PV204 Security technologies

Bitcoin mining, privacy, multisignatures and other topics

Petr Švenda ✉ ***svenda@fi.muni.cz*** ***@rngsec***

Centre for Research on Cryptography and Security, Masaryk University

CRoCS
Centre for Research on
Cryptography and Security

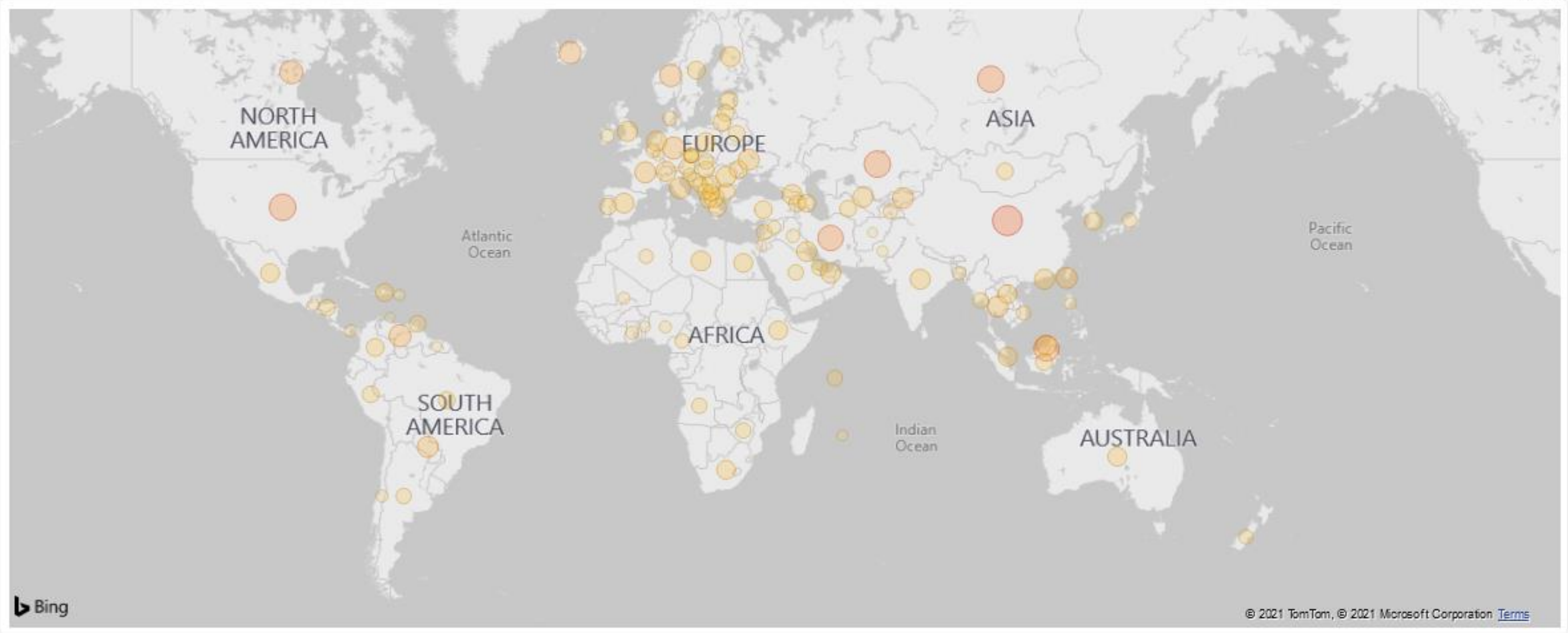
Please provide any corrections and comments here (thank you!):
[*https://drive.google.com/file/d/1DH1rooFx6ZXNflaHRHqvfOAHXc_qikc3/view?usp=sharing*](https://drive.google.com/file/d/1DH1rooFx6ZXNflaHRHqvfOAHXc_qikc3/view?usp=sharing)

MINING

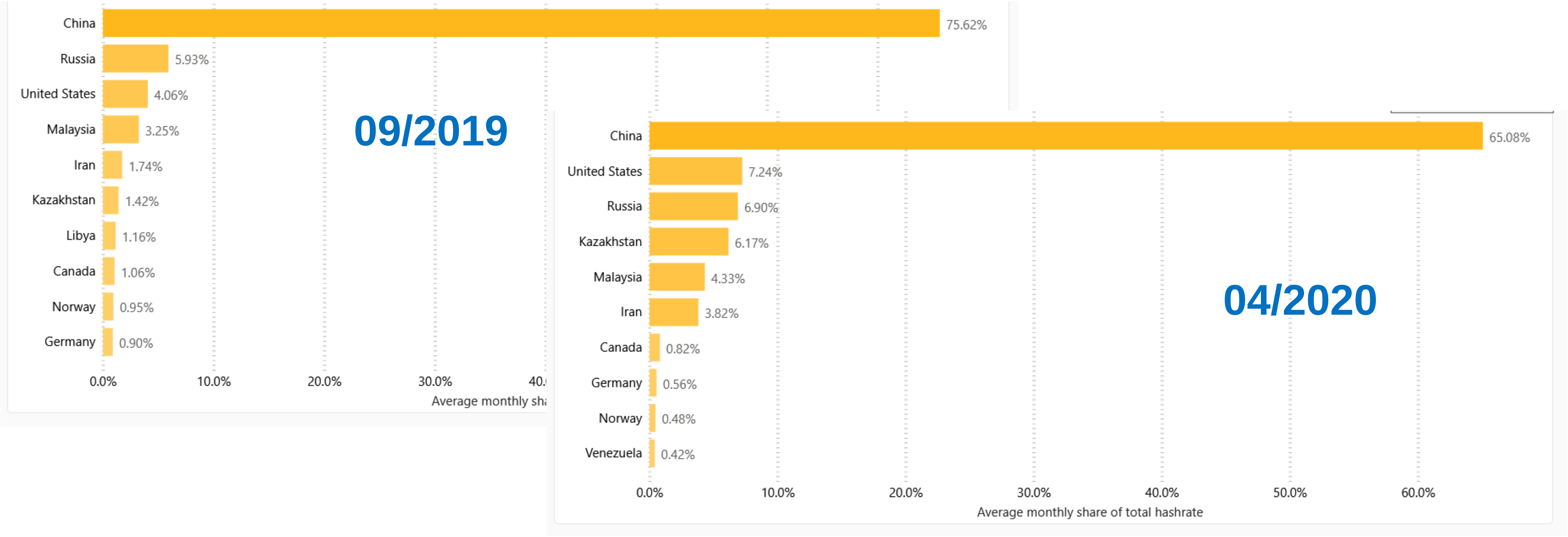
Mining in Proof of Work chains

- Crucial for security of blockchain (no rewrite)
- Initially on CPU (Satoshi: everyone can participate 1 CPU 1 vote)
- Initially solo mining
- CPU→GPU →FPGA →ASIC
- First mining pool: SlushPool in Prague
  - Miners join their hashrate, fraction of reward based on number of partial solutions
- Cambridge university centre for alternative finance (CBECI)
  - Where are miners? https://cbeci.org/mining_map/
  - More mining details: https://cbeci.org/cbeci/methodology

Bitcoin mining map in April 2020

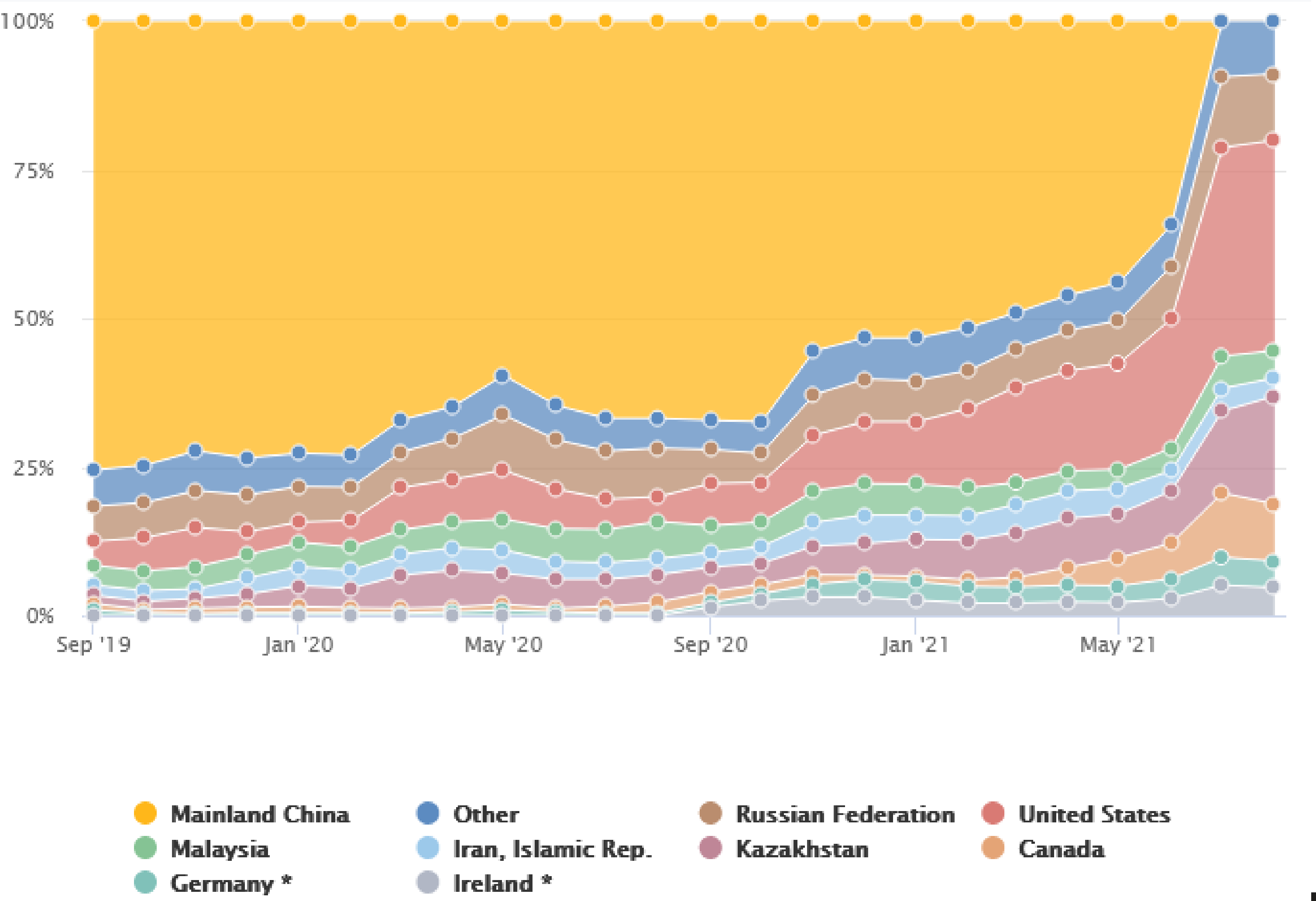


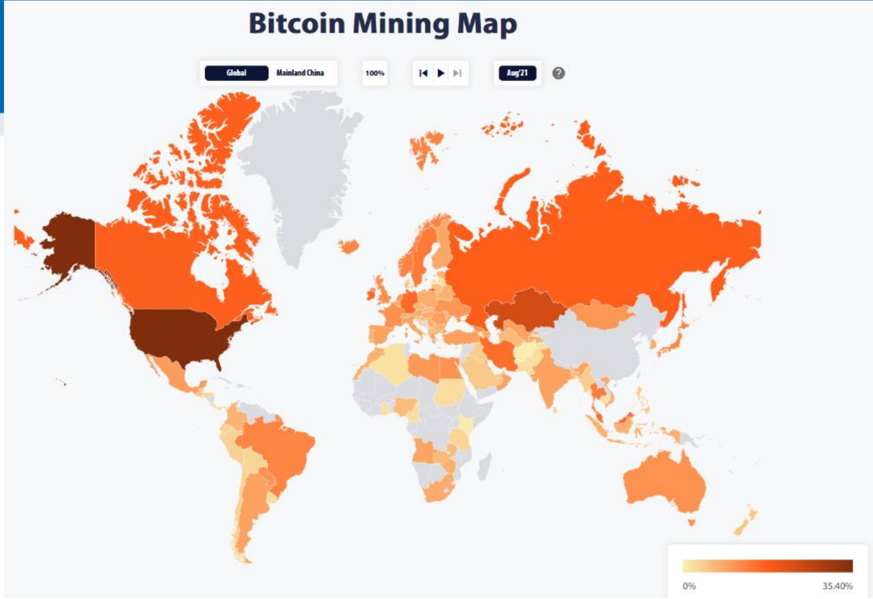
China mining dominance (09/2019→04/2020: 75.6%->65%)


09/2019

04/2020

Bitcoin mining map (August 2021)

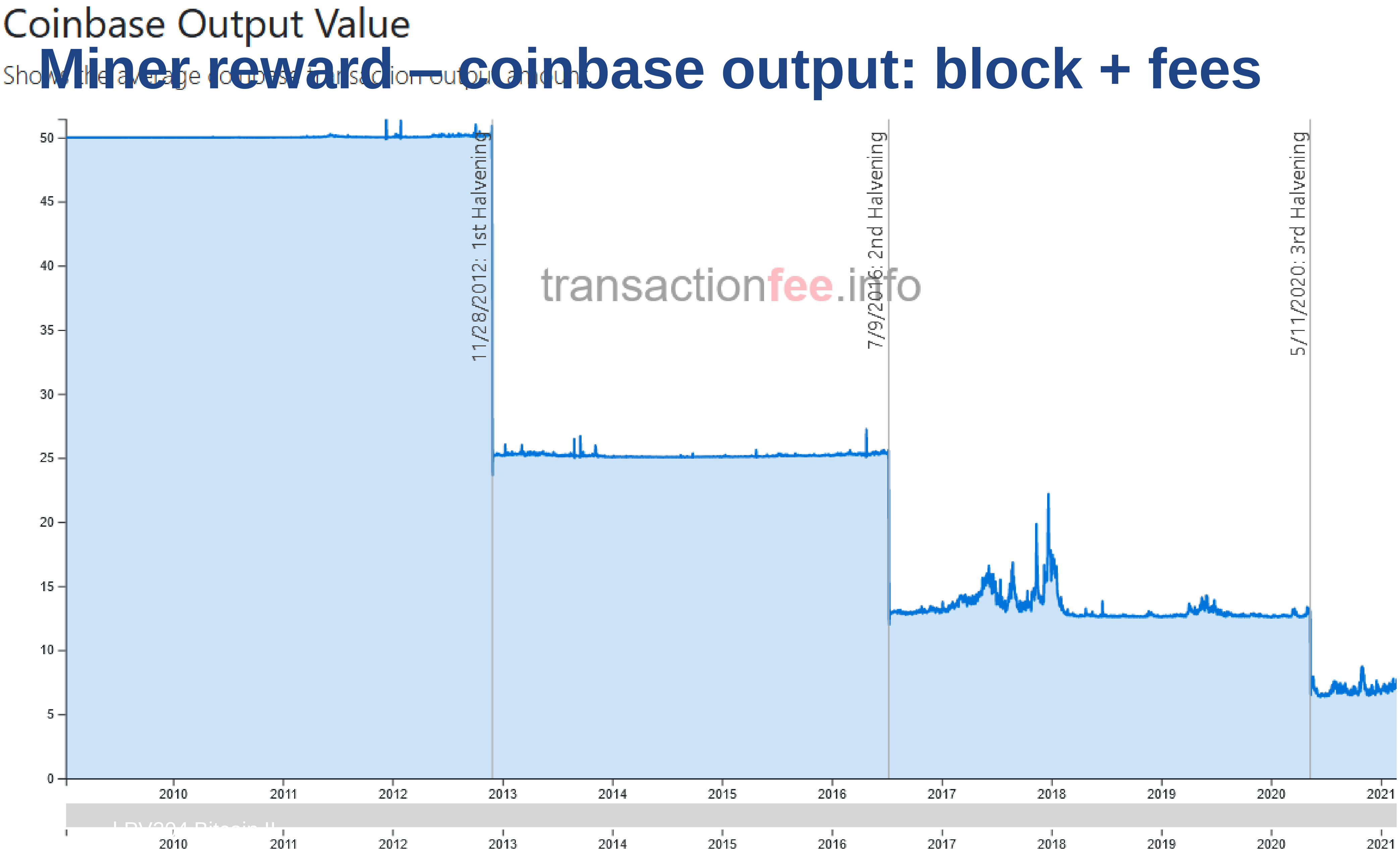




- China evicted “all” miners
- Strong increase in:
  - – US 35%
  - – Kazachstan 18.1
  - – Canada 9.5%

https://transactionfee.info/charts/block-coinbase-amount/?start=2009-01-09&end=2021-02-02

