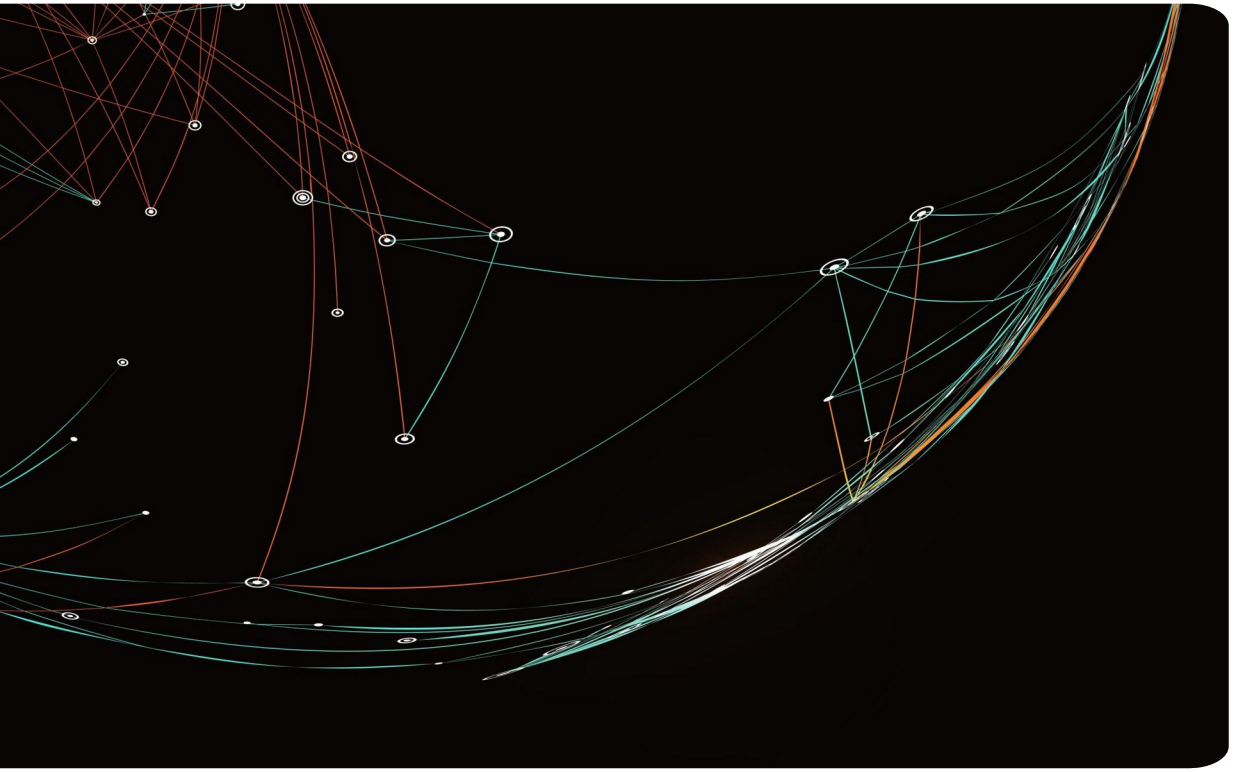


Elrond Network

Blockchain basics

Radu Chis

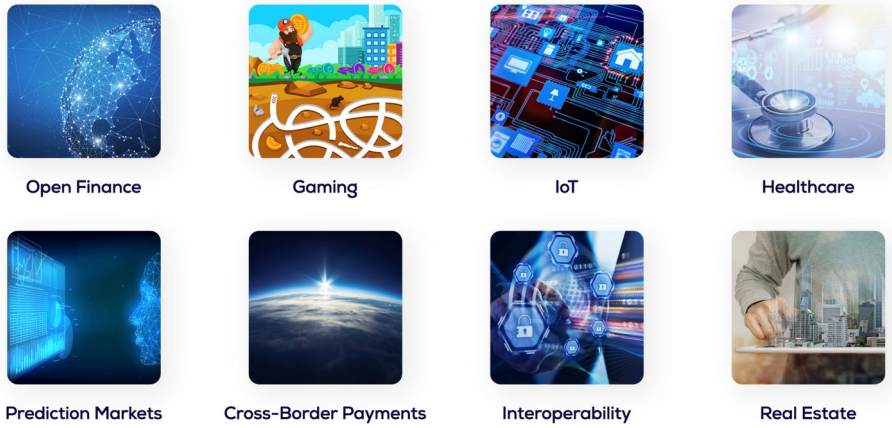
- Head of Technology
- Assistant Professor CS department ULBS
- PhD CS, multiobjective optimization
- supervisor prof. Lucian Vintan

Elrond - Introduction

- Idea + Team
- Blockchain 1.0, 2.0 si 3.0
- Nodes/Protocol
- Consensus and Security
- Smart Contracts and Virtual Machine
- Future work

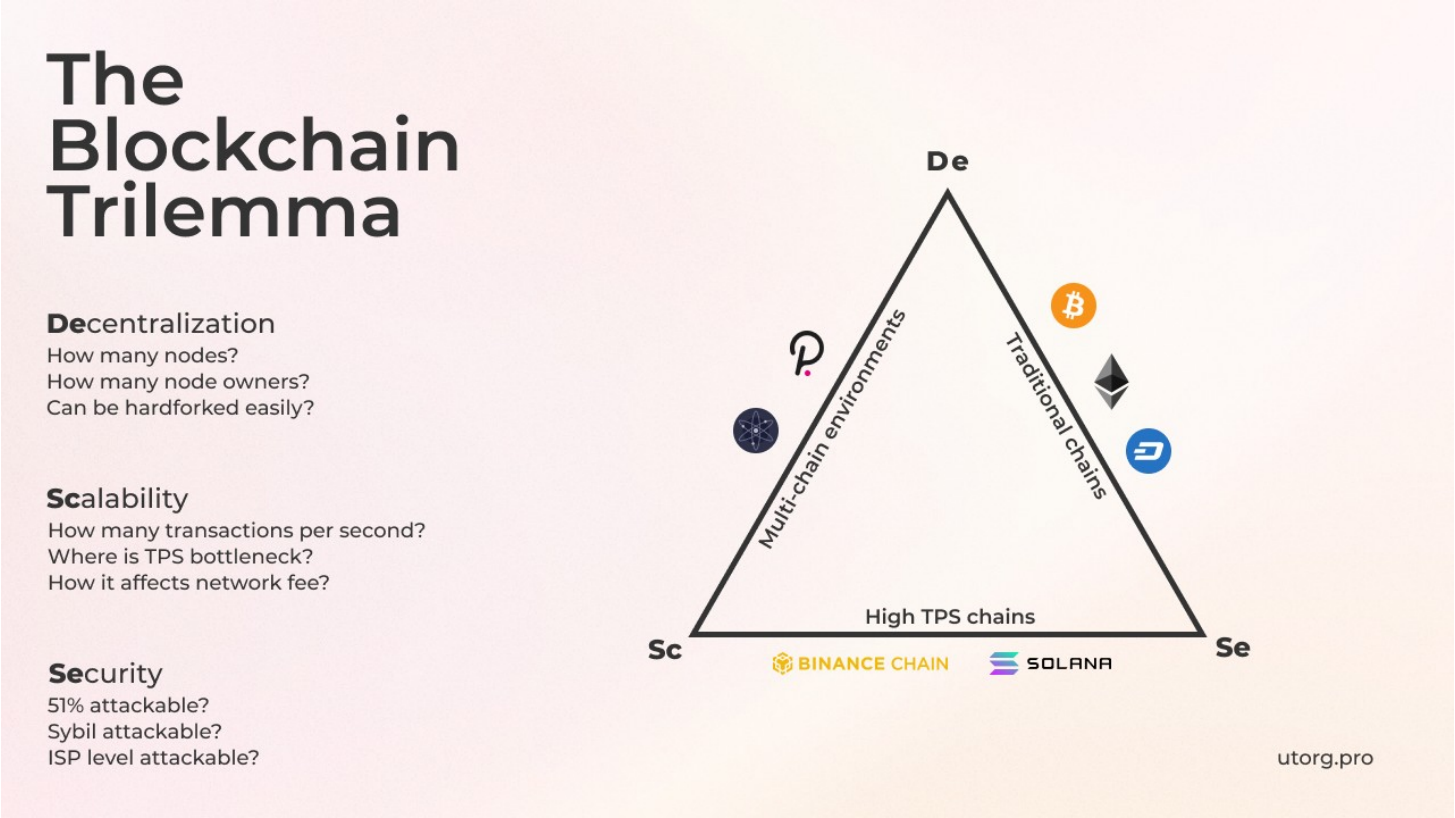
Blockchain

- 1.0 – Cryptocurrency – Bitcoin
  - ECash - 1980/1990
  - secured, anonymous, tokens from a decentralized entity
- 2.0 – Smart Contracts – Ethereum
  - Smart Contracts, Smart Property, Dapps, DAOs
- 3.0 - global, institutional and enterprise adoption
  - Seamless integration in different domains



