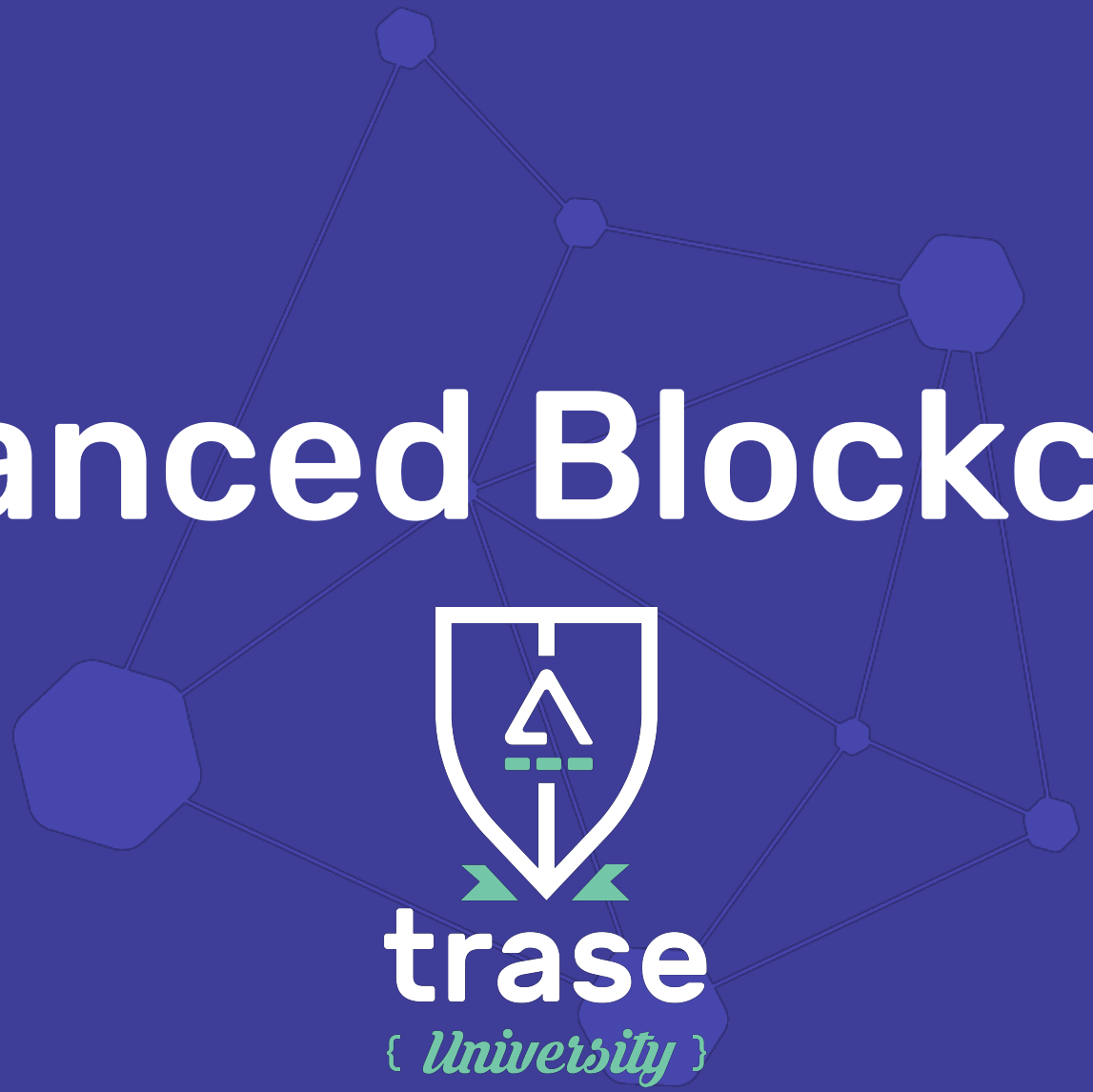
Advanced Blockchain



Content

trAse

Asymmetric encryption

Simply explained

CASE

Digitale handtekening eID

- Login with eID
- Sign digitally

How does it work?

- Private / Public key on the ID card
- Encryption on the card
- Lock with Pincode

A little recap..

