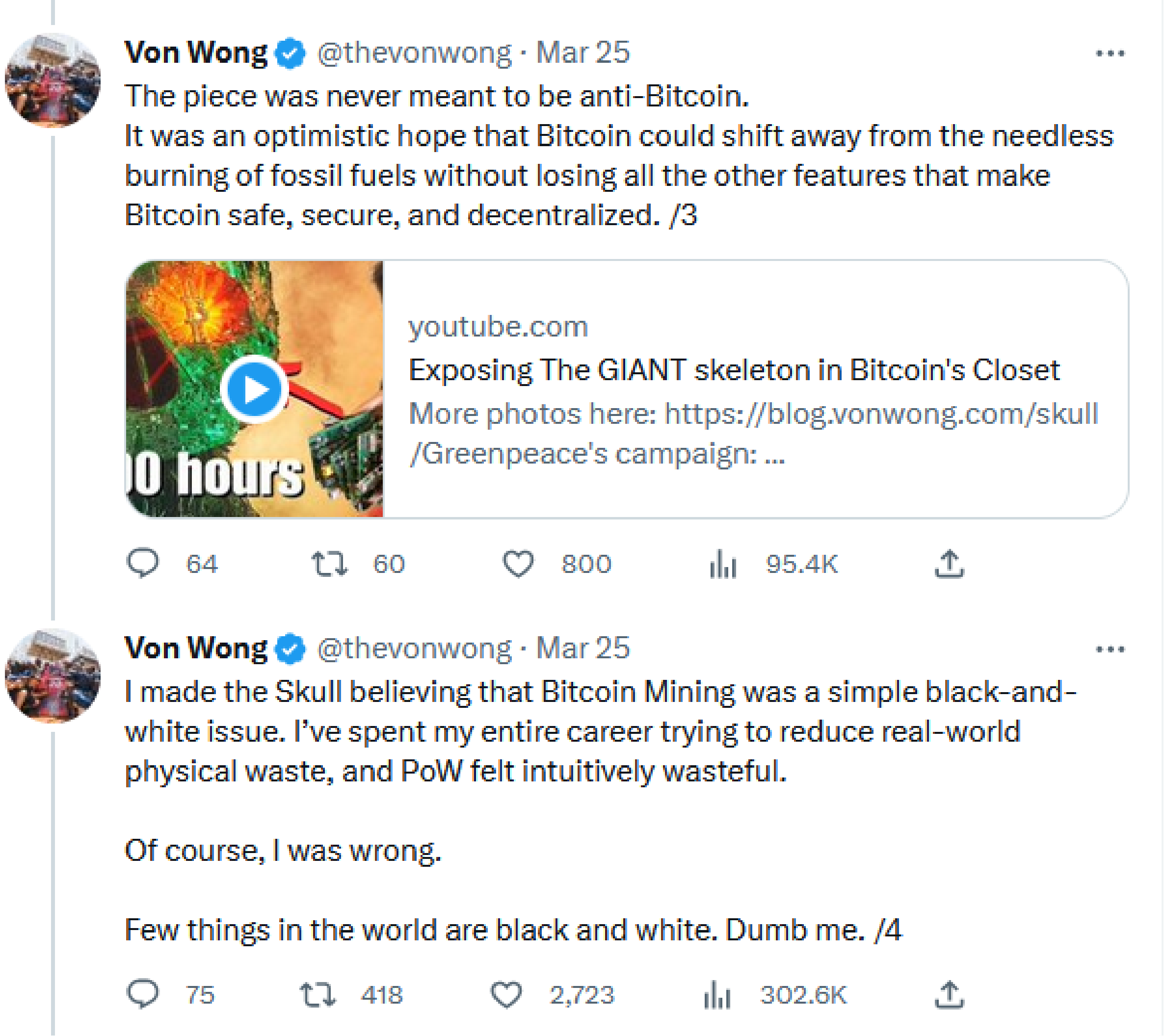
Bitcoin mining hardware efficiency

updated every 24 hours

Theoretical lower bound	Estimated	Theoretical upper bound
16.00 J/TH	28.52 J/TH	80.00 J/TH

Note: efficiency refers to the amount of electricity (in Joules) required to perform a given amount of computational work (one terahash) per second. Hence, the higher the value, the lower the efficiency.

@thevonwong



Von Wong @thevonwong · Mar 25

The piece was never meant to be anti-Bitcoin.
It was an optimistic hope that Bitcoin could shift away from the needless burning of fossil fuels without losing all the other features that make Bitcoin safe, secure, and decentralized. /3

youtube.com
Exposing The GIANT skeleton in Bitcoin's Closet
More photos here: https://blog.vonwong.com/skull /Greenpeace's campaign: ...

Von Wong @thevonwong · Mar 25

I made the Skull believing that Bitcoin Mining was a simple black-and-white issue. I've spent my entire career trying to reduce real-world physical waste, and PoW felt intuitively wasteful.

Of course, I was wrong.

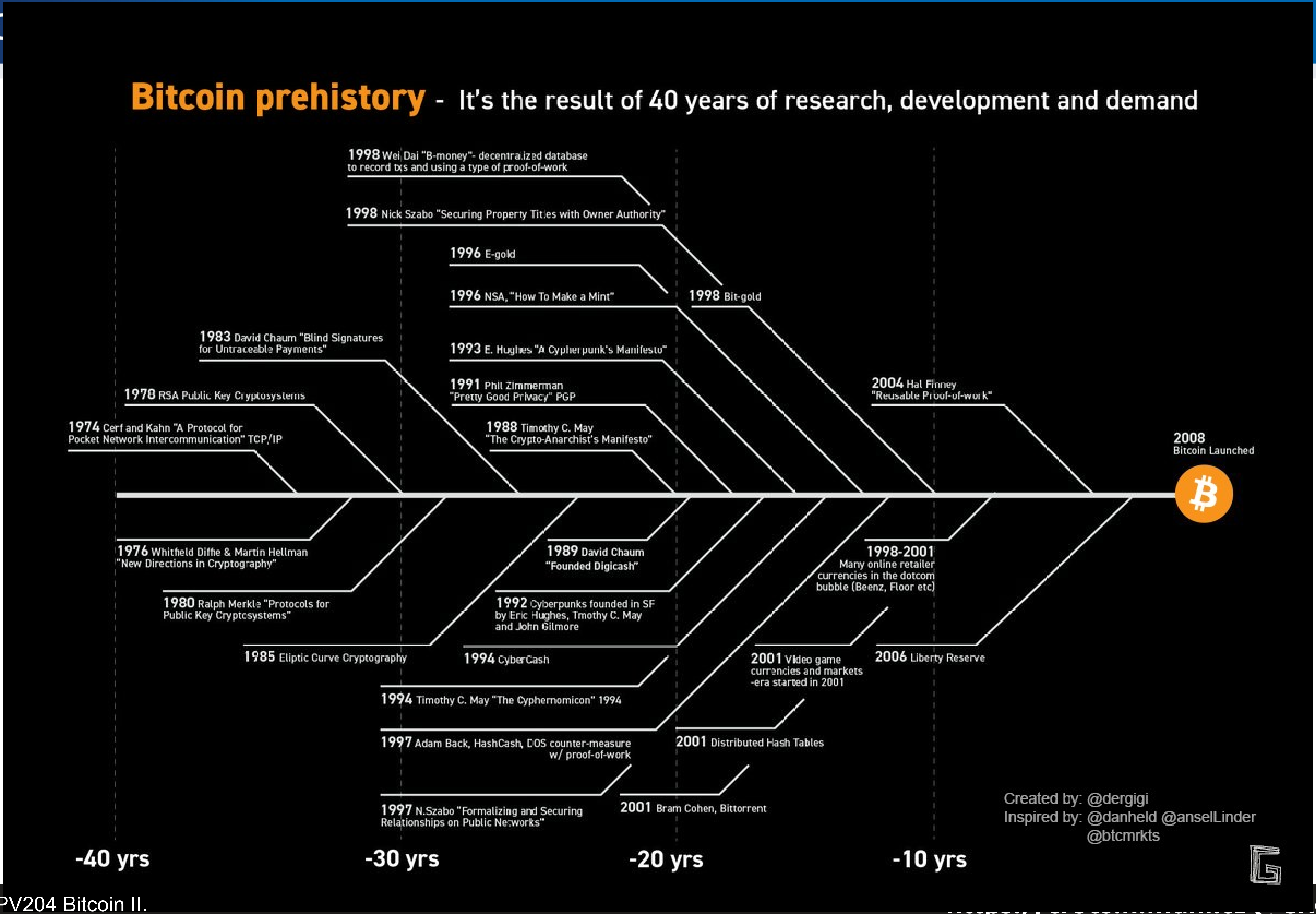
Few things in the world are black and white. Dumb me. /4

https://twitter.com/thevonwong/status/1639690663846375424

Is Bitcoin mining wasteful?

- Heavily discussed topic (“Bitcoin boils the oceans by 2020”)
- Some questions to ask (**Do your own research!**)
  - What value you are getting for the energy expended? (neutral decentralized monetary system)
  - Miners want the cheapest energy available to maximize profits => cheapest energy is energy nobody wants => waste energy
  - What is the source of the energy used? (btc mining ~60% “green” energy due to its low cost)
  - Can mining help to stabilize electrical grid with intermittent (solar, wind) sources? (instant turn on/off of mining ASICs, consumption only when cheap (= not demanded) energy)
  - How long is mining hardware profitable before dismantling? (depends on energy price, 5+ years)
  - Can miners finance construction of energy sources (hydro…) at places otherwise not viable financially (stranded energy)?
  - Can miners incentivize higher portion of intermittent (solar, wind) sources? (bigger source even when low sun/wind?)

UPGRADING BITCOIN FUNCTIONALITY



Bitcoin prehistory - It's the result of 40 years of research, development and demand

1998 Wei Dai "B-money"- decentralized database to record txs and using a type of proof-of-work

1998 Nick Szabo "Securing Property Titles with Owner Authority"

1996 E-gold

1996 NSA, "How To Make a Mint"

1998 Bit-gold

1983 David Chaum "Blind Signatures for Untraceable Payments"

1993 E. Hughes "A Cypherpunk's Manifesto"

1978 RSA Public Key Cryptosystems

1991 Phil Zimmerman "Pretty Good Privacy" PGP

2004 Hal Finney "Reusable Proof-of-work"

1974 Cerf and Kahn "A Protocol for Pocket Network Intercommunication" TCP/IP

1988 Timothy C. May "The Crypto-Anarchist's Manifesto"

2008 Bitcoin Launched

1976 Whitfield Diffie & Martin Hellman "New Directions in Cryptography"

1989 David Chaum "Founded Digicash"

1998-2001 Many online retailer currencies in the dotcom bubble (Beenz, Floor etc)

1980 Ralph Merkle "Protocols for Public Key Cryptosystems"

1992 Cyberpunks founded in SF by Eric Hughes, Tmothy C. May and John Gilmore

1985 Eliptic Curve Cryptography

1994 CyberCash

2001 Video game currencies and markets -era started in 2001

2006 Liberty Reserve

1994 Timothy C. May "The Cyphernomicon" 1994

1997 Adam Back, HashCash, DOS counter-measure w/ proof-of-work

2001 Distributed Hash Tables

1997 N.Szabo "Formalizing and Securing Relationships on Public Networks"

2001 Bram Cohen, Bittorrent

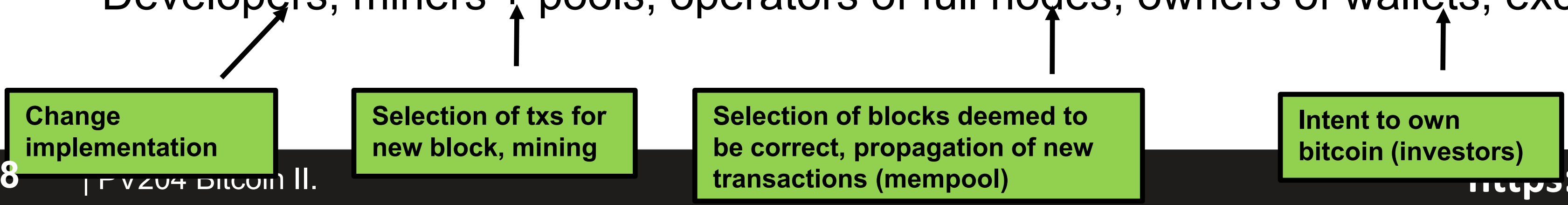
Created by: @dergigi
Inspired by: @danheld @anselLinder @btcmrkts

Options for upgrades

- Upgrading software in centralized environment is relatively easy
- Who sets rules for upgrades of Facebook WhatsApp?
  - Decision by FB management, implementation by FB developers
  - State regulation (e.g., customer protection laws, GDPR…)
  - Pressure of users (e.g., postponed date for EULA acceptation from February to May 2021)
- Who can influence technical consensus rules of Bitcoin?
  - Bitcoin Core full node is open-source (everybody can modify)
  - Softfork – backward compatible (**non-**actualized nodes will accept)
    - Old nodes only cannot use new functionality
  - Hardfork – backward incompatible (**non-**actualized nodes will reject)
    - E.g., change of block reward, block size, mining difficulty (=> average time per block), PoW vs. PoS…
- Bitcoin performs only softforks (to keep valid rules from time when you acquired your “bitcoins”)

How to agree on code changes in Bitcoin Core?