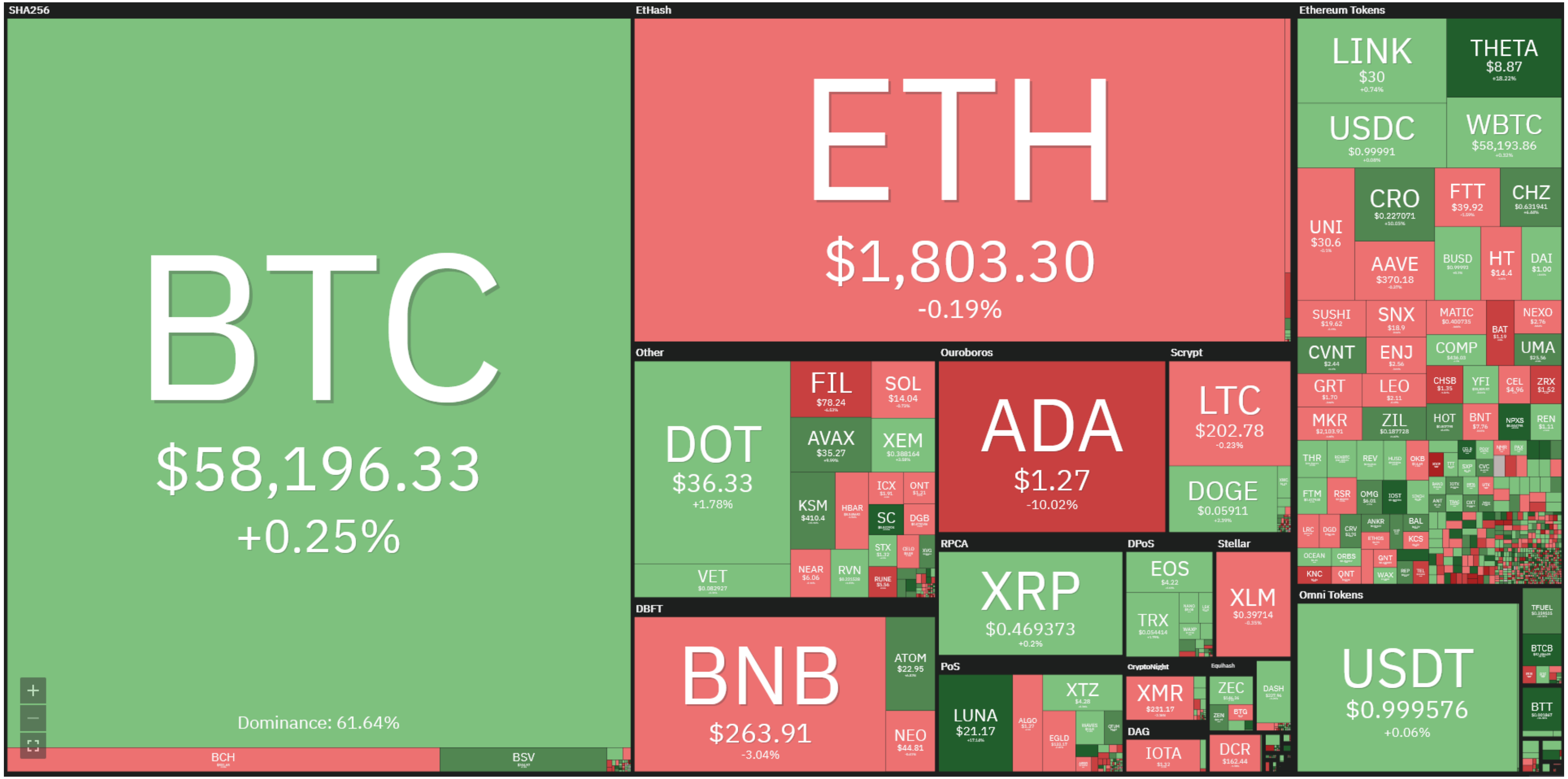
Miner reward – coinbase output: block + fees



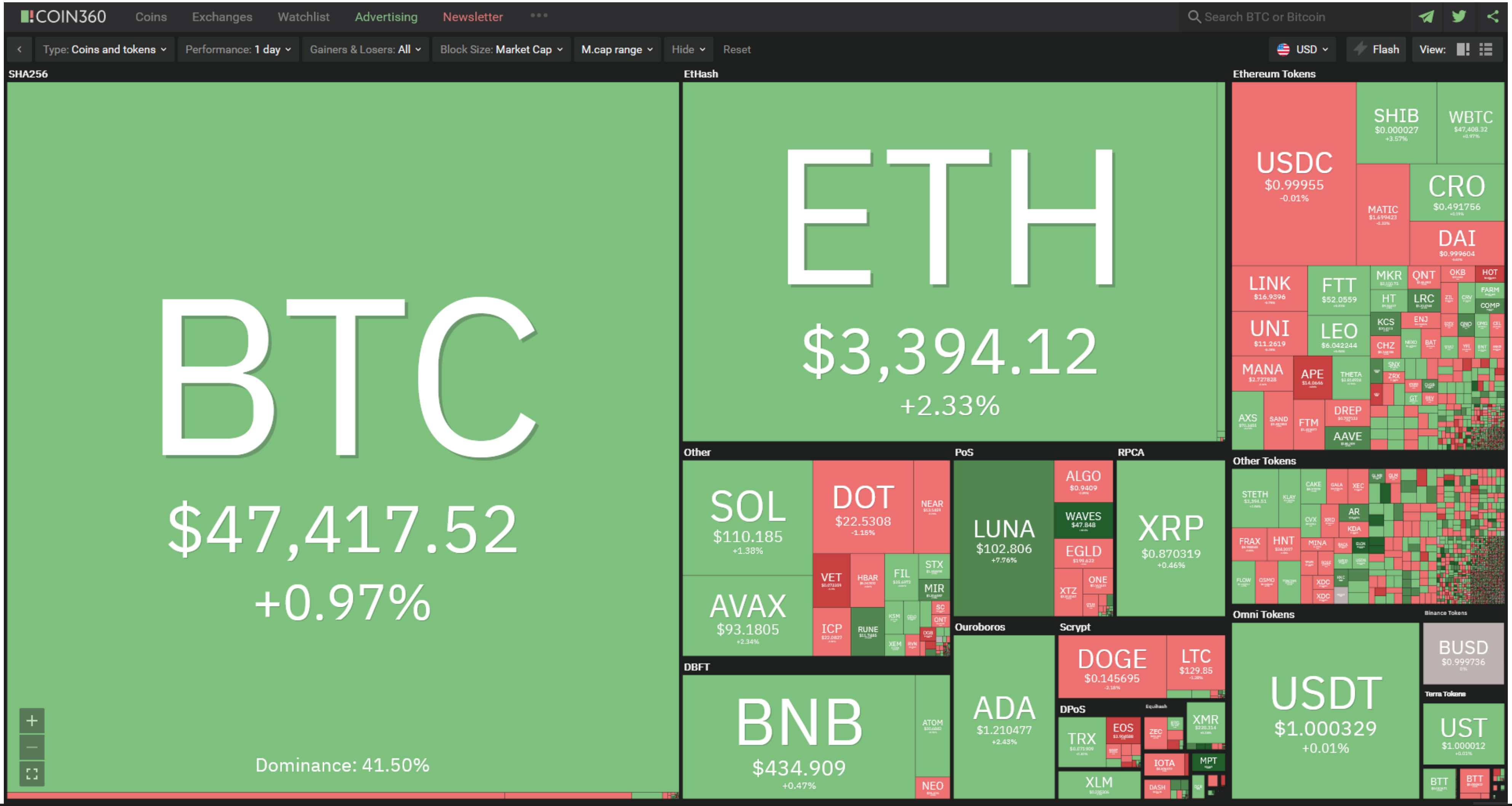
Coinbase Output Value

Shows the average coinbase transaction output amount

Coin mining algorithm https://coin360.com/

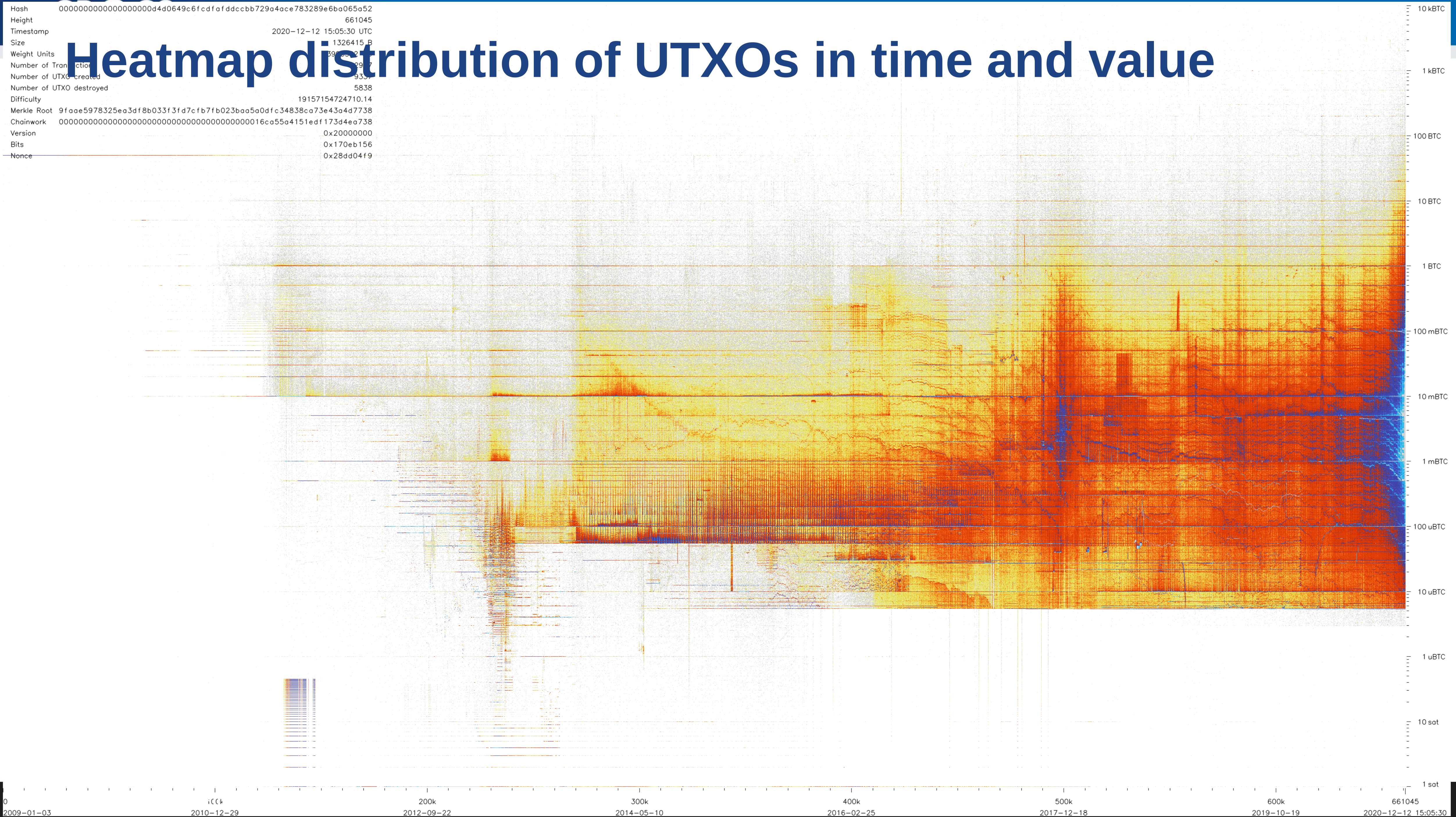


Coin mining algorithm https://coin360.com/



Type: Coins and tokens | Performance: 1 day | Gainers & Losers: All | Block Size: Market Cap | M.cap range | Hide | Reset | USD | Flash | View:

Heatmap distribution of UTXOs in time and value



```
Hash        0000000000000000000d4d0649c6fcdfafddccbb729a4ace783289e6ba065a52
Height                                                                661045
Timestamp                                                2020-12-12 15:05:30 UTC
Size                                                               1326415 B
Weight Units                                                    39[illegible]
Number of Transactions                                           29[illegible]7
Number of UTXO created                                          933[illegible]
Number of UTXO destroyed                                                5838
Difficulty                                                19157154724710.14
Merkle Root 9faae5978325ea3df8b033f3fd7cfb7fb023baa5a0dfc34838ca73e43a4d7738
Chainwork   000000000000000000000000000000000000000016ca55a4151edf173d4ea738
Version                                                           0x20000000
Bits                                                              0x170eb156
Nonce                                                             0x28dd04f9
```

Who can include next block to blockchain?