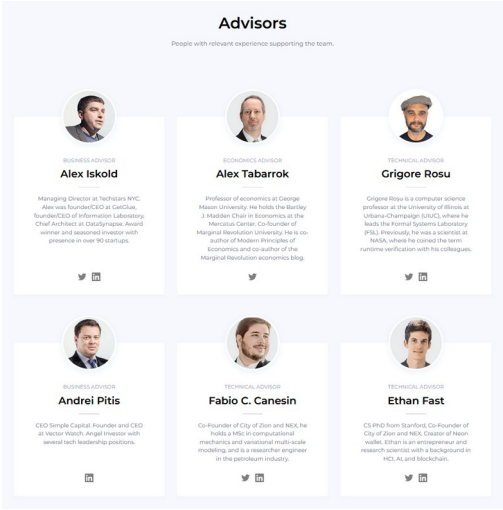
Blockchain Trilemma

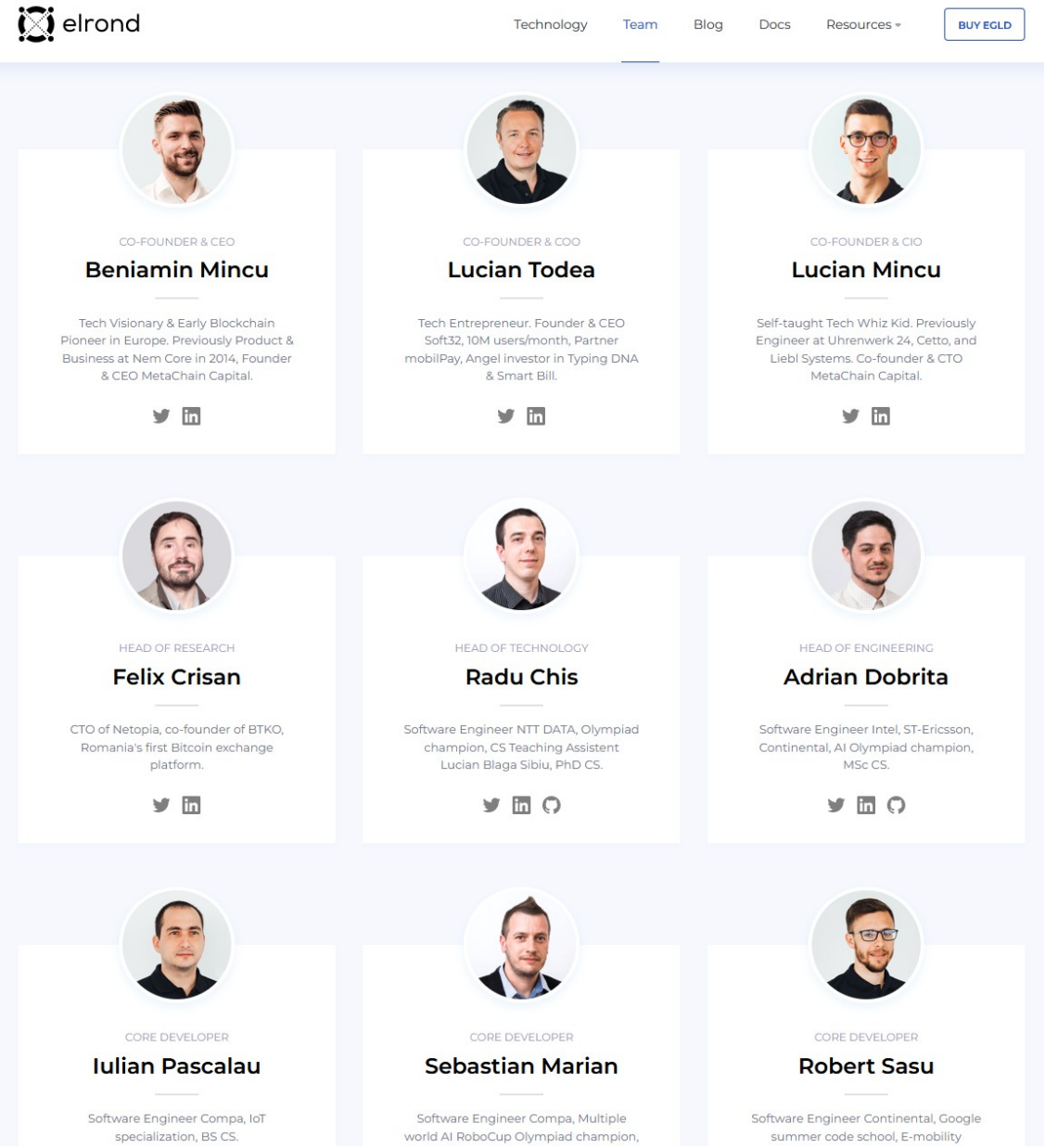
- Scalability
  - sharding
  - consensus
  - layer 2
    - sidechains
    - rollups



Elrond - beginning

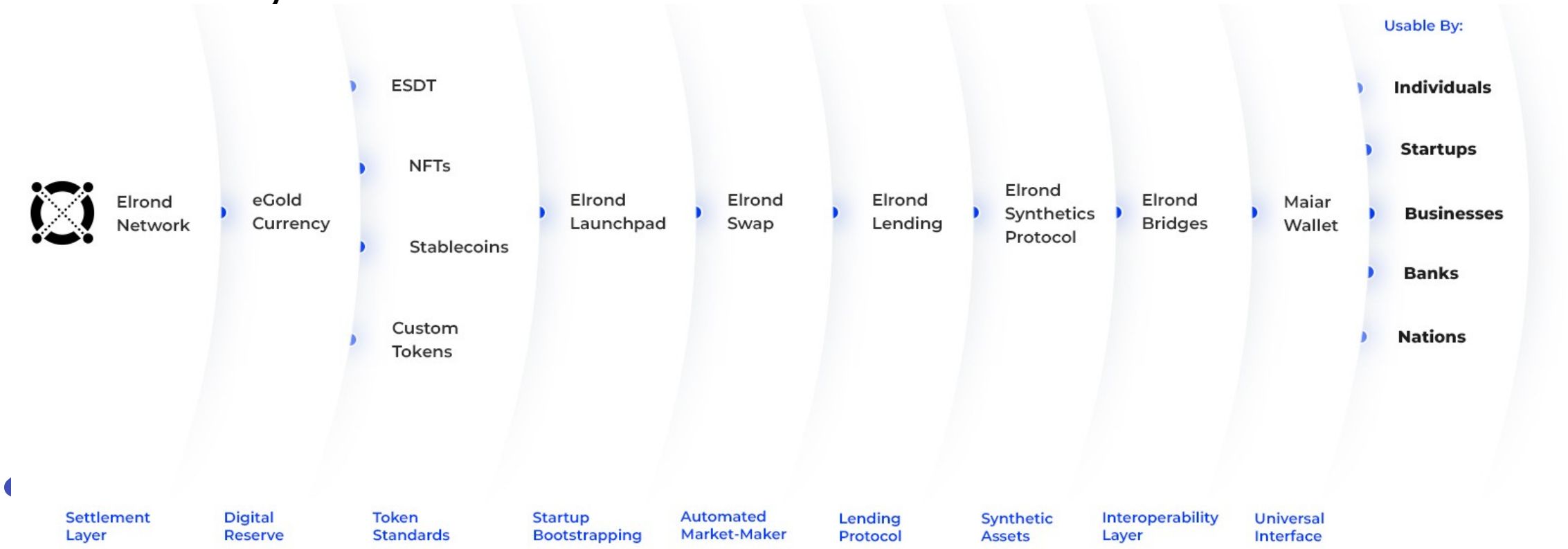
- First discussions end of 2017
- Blockchain
  - secured
  - fast
  - cheap
- CryptoKitties
- Onboarding 1 billion users





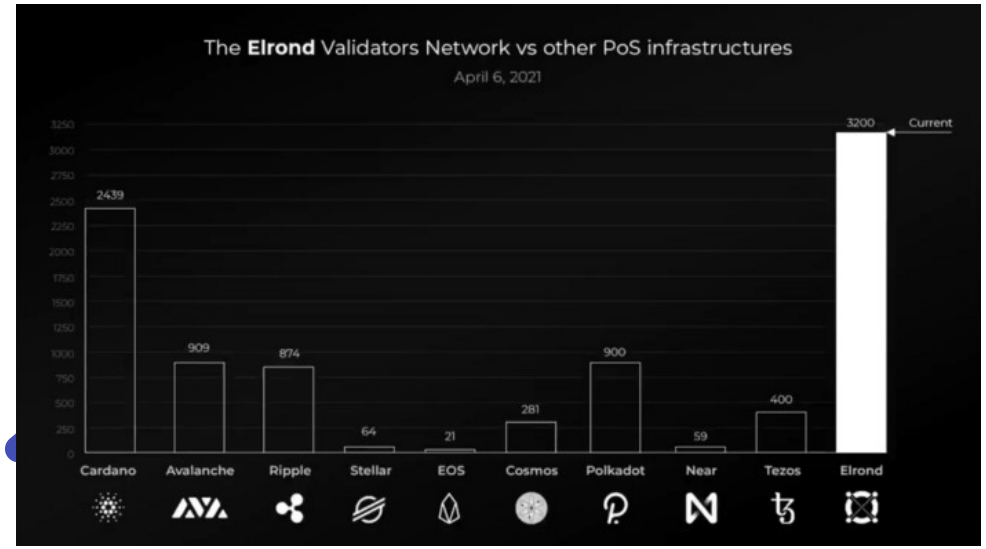
Elrond – The Internet Scale Blockchain

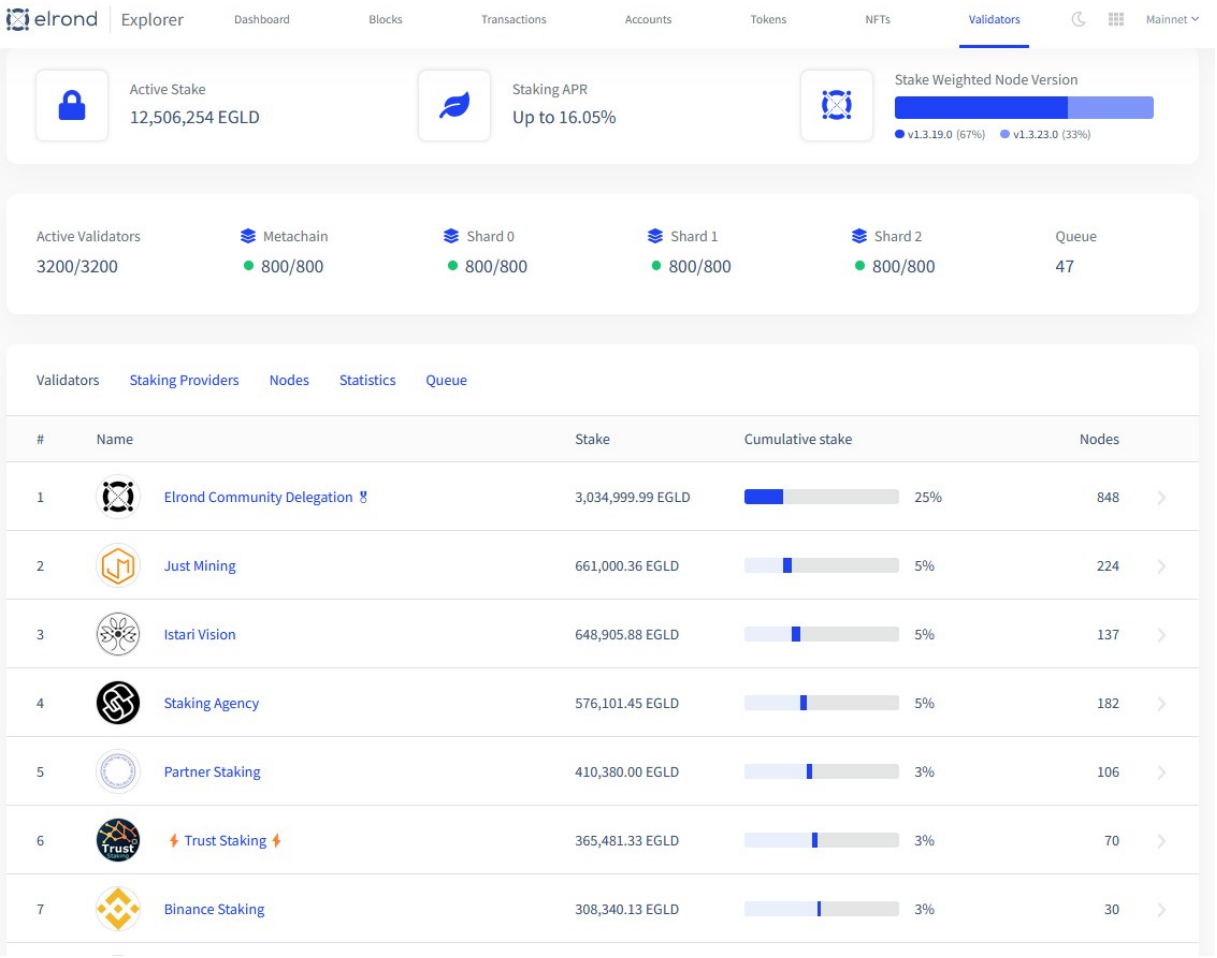
- A highly scalable, fast and secure blockchain platform for distributed apps, enterprise use cases and the new internet economy.