- Changes NOT influencing consensus rules
  - E.g., code optimizations, changes in GUI/CLI…
  - „Common“ development process, pull requests + discussion + thorough review
- Changes influencing consensus rules
  - Discussion of the proposed change idea + example implementation
  - After some time, an attempt to include change into main branch repository
- How to decide if change shall be accepted or rejected?
  - Initially direct changes by Satoshi Nakamoto
  - Later small group of Bitcoin Core developers
  - Later development of various methods for signalization of readiness for acceptance or rejection
- Basic economic actors of Bitcoin ecosystem
  - Developers, miners + pools, operators of full nodes, owners of wallets, exchanges…



Change implementation

Selection of txs for new block, mining

Selection of blocks deemed to be correct, propagation of new transactions (mempool)

Intent to own bitcoin (investors)

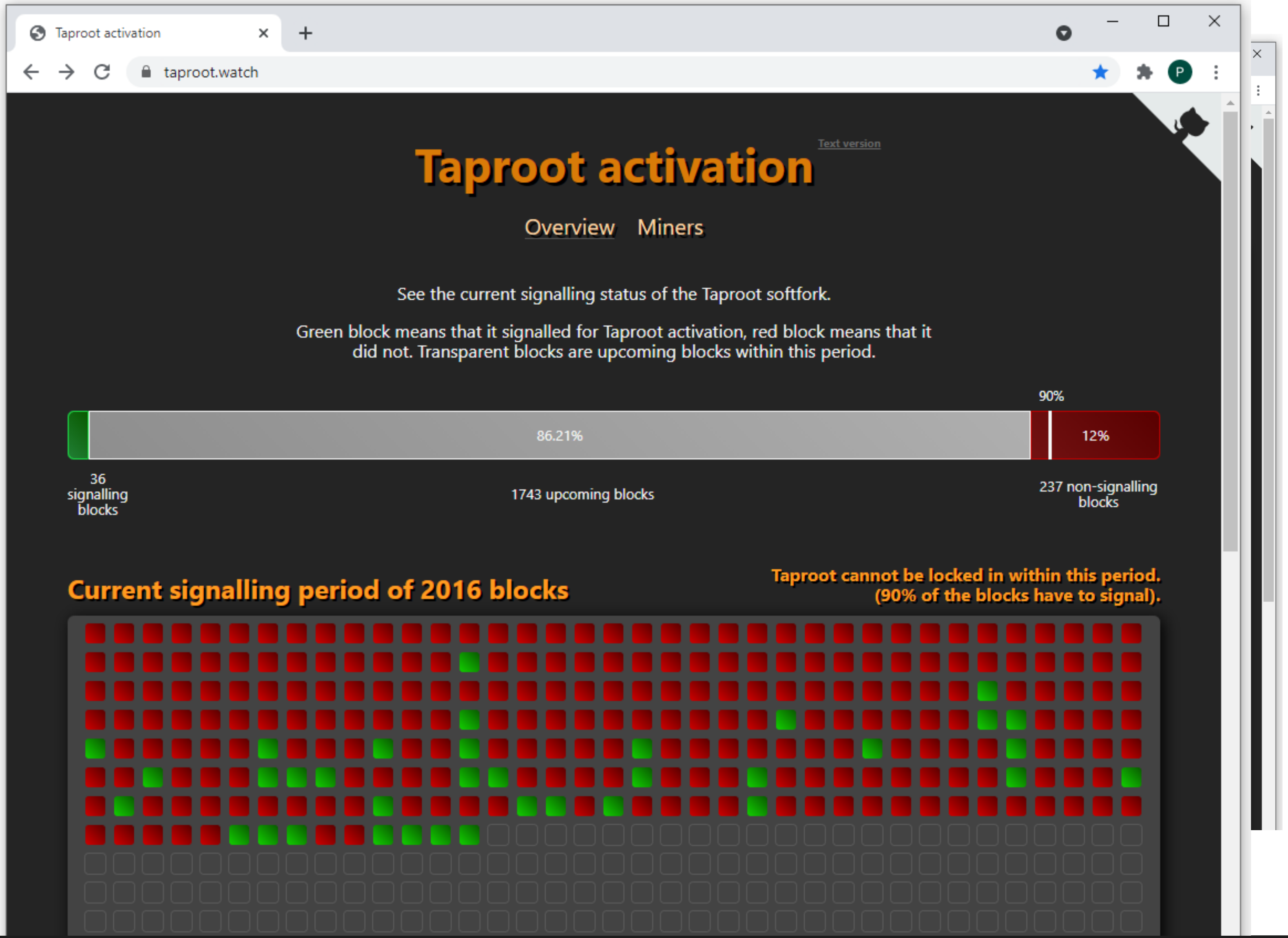
Segregated witness (Segwit), softfork, August 2017

- Backward-compatible upgrade (soft fork) activated in August 2017
- Introduced the following changes:
  - Block size increase (up to ~4MB, witness data bytes discounted by 1/4)
  - Fixes transaction malleability (signature excluded from transaction ID computation)
  - Support for clear future versioning (special code rule for **`OP_0 <20-byte hash>`**)
- Additional witness data send only to node which requests it
  - Backward compatible, older nodes will not ask
  - Segwit transaction looks to them as “anyone-can-spend” script
- Significant controversy called “Blocksize wars” (several hardforks)
  - “Big blockers” wanted larger blocks or dynamic blocks to keep transaction fee low “forever”
    - But larger blocks increase blockchain size => less people able to run fullnode => centralization
  - New York Agreement, User Activate Soft Fork (UASF)
  - Demonstrates problems of decentralized social consensus (Schelling point)

Taproot, softfork, October 2021

- Backward-compatible upgrade (soft fork) activated in October 2021
- Introduced the following changes:
  - Added support for Schnorr signatures (more compact, easier MPC…)
  - Increased privacy (Schnorr-based multiparty signature, Musig2, FROST…)
  - More powerful “Tapscript” added
- Not controversial, generally believed to be wanted improvement
  - “Speedy trial” used

https://taproot.watch/



Taproot activation

See the current signalling status of the Taproot softfork.

Green block means that it signalled for Taproot activation, red block means that it did not. Transparent blocks are upcoming blocks within this period.

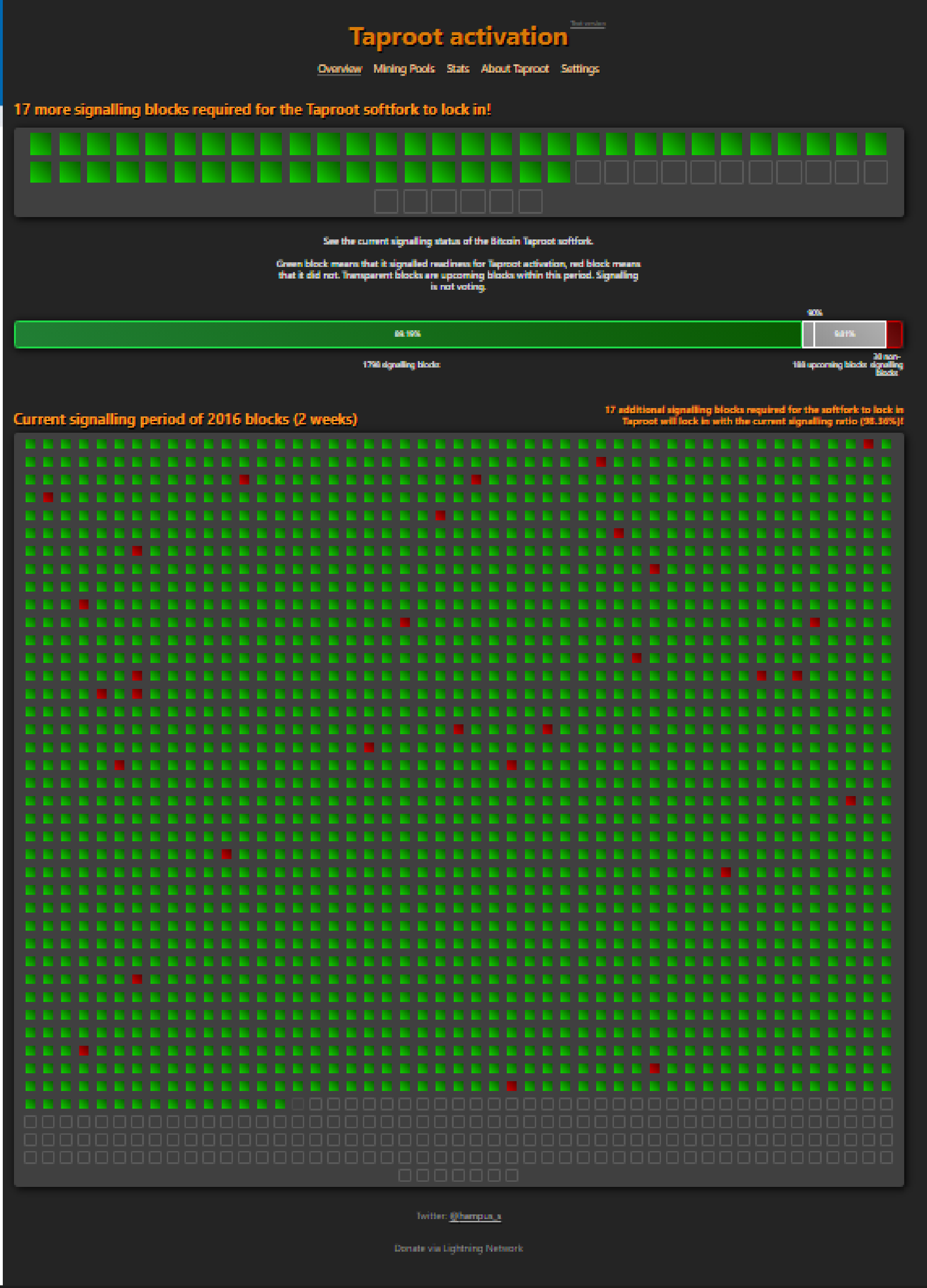
36 signalling blocks

1743 upcoming blocks

237 non-signalling blocks

Current signalling period of 2016 blocks

Taproot cannot be locked in within this period. (90% of the blocks have to signal).



Taproot activation

17 more signalling blocks required for the Taproot softfork to lock in!

See the current signalling status of the Bitcoin Taproot softfork.

Green block means that it signalled readiness for Taproot activation, red block means that it did not. Transparent blocks are upcoming blocks within this period. Signalling is not voting.

1798 signalling blocks

188 upcoming blocks

30 non-signalling blocks

Current signalling period of 2016 blocks (2 weeks)

17 additional signalling blocks required for the softfork to lock in
Taproot will lock in with the current signalling ratio (98.36%)!

twitter: @hampus_s

Donate via Lightning Network

Future Bitcoin upgrades

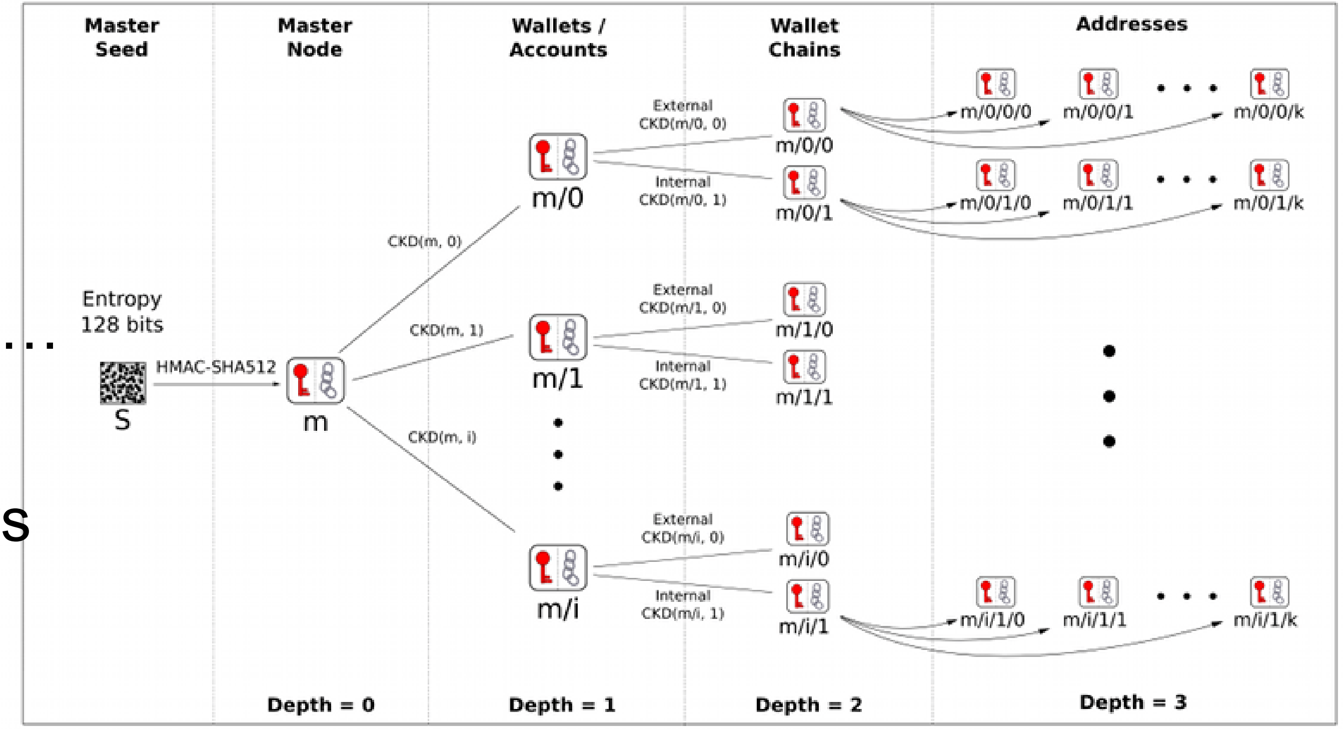
- Protocols tend to ossify with adoption (e.g., TCP protocol)
  - Difficult to update software at once, increased probability of problems after change
- Many discussed future changes (some already tested on Signet)
  - OP_VAULT (convenance)
  - SIGHASH_ANYPREVOUT (Eltoo, channel factories)
  - Cross-input signature aggregation (one signature for multiple inputs)
  - Drivechains, spacechains…
  - (Time representation in block will overflow in 2106)
- Potential hardforks?
  - (Quantum computer breaking ECDSA)

