Bitcoin Security Cryptography

757BTC

https://www.757btc.org/

Topics

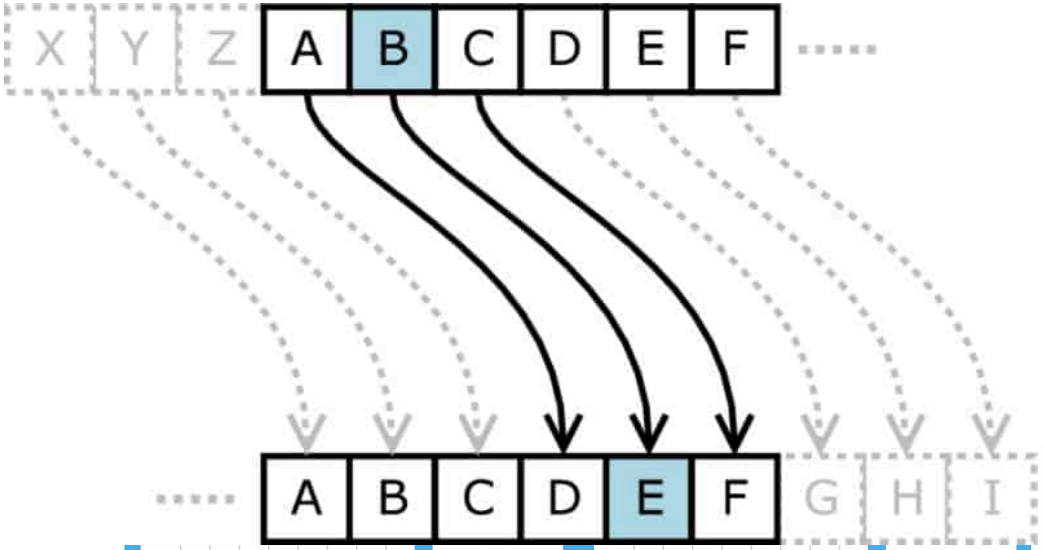
- Cyber-Security
- Cryptography
- Why Should I Care?
- Two Main Functions
- Demonstrate
- Common Fears

Cybersecurity

- CIA Triad
- Availability
  - System being online and available
  - Common attack is denial of service (DOS)
- Integrity
  - System being dependable or unchanged
  - Common attack is man in the middle or database hacks
- Confidentiality
  - Privacy
  - Common attacks data leakage, man in the middle, database hacks

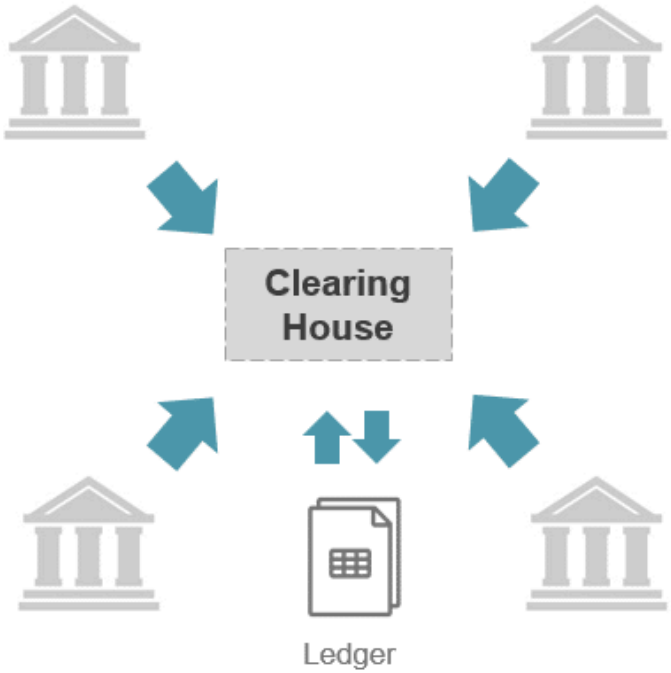
Cryptography

- The algorithmic means to hide information
  - Mathematical in approach
- Availability (proof of work)
- Integrity (hash function)
- Confidentiality (encryption)