Elrond – 3200 nodes

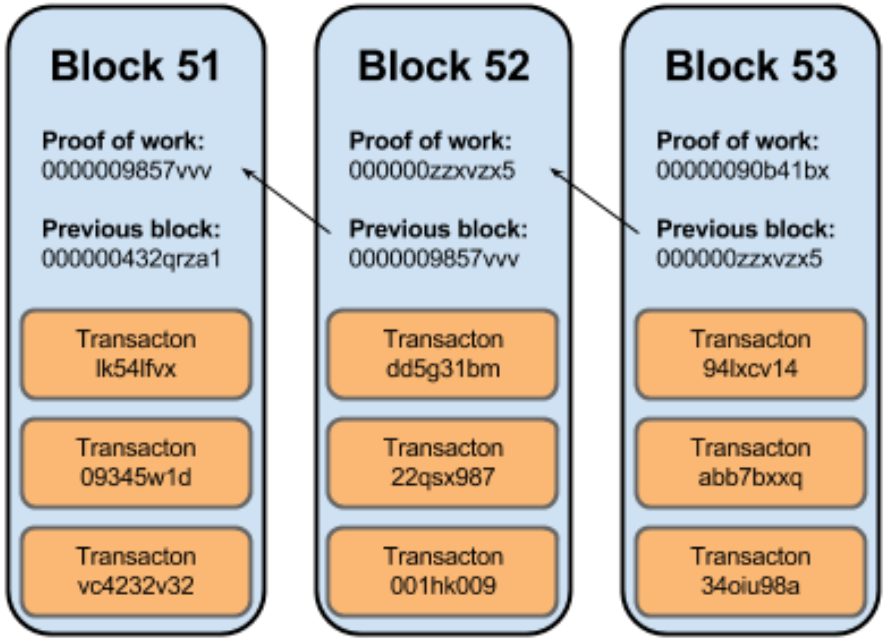
- Proof of Stake + Sharding
  - stake EGLD (2500)
  - consensus produce blocks
  - earn rewards (inflation + fees)
  - slashing
  - jailed based on rating

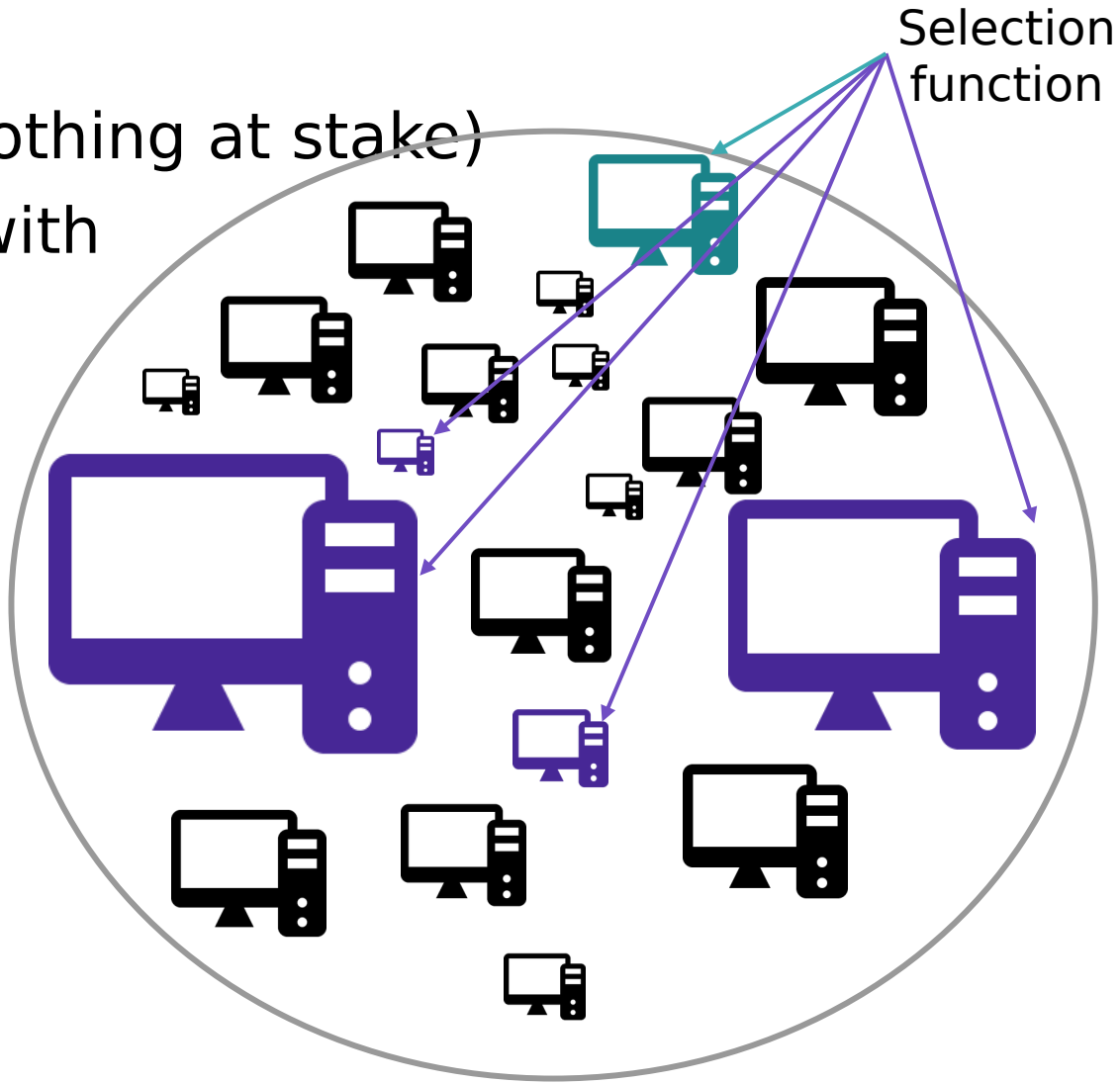




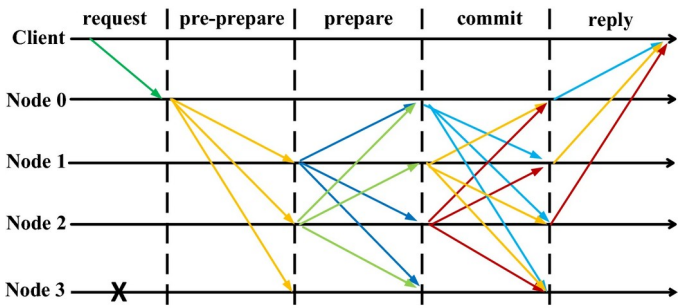
Consens – Proof of Stake

- Lock stake (sibling prevention/nothing at stake)
- Selection probability increases with
- stake size (e.g. more nodes)





Elrond – Secure Proof of Stake Consensus pBFT variant



Secure Proof of Stake

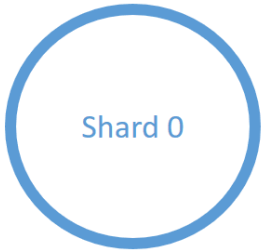
Elrond – Adaptive State Sharding - 1

- No sharding → inefficient, but secure
- Types:
  - Network (400 nodes)
  - Transaction (Zilliqa)
  - State