trAse

P2P networking

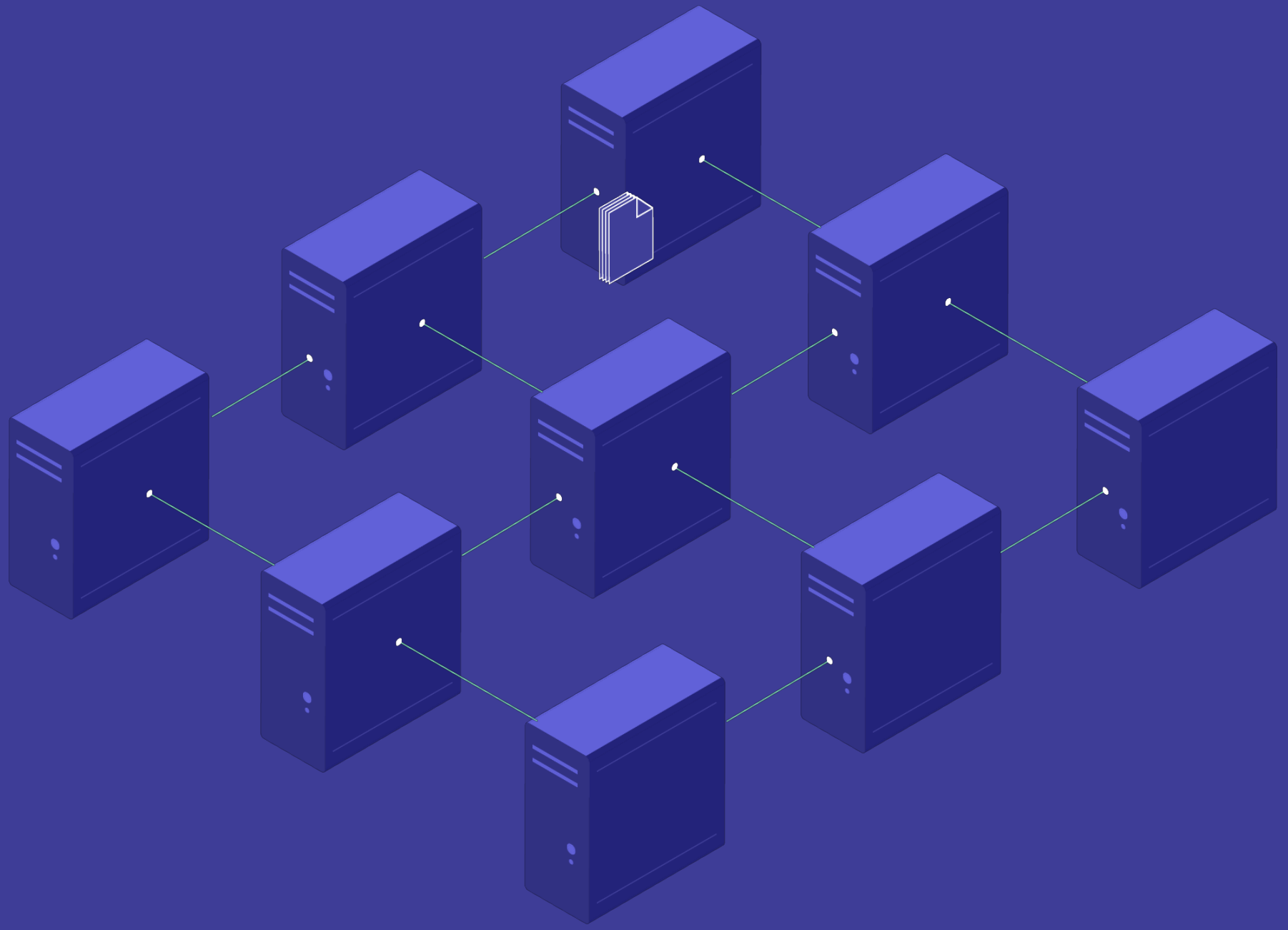
No client-server architecture

- Decentralized
- No governening party

No trust needed

- Everyone verifies
- Everyone is watching

trAse

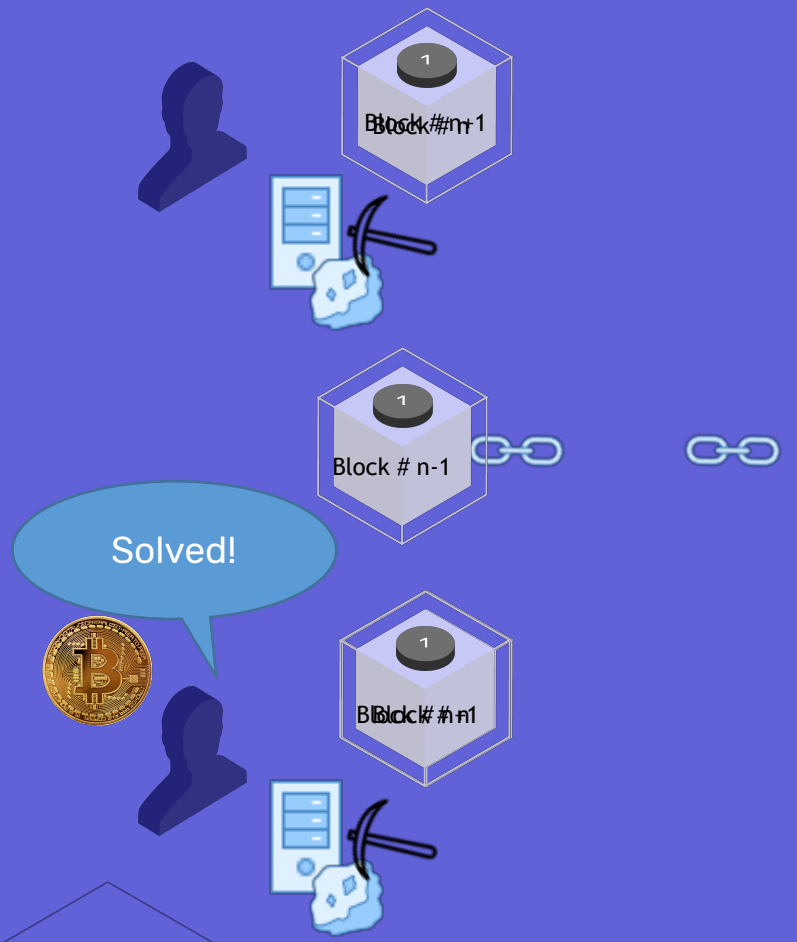


trAse

Consensus

Consensus

- Proof of Work
- Creation of coins
  - Solving a difficult math problem = mining



trAse

Proof of Work

Data hash([redacted] nce) < ? Difficulty

trAse

Proof of Work

hash( )

hash( )

hash( )

hash( )

< ?

< ?

< ?