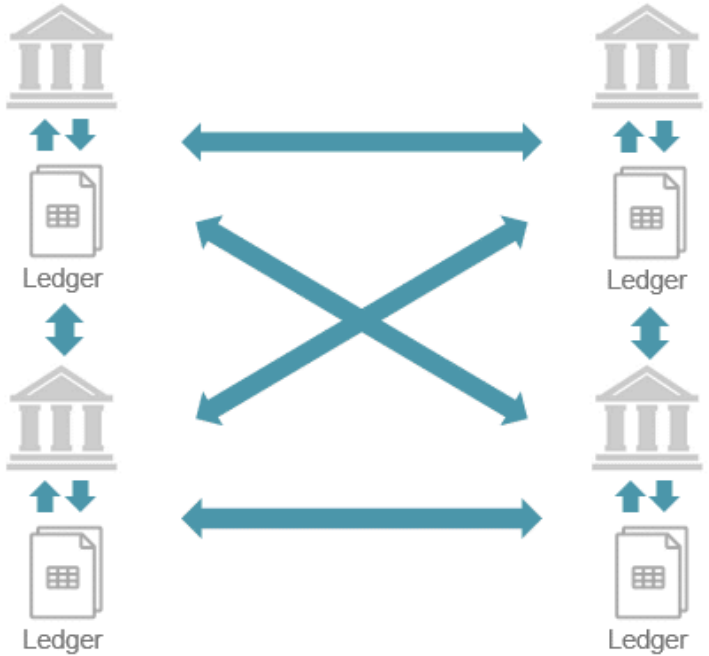


C	0	1	0	0	0	0	1	1	01000011	P	0	1	0	1	0	0	0	0	01010000
D	0	1	0	0	0	1	0	0	01000100	Q	0	1	0	1	0	0	0	1	01010001
E	0	1	0	0	0	1	0	1	01000101	R	0	1	0	1	0	0	1	0	01010010
F	0	1	0	0	0	1	1	0	01000110	S	0	1	0	1	0	0	1	1	01010011
G	0	1	0	0	0	1	1	1	01000111	T	0	1	0	1	0	1	0	0	01010100
H	0	1	0	0	1	0	0	0	01001000	U	0	1	0	1	0	1	0	1	01010101
I	0	1	0	0	1	0	0	1	01001001	V	0	1	0	1	0	1	1	0	01010110
J	0	1	0	0	1	0	1	0	01001010	W	0	1	0	1	0	1	1	1	01010111
K	0	1	0	0	1	0	1	1	01001011	X	0	1	0	1	1	0	0	0	01011000
L	0	1	0	0	1	1	0	0	01001100	Y	0	1	0	1	1	0	0	1	01011001
M	0	1	0	0	1	1	0	1	01001101	Z	0	1	0	1	1	0	1	0	01011010

Why should I care?