Elrond – Adaptive State Sharding - 2

Step 1:
Node to shard assignment

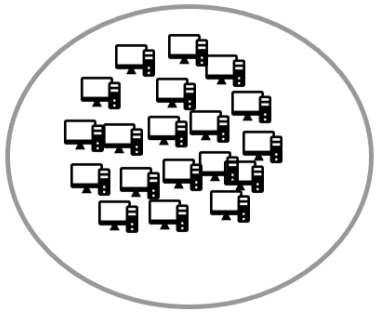
1 Shard



3bit Addresses			Shard
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

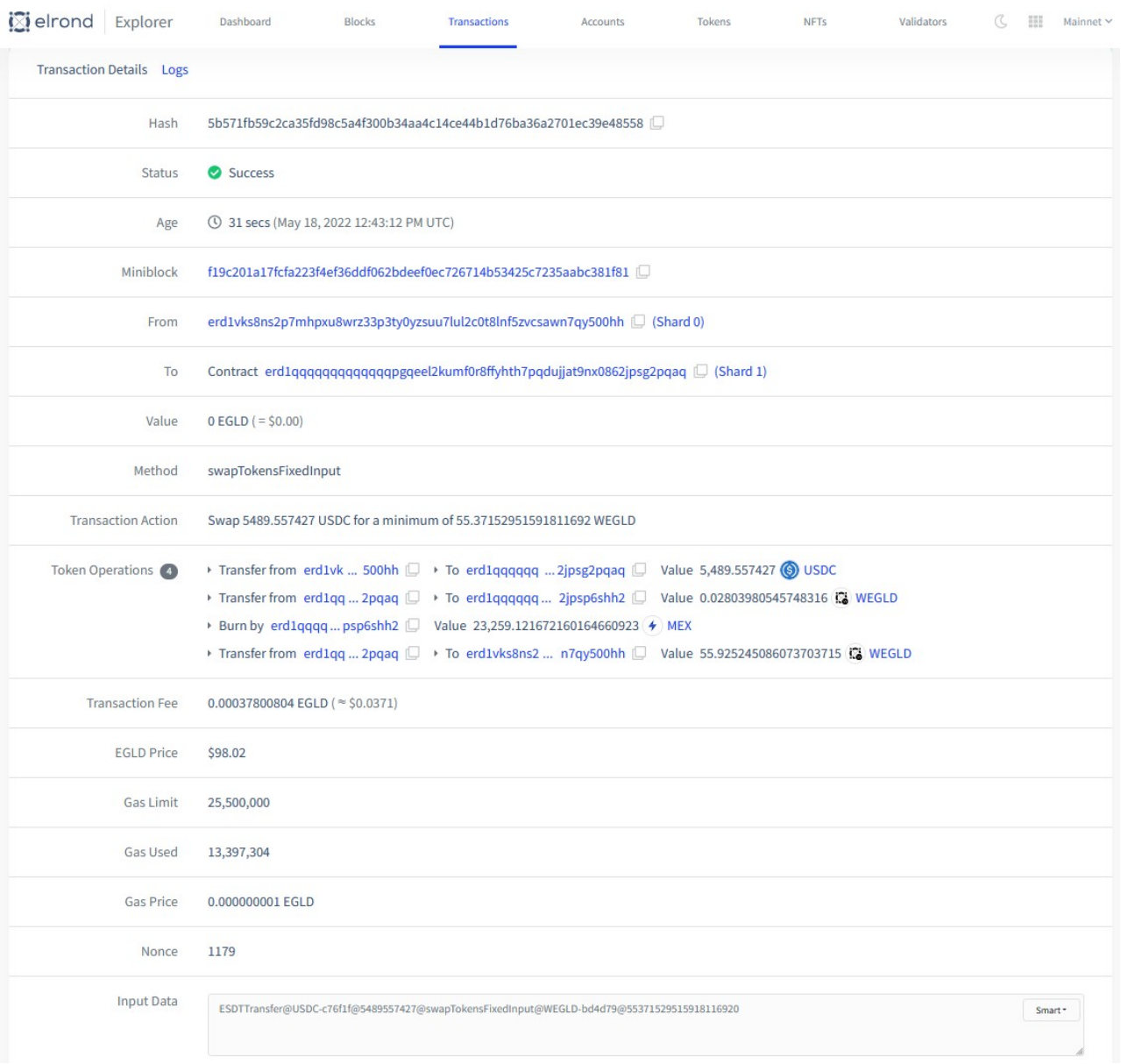
400 < Total Nodes < 800

Node Pool



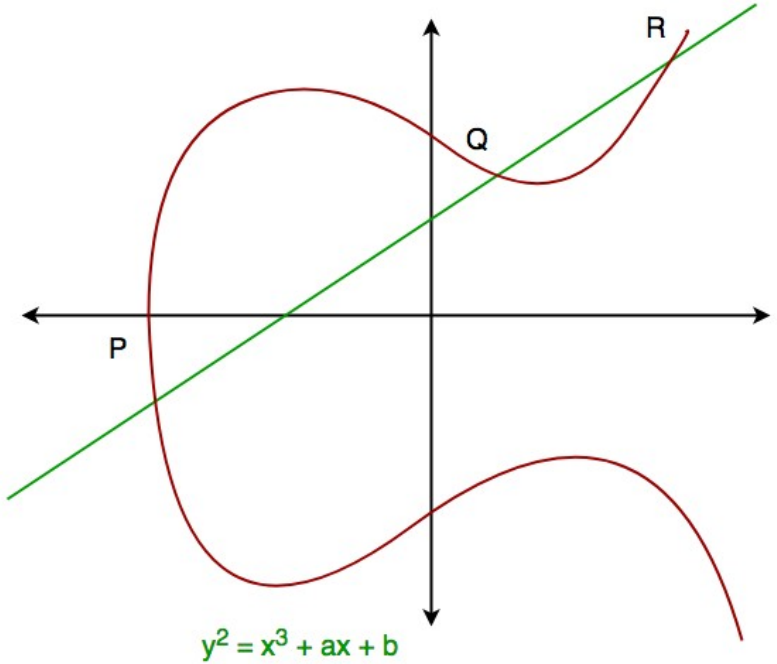
Elrond - Transaction

- Sender
- Receiver
- Value
- Fee
- Nonce
- Data
- Signature



Elrond – Transaction signing
Elliptic curve cryptography

- ECDSA (Elliptic Curve Digital Signature Algorithm) and secp256k1 curve
- EdDSA (Edwards curve DSA) and Curve 25519 (2^{255}-19) ~ 128 bit
- Curve 448: $2^{448}-2^{224}-1$ ~ 256 bit security