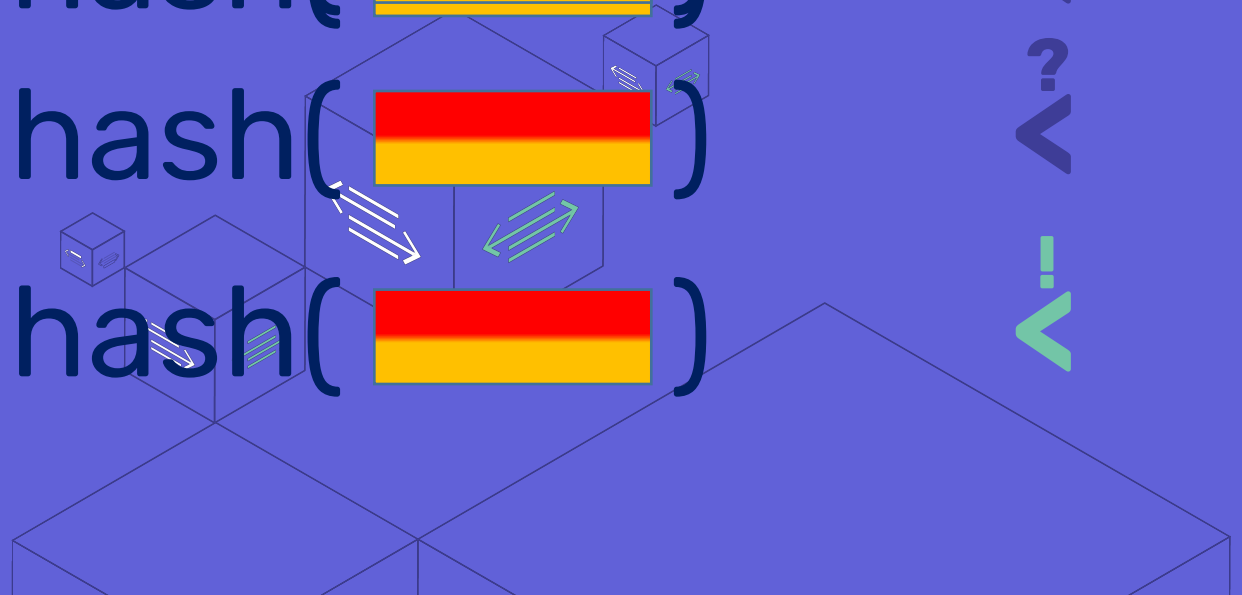
<

Difficulty

Difficulty

Difficulty

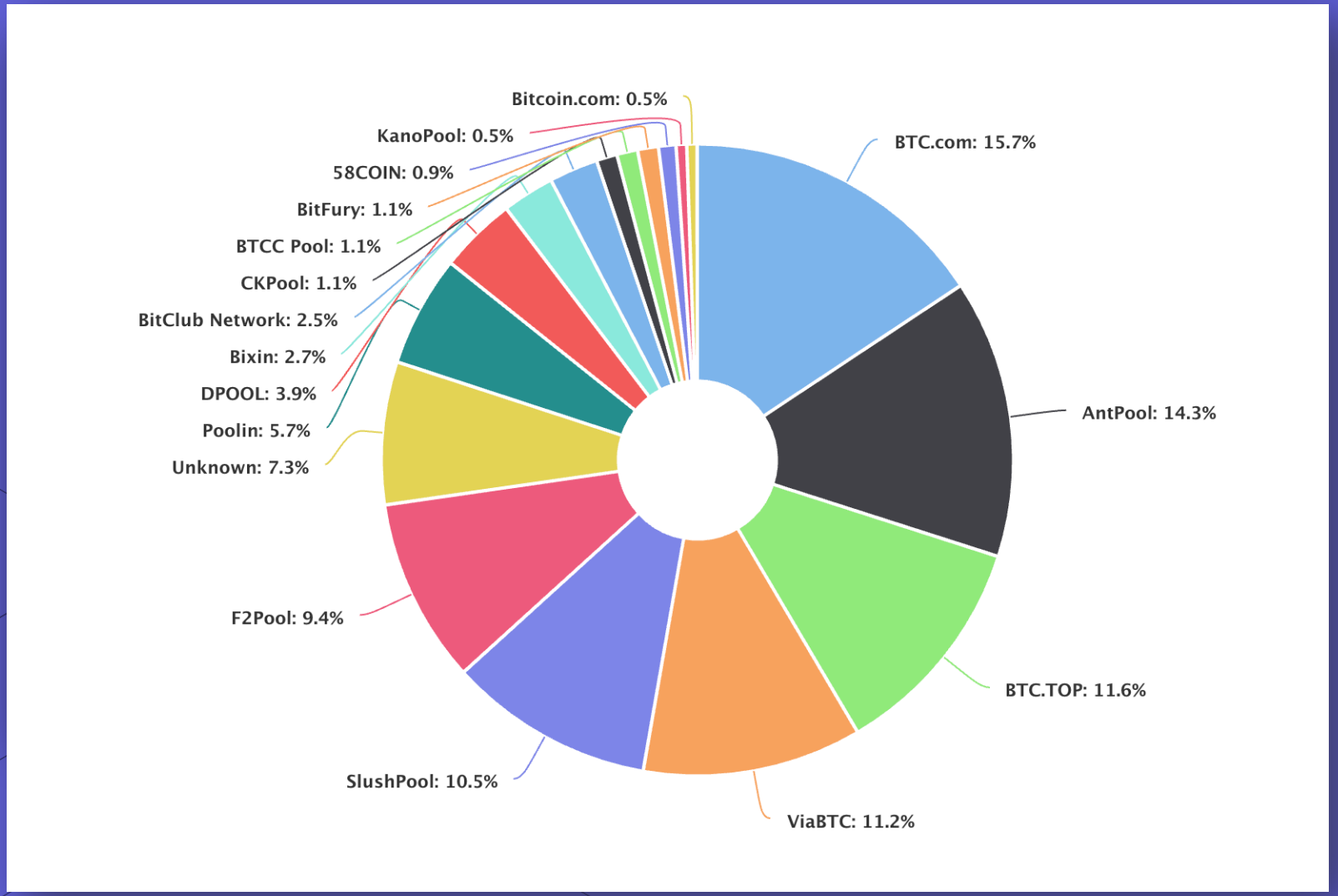
Difficulty



trAse

Proof of Work

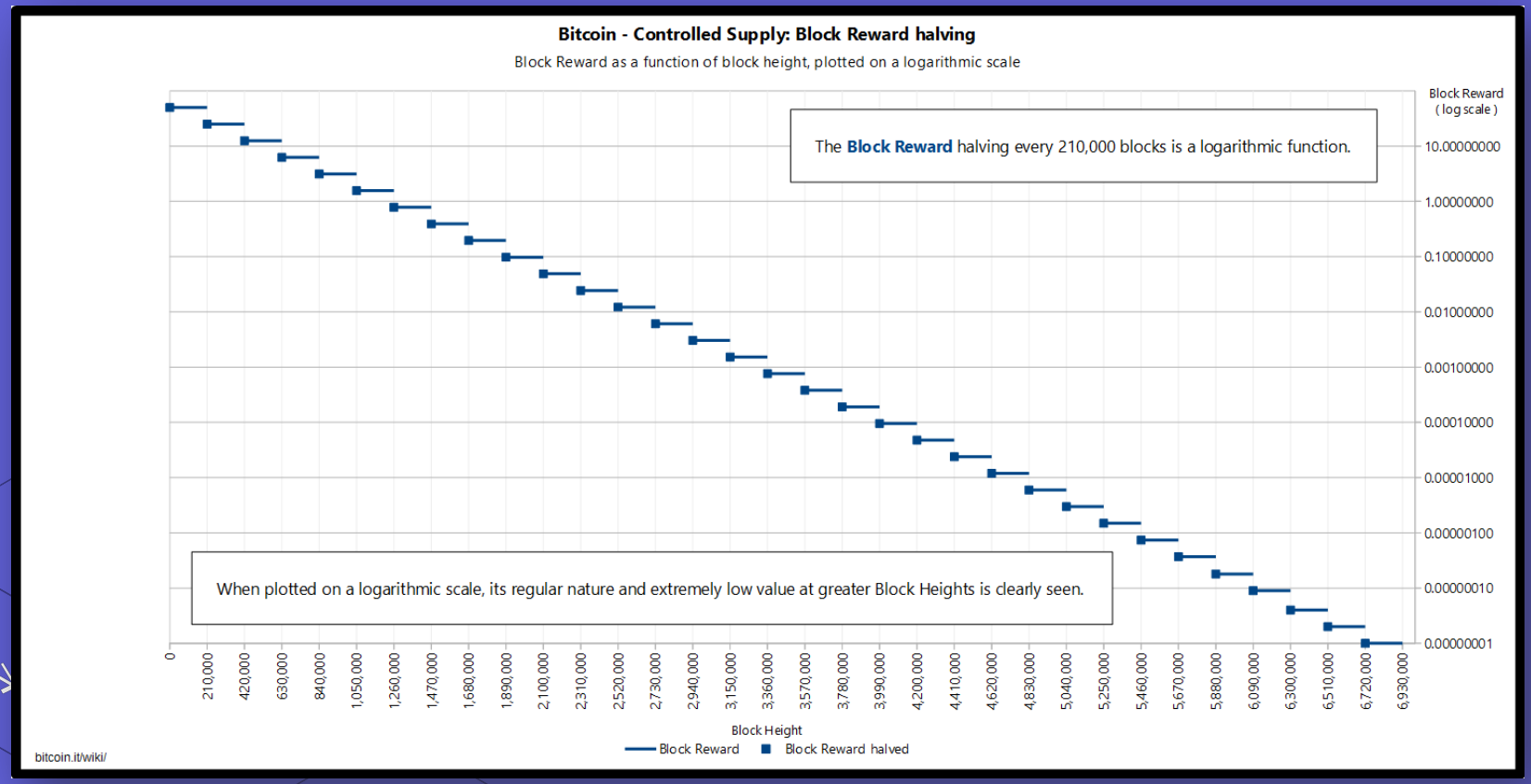
Difficulty



trAse

Proof of Work

Supply



trAse

Proof of Work

Preventing double spends

How?