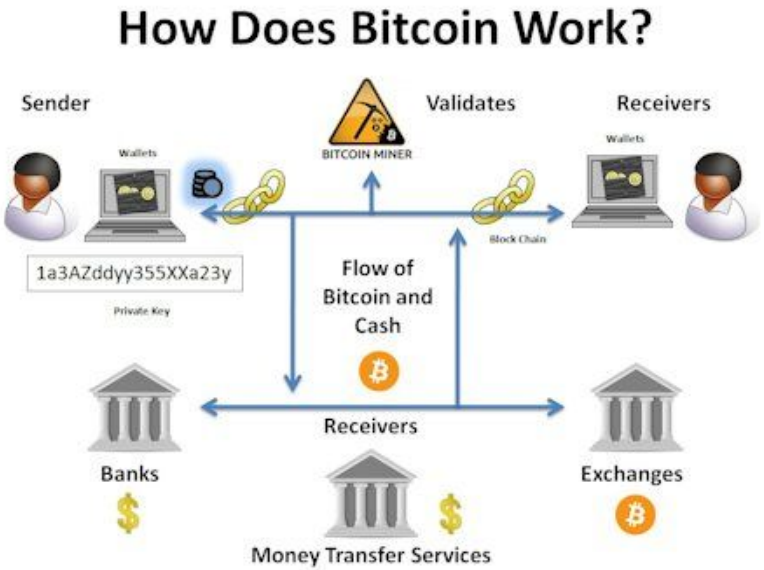


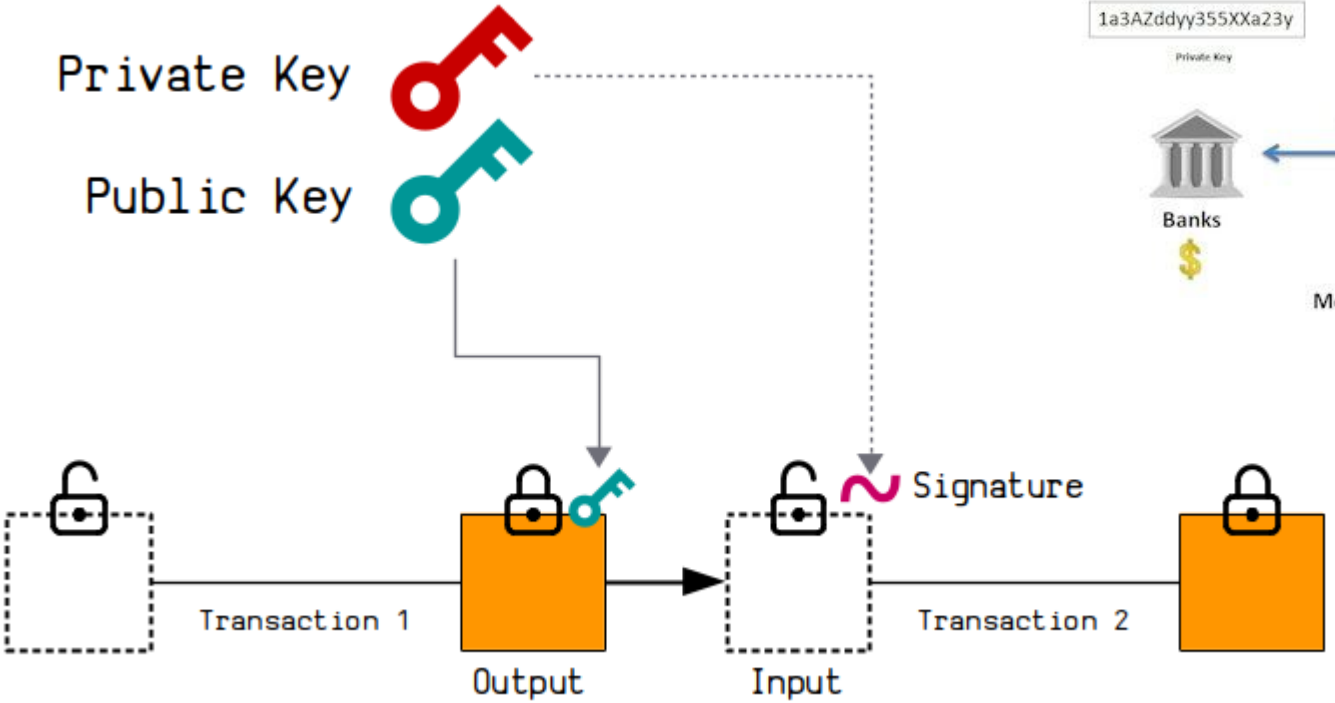
Centralized Model



Decentralized Model

Prove you control an address





Two main functions of cryptography

Digital Fingerprints

- Unchanged information
- Hash function

Digital Signatures

- ownership/authentication
- Public Private Keys

Entropy and key generation

3blue1brown

https://youtu.be/S9JGmA5_unY

```
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCDV8iNtW
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCDVDnfWG
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCDKcGBFx
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCDnkZFsr
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCDsRQpCy
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCE3t3X2L
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCE96xP4a
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCEGyFYbS
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCEKNyeW8
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCEkbag48
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCEcGhK6m
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCEiFMfAe
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCEnKipMg
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCExBhDCF
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCF3ZywyD
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCFALHvvr
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCFHrNYnn
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCFLeB6GA
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCFUCi1pg
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCFdey9Hq
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCFgkr1h9
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCFncsZoe
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCFxeXZbP
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCG7qEqQ6
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCGCbvdiR
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCGKiQJnn
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCGMZ2esz