THRESHOLD SIGNATURES VS. MULTISIG VS. MULTI-PARTY COMPUTATION

Making fresh private keys (with backup) BIP32, BIP44…

- Deterministic derivation from:
  - – master seed (key)
  - – derivation path (data)
    - m/purpose/coin/account/receive…
- Single master seed allows:
  - – Generate many distinct private keys
  - – Sharing sub-tree value allows:
    - Generate keys in sub-trees
    - Cannot generate keys from other trees
- Deterministic generation, Master Seed enough to recover whole tree

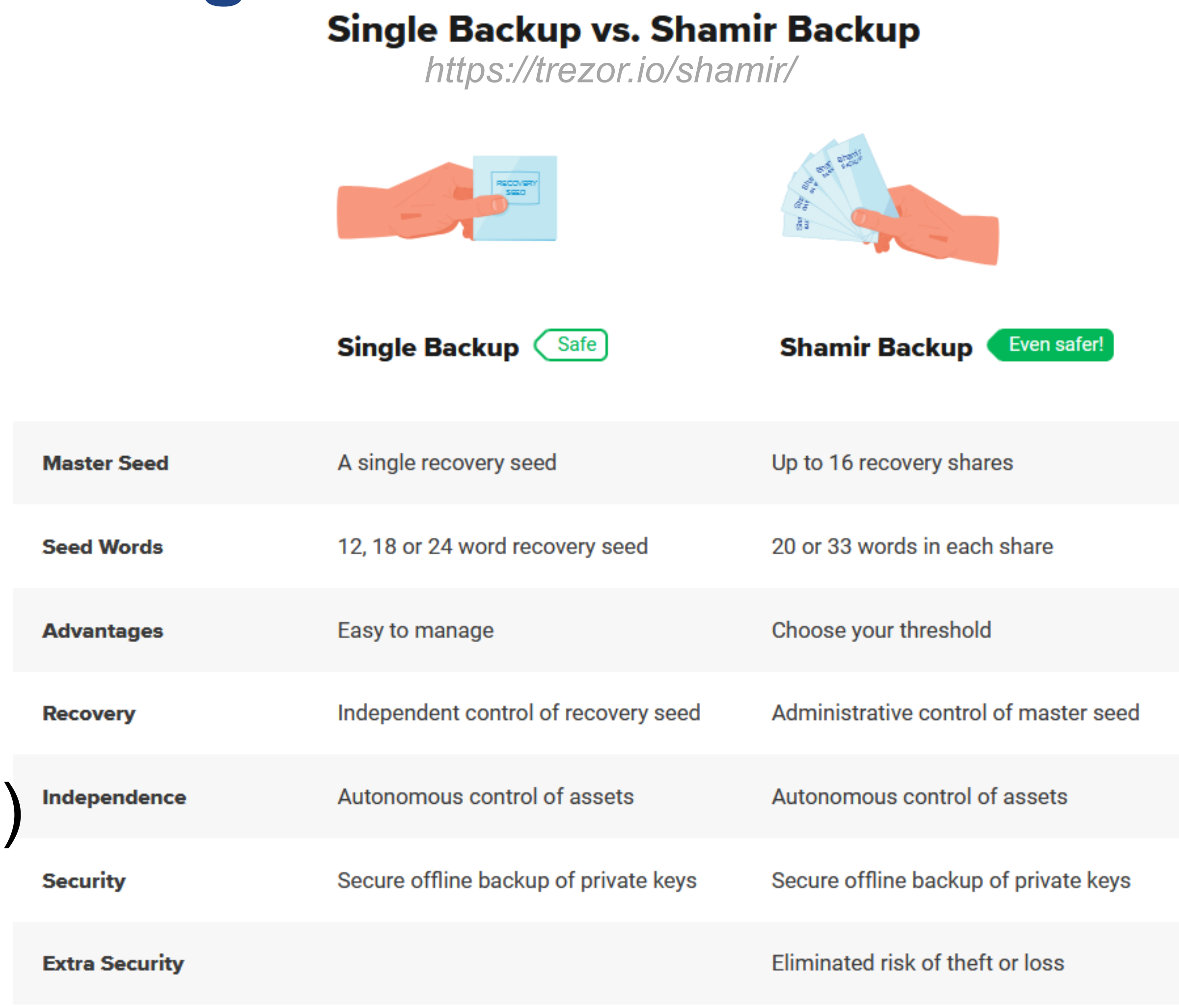
BIP 32 - Hierarchical Deterministic Wallets



Child Key Derivation Function ~ CKD(x,n) = HMAC-SHA512(x_{Chain}, x_{PubKey} || n)

1. Shamir’s threshold secret sharing scheme

- Private key is recovered from multiple shares
  - Then used at single place
  - An attacker can compromise private key after its recovery from shares
- Network is unaware of key split, single public key used in lock script
- Can be used to backup wallet seed (e.g., Trezor wallet https://trezor.io/shamir/)
  - n-out-of-n or k-out-of-n



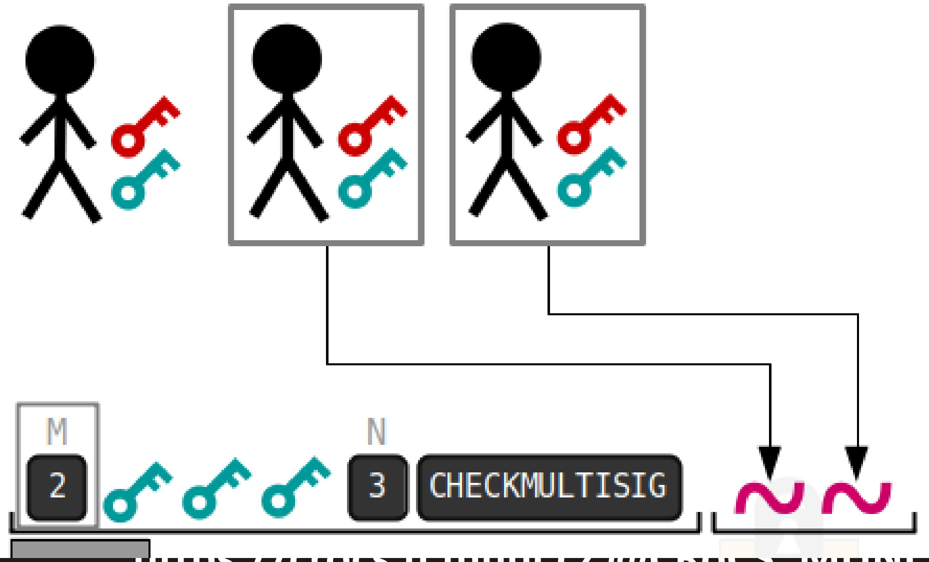
Single Backup vs. Shamir Backup

https://trezor.io/shamir/

	Single Backup Safe	Shamir Backup Even safer!
Master Seed	A single recovery seed	Up to 16 recovery shares
Seed Words	12, 18 or 24 word recovery seed	20 or 33 words in each share
Advantages	Easy to manage	Choose your threshold
Recovery	Independent control of recovery seed	Administrative control of master seed
Independence	Autonomous control of assets	Autonomous control of assets
Security	Secure offline backup of private keys	Secure offline backup of private keys
Extra Security		Eliminated risk of theft or loss

Multisignatures

- Lock script constructed to require multiple signatures (OP_CHECKMULTISIG)
  - transaction valid only if multiple signers provide signatures for unlock script
- n-out-of-n or k-out-of-n, https://en.bitcoin.it/wiki/Multisignature
- P2MS, P2MS wrapped in P2SH
  - https://learnmeabitcoin.com/technical/p2ms

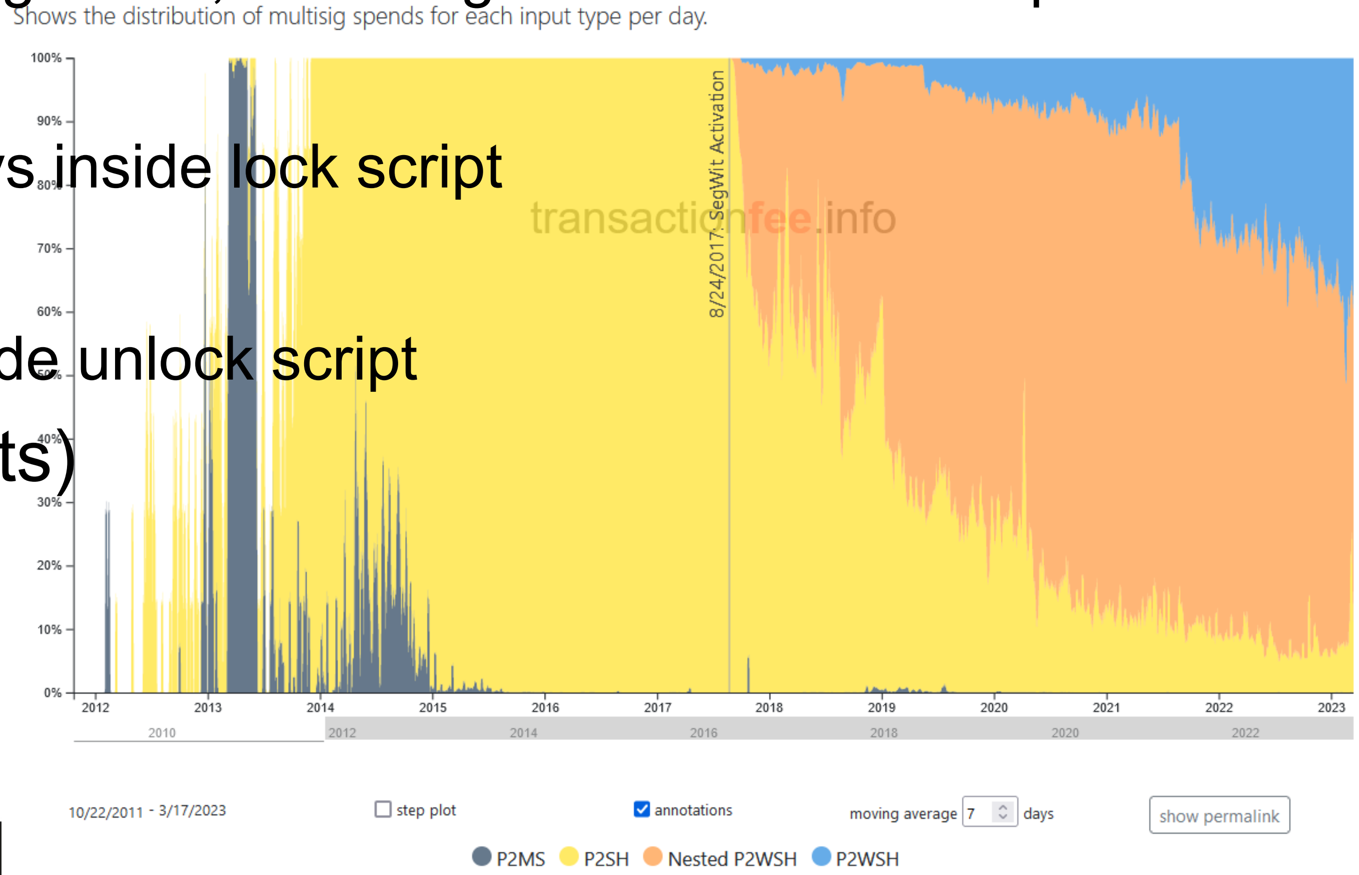


Secure multi-party computation (MPC)

- Single signature computed using multiple separated signers
  - Each signer has own private key
  - An attacker must comprise more than one entity
- Communication between signers
  - During initial key generation
  - Optionally during signing
- Legacy compatible schemes (produces valid ECDSA signature)
  - 2-party ECDSA, n-out-of-n or k-out-of-n ECDSA (only since 2016)
- Taproot-compatible schemes (activated since Nov 2021)
  - Schorr signatures, MuSig2 (BIP 327), FROST…
- https://academy.binance.com/en/articles/threshold-signatures-explained

Frequency of different multisignature scripts

- Cannot tell for Shamir, MPC ECDSA and Schnorr (e.g., MuSig)!
  - Resulting signature is standard signature, no change to lock/unlock scripts
- Can tell for P2MS
  - Threshold and allowed public keys inside lock script
- Can tell for P2SH (if spent)
  - Multisig script and used keys inside unlock script
- (analogically for Segwit variants)



Shows the distribution of multisig spends for each input type per day.