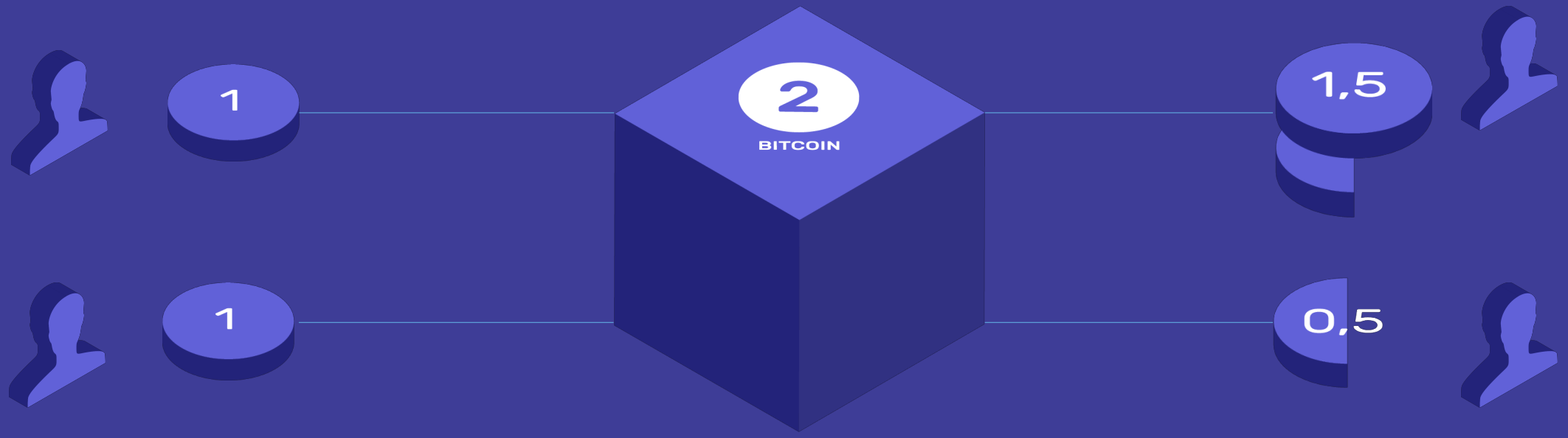
- Copy of the ledger on every node 9312
- For a transaction to be valid it has to be mined
- Blocks are chained so that if any is modified, all following blocks will have to be recomputed
- When multiple valid continuations appear, only the longest branch is accepted

trAse

Transactions

trAse

UTXO



trAse

Scripting Language

Stack oriented

- Instructions and data in frames
- Execute sequentially
- Locking vs Unlocking script

Execution

- When verifying transactions
- For example: digital signature

trAse

Scripting Language P2PKH

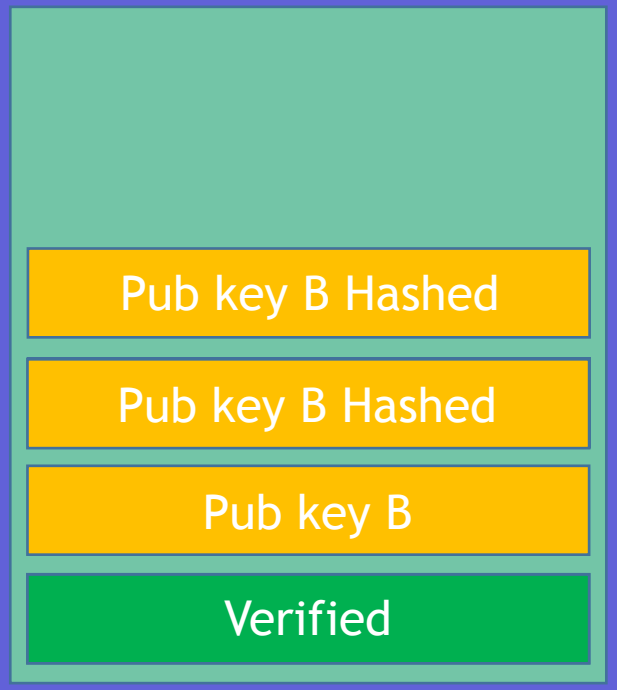
Locking Script

```
OP_DUP
OP_HASH160
PUSHDATA <address B>
OP_EQUALVERIFY
OP_CHECKSIG
```