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCGUguubp
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCGduVboU
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCGoDA2tr
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCGrocM3Y
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCGwqrs7B
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCH3kGQPg
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCHDE5bpg
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCHHn2wsy
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCHNks1WQ
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCHa6uhpp
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCHbhJpkU
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCHkD4PQT
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCHvpoq7o
0 btc (0 tx)  5Hx2jCbLwqWgJ5GooZgTCKS3DHwTnTRfHiCkXHyTpZcCHw4Tiui
```

Guessing a Bitcoin Private Key

Short answer: Pick an atom; any atom. And then see if someone else picks the same one.
Super-short answer: It's almost impossible. But there is still a chance.

blockdyor

How Bitcoin Transactions Work

Alice sends 1 BTC to Bob

1. Alice's Private Key

Alice uses her secret private key to authorize the transaction. Only she has this key.

2. Creates Digital Signature

The private key creates a unique signature for this specific transaction - like signing a check, but impossible to forge.

3. Network Verification

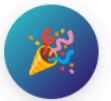
The Bitcoin network uses Alice's public key to verify the signature is authentic. Anyone can verify, but only Alice could create it.

4. Transaction Gets Hashed

Valid transactions are grouped into a block and sealed with a unique fingerprint (hash). Change anything, and the fingerprint changes.

5. Added to Blockchain

The block joins the permanent chain of all Bitcoin transactions. Each block references the previous one, making the history tamper-proof.



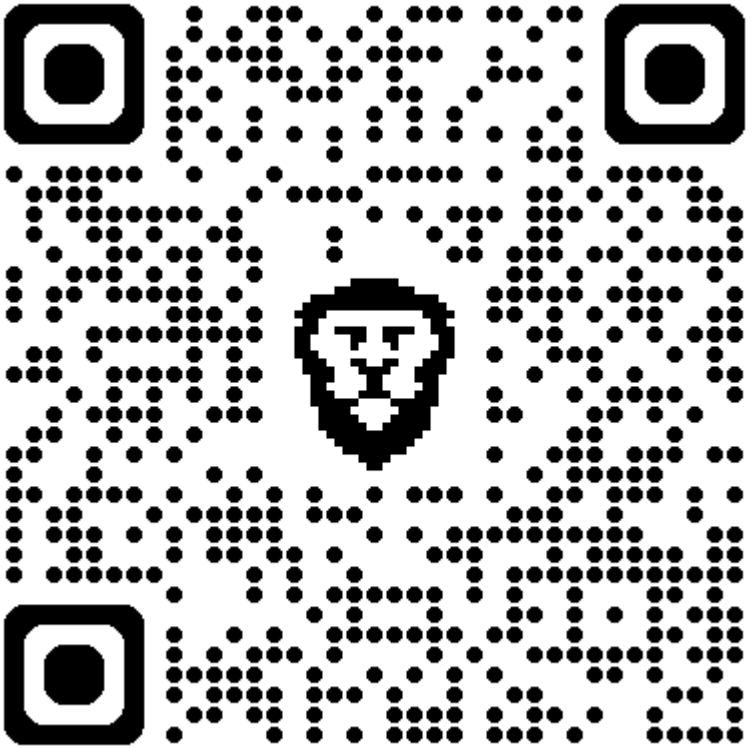
6. Bob Receives Bitcoin

The transaction is complete! Bob now controls the bitcoin and can spend it using his private key.