- Proof of Work (PoW, Bitcoin, Ethereum, 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 other chain is included in coinbase data of Bitcoin
  - Other chain is not performing own mining, Bitcoin miners are getting reward for included other chains
- Proof of Proof (PoP)
  - Hash of block from other chain is included in Bitcoin transaction (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

Interesting stats about mined transactions

- https://forkmonitor.info/nodes/btc
- https://transactionfee.info/
- https://cryptobriefing.com/unpacking-bitcoins-recent-double-spend-event

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…

Attacker models

- Blockchain-only analysis
- Malware, phishing
- Active network analysis, metadata
- Cryptographic analysis of used algorithms
- Side-channel analysis

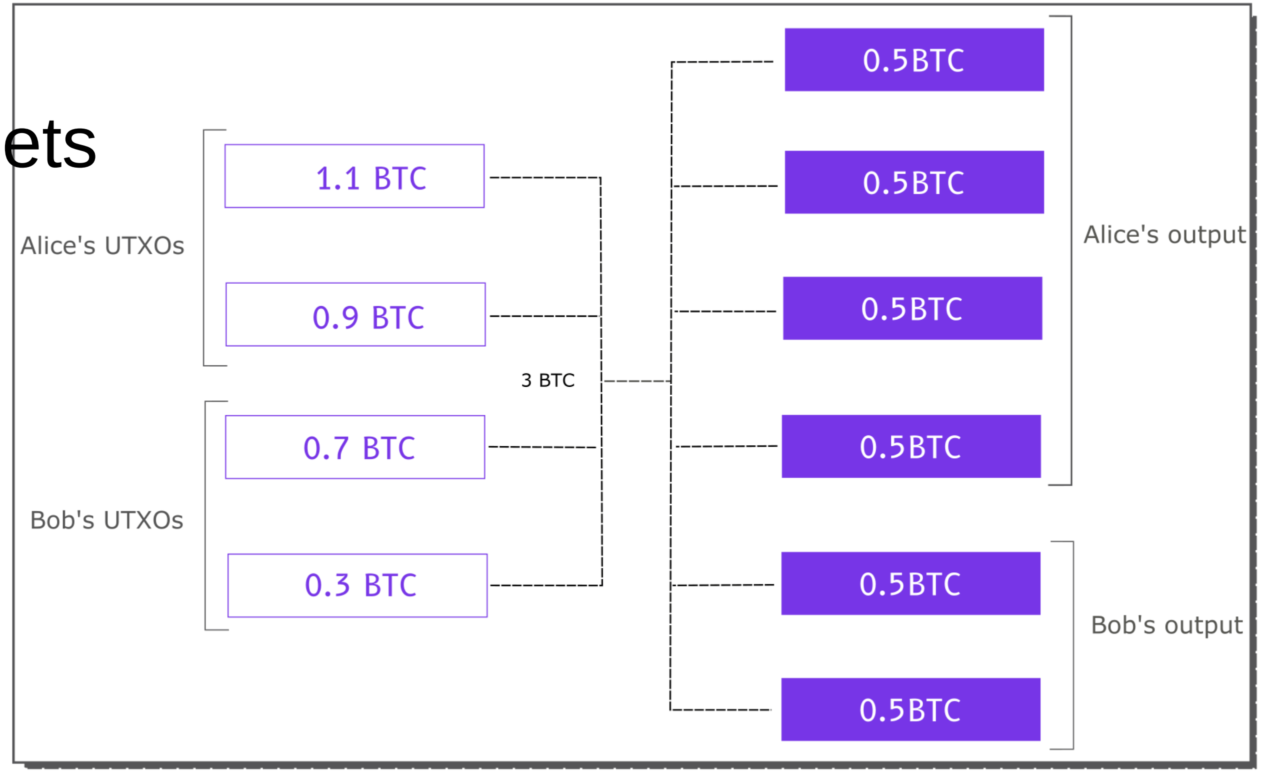
Improving privacy

- 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
- 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…)

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

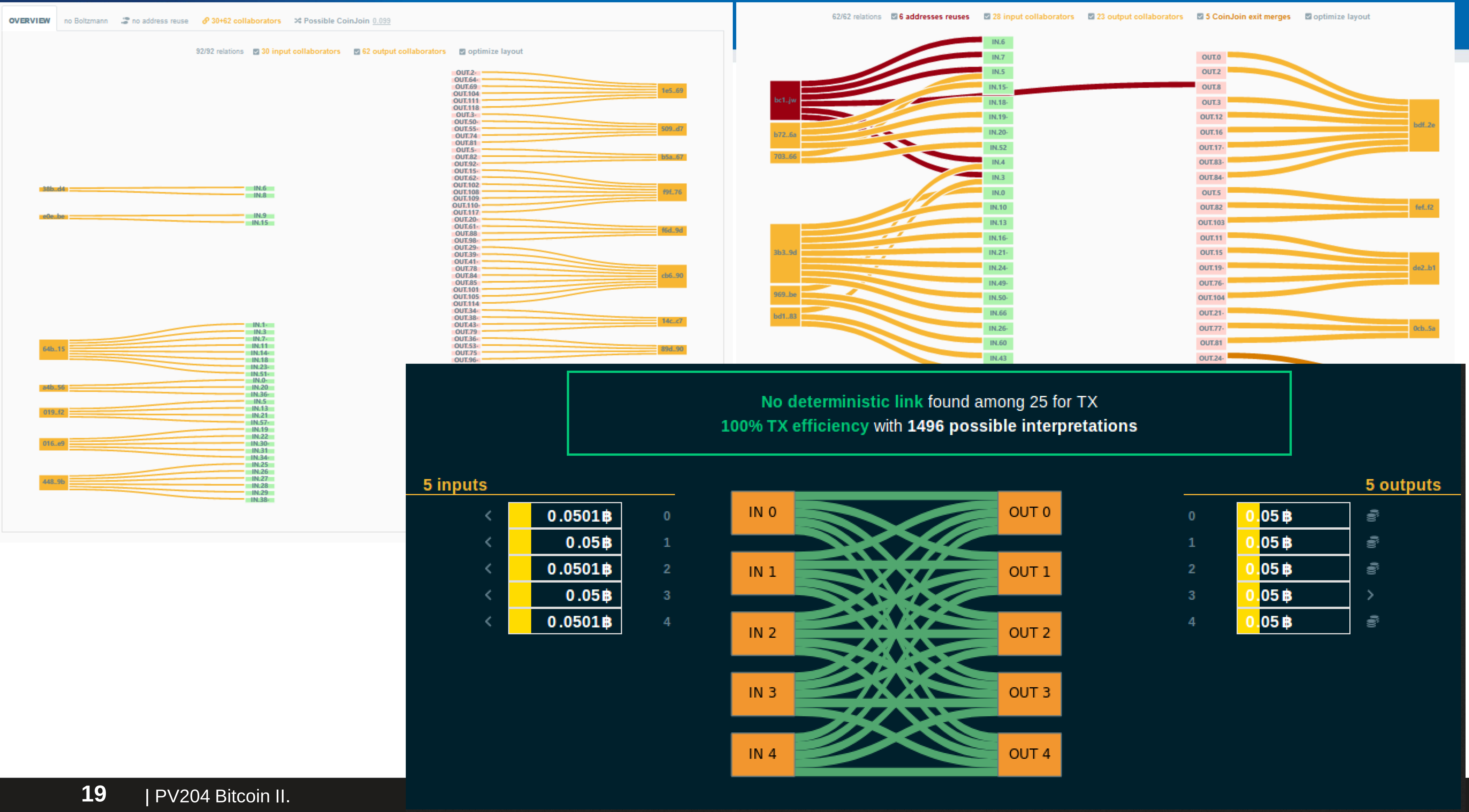
CoinJoin

- 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) will 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



92/92 relations ☑ 30 input collaborators ☑ 62 output collaborators ☑ optimize layout

62/62 relations ☑ 6 addresses reuses ☑ 28 input collaborators ☑ 23 output collaborators ☑ 5 CoinJoin exit merges ☑ optimize layout

No deterministic link found among 25 for TX
100% TX efficiency with **1496 possible interpretations**

5 inputs

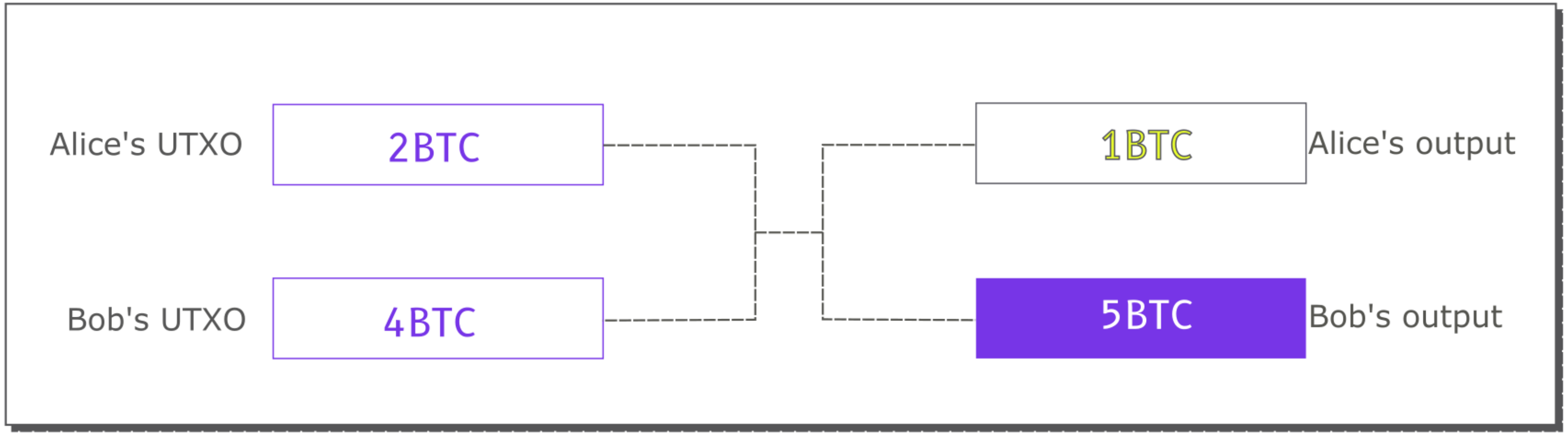
0.0501 ฿	0
0.05 ฿	1
0.0501 ฿	2
0.05 ฿	3
0.0501 ฿	4

5 outputs

0	0.05 ฿
1	0.05 ฿
2	0.05 ฿
3	0.05 ฿
4	0.05 ฿

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



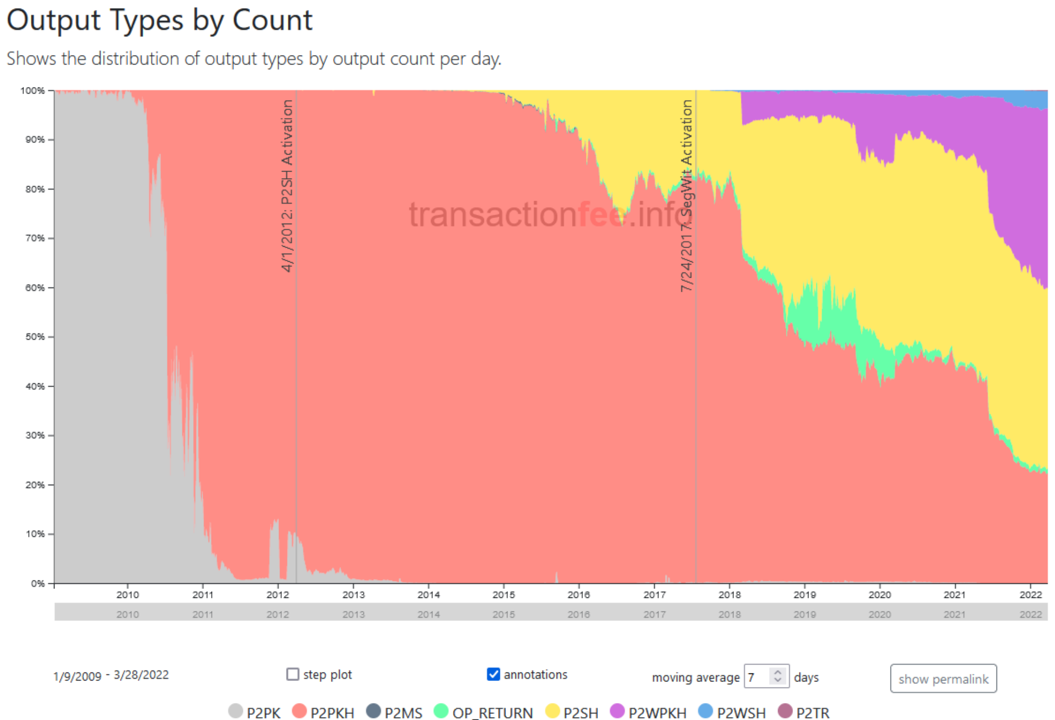
- https://cryptotesters.com/blog/what-are-coinjoins-and-how-do-they-improve-bitcoin-privacy

LOCK AND UNLOCK SCRIPTS

https://transactionfee.info/charts/output-type-distribution-count/

Types of receiving “addresses”

- There is no ”address” defined in Bitcoin network
- Standard patterns how to construct lock script emerged over the time
  - e.g., unlock if signature is verifiable with the public key stored in lock script (P2PK)
  - “Address” is the variable part of the lock script differing between different receivers and transactions
- *Notation warning: scriptSig (script + signature), scriptPubKey (initial meaning script + public key == P2PK)*
- Well-known standard types of lock scripts
  - Pay-to-public-key (P2PK)
  - Pay-to-public-key-hash (P2PKH, starts with 1)
  - Pay-to-script-hash (P2SH, BIP16, starts with 3)
  - OP_RETURN (any data 40B)
  - P2WSH-nested-in-P2SH
  - P2SH-P2WPKH, P2SH-P2WSH
  - Native P2WPK, P2WSH (Bech32, starts with bc1)
  - Pay-to-Taproot (P2TR, Schnorr signature, starts bc1p)



Output Types by Count

Shows the distribution of output types by output count per day.