Unlocking Script

```
PUSHDATA <signature>
PUSHDATA <pub key B>
```

Stack

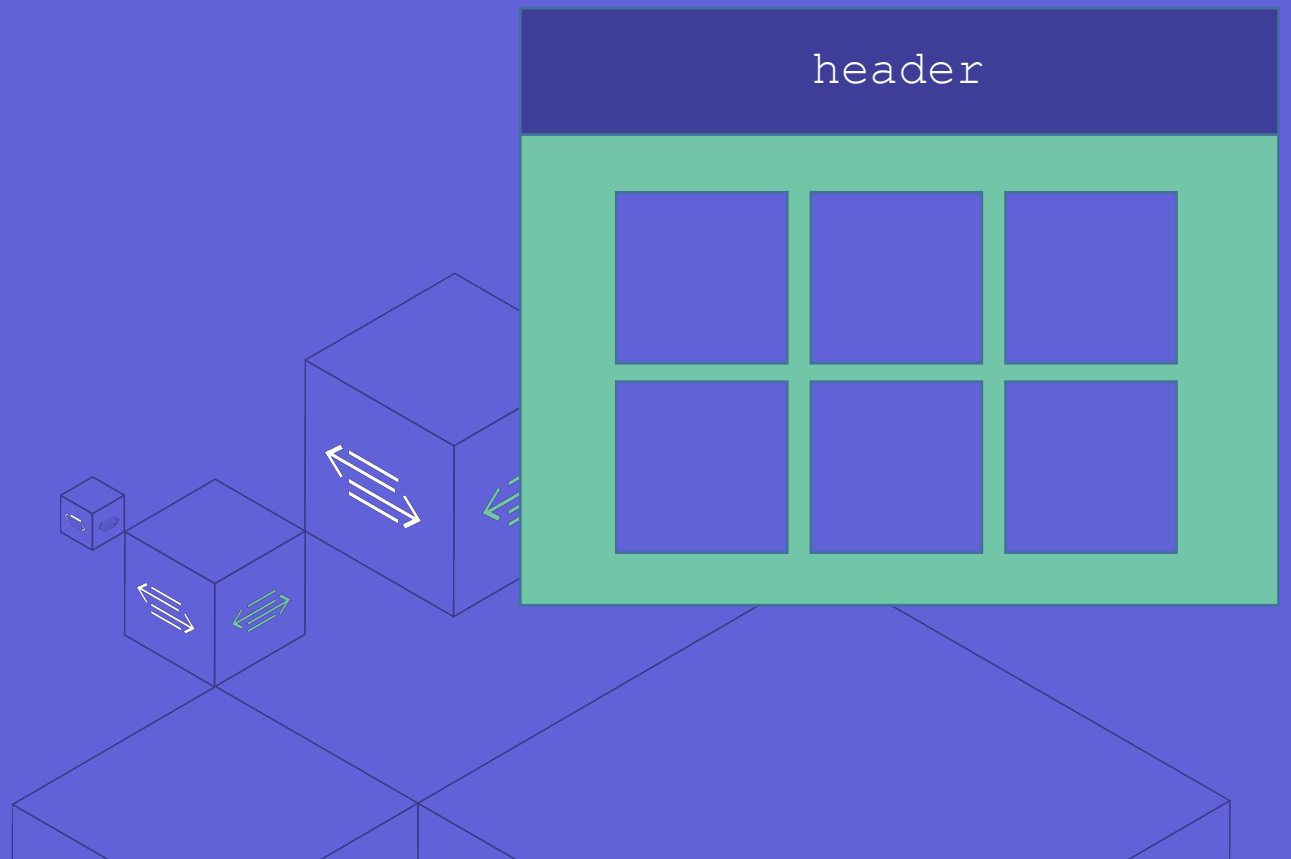


trAse

Blocks

trAse

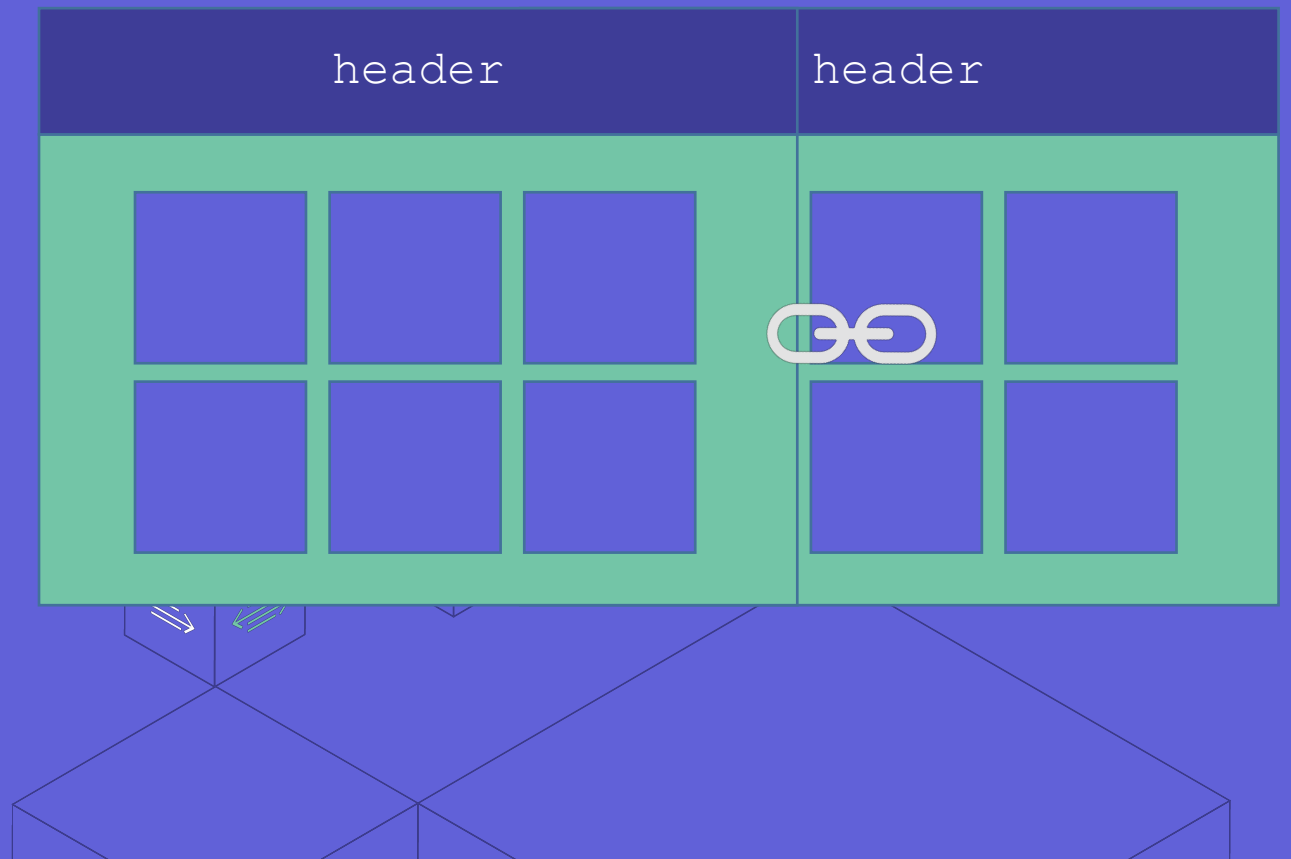
Block Structuur



Version
hashPrevBlock
hashMerkleRoot
Time
Bits
Nonce

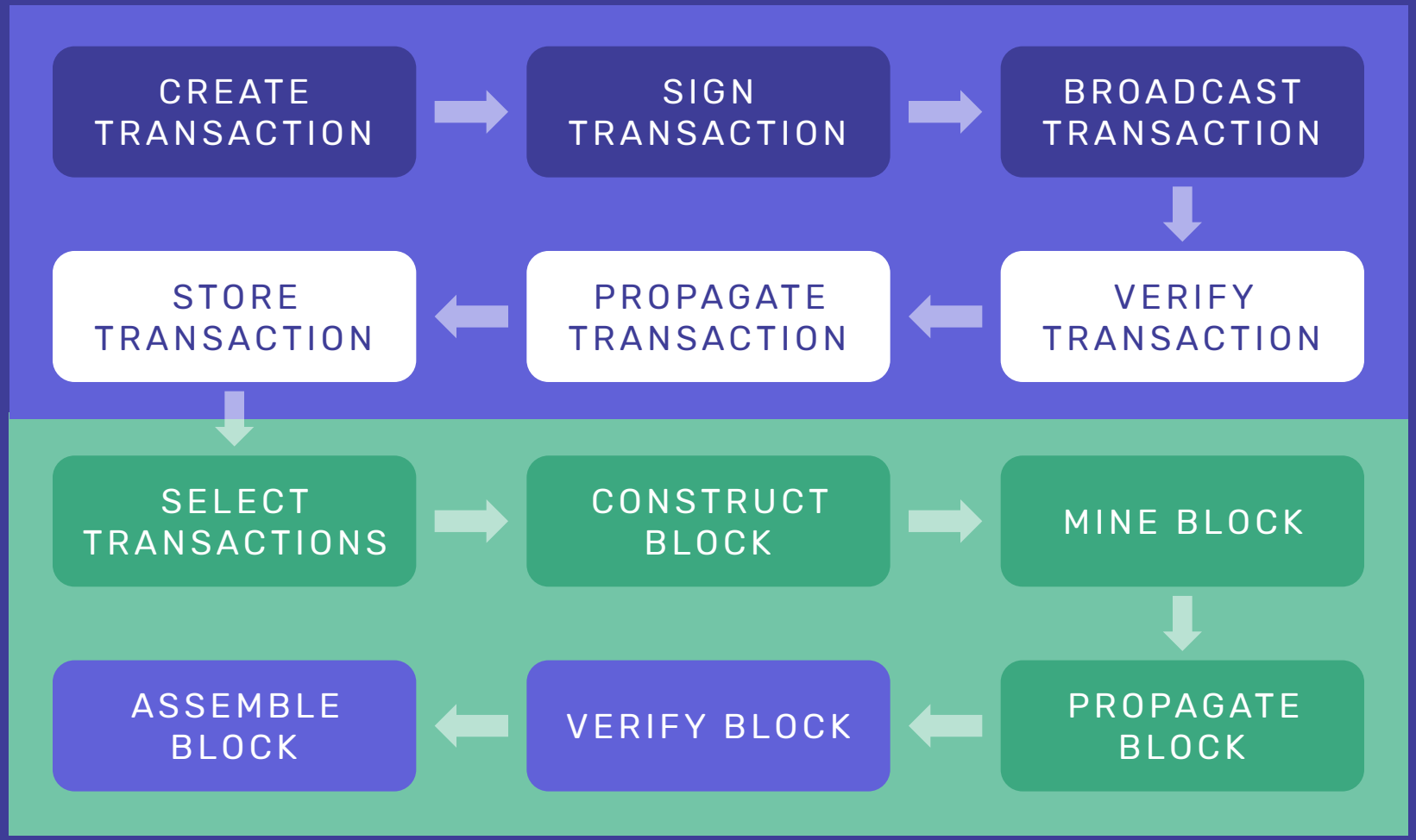