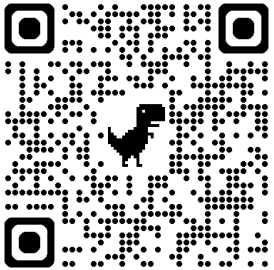
Private Key Cryptography Public Key Verification Hash Functions

Demonstrate Signature

https://bluewallet.github.io/VerifySignature?a=&m=&s=



https://www.browserling.com/tools/all-hashes



Hash Function

Hello World

- b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

HelloWorld

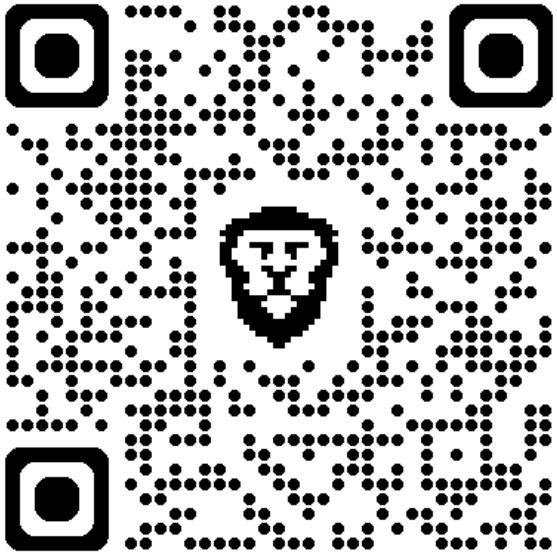
- 11d4ddc357e0822968dbfd226b6e1c2aac018d076a54da4f65e1dc8180684ac3

HelloWorld
b94d27b9934d3e08a52e52d7da7dabfac484efe37a5380ee9088f7ace2efcde9

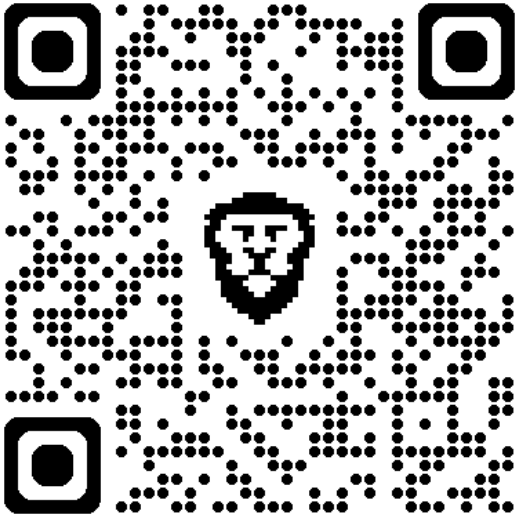
- 4b246ece3f13249715b14062f6354ce72f29f83e0dd884b912dde3fae44bb257