This approach uses six tuple {P, a, b, G, n, h}

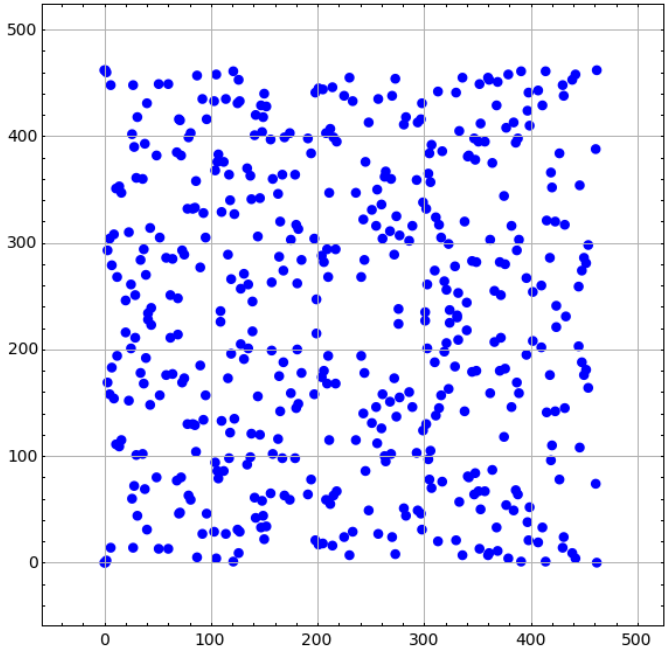
P = Field that the curve is define over

G = Generator point

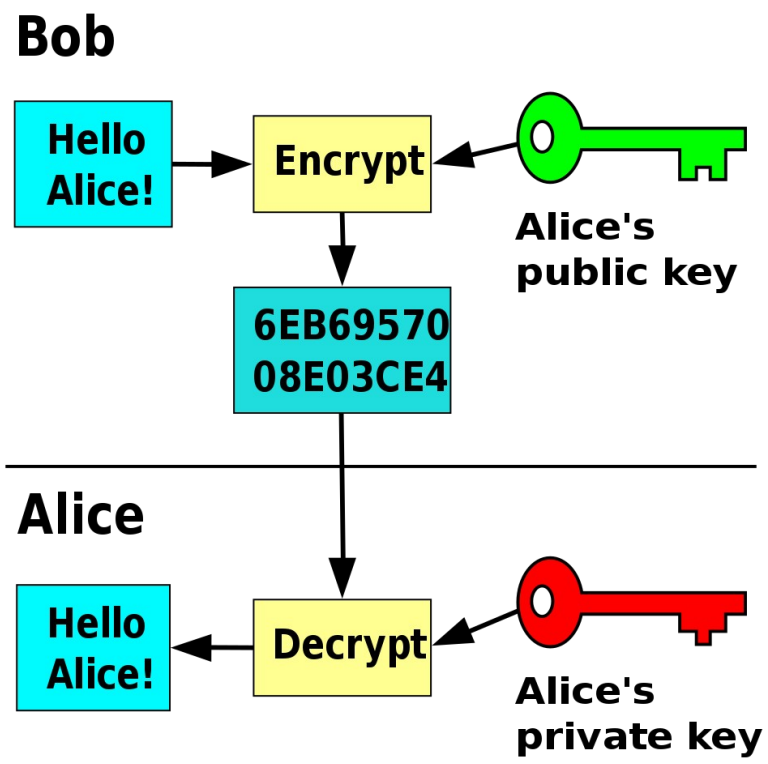
a, b = Values define the curve

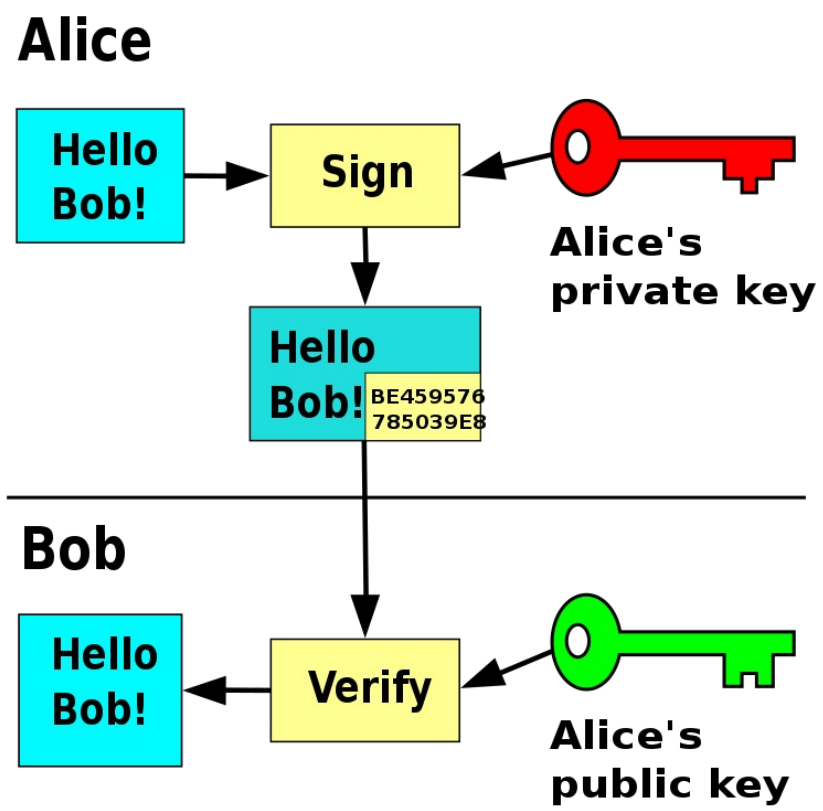
h = Co- factor

n = Prime order of G



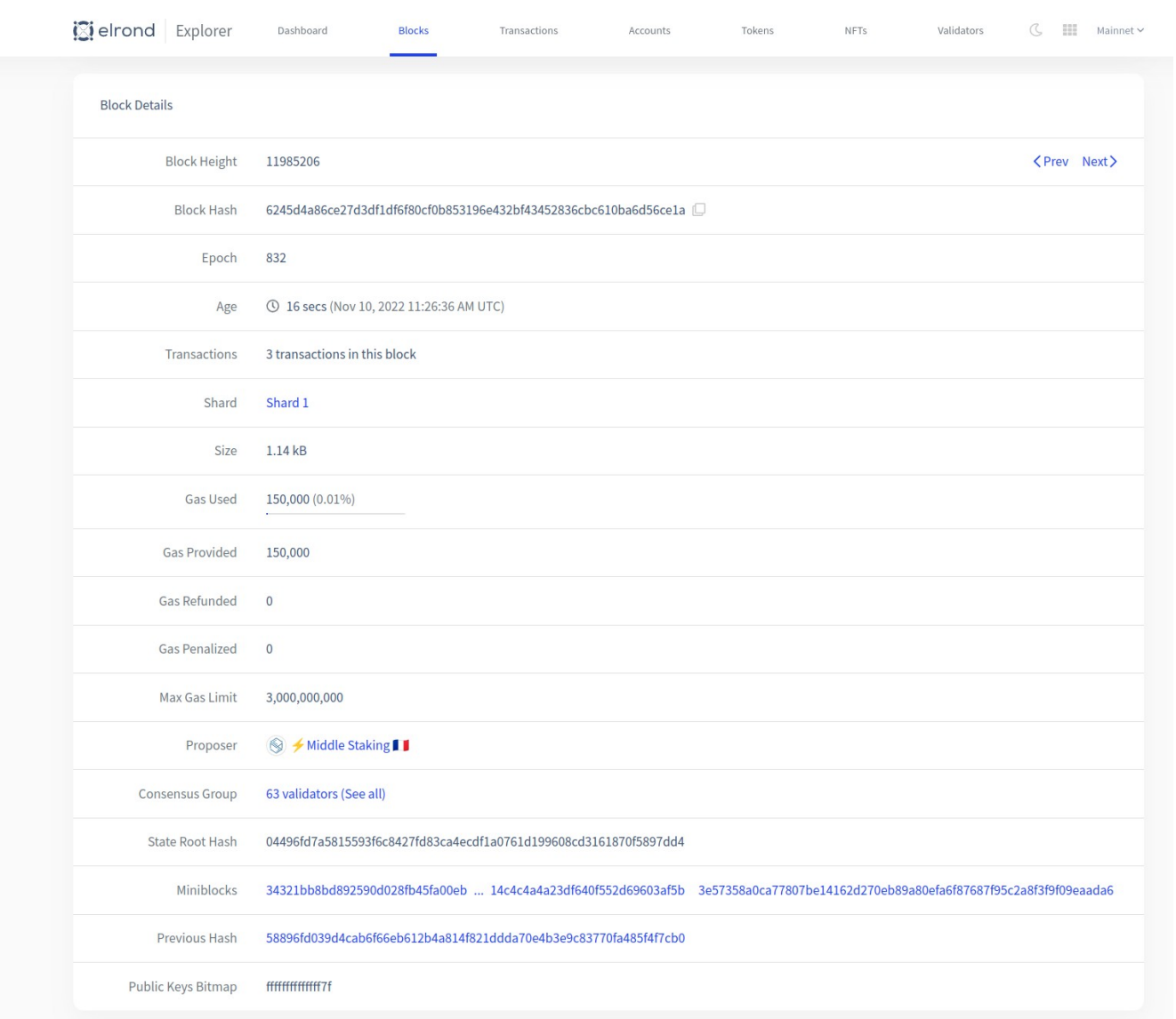
Elrond – Transaction signing - 2
Elliptic curve cryptography - assymetric





Elrond – Blocks

- Shard
- Proposer
- Consensus/PubkeysBitmap
- PreviousHash
- Miniblocks with Txs
- State Root Hash
- Randomness
- Signature



Elrond – Blocks Signing

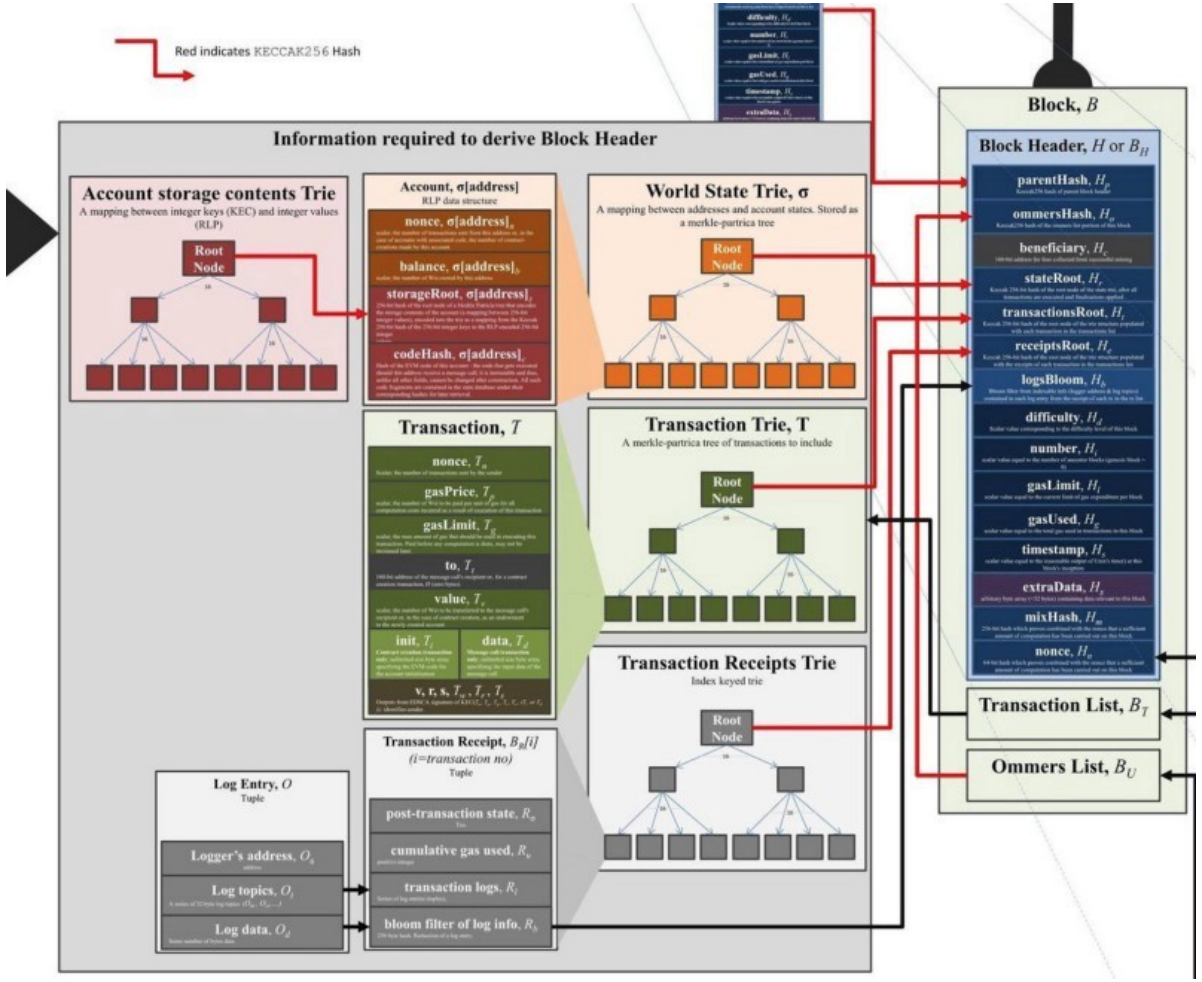
- ECDSA – multiple signatures
- Schnorr - merge signatures, aggregated (sums the signatures)
- BLS (Boneh–Lynn–Shacham) – privacy and trust, threshold

- Staking → 2500 EGLD + sign a message (BLS pubkey/address)→ knowledge of secret key

- 63 / 400 Nodes in consensus → 2/3+1

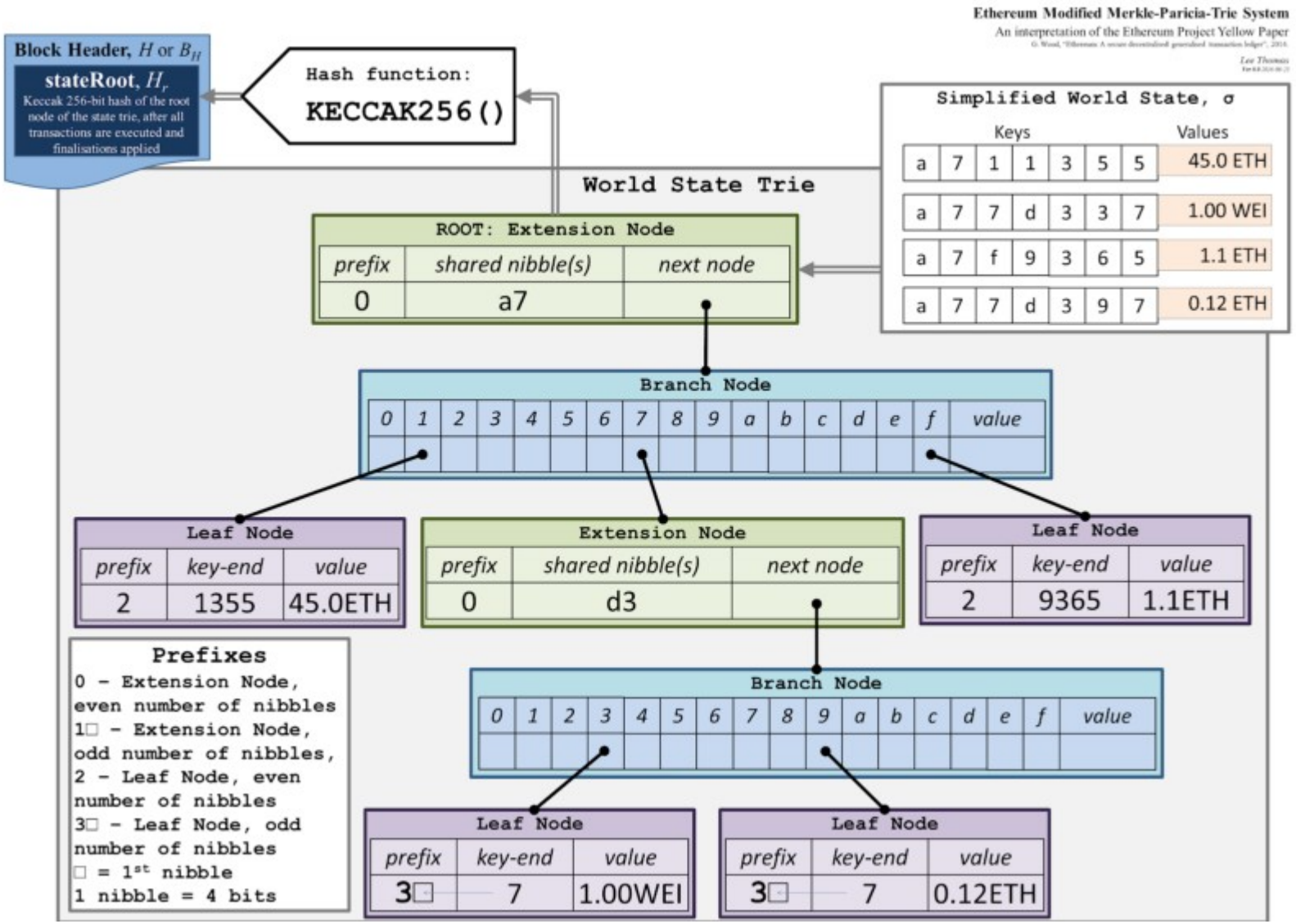
Elrond – Consensus (63/400)