trAse

Block Structuur



trAse

Lifecycle



CREATOR/ SIGNER

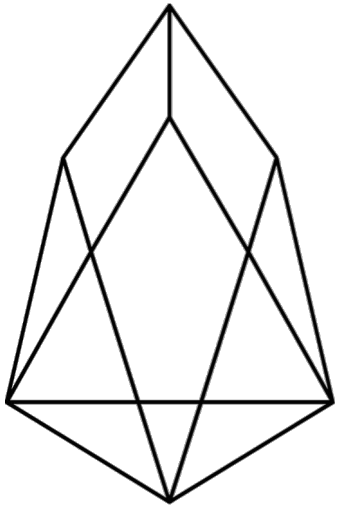
PEERS

MINERS

trAse

Exercise

trAse

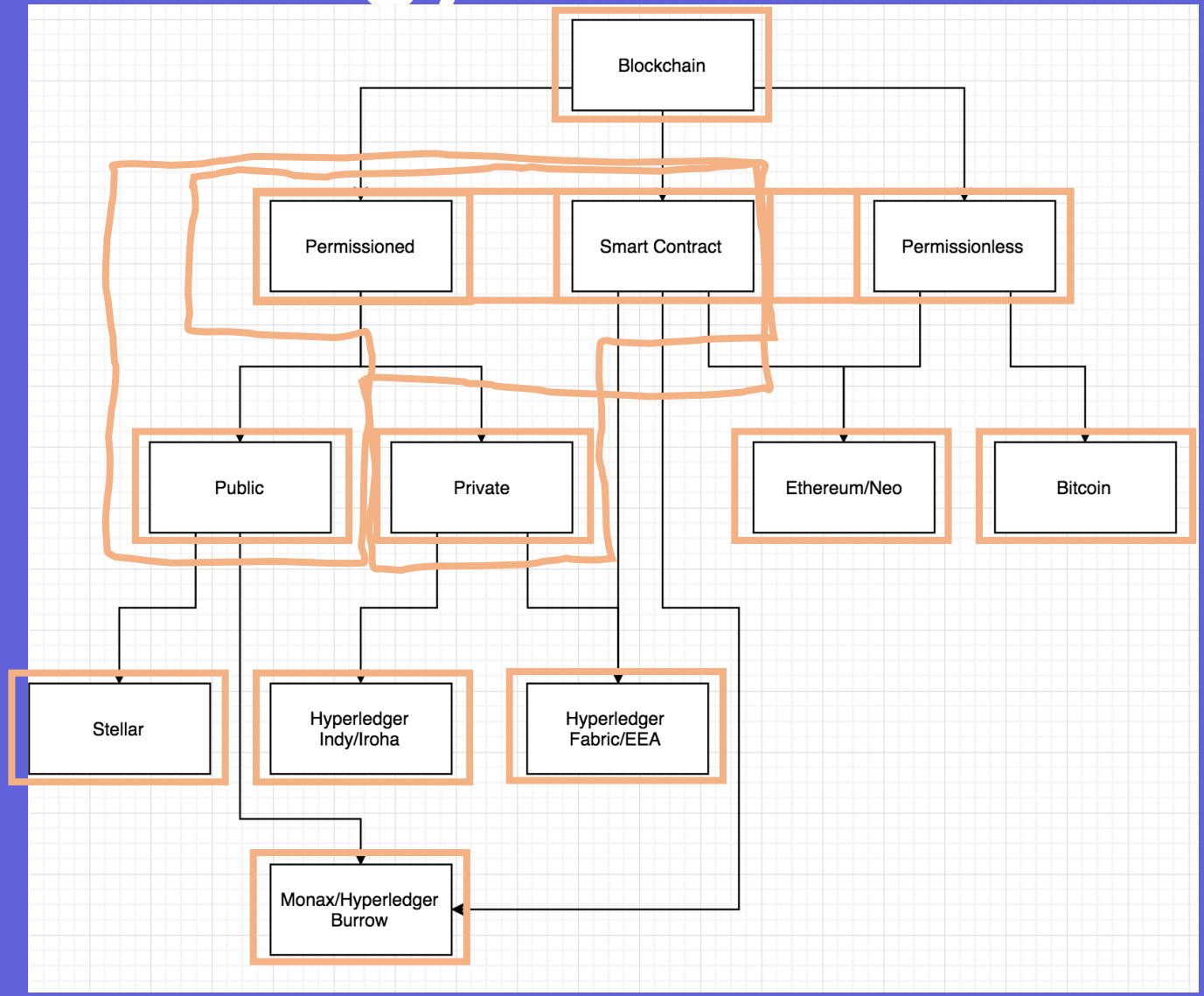


Exercise

- Technology
- Consensus
- Private, Permissioned, Public
- Transaction fees/model
- Smart Contracts