Block Hash

https://mempool.space/



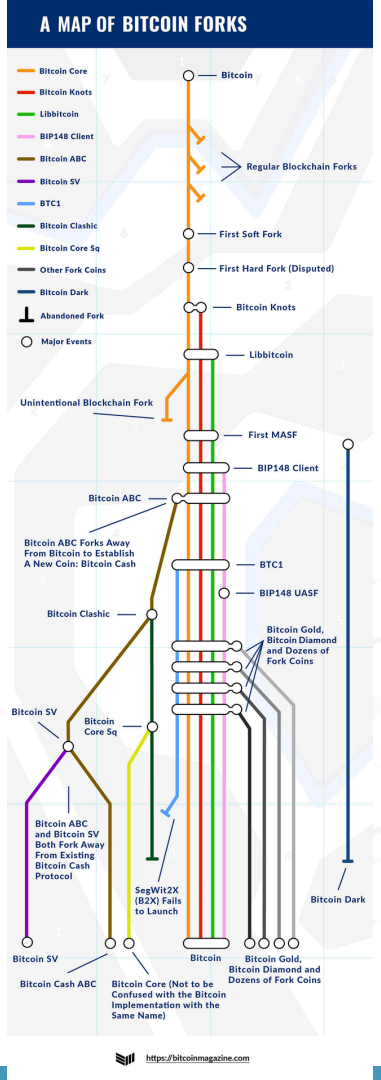
https://exp.btcme.com/



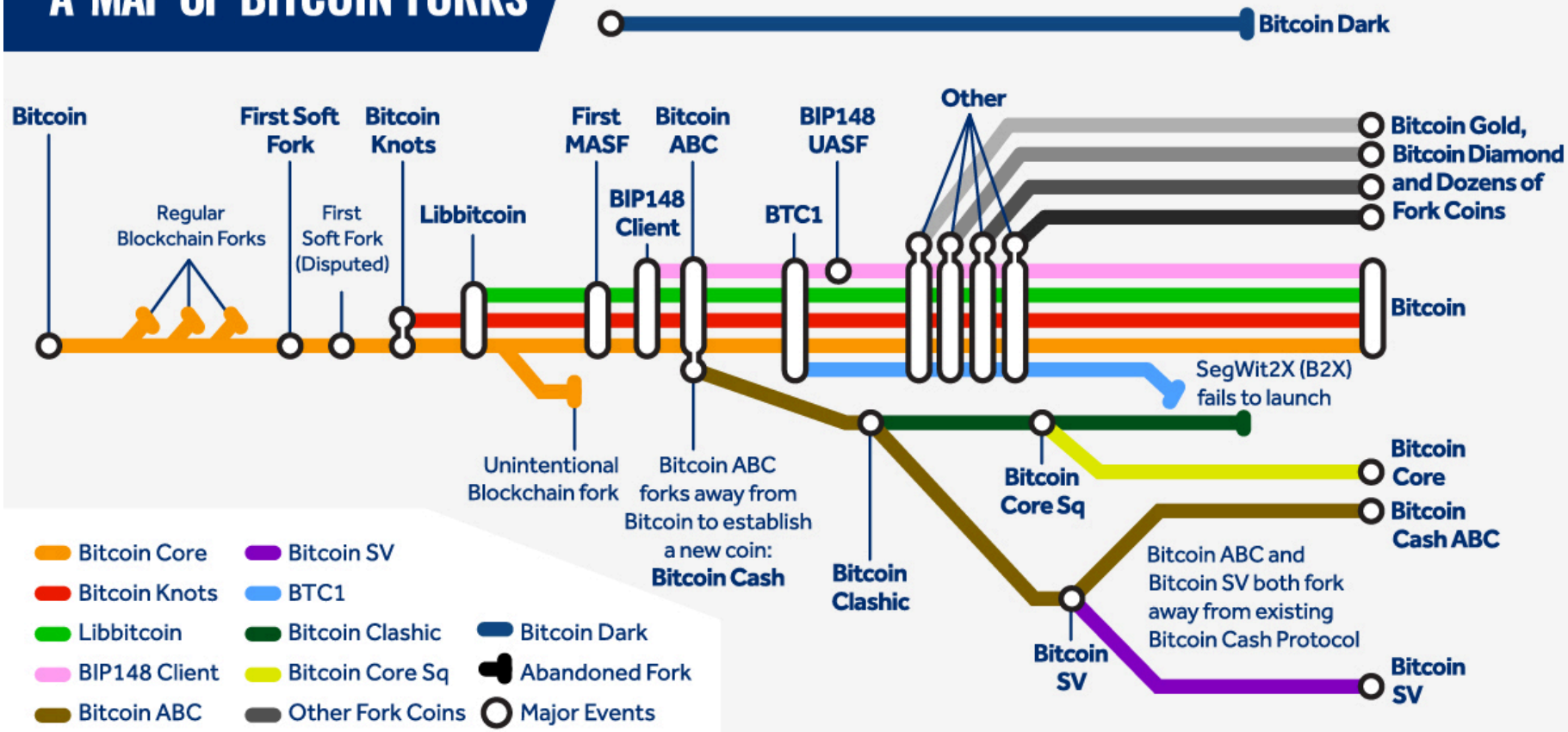
Network Concerns

Large fear of Bitcoin security (FORK)

- Forks (chain splits) are normal
- Hard forks are not normal
- Soft forks are backwards compatible
  - can lead to a hard fork?
  - has never happened
  - lots of uncertainty