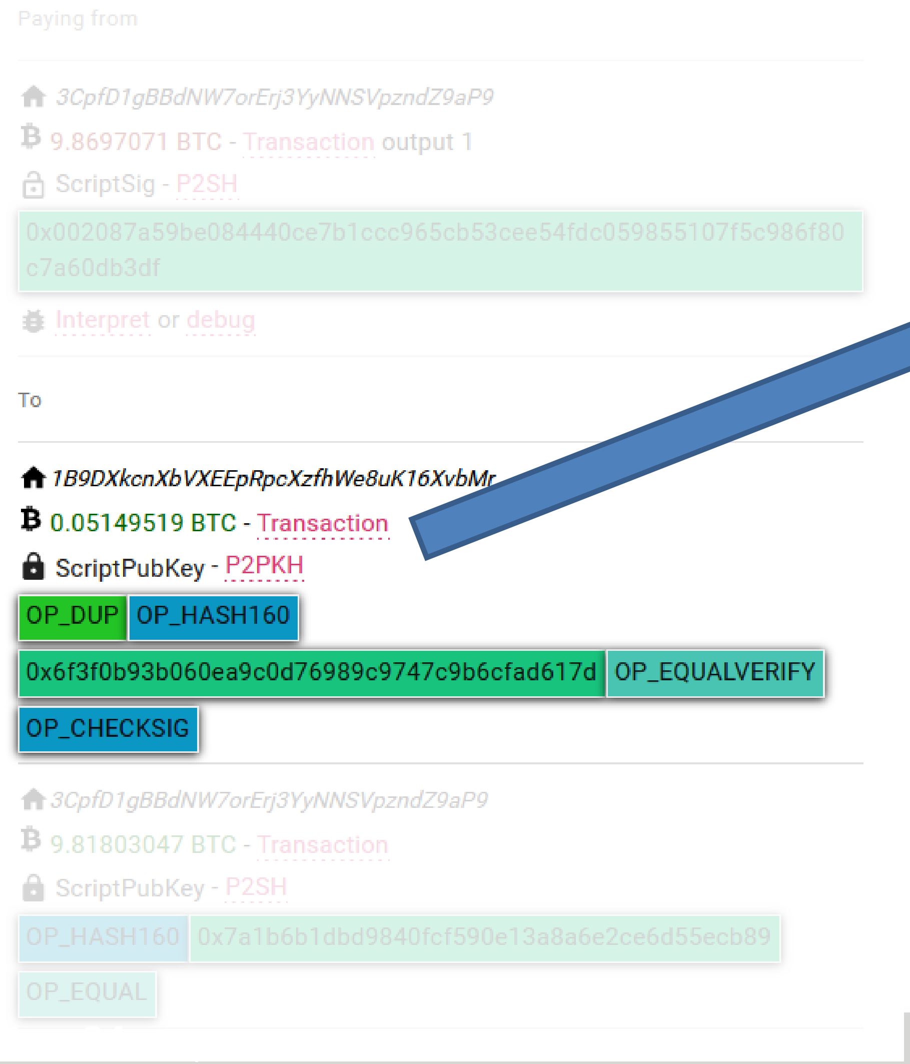
1/9/2009 - 3/28/2022 ☐ step plot ☑ annotations moving average 7 days show permalink

Pay-to-public-key (P2PK)

- Lock script contains direct value of public key and instructions to push signature and verify with the public key
- Used initially by Satoshi and others, now infrequent
- Disadvantage: if practical dlog attack against secp256k1 is found, private key can be computed

https://nioctib.tech/#/transaction/f2f398dace996dab12e0cfb02fb0b59de0ef0398be393d90ebc8ab397550370b
https://nioctib.tech/#/transaction/feff813f13340060f641c11ab1307bb1b8cabcdcc3af1aed8a089e38c8407aef

P2PKH - script execution (https://nioctib.tech/)



Paying from

3CpfD1gBBdNW7orErj3YyNNSVpzndZ9aP9

Ƀ 9.8697071 BTC - Transaction output 1

ScriptSig - P2SH

0x002087a59be084440ce7b1ccc965cb53cee54fdc059855107f5c986f80c7a60db3df

Interpret or debug

To

1B9DXkcnXbVXEEpRpcXzfhWe8uK16XvbMr

Ƀ 0.05149519 BTC - Transaction

ScriptPubKey - P2PKH

OP_DUP OP_HASH160

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d OP_EQUALVERIFY

OP_CHECKSIG

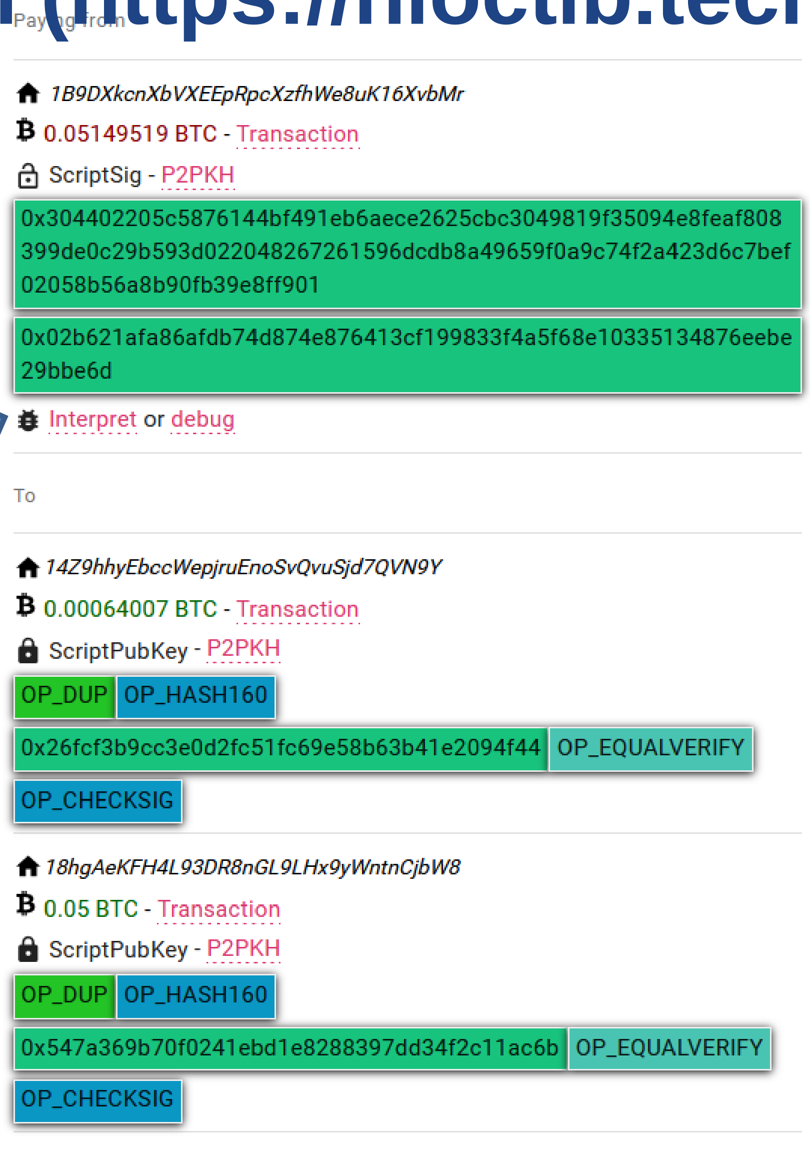
3CpfD1gBBdNW7orErj3YyNNSVpzndZ9aP9

Ƀ 9.81803047 BTC - Transaction

ScriptPubKey - P2SH

OP_HASH160 0x7a1b6b1dbd9840fcf590e13a8a6e2ce6d55ecb89

OP_EQUAL



Paying from

1B9DXkcnXbVXEEpRpcXzfhWe8uK16XvbMr

Ƀ 0.05149519 BTC - Transaction

ScriptSig - P2PKH

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef02058b56a8b90fb39e8ff901

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe29bbe6d

Interpret or debug

To

14Z9hhyEbccWepjruEnoSvQvuSjd7QVN9Y

Ƀ 0.00064007 BTC - Transaction

ScriptPubKey - P2PKH

OP_DUP OP_HASH160

0x26fcf3b9cc3e0d2fc51fc69e58b63b41e2094f44 OP_EQUALVERIFY

OP_CHECKSIG

18hgAeKFH4L93DR8nGL9LHx9yWntnCjbW8

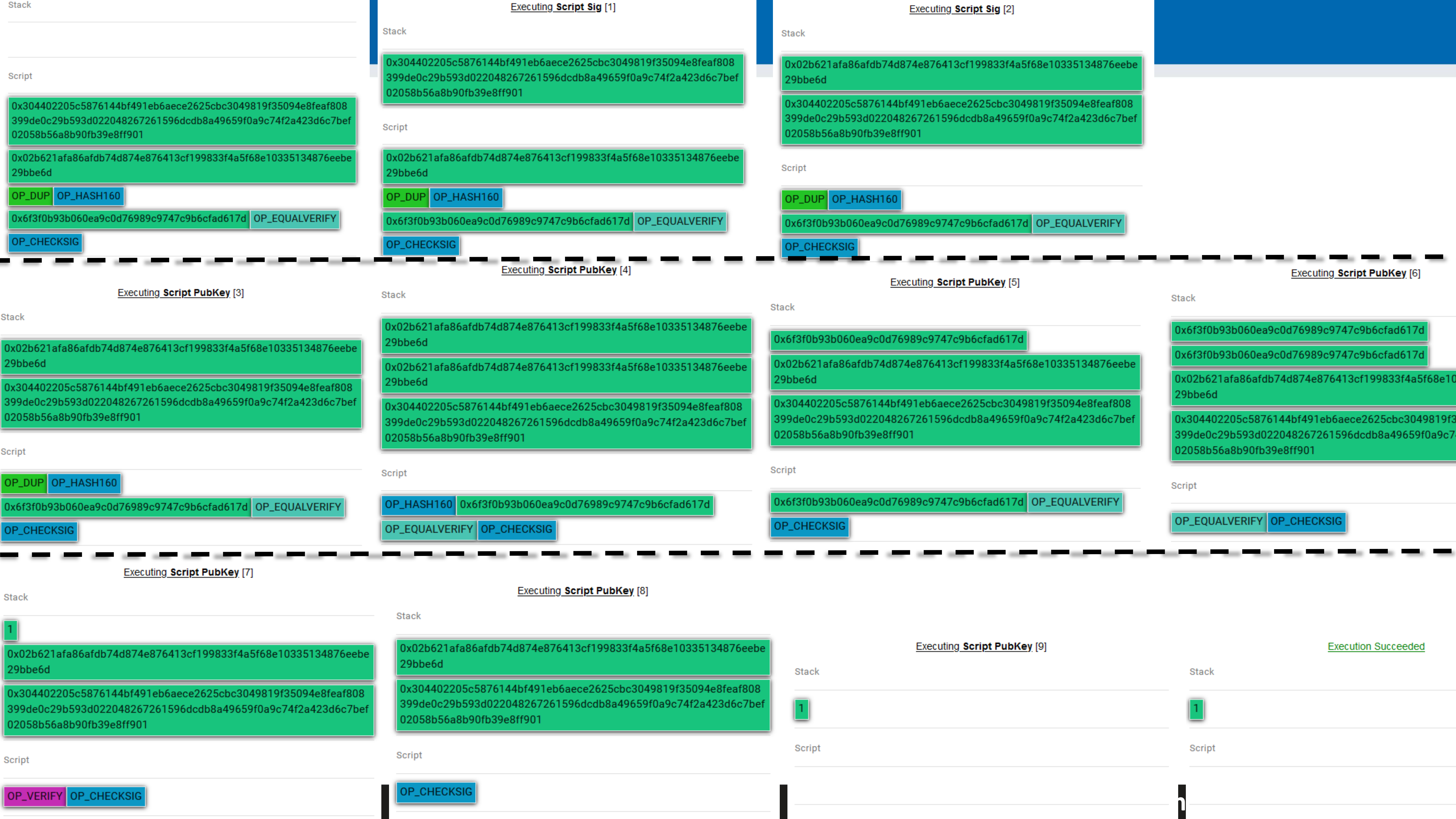
Ƀ 0.05 BTC - Transaction

ScriptPubKey - P2PKH

OP_DUP OP_HASH160

0x547a369b70f0241ebd1e8288397dd34f2c11ac6b OP_EQUALVERIFY

OP_CHECKSIG



Stack

Script

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808
399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef
02058b56a8b90fb39e8ff901

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

OP_DUP OP_HASH160

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d OP_EQUALVERIFY

OP_CHECKSIG

Executing Script Sig [1]

Stack

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808
399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef
02058b56a8b90fb39e8ff901

Script

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

OP_DUP OP_HASH160

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d OP_EQUALVERIFY

OP_CHECKSIG

Executing Script Sig [2]

Stack

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808
399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef
02058b56a8b90fb39e8ff901

Script

OP_DUP OP_HASH160

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d OP_EQUALVERIFY

OP_CHECKSIG

Executing Script PubKey [3]

Stack

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808
399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef
02058b56a8b90fb39e8ff901

Script

OP_DUP OP_HASH160

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d OP_EQUALVERIFY

OP_CHECKSIG

Executing Script PubKey [4]

Stack

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808
399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef
02058b56a8b90fb39e8ff901

Script

OP_HASH160 0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d

OP_EQUALVERIFY OP_CHECKSIG

Executing Script PubKey [5]

Stack

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808
399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef
02058b56a8b90fb39e8ff901

Script

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d OP_EQUALVERIFY

OP_CHECKSIG

Executing Script PubKey [6]

Stack

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d

0x6f3f0b93b060ea9c0d76989c9747c9b6cfad617d

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10
29bbe6d

0x304402205c5876144bf491eb6aece2625cbc3049819f3
399de0c29b593d022048267261596dcdb8a49659f0a9c7
02058b56a8b90fb39e8ff901

Script

OP_EQUALVERIFY OP_CHECKSIG

Executing Script PubKey [7]

Stack

1

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808
399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef
02058b56a8b90fb39e8ff901

Script

OP_VERIFY OP_CHECKSIG

Executing Script PubKey [8]

Stack

0x02b621afa86afdb74d874e876413cf199833f4a5f68e10335134876eebe
29bbe6d

0x304402205c5876144bf491eb6aece2625cbc3049819f35094e8feaf808
399de0c29b593d022048267261596dcdb8a49659f0a9c74f2a423d6c7bef
02058b56a8b90fb39e8ff901

Script

OP_CHECKSIG

Executing Script PubKey [9]