Case/Problem the technology can solve

Which technology?



trase

Blockchain trilemma

trAse

Does everyone remember this?

trAse

Statements of today

“Bitcoin is slow. It’s expensive, there are so many new coins that are much better. They are fast and inexpensive.”

“Ethereum couldn’t even handle CryptoKitties, how do you expect it to work with Web3.0!?”

“<insert coin ticker> is king, it can handle 60,000 transactions per second, has no fees and it has built-in smart contracts.”

trAse

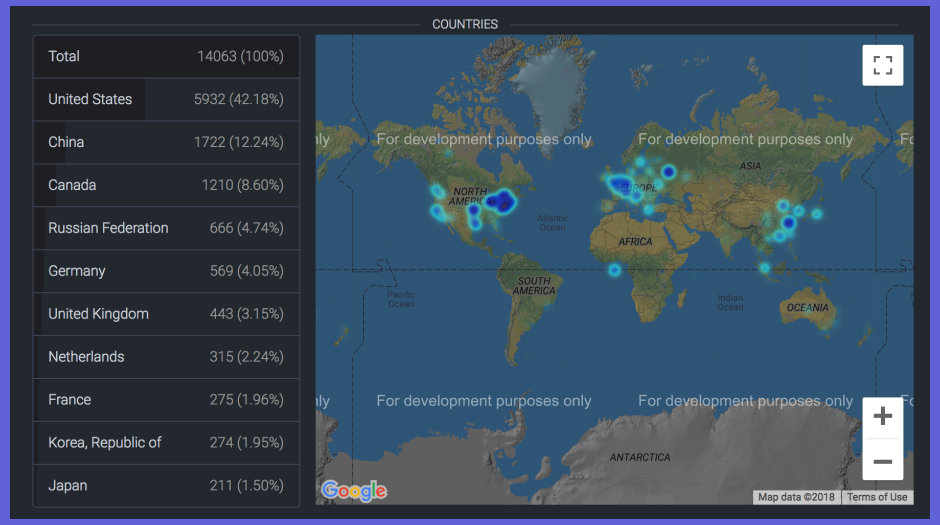
“Touka Koukan”

Equivalent exchange. Nothing comes for free.

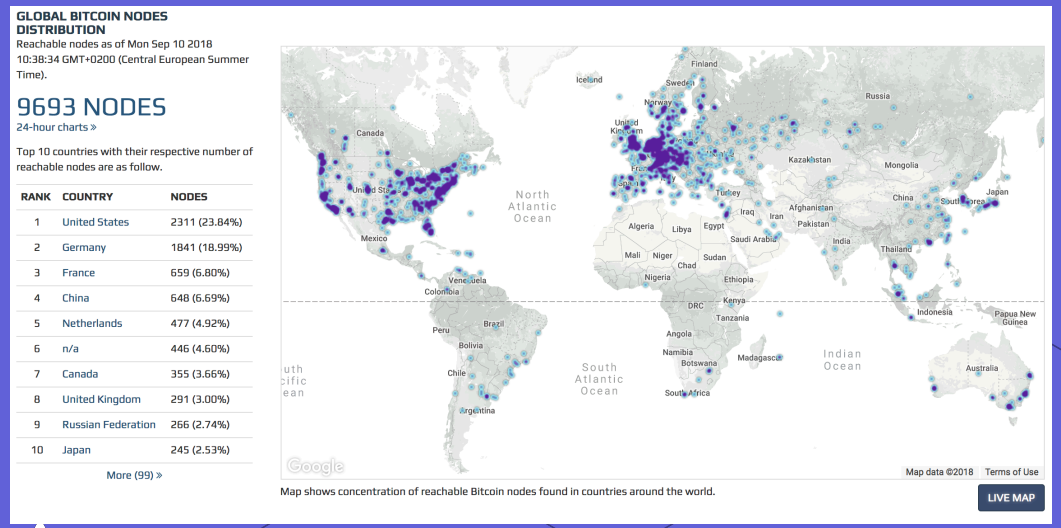
Decentralization
Scalability
Security

trAse

Decentralized vs Centralized



XRP: 20(*) Validating nodes



NEO: 4 nodes

trAse

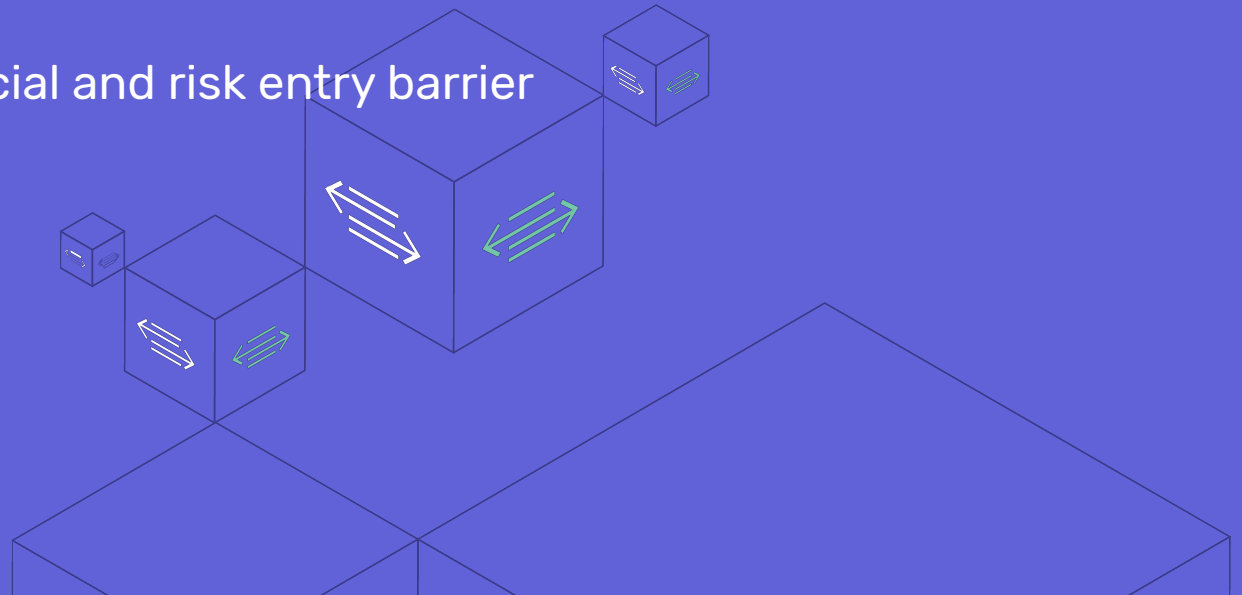
Scalability

Numbers
Transaction speed XRP: 1500/sec
Transaction speed BTC: 15/sec

Transition phase from centralized -> distributed -> decentralized by adding more nodes.