10/22/2011 - 3/17/2023

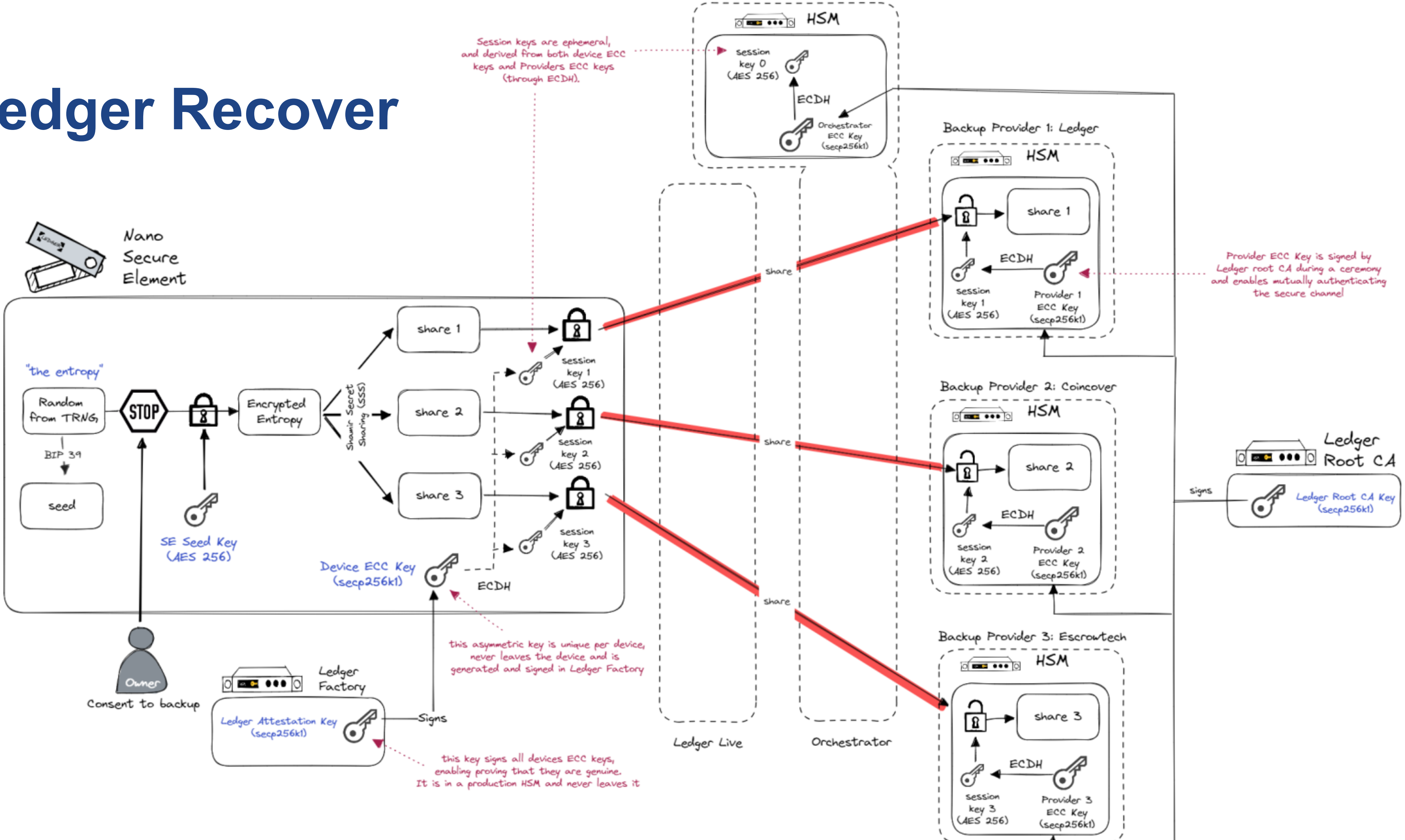
☐ step plot

☑ annotations

moving average 7 days

show permalink

Ledger Recover



Session keys are ephemeral, and derived from both device ECC keys and Providers ECC keys (through ECDH).

Provider ECC Key is signed by Ledger root CA during a ceremony and enables mutually authenticating the secure channel

this asymmetric key is unique per device, never leaves the device and is generated and signed in Ledger Factory

this key signs all devices ECC keys, enabling proving that they are genuine. It is in a production HSM and never leaves it

https://www.ledger.com/blog/part-1-genesis-of-ledger-recover-self-custody-without-compromise

BITCOIN PRIVACY

Risks

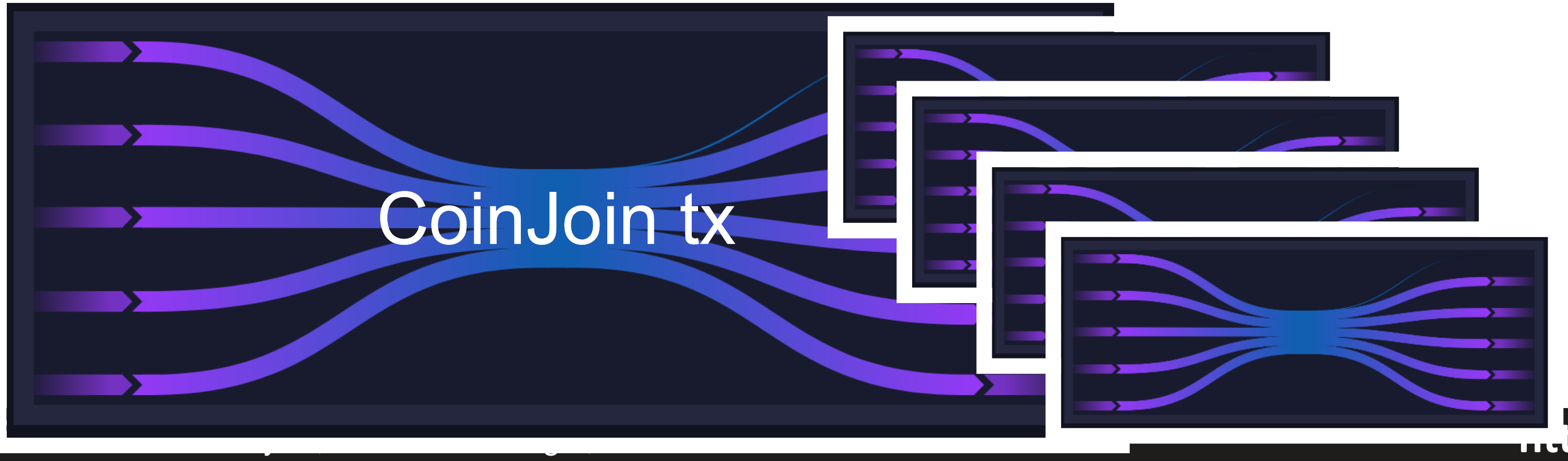
- Risk of lost coins
  - Lost wallet keys, forgotten access credentials
- Risk of stolen coins
  - Malware on computer (wallet keys), phishing/scam (recovery phrase)
  - Compromised trusted third party (exchange, web wallet…)
  - Random burglary (don’t know you have btc)
  - Targeted burglary (know you have btc), with(-out) you present
- Risk of traced coins
  - blockchain analysis, additional metadata correlation analysis (KYC/AML, scans, tx propagation, wallet peeling…)
  - Crooks, governments, wife…

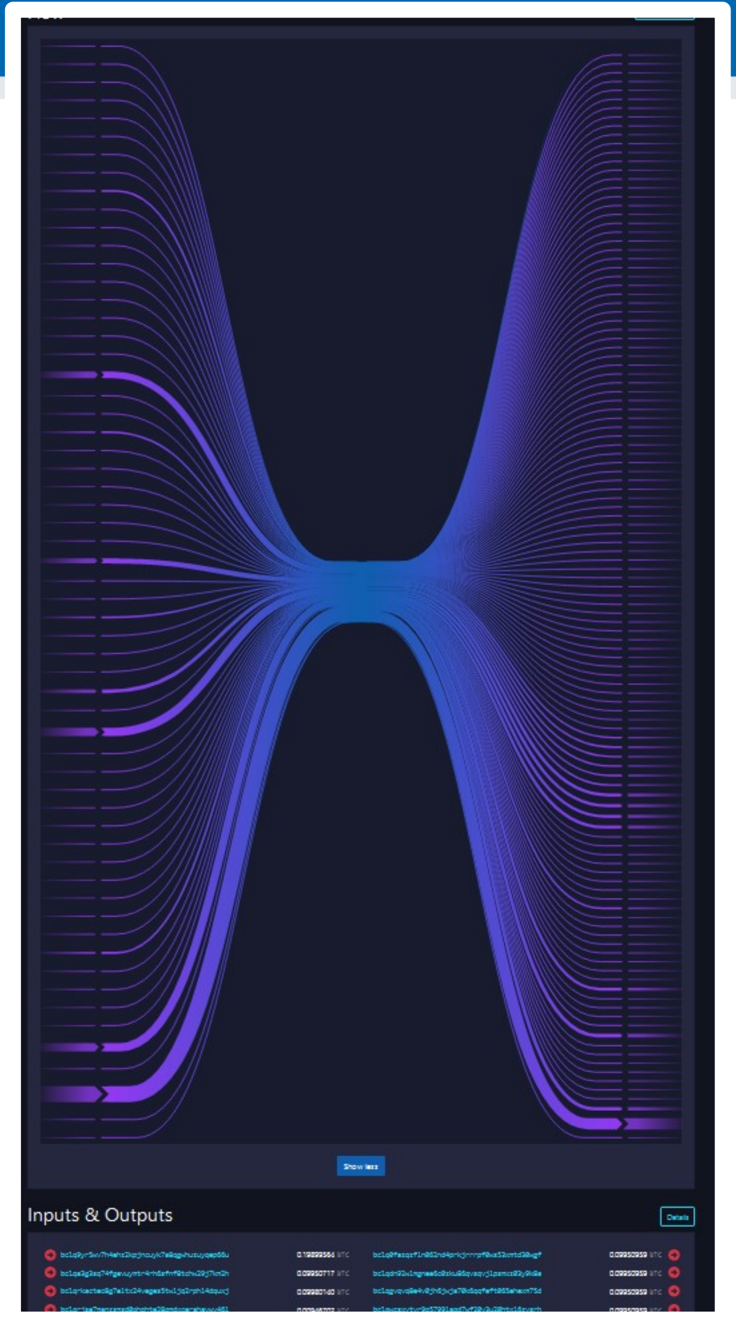
Improving privacy

- Hold your private keys (no custodial service like exchange…)
  - Cannot steal, cannot observe, cannot “vote” on your behalf
- Store private key in hardware wallet (Trezor, ColdCard, Ledger…)
  - Keys in “hot” software wallets are prone to malware attack
- Run own full node over Tor and connect your wallet to it
- Make on-chain analysis harder: https://en.bitcoin.it/wiki/Privacy
- Use manual coin selection, label coins by its origin (in your wallet only)
- Use CoinJoin, PayJoin (multiple users mix their inputs in single transaction)
- Have good opsec (no posting of own btc addresses, use Tor to broadcast tx, delink via CoinJoin after KYC…)

CoinJoin privacy mixing

- CoinJoin tx is created by several participants
  - Obfuscate/break link between input and output coins
  - Different CoinJoin designs and parameterizations
- How good is the resulting anonymity set?
- Untrusted coordinator required
  - Chaumian blind signatures, Tor connections…

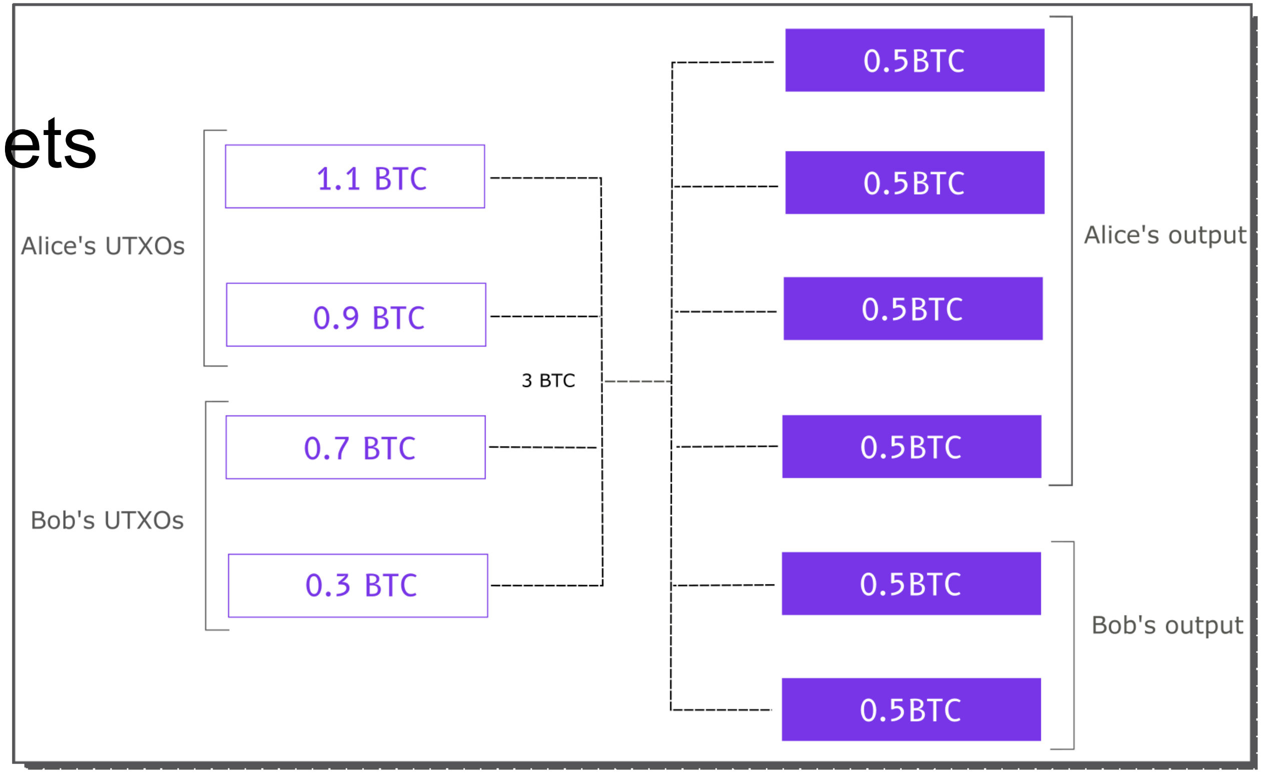




https://en.bitcoinwiki.org/wiki/CoinJoin
https://cryptotesters.com/blog/what-are-coinjoins-and-how-do-they-improve-bitcoin-privacy