Stack

1

Script

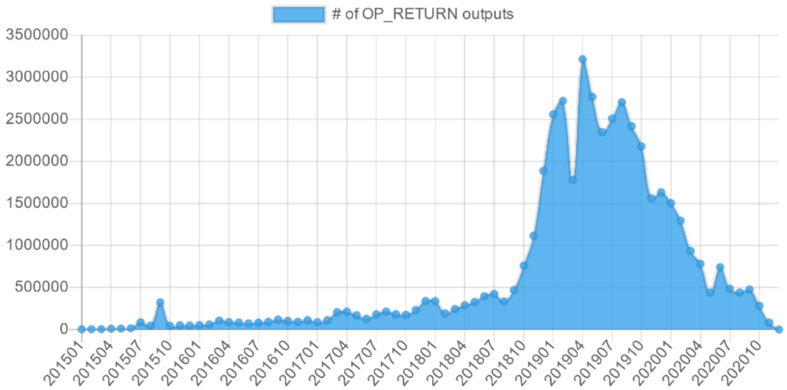
Execution Succeeded

Stack

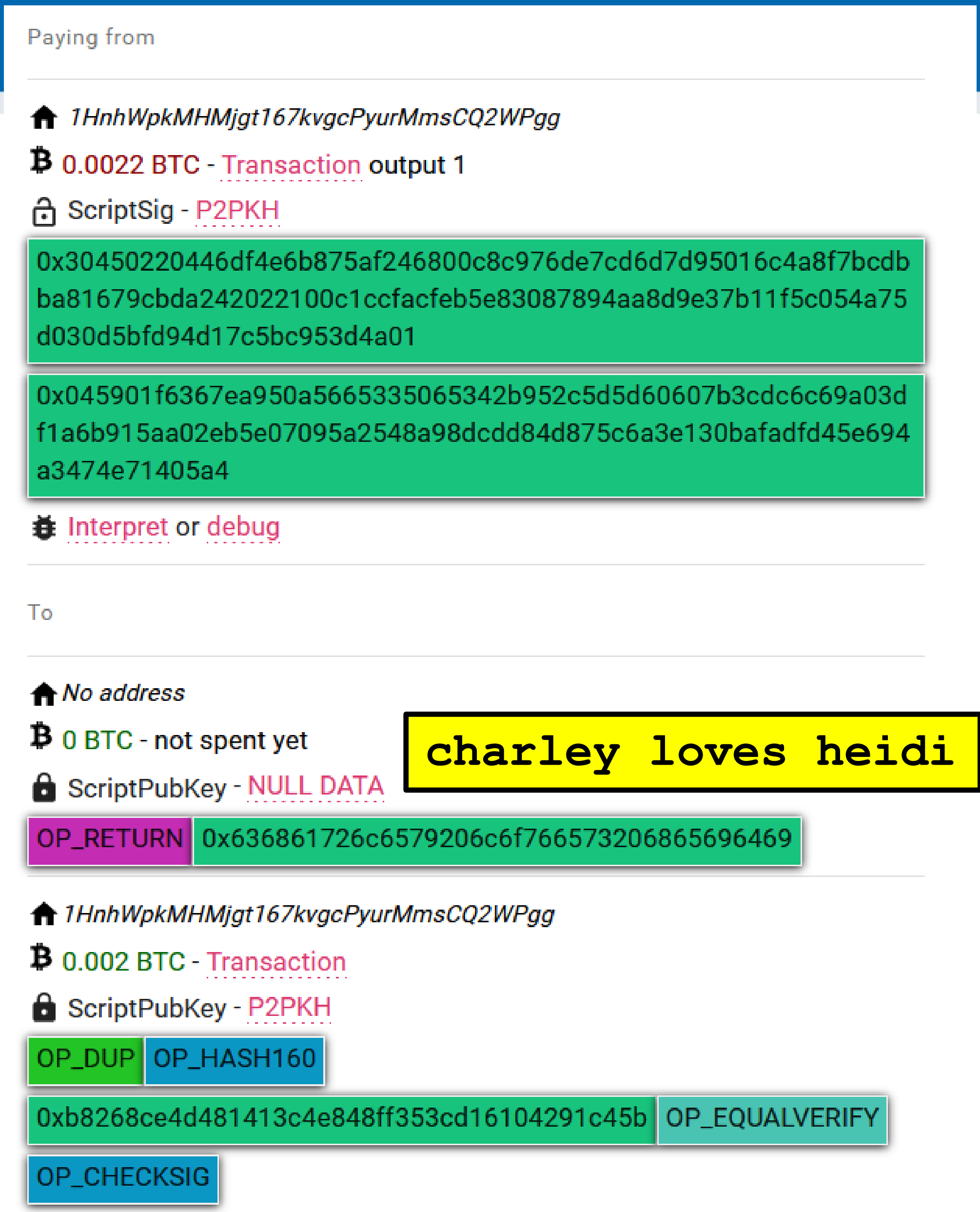
1

Script

OP_RETURN



- If OP_RETURN is encountered during execution of unlock+lock script, it is FALSE
  - Such output is provably unspendable
- Somewhat controversial instruction
  - Some feels, that blockchain shall not be used for non-financial data (USDT was initially on Bitcoin via OP_RETURN)
  - But there were already ways how to store arbitrary data into blockchain anyway (e.g., bytes of value, invalid address)
- Analysis of OP_RETURN data
  - https://www.blockchainresearchlab.org/2020/03/13/how-do-op-return-transactions-impact-bitcoin/
  - https://opreturn.org/



Paying from

1HnhWpkMHMjgt167kvgcPyurMmsCQ2WPgg

Ƀ 0.0022 BTC - Transaction output 1

ScriptSig - P2PKH

0x30450220446df4e6b875af246800c8c976de7cd6d7d95016c4a8f7bcdbba81679cbda242022100c1ccfacfeb5e83087894aa8d9e37b11f5c054a75d030d5bfd94d17c5bc953d4a01

0x045901f6367ea950a5665335065342b952c5d5d60607b3cdc6c69a03df1a6b915aa02eb5e07095a2548a98dcdd84d875c6a3e130bafadfd45e694a3474e71405a4

Interpret or debug

To

No address

Ƀ 0 BTC - not spent yet

ScriptPubKey - NULL DATA

OP_RETURN 0x636861726c6579206c6f76657320686569646469

charley loves heidi

1HnhWpkMHMjgt167kvgcPyurMmsCQ2WPgg

Ƀ 0.002 BTC - Transaction

ScriptPubKey - P2PKH

OP_DUP OP_HASH160

0xb8268ce4d481413c4e848ff353cd16104291c45b OP_EQUALVERIFY

OP_CHECKSIG

https://nioctib.tech/#/transaction/f2f398dace996dab12e0cfb02fb0b59de0ef0398be393d90ebc8ab397550370b

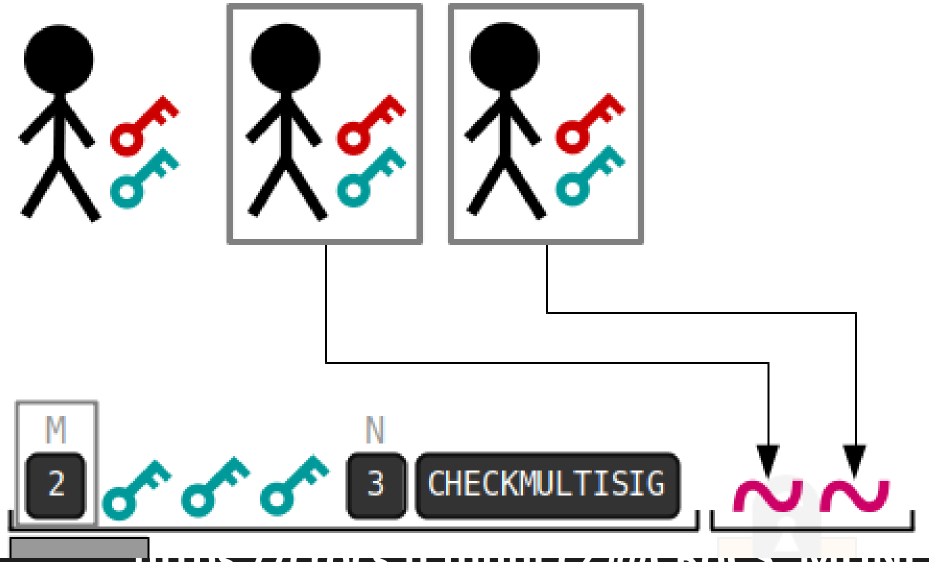
THRESHOLD SIGNATURES VS. MULTISIG VS. MULTI-PARTY COMPUTATION

Shamir 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

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

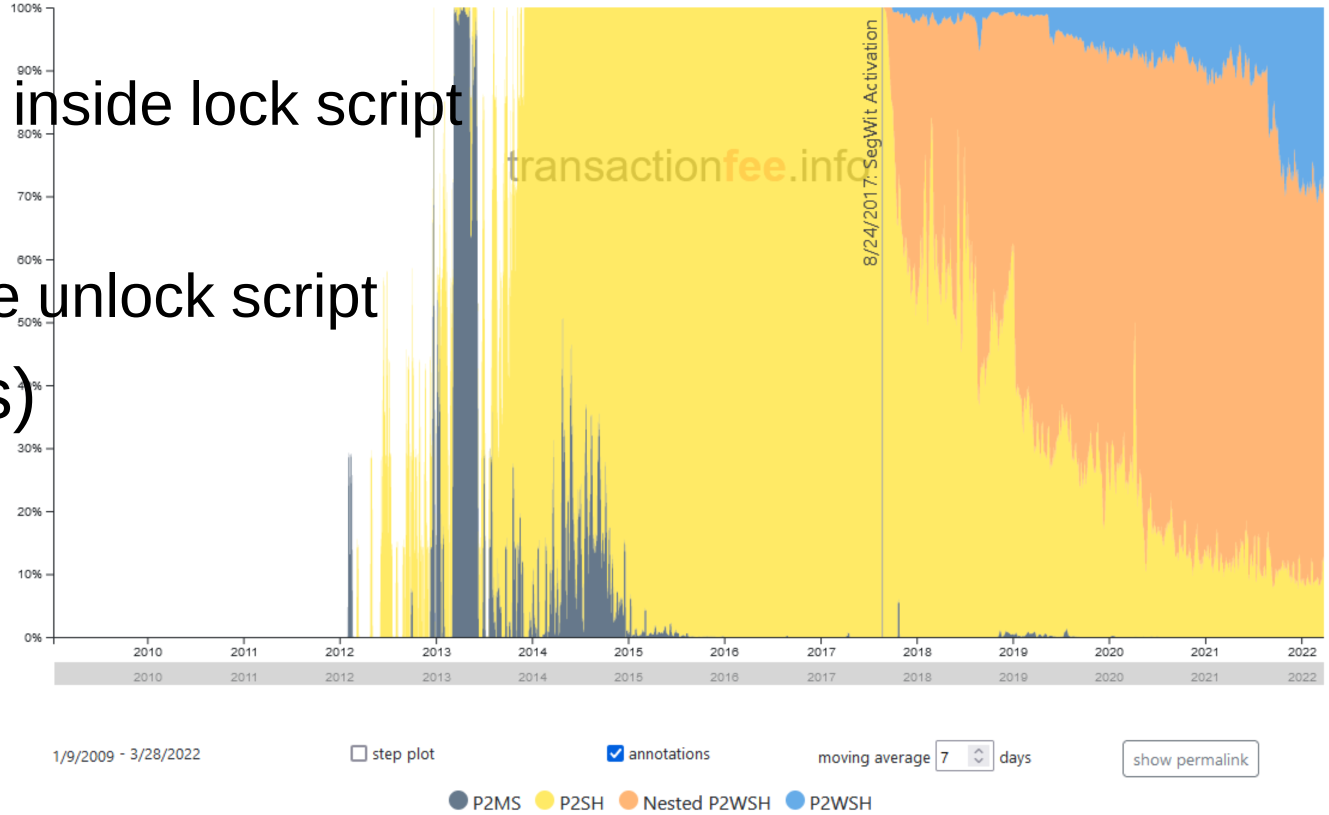


Secure multi-party computation (MPC)

- 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
- 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)



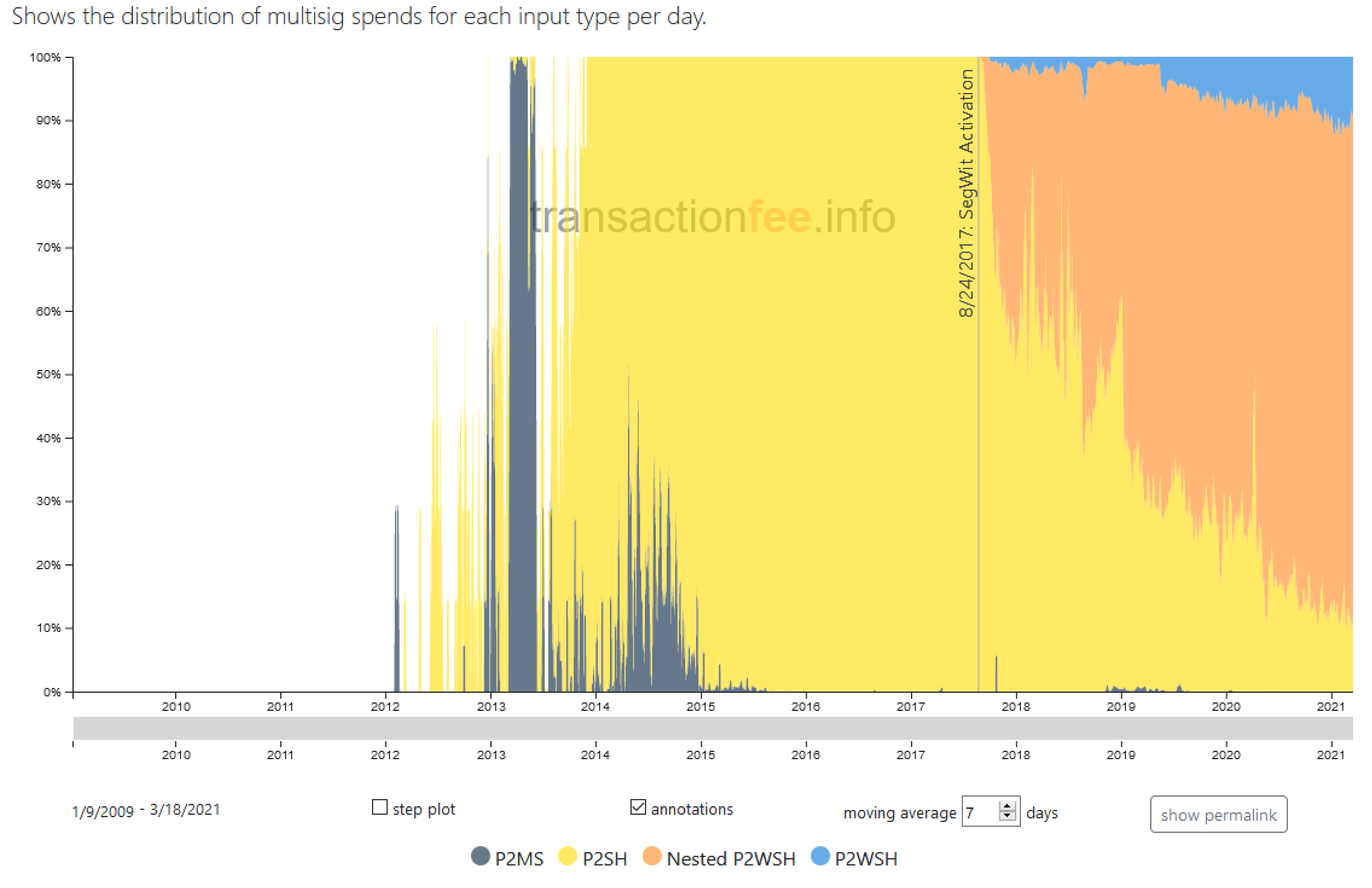
1/9/2009 - 3/28/2022

☐ step plot

☑ annotations

moving average 7 days

Frequency of different multisignature scripts



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

ON-CHAIN BITCOIN ALTERNATIVES

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

- Why something else than on-chain Bitcoin? List of typical “arguments”

1. Cost of sending transaction
   - Peak was tens of dollars (for every transfer), variable (now 1sat/vB), but has to increase in future
2. Time to confirm transaction (+ limited block size)
   - 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
   - Proof of Work is energy intensive