- Chronology:
  - Round: 6 sec
  - Epoch: 14400 rounds
- Transactions ordering
- Proposer
- Correct execution



Elrond – Trie

- Sharded state
- Patricia Merkle Trie:
- tree that has a root node which contains the hash value of the entire data structure
- Trie sync at the epoch start if shuffled out



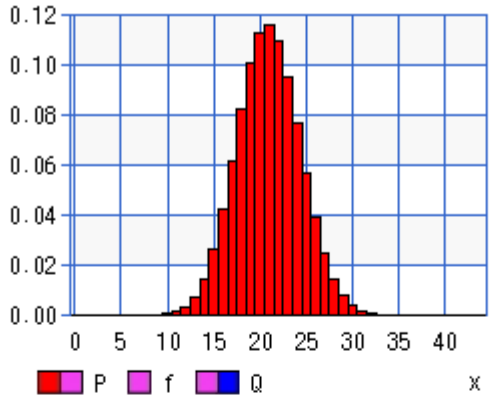
Elrond – random consensus groups

- Sharding → decreased security
- Malicious nodes

- Randomness source → Sign(PrevRandomness source)
- Initially aggregated signature → problem

- BFT assumptions malicious actors:
  - < 25% per network
  - < 33 % per shard

- Consensus → random sampling 63/400 – first is proposer



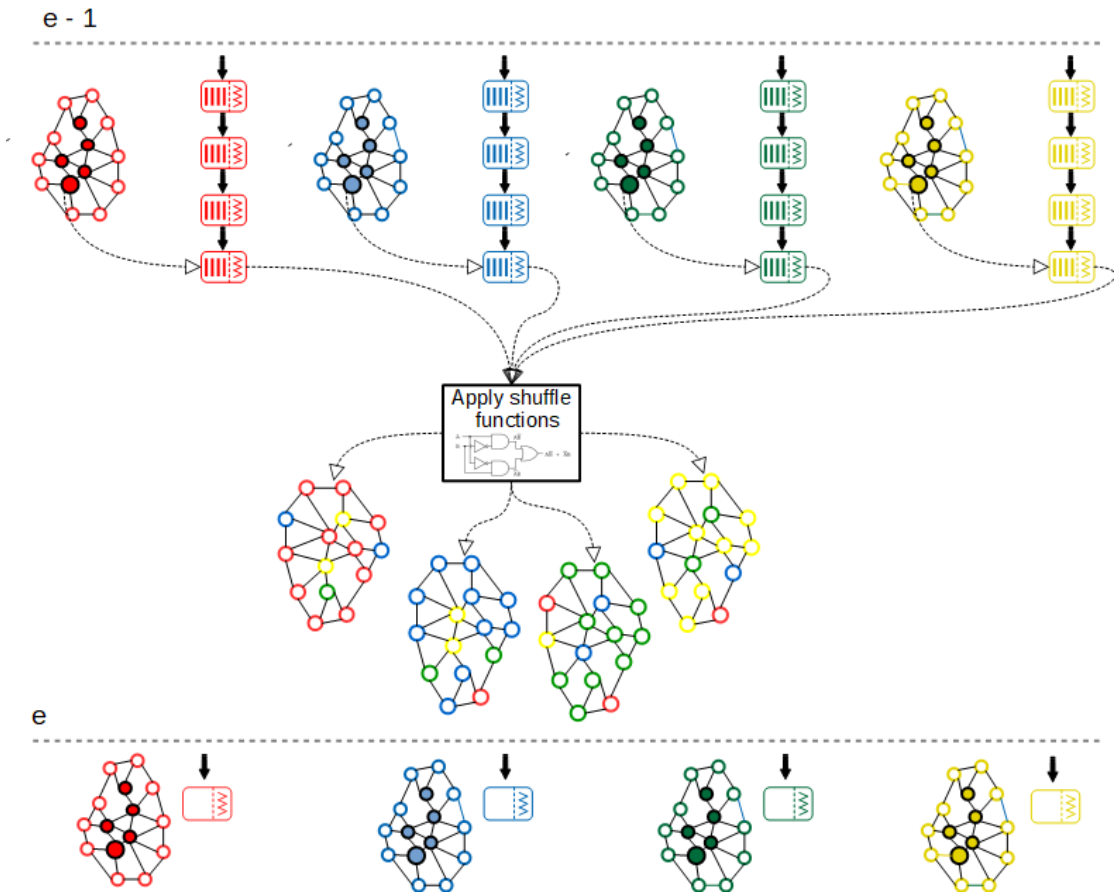
successes of sample x	43	x=0,1,2,.. x≦n
sample size n	63	n=0,1,2,.. n≦N
successes of lot M	133	M=0,1,2,.. x≦M
lot size N	400	N=0,1,2,.. M≦N

Execute Clear Store/Read Print 22digit

hypergeometric distribution	value
probability mass f	4.5125292571885902679E-10
lower cumulative P	0.9999999999125636288
upper cumulative Q	5.3868929691718052822 69E-10
mean	20.9475

Elrond – random shuffling

- 400 Eligible + 400 Waiting per shard
- every epoch – 80 shuffled out and moved to other shards



Elrond – Peer rating

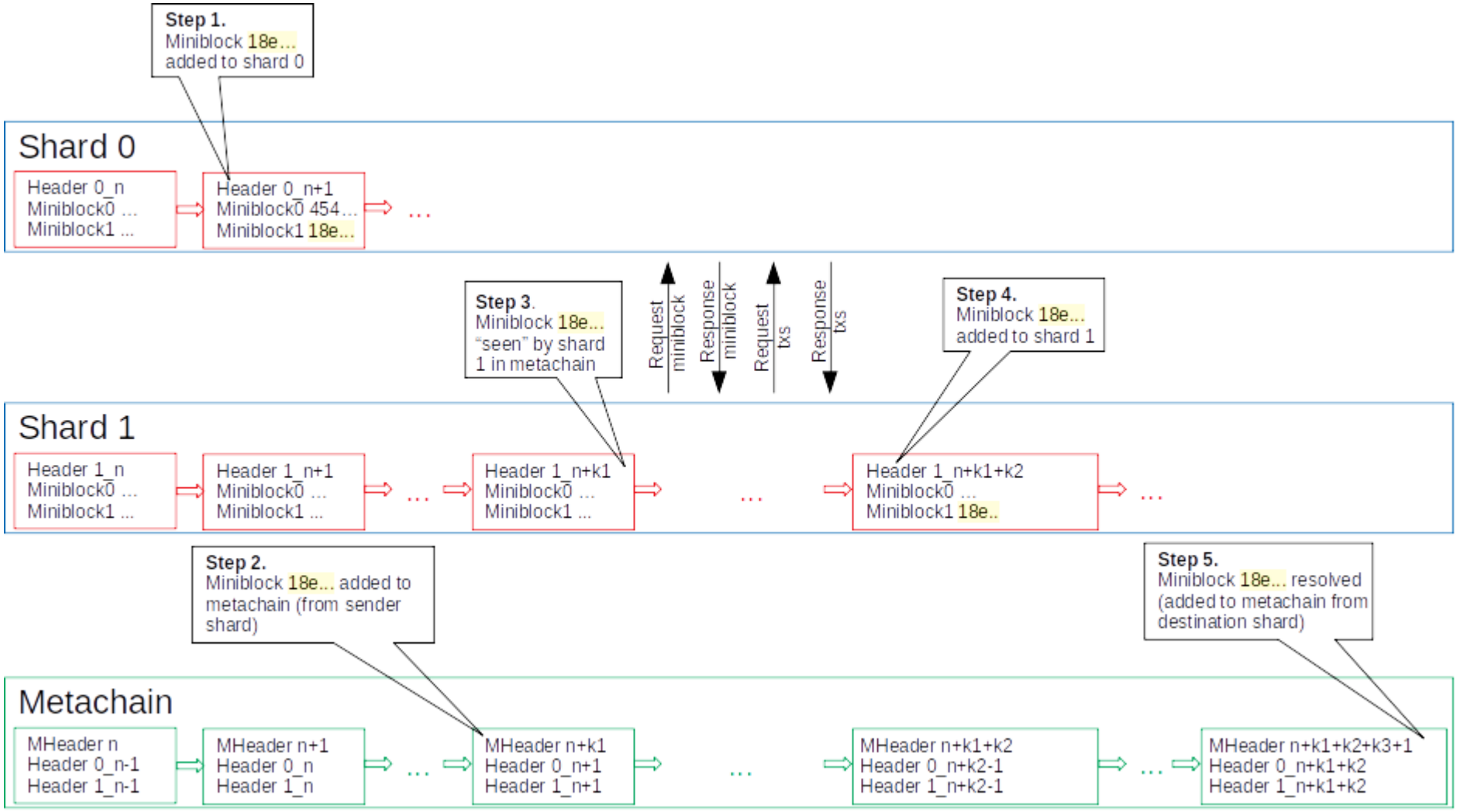
- every round → 1 block proposed (leader + consensus)
- not proposed → rating decrease
  - leader offline
  - consensus offline
  - block too late
  - signatures too late
- rating below 10 → jailed

```
[General]
    StartRating = 5000001
    MaxRating = 10000000
    MinRating = 1
    SignedBlocksThreshold = 0.01
    SelectionChances = [
        { MaxThreshold = 0, ChancePercent = 5},
        { MaxThreshold = 1000000,ChancePercent = 0},
        { MaxThreshold = 2000000,ChancePercent = 16},
        { MaxThreshold = 3000000,ChancePercent = 17},
        { MaxThreshold = 4000000,ChancePercent = 18},
        { MaxThreshold = 5000000,ChancePercent = 19},
        { MaxThreshold = 6000000,ChancePercent = 20},
        { MaxThreshold = 7000000,ChancePercent = 21},
        { MaxThreshold = 8000000,ChancePercent = 22},
        { MaxThreshold = 9000000,ChancePercent = 23},
        { MaxThreshold = 10000000,ChancePercent = 24},
    ]

[ShardChain.RatingSteps]
    HoursToMaxRatingFromStartRating = 72
    ProposerValidatorImportance = 1.0
    ProposerDecreaseFactor = -4.0
    ValidatorDecreaseFactor = -4.0
    ConsecutiveMissedBlocksPenalty = 1.10

[MetaChain.RatingSteps]
    HoursToMaxRatingFromStartRating = 55
    ProposerValidatorImportance = 1.0
    ProposerDecreaseFactor = -4.0
    ValidatorDecreaseFactor = -4.0
    ConsecutiveMissedBlocksPenalty = 1.10
```