CoinJoin

- Multiple users collaborates trustlessly in creating large transaction
- Outputs are all the same value => cannot be attributed to one of senders based on the value
- Supported by more advanced wallets
  - – Wasabi wallet, Samurai wallet

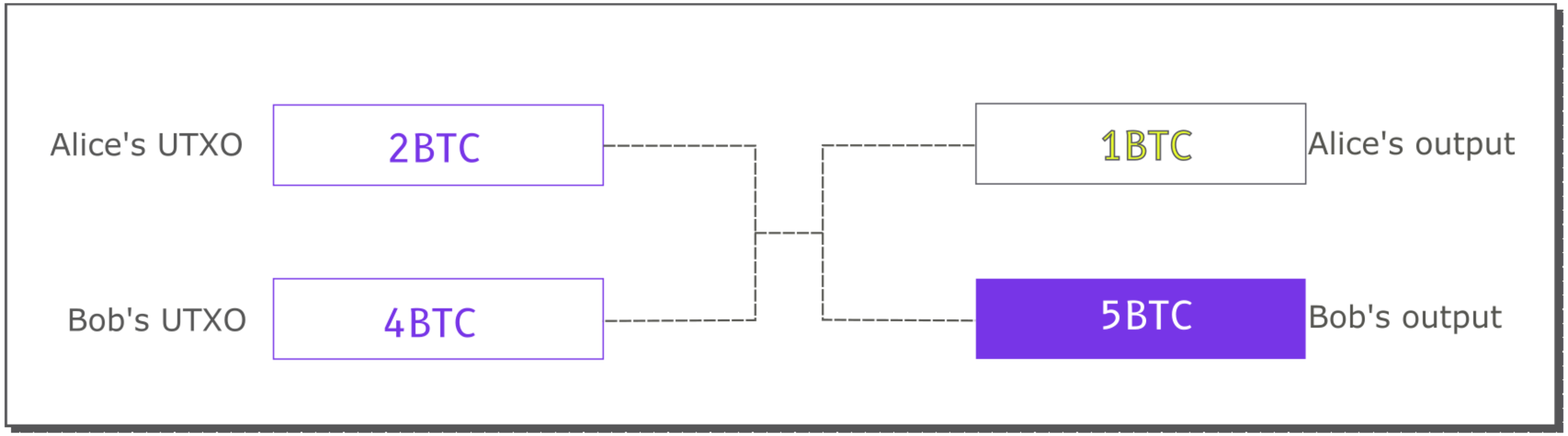


CoinJoin implementations

- Wasabi wallet https://github.com/zkSNACKs/WalletWasabi/
  - Centralized trustless coordinator, Tor, selected number of rounds executed within hours
    - https://docs.wasabiwallet.io/using-wasabi/CoinJoin.html
  - Wasabi 2.0 (beta) offer non-equal output coinjoin https://blog.wasabiwallet.io/privacy-guarantees-of-wasabi-wallet-2-0/
  - Anonymity set decrease over the time as people send their outputs to KYC exchanges
- Samourai Whirpool https://docs.samourai.io/en/whirlpool
  - CoinJoin with variable number of rounds, centralized trustless coordinator
  - CoinJoin runs until output is send away from Whirpool (days/months)
  - If not fullnode then xpub must be provided => privacy risk, decreased anonymity set
    - e.g., Samurai RoninDojo https://ronindojo.io/
  - Clients: Samourai wallet / Whirpool cli, SparrowWallet (using Samourai code)
- JoinMarket
  - No central coordinator, market Maker(s) run own fullnode and provide liquidity
  - Coinjoin transaction creation is coordinated by Taker who is paying also fee (on-chain and to the Maker)
  - JoininBox - JoinMarket cmdline-focused distribution https://github.com/openoms/joininbox

PayJoin

- PayJoin is special case of CoinJoin, but with less participants (typically only two: sender, receiver) and without equal UTXO sizes
- Faster than CoinJoin, done during a normal payment



- https://cryptotesters.com/blog/what-are-coinjoins-and-how-do-they-improve-bitcoin-privacy

ON-CHAIN BITCOIN ALTERNATIVES

Why search for other options (L2/sidechain/altcoins)?

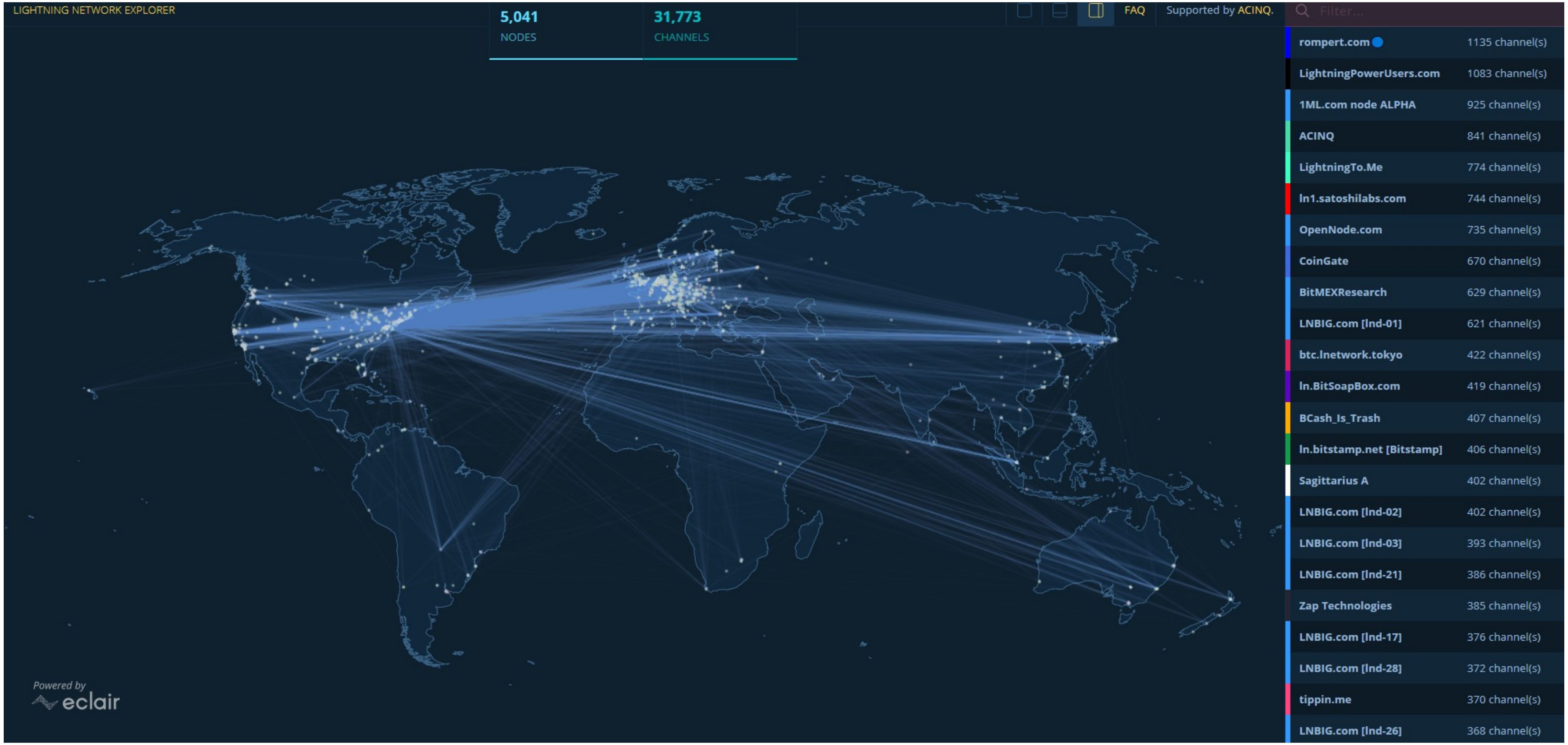
- Why something else than on-chain Bitcoin? List of typical reasons given:

1. Cost of sending transaction
   - Peak was tens of dollars (for every transfer), variable (from 1sat/vB), but has to increase in future due to decreasing reward
2. Time to confirm transaction (+ limited block size)
   - At least 1, but typically 4 blocks inside chain commonly required, ~10 minutes per block => ~40 min
3. Traceability of transactions
   - Source, destination and amount is on public ledger
4. Limited scripting language (lock script)
   - For more complicated smart contracts
5. Mining requirements
   - Specialized mining equipment required (ASICs) => may cause centralization if not enough widespread
   - Proof of Work is energy intensive (what it means?)

- …

LIGHTING NETWORK

Lighting network https://explorer.acinq.co/

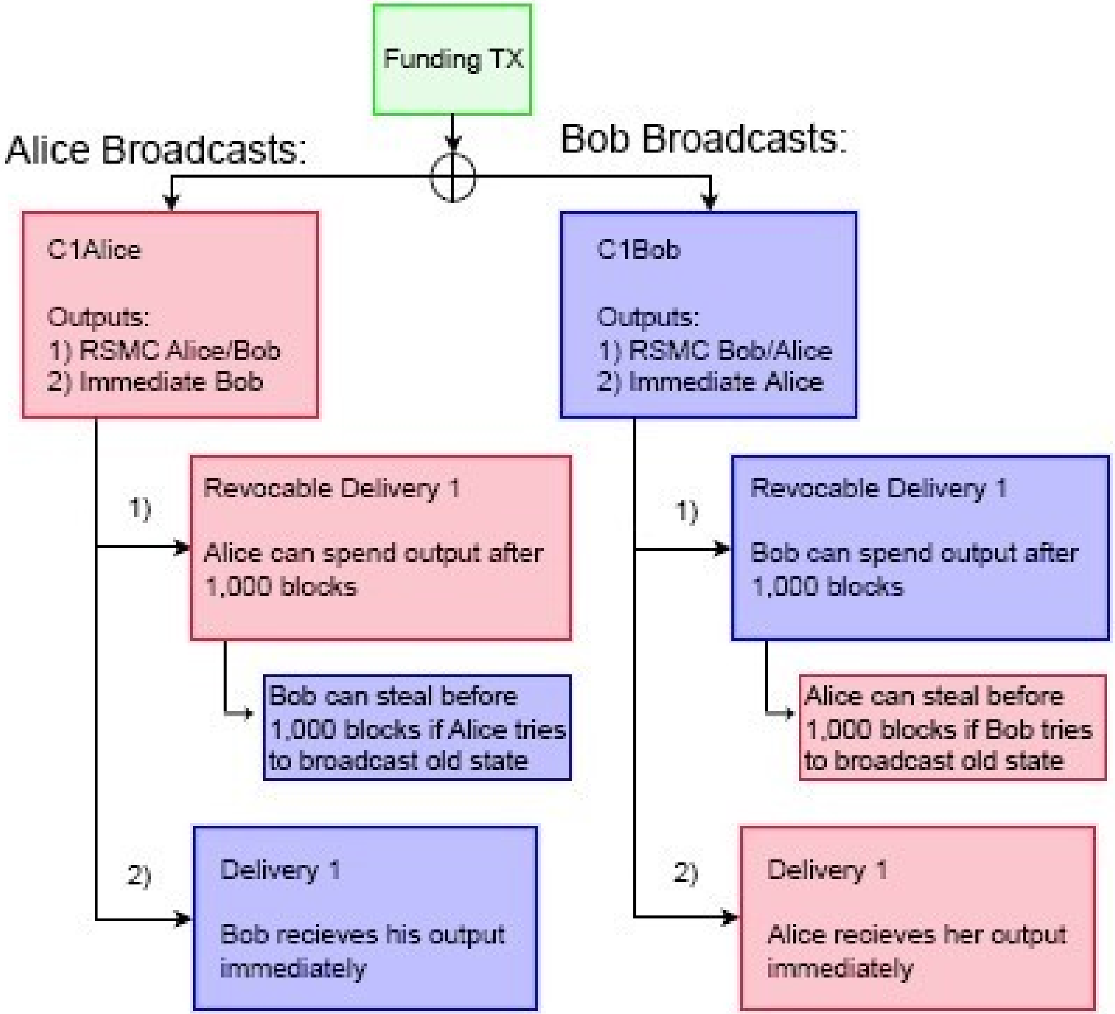


5,041 NODES

31,773 CHANNELS

rompert.com	1135 channel(s)
LightningPowerUsers.com	1083 channel(s)
1ML.com node ALPHA	925 channel(s)
ACINQ	841 channel(s)
LightningTo.Me	774 channel(s)
ln1.satoshilabs.com	744 channel(s)
OpenNode.com	735 channel(s)
CoinGate	670 channel(s)
BitMEXResearch	629 channel(s)
LNBIG.com [lnd-01]	621 channel(s)
btc.lnetwork.tokyo	422 channel(s)
ln.BitSoapBox.com	419 channel(s)
BCash_Is_Trash	407 channel(s)
ln.bitstamp.net [Bitstamp]	406 channel(s)
Sagittarius A	402 channel(s)
LNBIG.com [lnd-02]	402 channel(s)
LNBIG.com [lnd-03]	393 channel(s)
LNBIG.com [lnd-21]	386 channel(s)
Zap Technologies	385 channel(s)
LNBIG.com [lnd-17]	376 channel(s)
LNBIG.com [lnd-28]	372 channel(s)
tippin.me	370 channel(s)
LNBIG.com [lnd-26]	368 channel(s)