- …

ALTCOINS

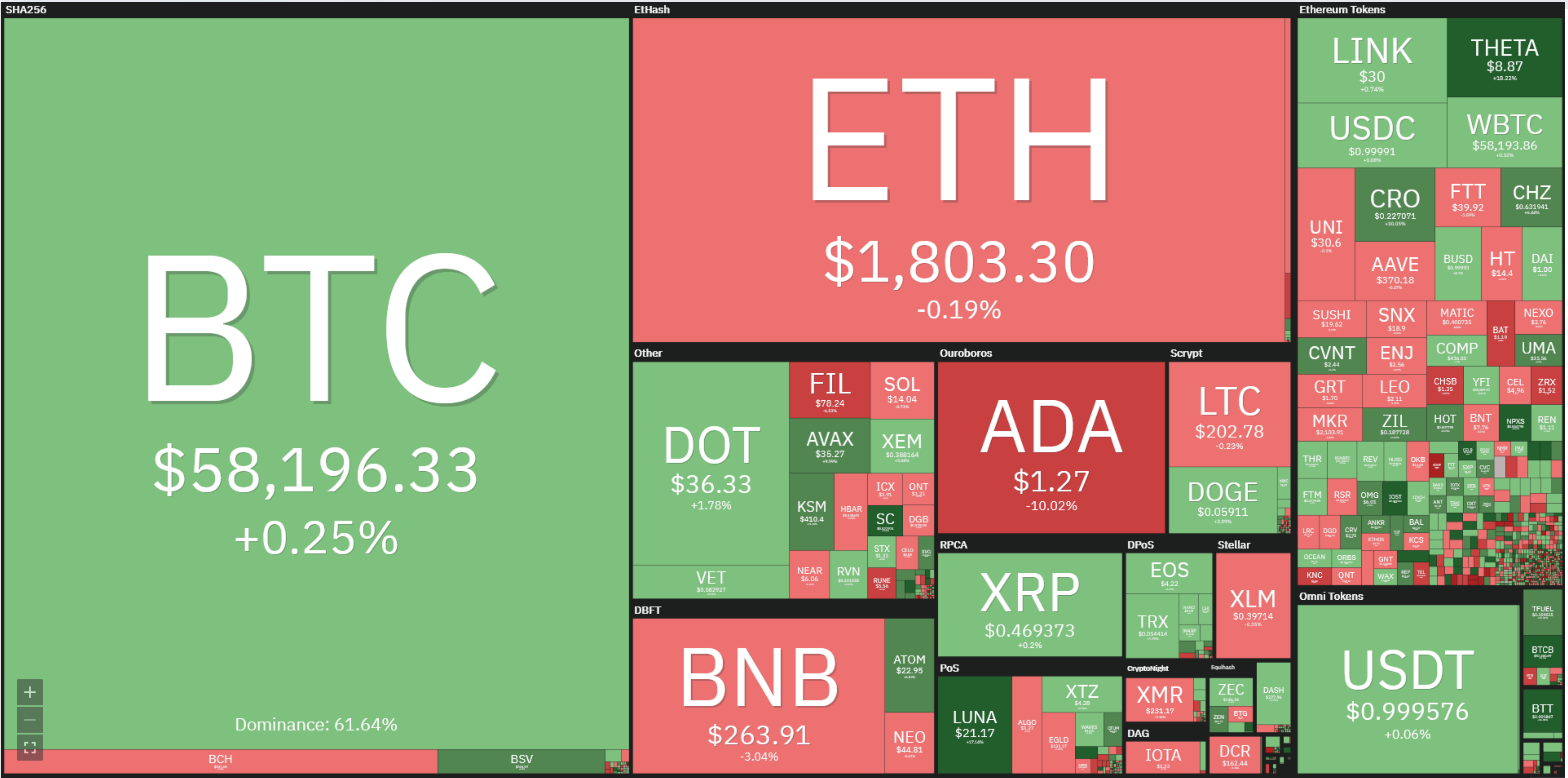
Why other cryptocurrencies (altcoins)

- Why something else than Bitcoin?

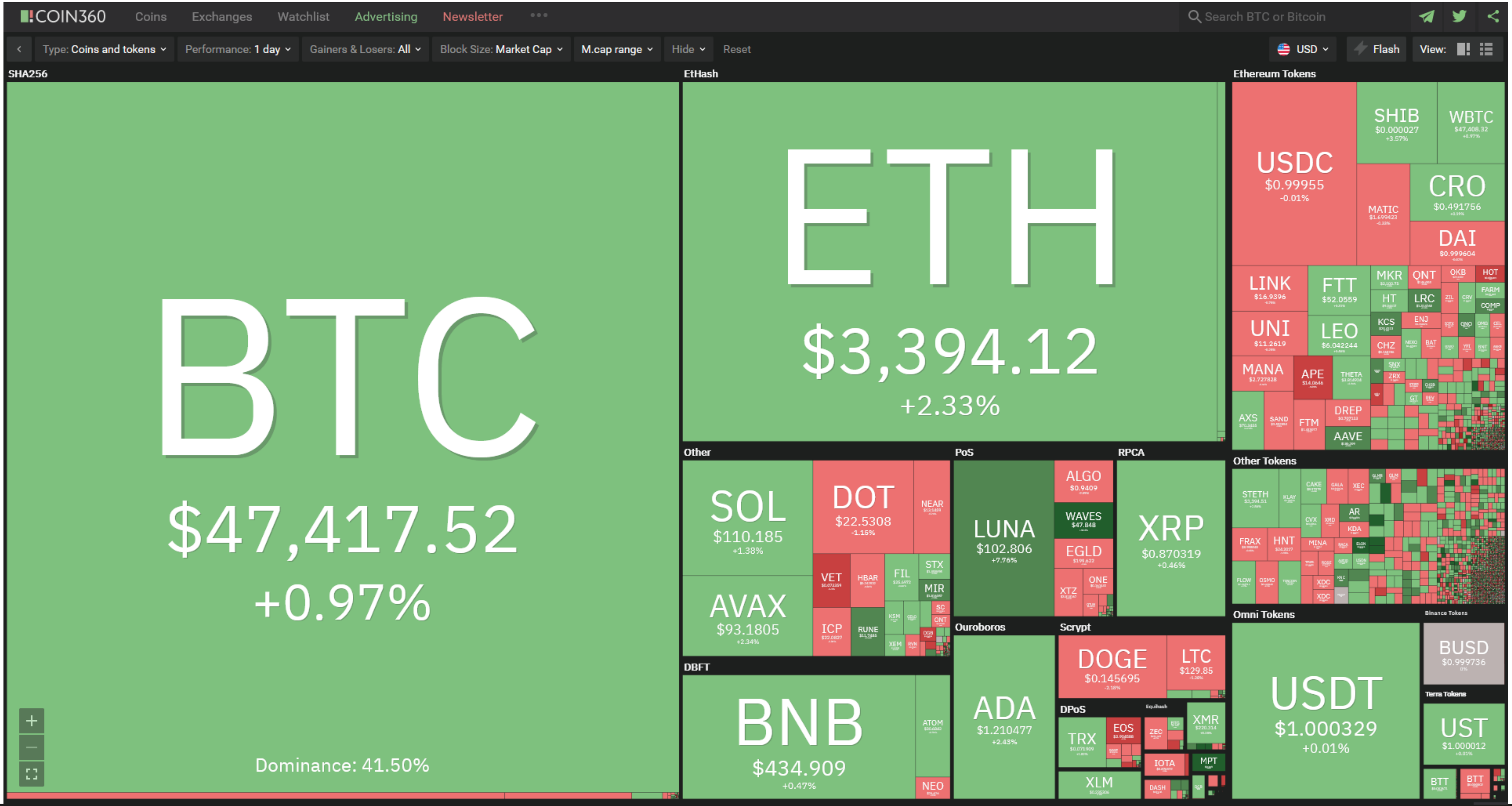
1. Cost of sending transaction
   - Peak was tens of dollars (for every transfer), variable (now 1sat/vB), but has to increase in future
2. Time to confirm transaction (+ limited block size)
   - 4 blocks inside chain commonly required, ~10 minutes per block => ~40 min
3. Traceability of transactions
   - Source, destination and amount is on public ledger
4. Limited scripting language
   - For more complicated smart contracts
5. Specialized mining equipment required
   - Bitcoin mining only possible via ASICs => may cause centralization
   - Proof of Work is energy intensive

- …

April 2021


SHA256
BTC
$58,196.33
+0.25%
Dominance: 61.64%
BCH
BSV
EtHash
ETH
$1,803.30
-0.19%
Ethereum Tokens
LINK
$30
+0.74%
THETA
$8.87
+18.22%
USDC
$0.99991
WBTC
$58,193.86
UNI
$30.6
CRO
$0.227071
FTT
$39.92
CHZ
$0.631941
AAVE
$370.18
BUSD
HT
$14.4
DAI
$1.00
SUSHI
$19.62
SNX
$18.9
MATIC
$0.400735
BAT
$1.19
NEXO
$2.76
CVNT
$2.44
ENJ
$2.56
COMP
$436.03
UMA
$25.56
GRT
$1.70
LEO
$2.11
CHSB
$1.35
YFI
CEL
$4.96
ZRX
$1.52
MKR
$2,103.91
ZIL
$0.187728
HOT
BNT
$7.76
NPXS
REN
$1.11
THR
REV
OKB
FTM
RSR
OMG
$6.01
IOST
LRC
DGD
CRV
ANKR
BAL
KCS
OCEAN
ORBS
GNT
KNC
QNT
WAX
REP
TEL
Other
DOT
$36.33
+1.78%
VET
$0.082927
FIL
$78.24
SOL
$14.04
AVAX
$35.27
XEM
$0.388164
KSM
$410.4
HBAR
ICX
$1.91
ONT
$1.21
SC
DGB
STX
$1.32
CELO
NEAR
$6.06
RVN
RUNE
$5.56
Ouroboros
ADA
$1.27
-10.02%
Scrypt
LTC
$202.78
-0.23%
DOGE
$0.05911
RPCA
XRP
$0.469373
+0.2%
DPoS
EOS
$4.22
TRX
$0.054414
Stellar
XLM
$0.39714
-0.35%
DBFT
BNB
$263.91
-3.04%
ATOM
$22.95
NEO
$44.81
PoS
LUNA
$21.17
ALGO
$1.27
XTZ
$4.28
WAVES
EGLD
$132.17
CryptoNight
XMR
$231.17
Equihash
ZEC
ZEN
BTG
DASH
DAG
IOTA
$1.32
DCR
$162.44
Omni Tokens
USDT
$0.999576
+0.06%
TFUEL
BTCB
BTT
+
−

Coin mining algorithm https://coin360.com/



Type: Coins and tokens

Performance: 1 day

Gainers & Losers: All

Block Size: Market Cap

M.cap range

Hide

Reset

USD

Flash

View:

Search BTC or Bitcoin

Other cryptocurrencies (altcoins)

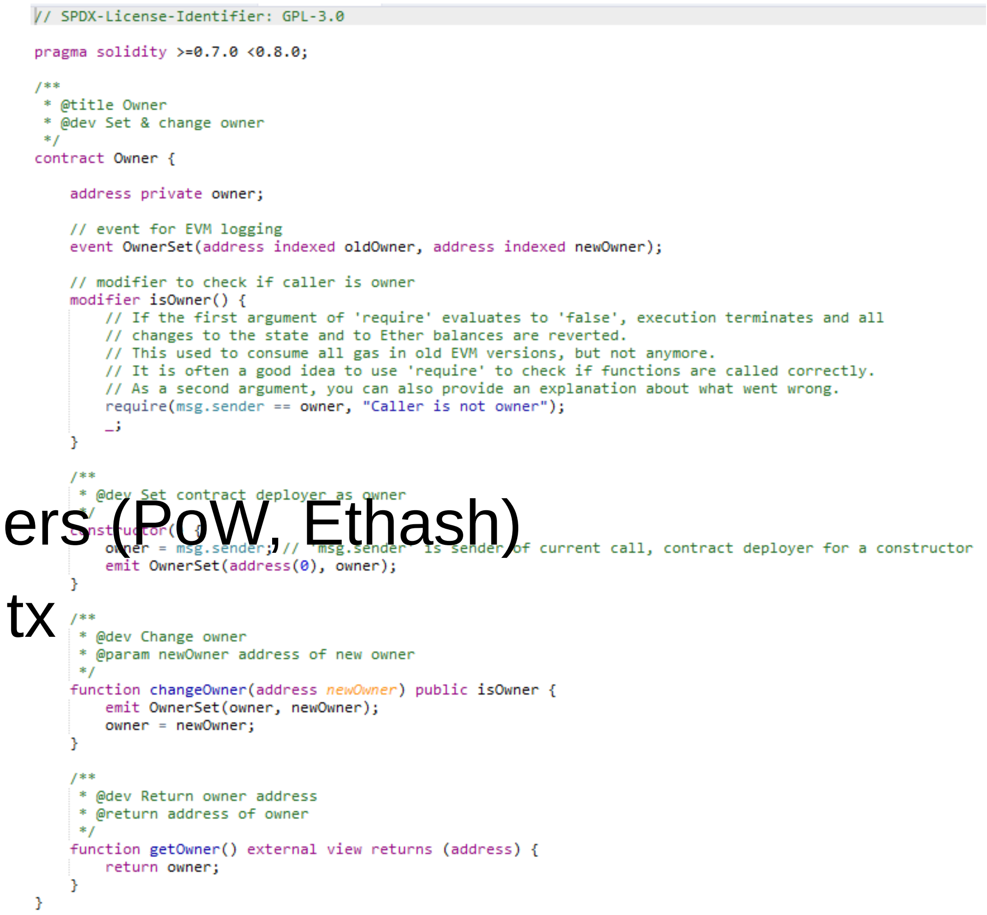
- Copycats (huge number of them)
  - Take Bitcoin’s source code, change name and basic params (mining alg, time and size of block…)
  - E.g., Litecoin
- Bitcoin-style, but adding some distinct features
  - Ethereum: Turing-complete scripting for smart contracts, (EthHash mining alg), Eth2.0 move to PoS
  - Zcash: zero-knowledge proof for sender/receiver/amount (shielded transactions), aim to have GPU-friendly mining (Equihash, large memory required)
  - Monero: private transactions via mixing (Ring Confidential Transactions, CryptoNote)
- More traditional styles (Ripple, Stellar…)
  - Somewhat decentralized network of verification nodes (=> faster and cheaper txs)
  - Typically, less privacy and overall resilience against central control
- Stable coins (USDT, USDC…)
  - Idea: digital equivalent to real dollars stored in “safe”
  - New 1 USDT is created when someone deposits $1 to company, destroyed when $1 is cashed back

Tokens, ICO, DeFi, CBDC…

- Initial Coin Offerings (ICO), boom in 2017
  - Kind of crowdfunding campaign - often via Ethereum smart contracts, ERC-20 contracts
  - Frequently scam, frequently large pre-allocation to founders and investors
- Decentralized Finance (DeFi)
  - Smart contract with defined (financial-related) behavior – e.g., lending…
- Non-fungible tokens
  - Representation of physical item on the blockchain
  - Allows to pass ownership by “sending” token to another person
  - Possible on almost any chain (colored coins at Bitcoin)
  - Some chains build for it intentionally
- Central bank digital currency (CBDC)
  - Permissioned ledger by central banks