A MAP OF BITCOIN FORKS



Costs of Chain Splits

- Double spend risk and merchant losses
- Wasted mining resources
- Exchange and custodian chaos
- Network reliability degradation
- Increased orphan rate
- Transaction uncertainty
- Smart contract and protocol failures
- Systemic risk escalation
- Governance and coordination costs

fork-observer

Network Testnet4 | Connection

Network: Testnet4

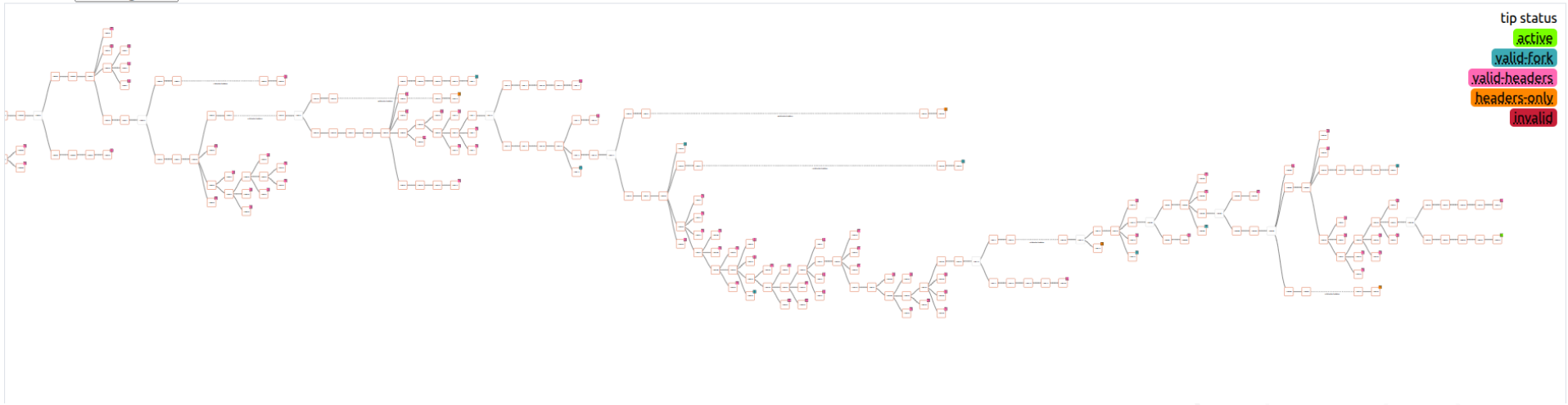
The new testnet4.

Recent forks Invalid blocks Lagging nodes Unreachable nodes

Nodes

Bitcoin Core (rs)	mempool.space	blackie.c3-soft.com	bitcoin.stagemole.eu	testnet4-electrumx....
Bitcoin Core 28.0.0	esplora (version unknown)	electrum Fulcrum 2.0	electrum ElectrumX 1.17.0	electrum ElectrumX 1.16.0
A Bitcoin Core node.	testnet4 on mempool.space	ssl://blackie.c3-soft.com:57010	ssl://bitcoin.stagemole.eu:5010	ssl://testnet4-electrumx.wakiy...
tip changed 4m ago	tip changed 6m ago	tip changed 6m ago	tip changed 6m ago	tip changed 6m ago
height: 105970	height: 105970	height: 105970	height: 105970	height: 105970
tip hash: ...eb88790c02	tip hash: ...eb88790c02	tip hash: ...eb88790c02	tip hash: ...eb88790c02	tip hash: ...eb88790c02

orientation left to right



Nodes

electrum.bitrefill.com
unreachable | electrum (version unknown)
ssl://electrum.bitrefill.com:50...
tip changed a long time ago
height: 0
tip hash: ...ffffffdead

Node A
Bitcoin Core 25.0.0
A (minimally) patched and pru...
tip changed 89s ago
height: 918483
tip hash: ...145a0f3a3d

Node C
Bitcoin Core 29.0.0
A development node in a diffe...
tip changed 89s ago
height: 918483
tip hash: ...145a0f3a3d

btcd v0.24.2-beta.rc1
btcd (version unknown)
A btcd node.
tip changed 1m ago
height: 918483
tip hash: ...145a0f3a3d