Opening channel



Funding TX

Alice Broadcasts:

Bob Broadcasts:

C1Alice

Outputs:
1) RSMC Alice/Bob
2) Immediate Bob

C1Bob

Outputs:
1) RSMC Bob/Alice
2) Immediate Alice

1)

Revocable Delivery 1

Alice can spend output after 1,000 blocks

Bob can steal before 1,000 blocks if Alice tries to broadcast old state

2)

Delivery 1

Bob recieves his output immediately

1)

Revocable Delivery 1

Bob can spend output after 1,000 blocks

Alice can steal before 1,000 blocks if Bob tries to broadcast old state

2)

Delivery 1

Alice recieves her output immediately

Note: In future, P2TR will be used - opening and (collaborative) closing of channel looks same as ordinary payment

https://medium.com/@jkendzicky16/the-bitcoin-lightning-network-a-technical-primer-d8e073f2a82f

Some Lighting topics I.

- Custodial Lighting wallet (e.g., Wallet of Satoshi)
  - Service hold your private key, full trust in service
- Semi-custodial Lighting wallet (e.g., default BlueWallet, Zap…)
  - own key, but trust in 3rd party providing blockchain info
- Non-custodial (e.g., BlueWallet collected to own full node)
  - own key, blockchain info and monitoring by own full node
- Inbound, outbound capacity of channel between A and B
  - Initial value is given by initial on-chain 2-2 multisig transaction (x:0, x:y, 0:y)
  - Changes with every off-chain transaction executed (between A and B)

Some Lighting topics II.

- Sentinel service
  - trustless blockchain observer, broadcasts justice transaction in case of old state detected
  - No need for your full node to be always online
- Privacy considerations
  - Most of the transactions are NOT recorded on the blockchain
    - Good for speed as well as privacy
  - Doesn’t mean that payments are not traceable
    - Same as with internet connection => need to use Tor, ideally mixes…
    - Privacy of sender is significantly better than receiver
  - Taproot introduced ability to open channel indistinguishable from normal P2TR

Q&A

slido

Audience Q&A Session

ⓘ Start presenting to display the audience questions on this slide.

NON-FINANCIAL USES

Non-financial data on Bitcoin blockchain

- Occasional messaging (coinbase data, OP_RETURN, lockScript)
- Inscriptions, Stamps (BRC-20)…
- Controversial topic
  - Other use-cases increase burned on full node operators
  - Price out some current financial users (but temporarily)

OpenTimestamps protocol (https://opentimestamps.org/)

- Prove that document existed at date X (at latest)
- Merkle tree of all submitted document hashes within given period committed to Bitcoin blockchain (OP_RETURN)
  - https://petertodd.org/2016/opentimestamps-announcement
- Currently free to use (only one OP_RETURN embed)
  - Client needs to remember Merkle tree path + file => *.ots file

```
$ pip3 install opentimestamps-client
$ ots stamp secret.txt

$ ots info secret.txt
$ ots verify secret.txt.ots
Assuming target filename is 'secret.txt'
Calendar https://alice.btc.calendar.opentimestamps.org: Pending confirmation in Bitcoin blockchain
```

https://github.com/opentimestamps/opentimestamps-client

CASE STUDY: ORDINALS/INSCRIPTIONS

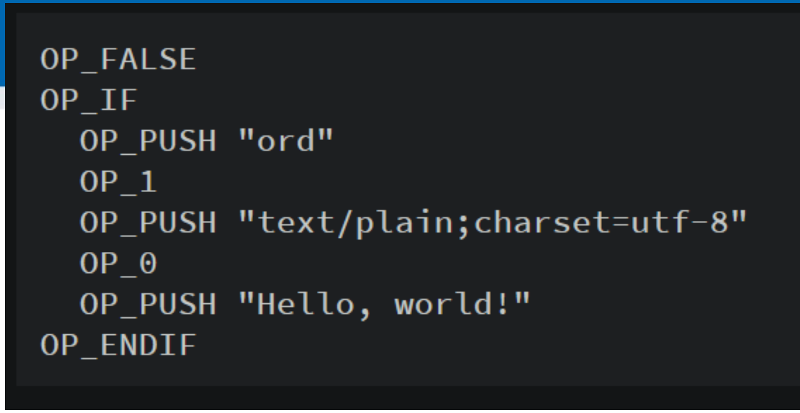
Case study: Ordinals/Inscription (NFT)

- Non-Fungible Token (NFT)
  - Unique digital asset, cannot be exchanged for other units of the same type
  - Dollars or satoshis are fungible (1$ = 1$), while NFT is non-fungible
  - Examples: jpegs, movie, music, numbered ticket, numbered equity…
  - Ownership can be transferred (methods depends on the underlying chain)
- Frequently, tied to blockchain like Bitcoin (Colored Coins) or Ethereum
  - Only URI and hash is stored in contract, actual picture/NFT stored elsewhere
  - Centralized DB (S3), Decentralized filesystem (e.g., IPFS)…
- Problem: What if storage place is erased?
  - Actual NFT is lost, only reference on-chain is kept

Case study: Ordinals/Inscriptions (NFT)

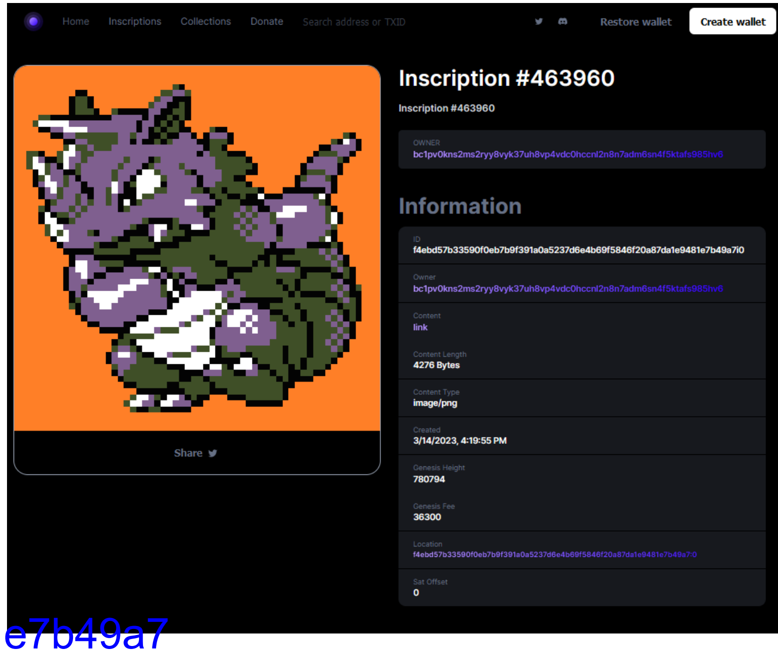
- NFT needs two principal components
  - Non-fungible (transferable) reference for NFT [Ordinals]
  - Storage place for actual NFT content (picture, movie, 3d model) [Inscriptions]
- Ordinals (https://docs.ordinals.com/overview.html)
  - Virtual unambiguous numbering scheme for every **`satoshi`** mined so far
    - xth **`satoshi`** mined, keeps its number
  - When UTXO is spent, all its satoshies (already numbered) are distributed on ordered basis (FIFO, first-satoshi-in-first-satoshi-out)
  - Important: no “serial number” is put on blockchain, everything is just virtual overlay
  - https://github.com/casey/ord/blob/master/bip.mediawiki

Case study: Ordinals/Inscriptions (NFT)



```
OP_FALSE
OP_IF
  OP_PUSH "ord"
  OP_1
  OP_PUSH "text/plain;charset=utf-8"
  OP_0
  OP_PUSH "Hello, world!"
OP_ENDIF
```

- Inscriptions (https://ordinals.com/inscriptions)
  - – Requires Taproot (P2TR address), first tx spends sats, second reveals script
  - – Embedding of data into witness script in non-spendable path (OP_FALSE)
  - – Inscription is on first sat of first output
  - – Ownership can be transferred to other person (ordinals)
- Transaction fee needs to be paid
  - – Data are in discounted Segwit bytes (¼ price)
  - – But inscriptions are typically significantly larger than tx
    - Ordinary tx is 100-200 sats, data 1024 sats / kB
  - – Significant number of transactions in Jan-March 2023



Inscription #463960

Inscription #463960

OWNER
bc1pv0kns2ms2ryy8vyk37uh8vp4vdc0hccnl2n8n7adm6sn4f5ktafs985hv6

Information

ID
f4ebd57b33590f0eb7b9f391a0a5237d6e4b69f5846f20a87da1e9481e7b49a7i0

Owner
bc1pv0kns2ms2ryy8vyk37uh8vp4vdc0hccnl2n8n7adm6sn4f5ktafs985hv6

Content
link

Content Length
4276 Bytes

Content Type
image/png

Created
3/14/2023, 4:19:55 PM

Genesis Height
780794

Genesis Fee
36300

Location
f4ebd57b33590f0eb7b9f391a0a5237d6e4b69f5846f20a87da1e9481e7b49a7:0

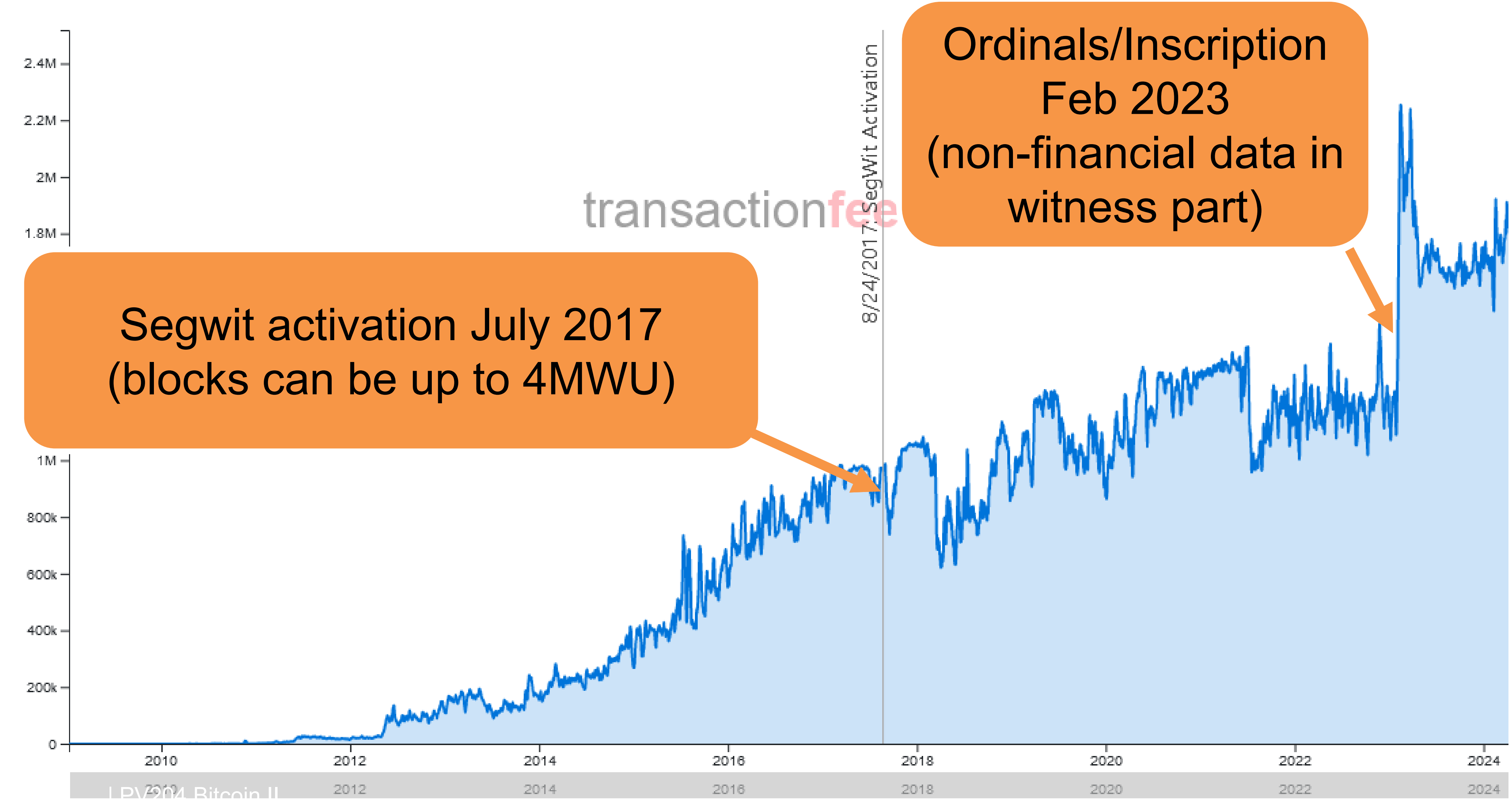
Sat Offset
0

https://mempool.space/tx/f4ebd57b33590f0eb7b9f391a0a5237d6e4b69f5846f20a87da1e9481e7b49a7
https://ordinals.com/inscription/f4ebd57b33590f0eb7b9f391a0a5237d6e4b69f5846f20a87da1e9481e7b49a7i0