Ethereum basics

- Basic idea: Make script Turing complete
  - Executed by Ethereum Virtual Machine
  - 256-bit register stack
- Ether (ETH) is native currency rewarded to miners (PoW, Ethash)
- Gas is transaction fee payed to miners for new tx
- Block time is 13 seconds on average
  - But Difficulty bomb to force periodic protocol updates
- Two types of accounts: users and contracts
- See some example eth scripts https://remix.ethereum.org/
- Mastering Ethereum, A. Antonopoulos, https://github.com/ethereumbook/ethereumbook



```
// SPDX-License-Identifier: GPL-3.0

pragma solidity >=0.7.0 <0.8.0;

/**
 * @title Owner
 * @dev Set & change owner
 */
contract Owner {

    address private owner;

    // event for EVM logging
    event OwnerSet(address indexed oldOwner, address indexed newOwner);

    // modifier to check if caller is owner
    modifier isOwner() {
        // If the first argument of 'require' evaluates to 'false', execution terminates and all
        // changes to the state and to Ether balances are reverted.
        // This used to consume all gas in old EVM versions, but not anymore.
        // It is often a good idea to use 'require' to check if functions are called correctly.
        // As a second argument, you can also provide an explanation about what went wrong.
        require(msg.sender == owner, "Caller is not owner");
        _;
    }

    /**
     * @dev Set contract deployer as owner
     */
    constructor() {
        owner = msg.sender; // 'msg.sender' is sender of current call, contract deployer for a constructor
        emit OwnerSet(address(0), owner);
    }

    /**
     * @dev Change owner
     * @param newOwner address of new owner
     */
    function changeOwner(address newOwner) public isOwner {
        emit OwnerSet(owner, newOwner);
        owner = newOwner;
    }

    /**
     * @dev Return owner address
     * @return address of owner
     */
    function getOwner() external view returns (address) {
        return owner;
    }
}
```

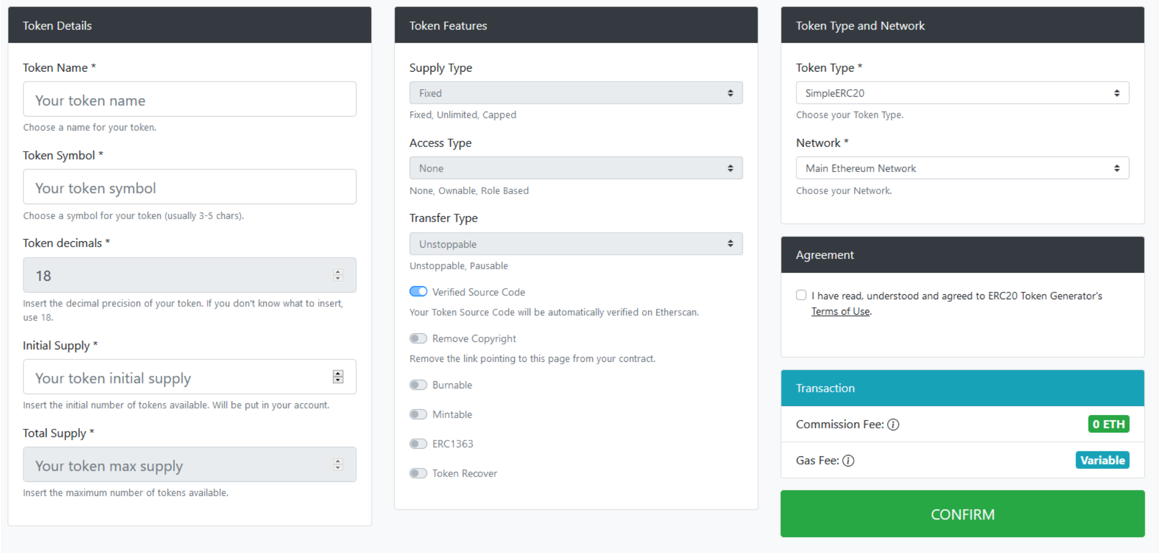
ERC-20 tokens

- Defined in EIP20 (Eth. Improvements Proposals):
  - https://ethereum.org/en/developers/docs/standards/tokens/erc-20/
- API for tokens within Smart Contracts
  - template contract implementations exists
    - https://academy.binance.com/en/articles/an-introduction-to-erc-20-tokens
  - you need to have ETH on your balance to send/exchange ERC20 ETH tokens (for GAS)
  - to move ERC-20 tokens, user creates and send (ethereum) transaction to the contract asking it to allocate some of the balance elsewhere
- No sending of ether, but Gas required for inclusion of transaction with script or interaction with script into blockchain

STARTING NEW COIN

Create own ERC-20 token

- Create own ERC-20 token: https://vittominacori.github.io/erc20-generator/



Token Details

Token Name *
Your token name
Choose a name for your token.

Token Symbol *
Your token symbol
Choose a symbol for your token (usually 3-5 chars).

Token decimals *
18
Insert the decimal precision of your token. If you don't know what to insert, use 18.

Initial Supply *
Your token initial supply
Insert the initial number of tokens available. Will be put in your account.

Total Supply *
Your token max supply
Insert the maximum number of tokens available.

Token Features

Supply Type
Fixed
Fixed, Unlimited, Capped

Access Type
None
None, Ownable, Role Based

Transfer Type
Unstoppable
Unstoppable, Pausable

● Verified Source Code
Your Token Source Code will be automatically verified on Etherscan.

○ Remove Copyright
Remove the link pointing to this page from your contract.

○ Burnable

○ Mintable

○ ERC1363

○ Token Recover

Token Type and Network

Token Type *
SimpleERC20
Choose your Token Type.

Network *
Main Ethereum Network
Choose your Network.

Agreement

□ I have read, understood and agreed to ERC20 Token Generator's Terms of Use.

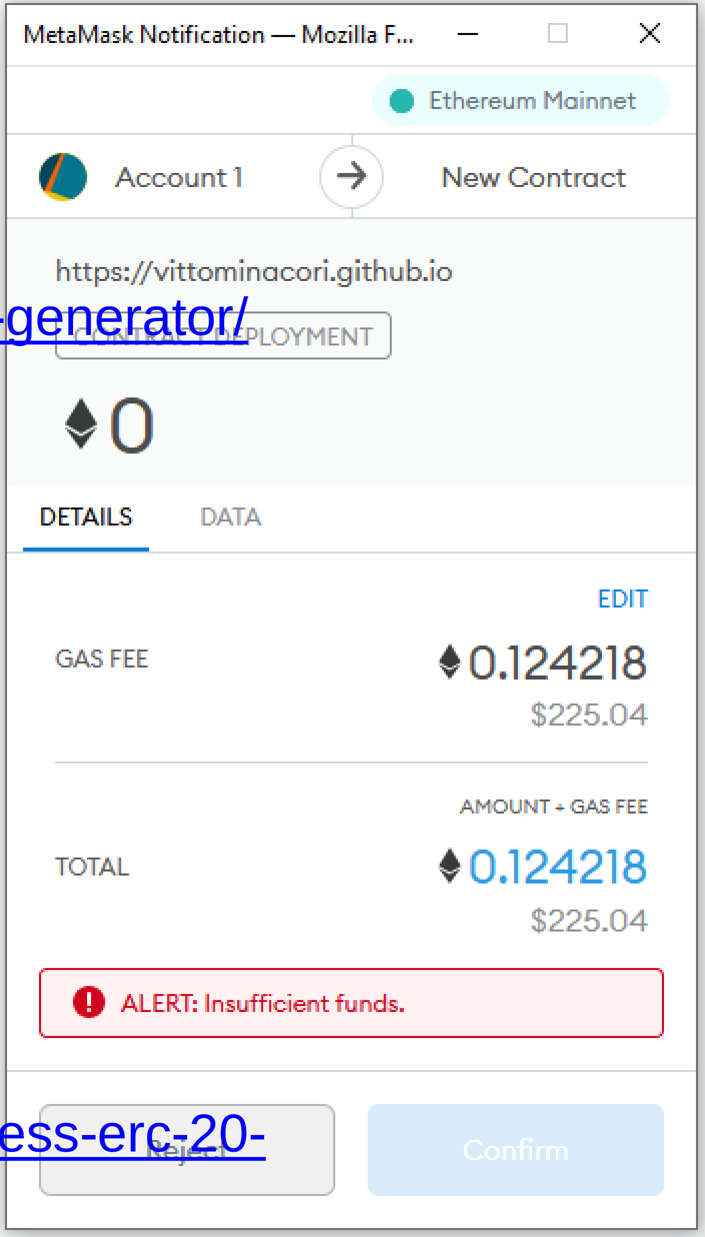
Transaction

Commission Fee: ⓘ 0 ETH

Gas Fee: ⓘ Variable

CONFIRM

- As a result, creating token with no value is very easy
  - https://medium.com/blocktoken/how-to-launch-your-very-own-useless-erc-20-token-cfdb4100fc1d



MetaMask Notification — Mozilla F...

Ethereum Mainnet

Account 1 → New Contract

https://vittominacori.github.io

CONTRACT DEPLOYMENT

0

DETAILS DATA

EDIT

GAS FEE 0.124218
$225.04

AMOUNT + GAS FEE

TOTAL 0.124218
$225.04

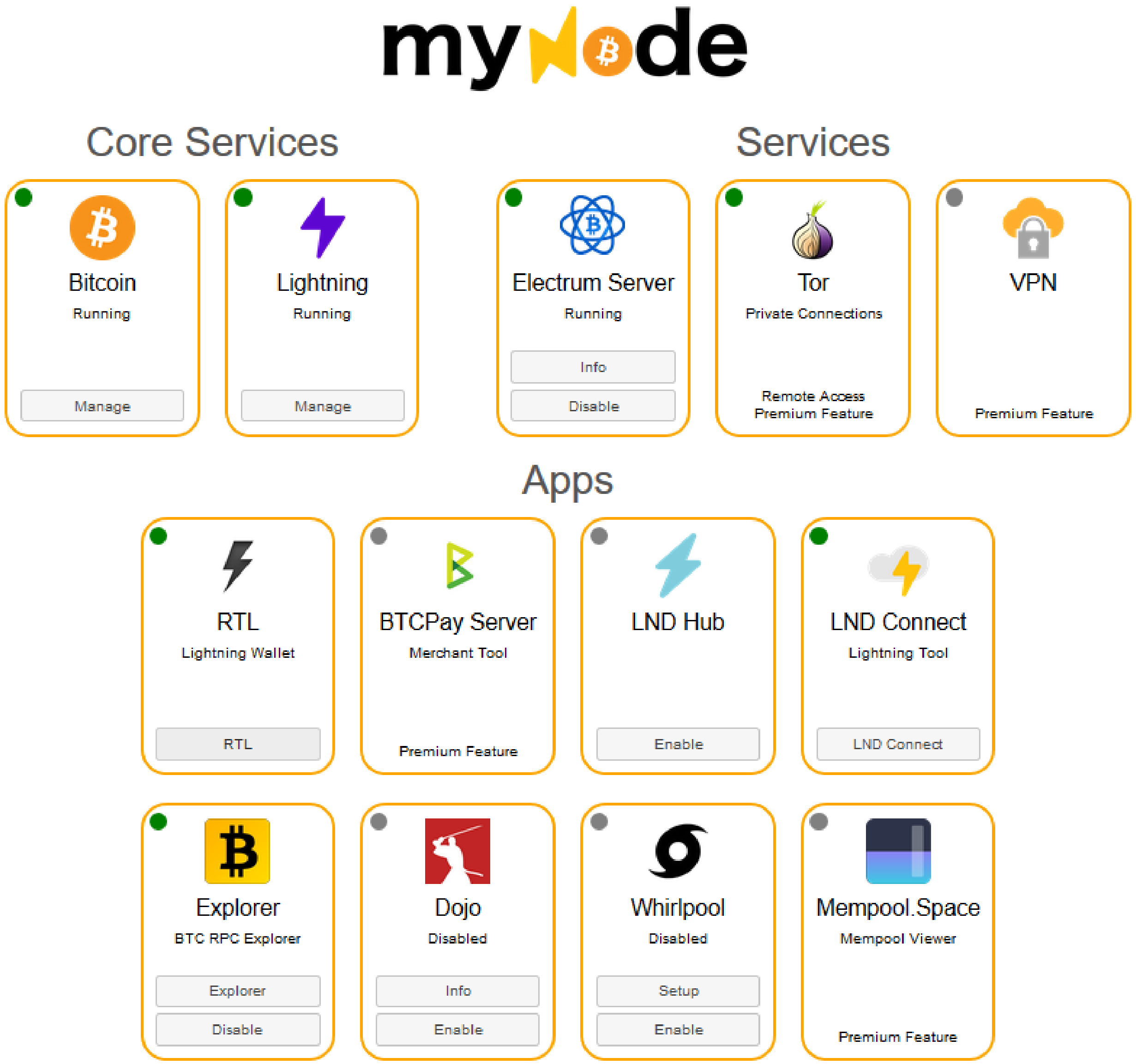
ALERT: Insufficient funds.

Starting new cryptocoin?

- Own chain or atop existing (e.g., ERC-20)?
- Consensus algorithm, cryptography used (e.g., ECDSA vs. Ed25519)
- Parameters of blockchain (fixed size vs. larger vs. flexible)
- Monetary policy
  - Total coins cap (fixed cap, fixed inflation, variable, stablecoins)
  - Starting conditions: bitcoin-like, premine, hidden premine, fixed mining fraction for development foundation…
- Community (serious vs. friendly), promotions
- Level of centralization
  - also influenced by other parameters – size of chain, type of consensus…
- Attitude towards hardforks vs. softforks (fixed policy vs. changing)
- Transactions on-chain or support for second-layer networks?