Constraints: all nodes must process every transaction on some platforms.
-> High cost. E.g. NEO Master node minimum $21,000; DASH: $1,000,000

High financial and risk entry barrier



trase

Are we decentralized yet?

are we decentralized yet? </> JSON API Contribute on

Name	Symbol	Consensus	Miners/voters Incentivized?	# of entities in control of >50% of voting/mining power	% of money supply held by top 100 accounts	# of client codebases that account for > 90% of nodes	# of public nodes
Bitcoin	BTC	PoW	Y	4	19%	1	9624
Ethereum	ETH	PoW	Y	3	34%	2	17341
XRP	XRP	RPCA (voting system)	N	2	81%	1	789
Bitcoin Cash	BCH	PoW	Y	3	24.12%%	2	2124
Stellar	XLM	FBA	N	1	95%	1	111
Litecoin	LTC	PoW	Y	3	44%	3	261
Cardano	ADA	PoS	N	1	40%	1	1
Monero	XMR	PoW	Y	3	?	1	1691
Dash	DASH	PoW	Y	3	14.65%	1	4649
IOTA	MIOTA	Tangle (DAG)	Y	1	62%	1	484
Neo	NEO	DBFT	N	1	70%	2	46
Ethereum Classic	ETC	PoW	Y	2	?	2	?
NEM	XEM	POI	Y	?	53%	1	530
Tezos	XTZ	LPoS	Y	2	43%	1	76
Dogecoin	DOGE	PoW	Y	4	50.91%	?	?
Zcash	ZEC	PoW	Y	2	?	1	1476
Qtum	QTUM	PoS	Y	45	73.102%	1	6787
Decred	DCR	PoW/PoS	Y	2	39%	1	259
Nano	NANO	DPoS	N	3	62%	1	548

trAse

Security

Permissioned Private Blockchains

- **Good security**
- **Good scalability**
- **Bad decentralization**

Internet vs Intranet

trase

Solutions

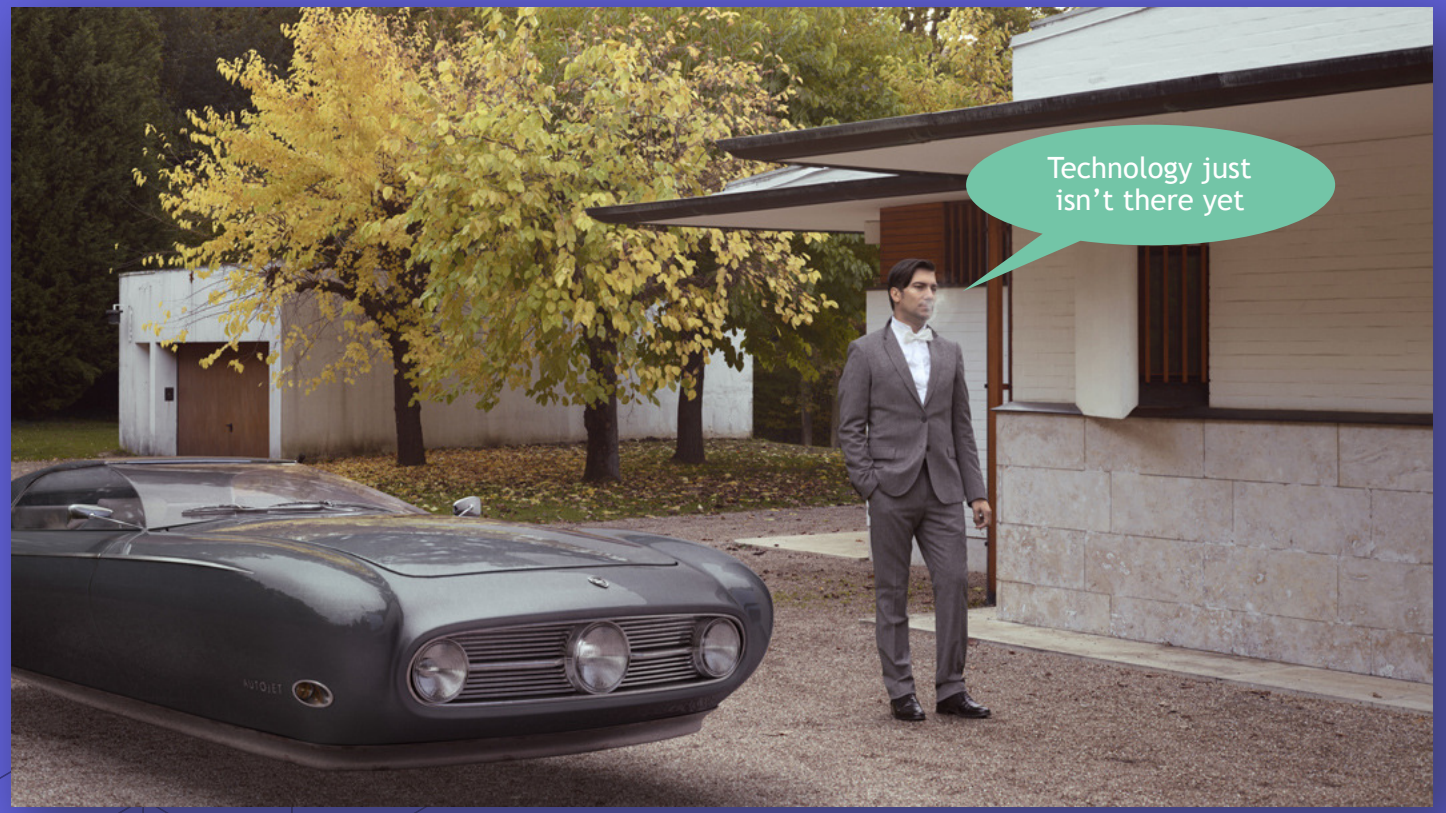
Scalability: Bigger blocks, offchain transactions, sharding

Security: Consensus

Decentralization: Public/Private compromise

trAse

Conlusion



trAse

Q & A

trAse


trAse

Hyperledger Fabric Network