Block Size

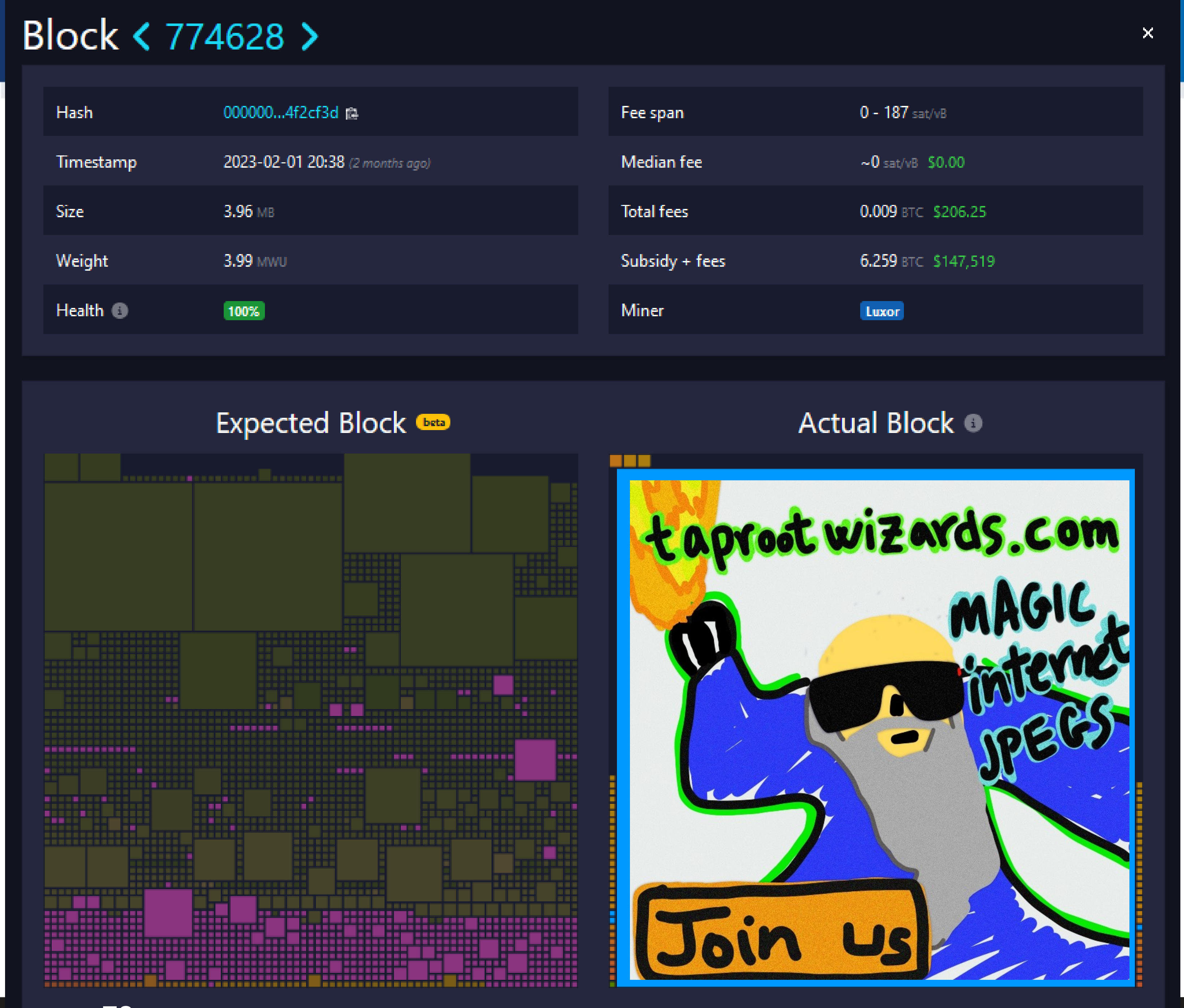
Shows the daily average block size in bytes.

https://transactionfee.info/charts/block-size/



Segwit activation July 2017 (blocks can be up to 4MWU)

Ordinals/Inscription Feb 2023 (non-financial data in witness part)



Block < 774628 >

Hash	000000...4f2cf3d	Fee span	0 - 187 sat/vB
Timestamp	2023-02-01 20:38 (2 months ago)	Median fee	~0 sat/vB $0.00
Size	3.96 MB	Total fees	0.009 BTC $206.25
Weight	3.99 MWU	Subsidy + fees	6.259 BTC $147,519
Health	100%	Miner	Luxor

Inscriptions: the largest block mined so far (3.96MB)

- https://mempool.space/block/00000000000000000000515e202c8ae73c8155fc472422d7593af87aa74f2cf3d

Case study: Ordinals/Inscriptions discussion

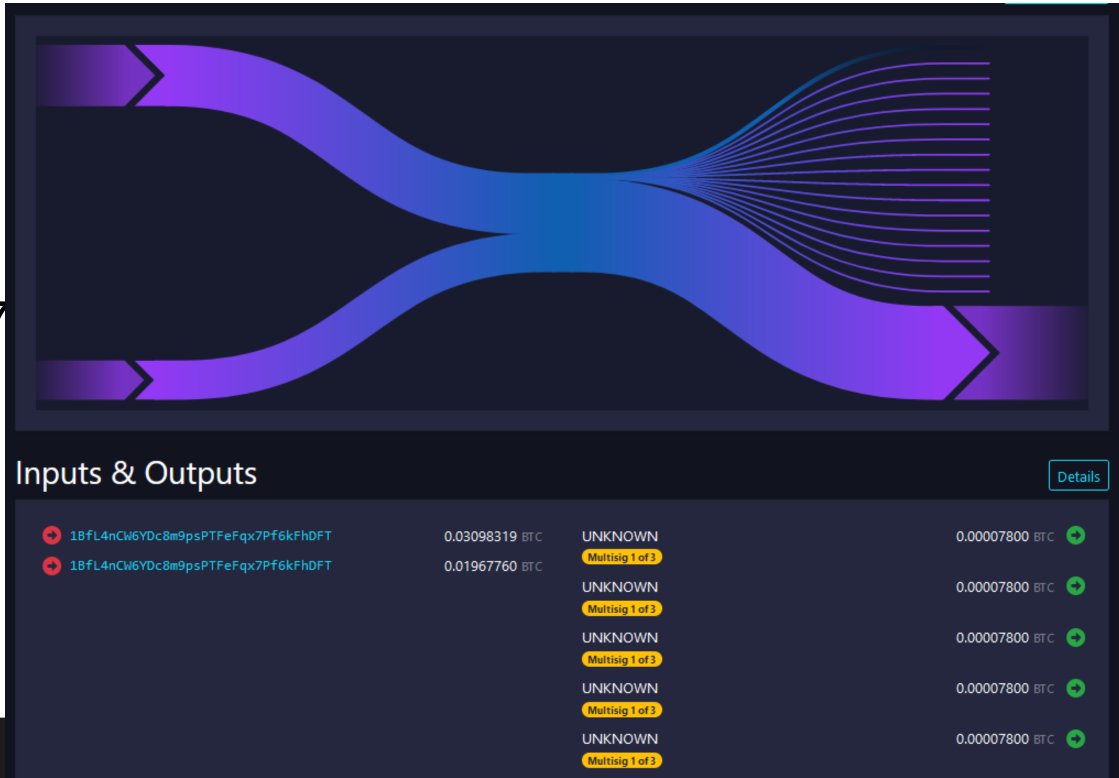
- Inscriptions are controversial and discussed (March 2023)
- What do you think?

Case study: Ordinals/Inscriptions discussion

- Inscriptions are controversial and discussed (March 2023)
- Discussion points (Do your own research!)
  - Blockspace used for non-financial data, needs to be downloaded/stored by all
    - Segwit part, only download, fast verification (OP_FALSE), no UTXO set bloat
  - Legal implications (3d printed guns, child abuse material…)
  - NFT getting discount price, spam
    - Segwit data bytes are discounted, but ordinary tx is significantly more dense => shall outprice Inscriptions
  - Pricing out people wanting to do on-chain transactions for small value
    - Mainnet not meant for small tx longer (Lighting, sidechains)
    - Is now increasing rewards for miners => more blockchain security
  - Impacting fungibility of Bitcoin, push for more smaller transactions (UTXO set)

Another recent protocol for NFT storage (Bitcoin Stamps)

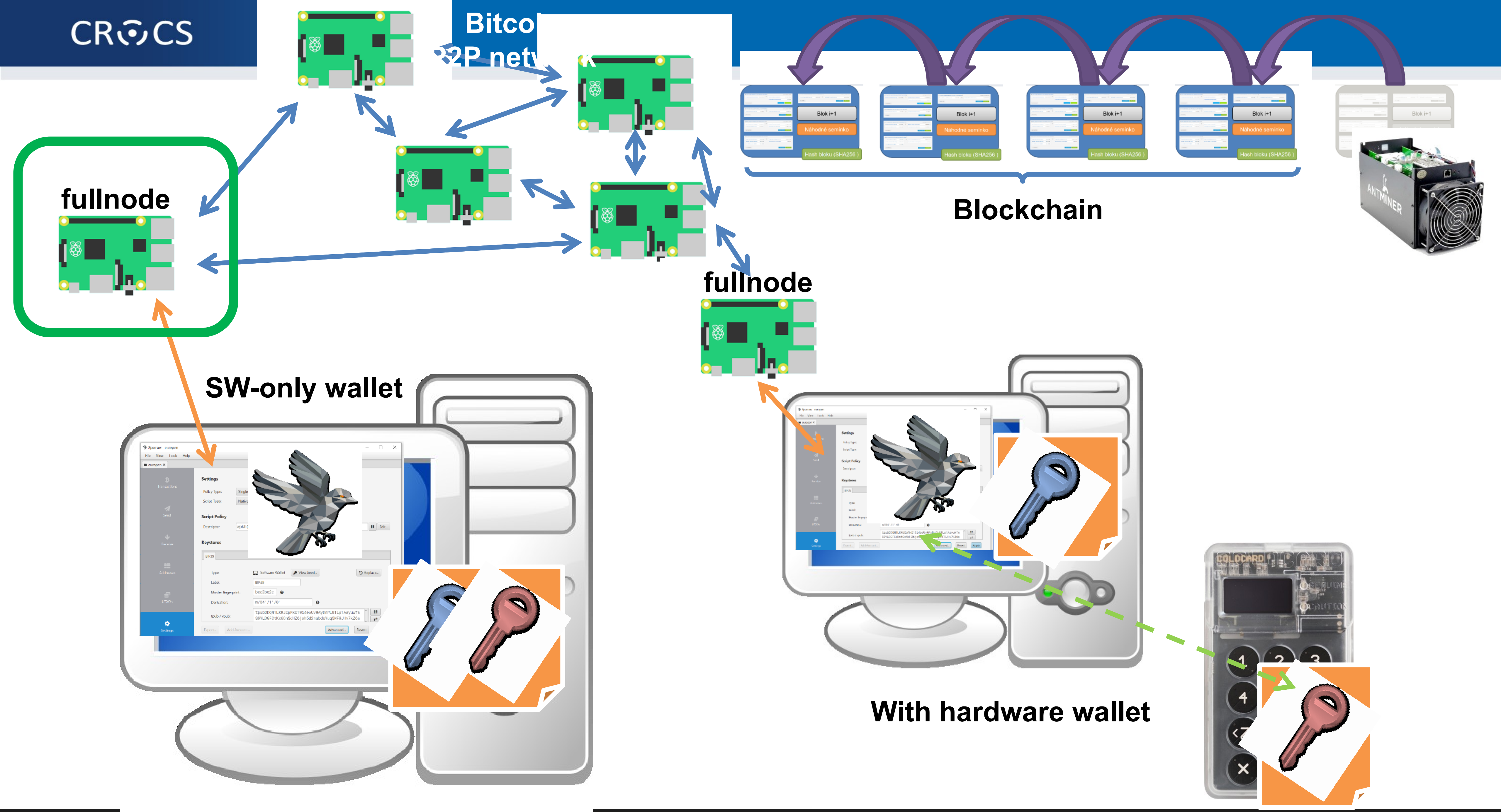
- Different project than Inscriptions
- Intentionally unpruneable from blockchain
  - Data split over multiple UTXOs
  - Data encoded as pubkeys of 1-of-3 P2MS
  - Stays (forever) in UTXO set
  - Example
    - https://mempool.space/tx/9b7327631cc3e0dff7 7e9d5844791
- What do you think?