RUNNING OWN FULL NODE

https://mynodebtc.com



mynode

Core Services

Bitcoin
Running
Manage

Lightning
Running
Manage

Services

Electrum Server
Running
Info
Disable

Tor
Private Connections
Remote Access Premium Feature

VPN
Premium Feature

Apps

RTL
Lightning Wallet
RTL

BTCPay Server
Merchant Tool
Premium Feature

LND Hub
Enable

LND Connect
Lightning Tool
LND Connect

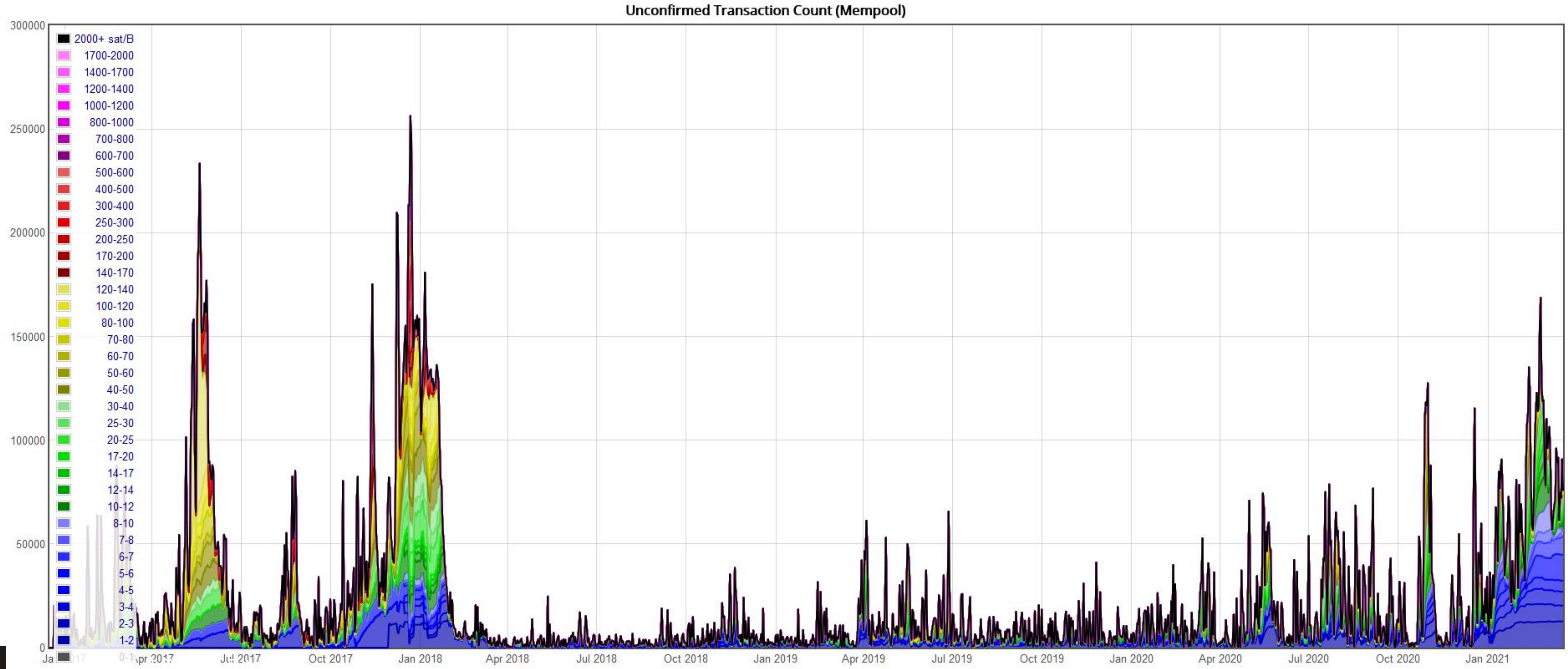
Explorer
BTC RPC Explorer
Explorer
Disable

Dojo
Disabled
Info
Enable

Whirlpool
Disabled
Setup
Enable

Mempool.Space
Mempool Viewer
Premium Feature

Mempool statistics https://jochen-hoenicke.de/queue



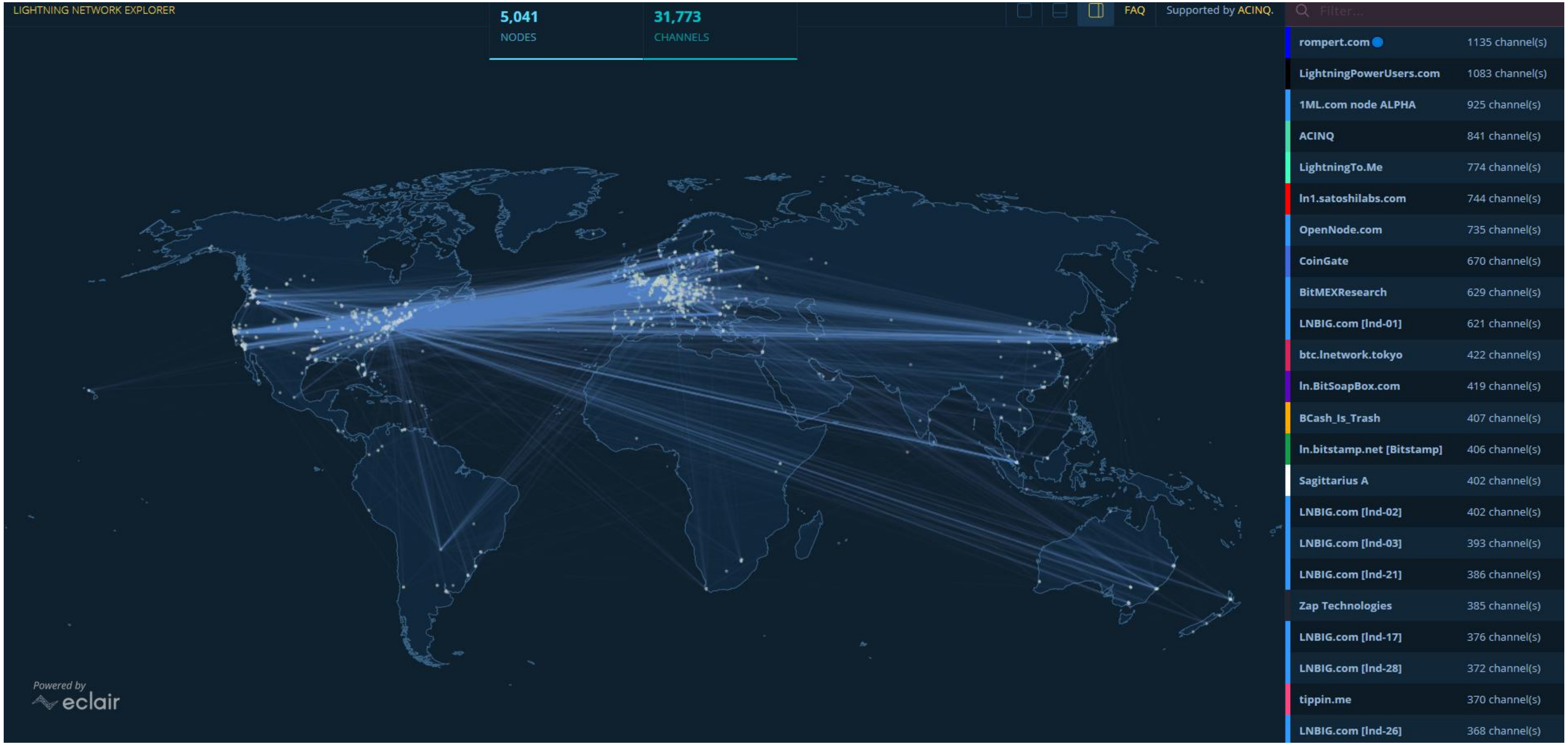
Operating own Bitcoin full node with Lighting

- Download presync part of blockchain from other mynodes (2 days)
- Download the rest of blocks from Bitcoin P2P network (1-2 days)
- Enable Lighting, create new wallet, send some sats to it (on-chain)
- Download Lighting wallet (e.g., BlueWallet, Zap)
- Pair Lighting wallet with your node
- Open channel to some other node
  - E.g., Lightning Node Suggestions at https://store.blockstream.com/
  - Opening channel performs one on-chain transaction

- *Analyze all other options in mynodebtc web GUI!*
- *Enable Electrum Server, Enable BTC RPC Explorer, Browse transactions…*

IF YOU LIKE TO DIG DEEPER (AND LIGHTER)

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



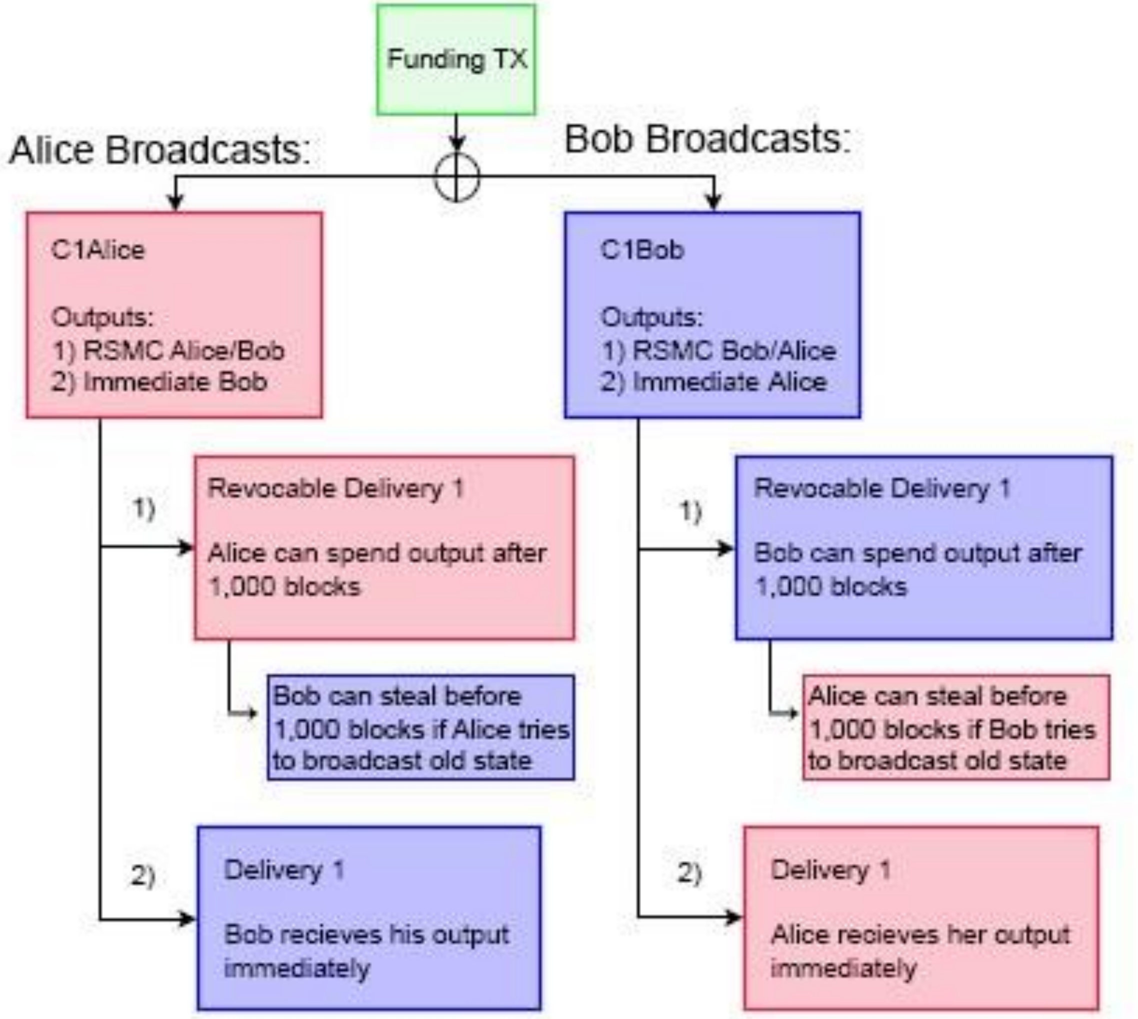
LIGHTNING NETWORK EXPLORER

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

https://blog.usejournal.com/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.

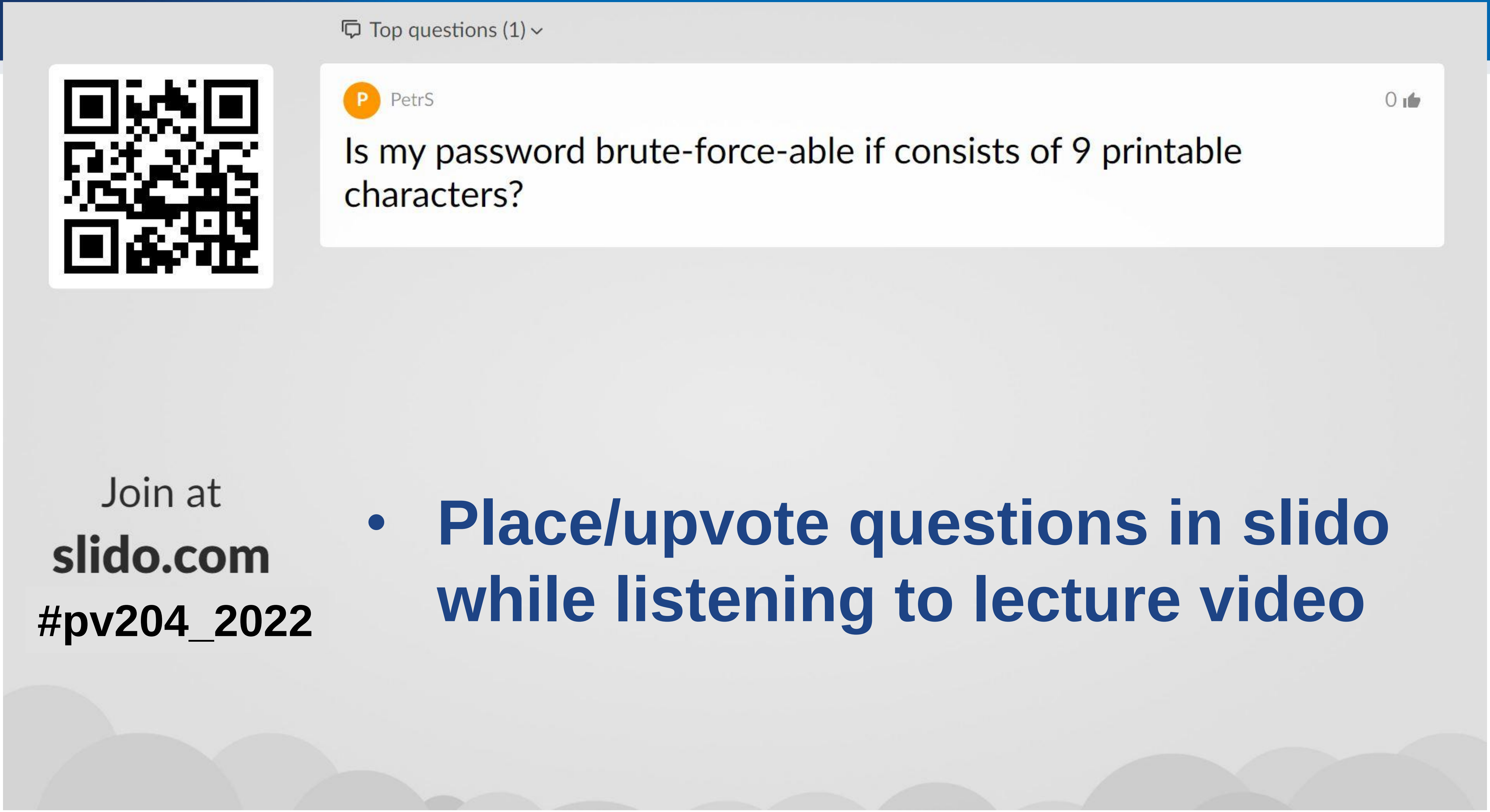
- Sentinel service
  - trustless blockchain observer, broadcasts justice transaction in case of old state detected
  - No need for your full node to be always online
- Privacy considerations
  - Most of the transactions are NOT recorded on the blockchain
    - Good for speed as well as privacy
  - Doesn’t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

Lightning network – study more

- Description of Lighting Network basic principles
  - https://blog.usejournal.com/the-bitcoin-lightning-network-a-technical-primer-d8e073f2a82f
- Presentation by original Lighting creators
  - https://lightning.network/lightning-network.pdf
- List of Lighting nodes ready for channel opening
  - Bottom of the https://store.blockstream.com/

Further reading

- Mastering Bitcoin (Andreas M. Antonopoulos and others)
  - https://github.com/bitcoinbook/bitcoinbook
- List of interesting resources
  - https://blockonomi.com/bitcoin-educational-resources/
  - https://learnmeabitcoin.com/, https://learnmeabitcoin.com/technical/



Top questions (1)

PetrS

0

Is my password brute-force-able if consists of 9 printable characters?

Join at

slido.com

#pv204_2022

- **Place/upvote questions in slido while listening to lecture video**