Elrond – Cross shard execution



1000x improvement over existing architectures

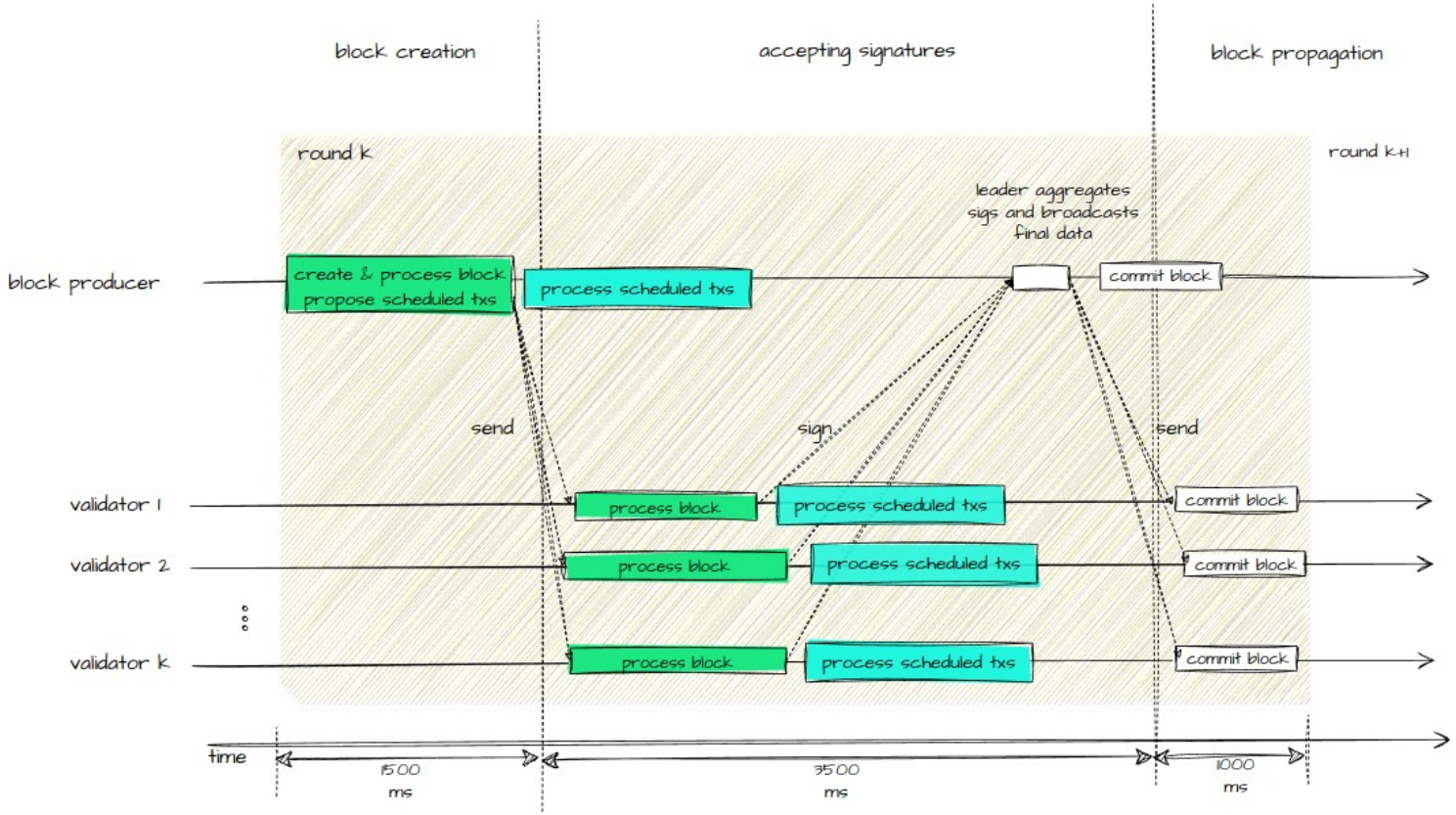
- 15000 TPS with 3 shards (max 1.5 Bil gas)

- Scheduled Transactions
- Partial Miniblocks Execution
- 2x → 30000 TPS

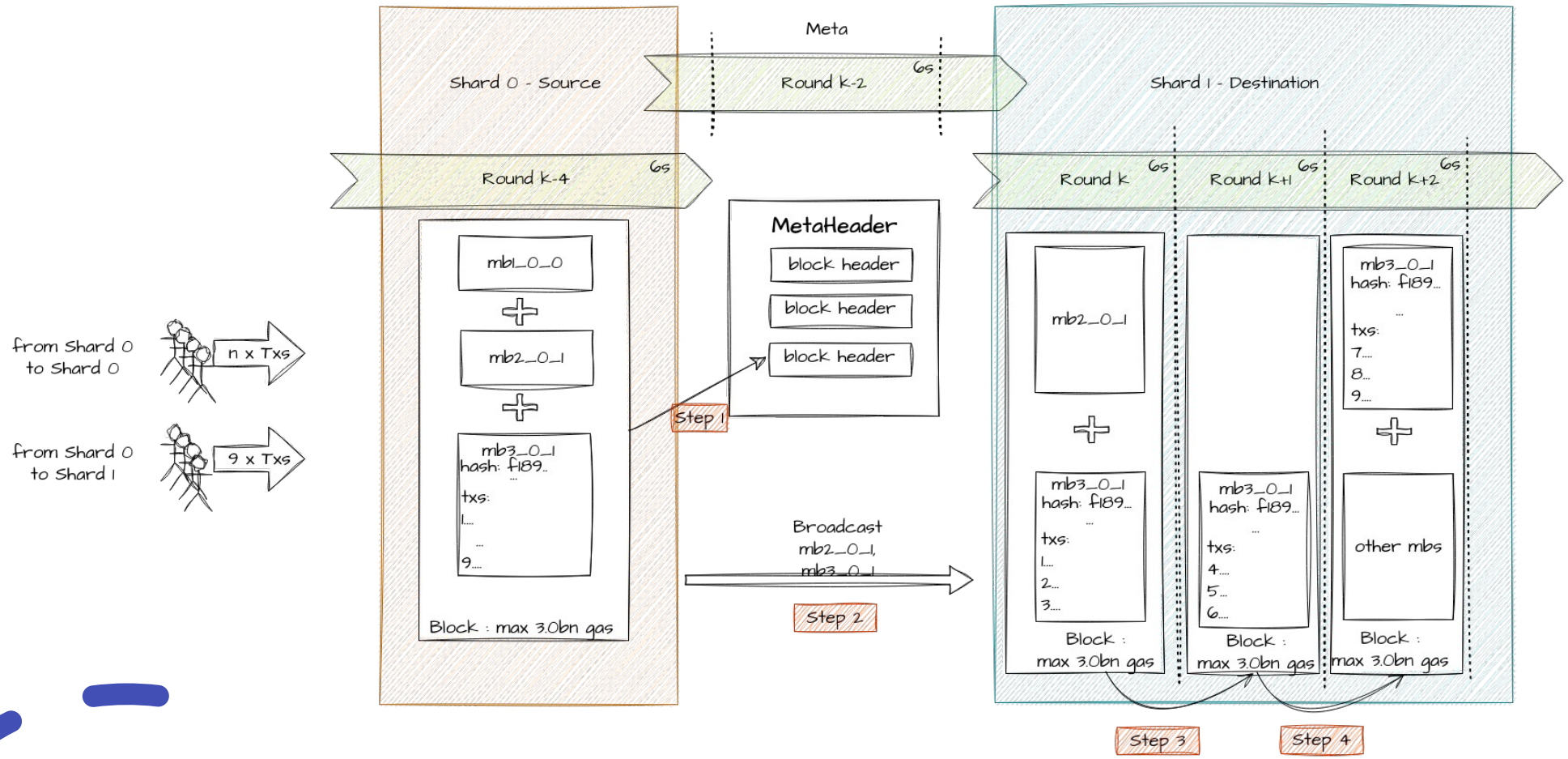
- New Target: 50000 TPS

Scheduled Transactions

processingThresholdPercent = 85%
srStartEndTime = 5%
srBlockEndTime = 25%
srSignatureEndTime = 85%
srEndEndTime = 95%