Inputs & Outputs

```
1BfL4nCW6YDc8m9psPTFeFqx7Pf6kFhDFT   0.03098319 BTC   UNKNOWN           0.00007800 BTC
                                                      Multisig 1 of 3
1BfL4nCW6YDc8m9psPTFeFqx7Pf6kFhDFT   0.01967760 BTC   UNKNOWN           0.00007800 BTC
                                                      Multisig 1 of 3
                                                      UNKNOWN           0.00007800 BTC
                                                      Multisig 1 of 3
                                                      UNKNOWN           0.00007800 BTC
                                                      Multisig 1 of 3
                                                      UNKNOWN           0.00007800 BTC
                                                      Multisig 1 of 3
```

RUNNING OWN FULL NODE



Sparrow europen

File View Tools Help

europen ✕

Transactions
Send
Receive
Addresses
UTXOs
Settings

Settings

Policy Type: Single

Script Type: Native

Script Policy

Descriptor: wpkh(

Edit...

Keystores

BIP39

Type: Software Wallet View Seed... Replace...

Label: BIP39

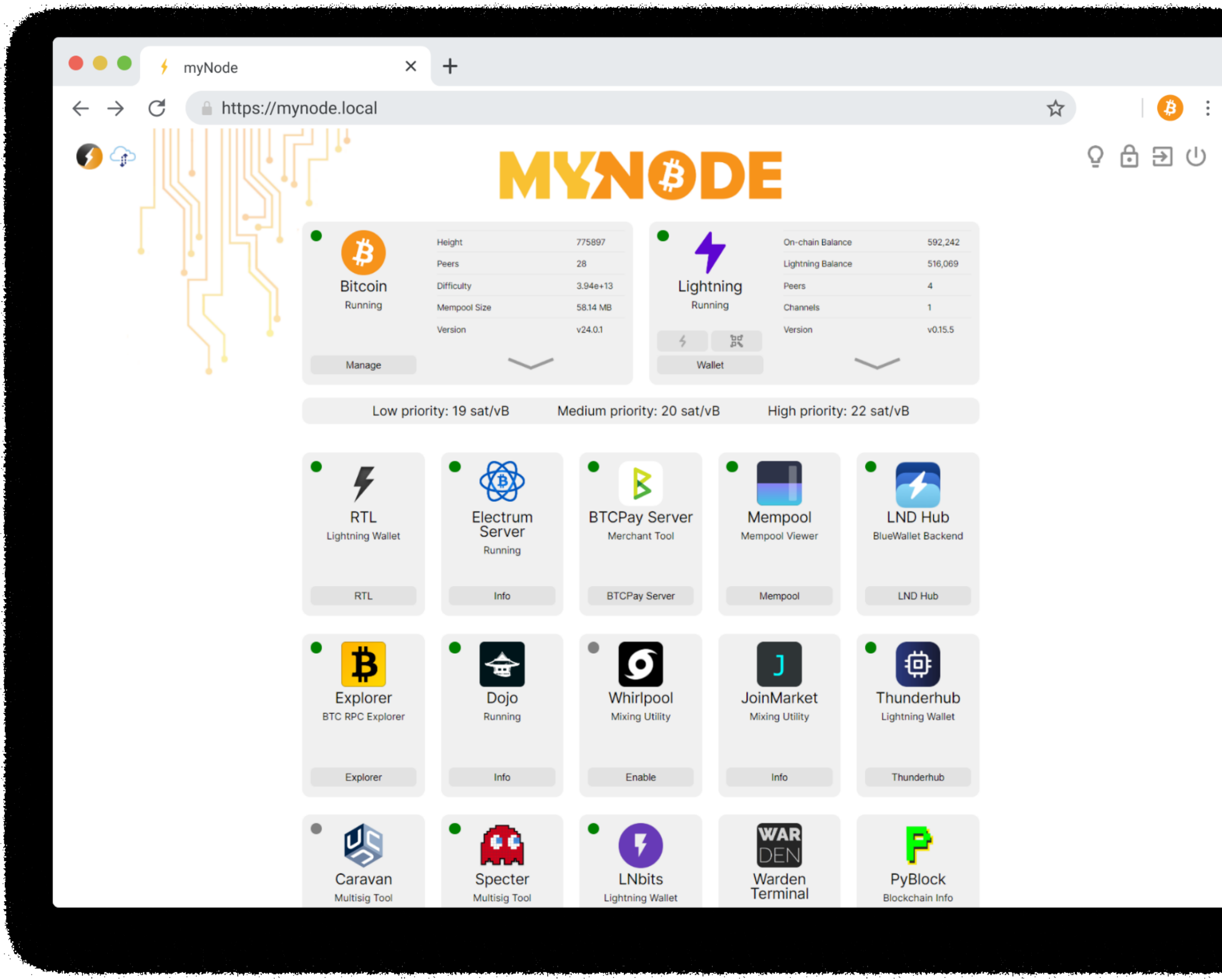
Master fingerprint: bec2be2c

Derivation: m/84'/1'/0'

tpub / vpub: tpubDDQN1LKMJEpRkE1914eoUvMAyDnPL81Lp1Aayuwfs S9YLDGFCtKx6Cn5dIZ6jxh5d2nabdsYuq5MF9JIv7kZ6e

Export... Add Account... Advanced... Revert

Running own full node



Bitcoin
Running

Height	775897
Peers	28
Difficulty	3.94e+13
Mempool Size	58.14 MB
Version	v24.0.1

Lightning
Running

On-chain Balance	592,242
Lightning Balance	516,069
Peers	4
Channels	1
Version	v0.15.5

Low priority: 19 sat/vB   Medium priority: 20 sat/vB   High priority: 22 sat/vB

Additional software to run on “full node”

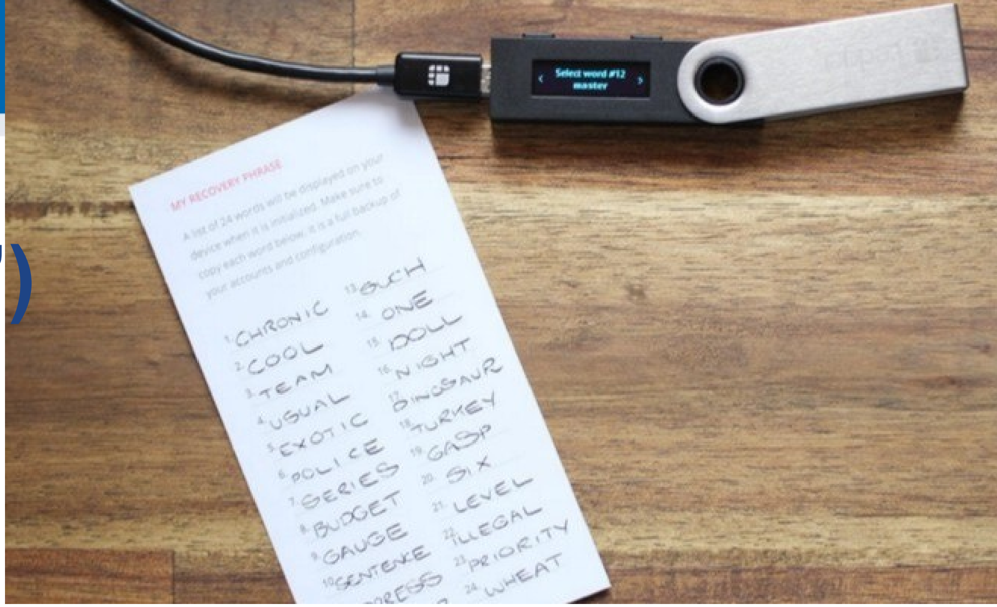
- Bitcoin Core basic client (bitcoind, bitcoin-qt)
  - Many additional software packages possible
- Lighting network software (LND, c-Lighting, Eclaire, RTL, LNbits…)
- Payment servers (BTCPay server)
- Blockchain explorers / indexers (Electrum, mempool.space, Explorer…)
- CoinJoin clients (Whirpool, JoinMarket…)
- Multisignature coordinators (DoJo, Specter, CKBunker…)
- Pre-prepared fullnode distributions (software above included)
  - MyNode, Umbrel, RaspiBlitz…

Summary

WHERE SHOULD WE FOCUS THIS YEAR?
"BLOCKCHAIN"
IT WILL CHANGE EVERYTHING.
EVERYBODY IS TALKING ABOUT IT.
THE POTENTIAL APPLICATIONS ARE ENDLESS.
WE DON'T WANT TO BE LEFT BEHIND.
WHAT EXACTLY IS BLOCKCHAIN?
ALSO, "ARTIFICIAL INTELLIGENCE"
TOM FISH BURNE
© marketoonist.com

WALLET TOPICS

Backing up entropy ("master seed")



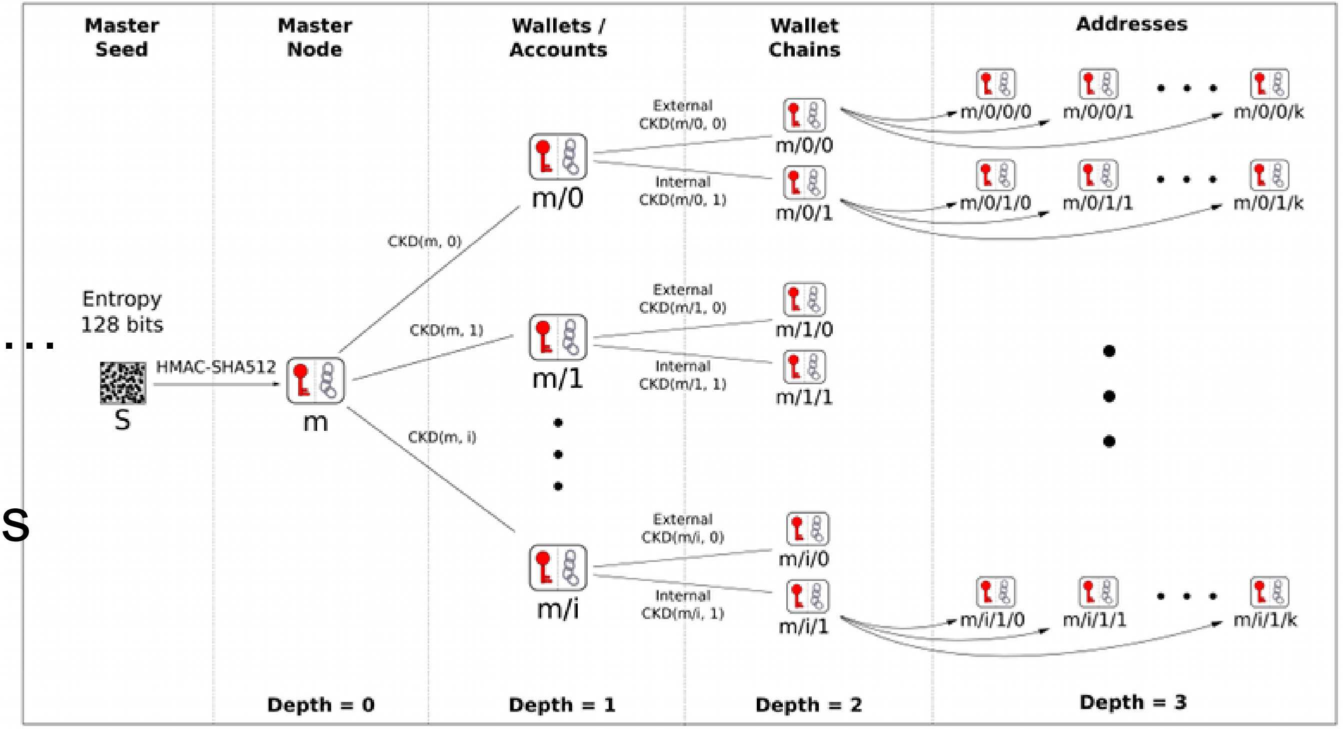
- 128 or 256 bits of entropy (12 or 24 words)
- How to store securely?
  - Write on paper, punch into metal plate, carve into stone…
  - How to prevent human typing error (bits → mnemonics, BIP39)
  - Do not write somewhere digitally (malware may steal it)
- How to prevent single point of failure?
  - Make two copies (=> more robust against accidental loss)
  - Make (threshold) parts Shamir (=> more robust against intentional theft and loss - threshold)
  - Require multiple signatures (multisig, MPC)

https://coldbit.com

Making fresh private keys (with backup) BIP32, BIP44…

- Deterministic derivation from:
  - master seed (key)
  - derivation path (data)
    - m/purpose/coin/account/receive…
- Single master seed allows:
  - Generate many distinct private keys
  - Sharing sub-tree value allows:
    - Generate keys in sub-trees
    - Cannot generate keys from other trees
- Deterministic generation, Master Seed enough to recover whole tree

BIP 32 - Hierarchical Deterministic Wallets



Child Key Derivation Function ~ CKD(x,n) = HMAC-SHA512(x_{Chain}, x_{PubKey} || n)