EU mempool.space
esplora (version unknown)
node212.fra.mempool.space
tip changed 89s ago
height: 918483
tip hash: ...145a0f3a3d

bmon1
Bitcoin Core 28.99.0
A bmon node.
tip changed 89s ago
height: 918483
tip hash: ...145a0f3a3d

electrum.emzy.de
electrum ElectrumX 1.18.0
ssl://electrum.emzy.de:50002
tip changed 85s ago
height: 918483
tip hash: ...145a0f3a3d

electrum.blockstrea...
electrum electrs-esplora 0.4.1
ssl://electrum.blockstream.inf...
tip changed 85s ago
height: 918483
tip hash: ...145a0f3a3d

fulcrum.sethforpriv...
electrum Fulcrum 2.0
ssl://fulcrum.sethforprivacy.co...
tip changed 89s ago
height: 918483
tip hash: ...145a0f3a3d

mempool.8333.mobi
electrum Fulcrum 1.11.1
ssl://mempool.8333.mobi:50002
tip changed 85s ago
height: 918483
tip hash: ...145a0f3a3d

electrum.bitaroo.net
electrum ElectrumX 1.16.0
ssl://electrum.bitaroo.net:50002
tip changed 89s ago
height: 918483
tip hash: ...145a0f3a3d

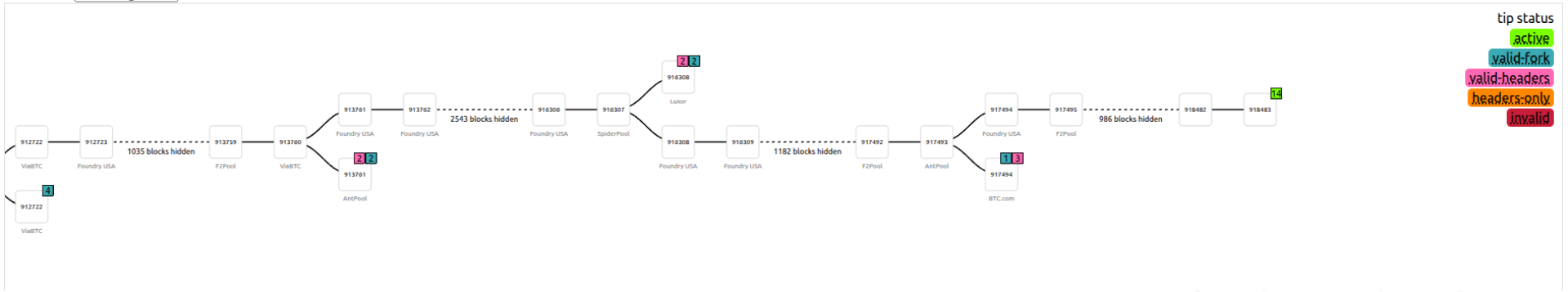
mainnet.foundation...
electrum Fulcrum 1.11.1
ssl://mainnet.foundationdevic...
tip changed 89s ago
height: 918483
tip hash: ...145a0f3a3d

electrum.jochen-ho...
electrum Fulcrum 1.12.0
ssl://electrum.jochen-hoenick...
tip changed 89s ago
height: 918483
tip hash: ...145a0f3a3d

electrum.acinq.co
electrum ElectrumX 1.15.0
ssl://electrum.acinq.co:50002
tip changed 73s ago
height: 918483
tip hash: ...145a0f3a3d

btc2.shiftcrypto.io
electrum ElectrumX 1.16.0
ssl://btc2.shiftcrypto.io:50002
tip changed 83s ago
height: 918483
tip hash: ...145a0f3a3d

orientation left to right



Warnet Project

https://github.com/bitcoin-dev-project/warnet

Generates Bitcoin networks as nodes and edges

- currently uses a custom regtest and bitcoin rpc
- runs the network as a virtual network and allows connections to be modified
- mining is a scenario (currently using a round robin approach but can be random)
- transactions is another scenario (currently random from all nodes)

Warnet scenario discovery

https://github.com/pfoytik/warnetScenarioDiscovery

A comprehensive Python framework for testing Bitcoin network fork scenarios using Warnet.

🎯 **What This Framework Does**

- **Systematically induce blockchain forks** by partitioning your Warnet network
- **Monitor fork behavior in real-time** with detailed metrics
- **Analyze fork resolution** and chain reorganizations
- **Compare different Bitcoin Core versions** under identical conditions
- **Generate comprehensive reports** with visualizations
- **Automate regression testing** for Bitcoin Core development