Partial Miniblocks Execution



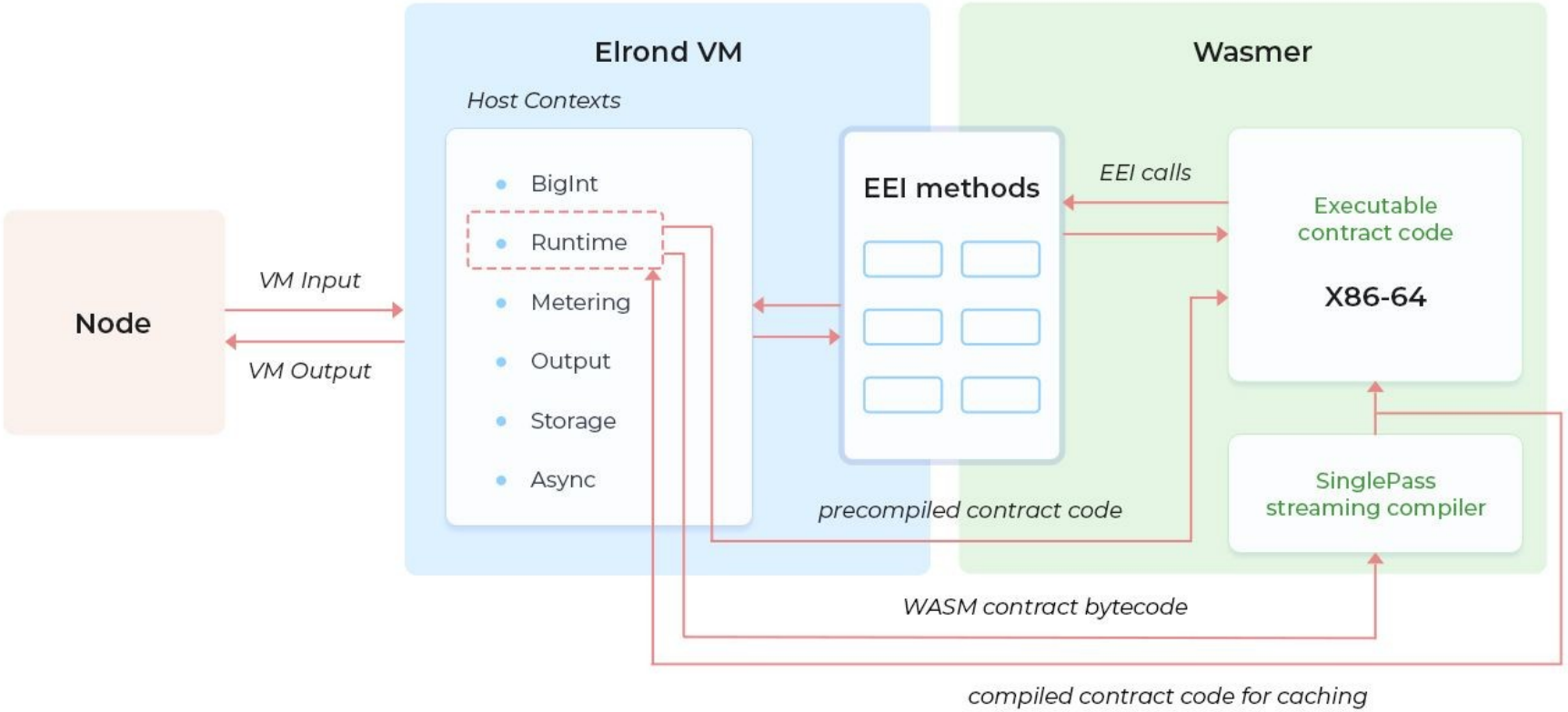
Elrond – ESDT

- Custom tokens at native speed and scalability, without ERC20

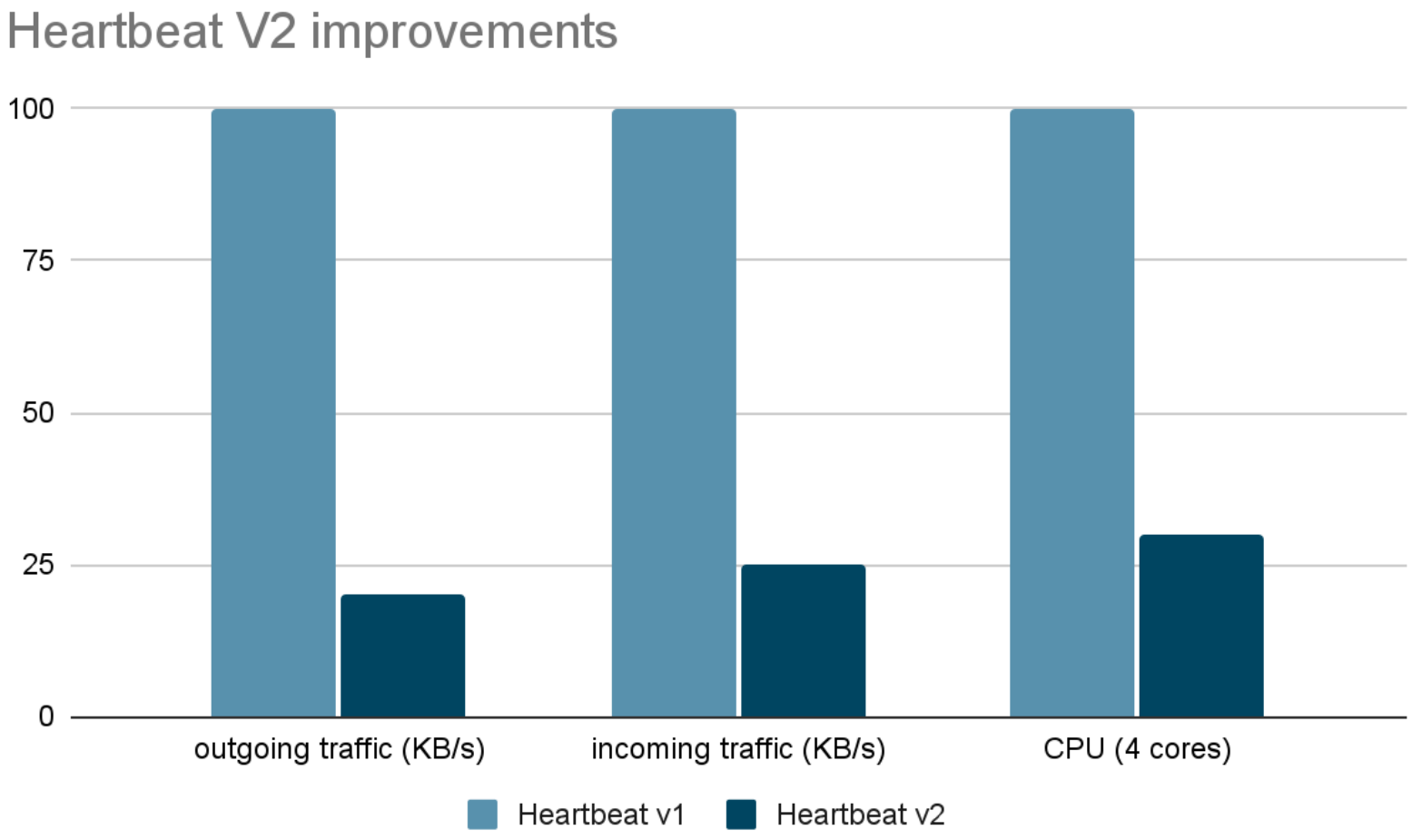
- NFT/SFT/MetaESDT:
- metadata and attributes

```
IssuanceTransaction {
    Sender: <account address of the token manager>
    Receiver: erd1qqqqqqqqqqqqqqqqpqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqzlllls8a5w6u
    Value: 50000000000000000 # (0.05 EGLD)
    GasLimit: 60000000
    Data: "issue" +
          "@" + <token name in hexadecimal encoding> +
          "@" + <token ticker in hexadecimal encoding> +
          "@" + <initial supply in hexadecimal encoding> +
          "@" + <number of decimals in hexadecimal encoding> +
          "@" + <"canFreeze" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encode
          "@" + <"canWipe" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encoded>
          "@" + <"canPause" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encoded
          "@" + <"canMint" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encoded>
          "@" + <"canBurn" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encoded>
          "@" + <"canChangeOwner" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal e
          "@" + <"canUpgrade" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encod
          "@" + <"canAddSpecialRoles" hexadecimal encoded> + "@" + <"true" or "false" hexadecim
}
```

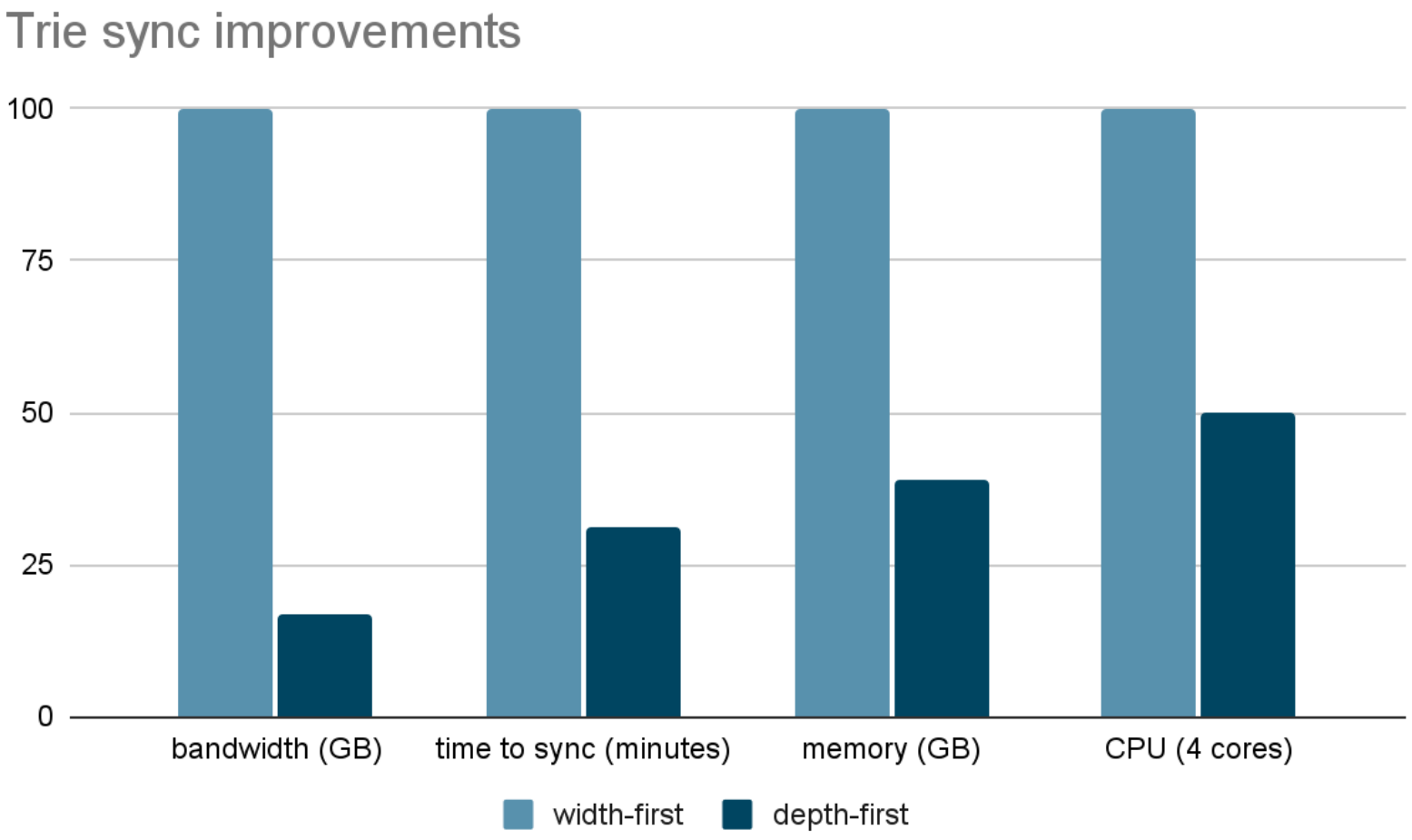
Elrond - VM


Elrond VM
Host Contexts
BigInt
Runtime
Metering
Output
Storage
Async
Node
VM Input
VM Output
EEI methods
EEI calls
Wasmer
Executable contract code
X86-64
SinglePass streaming compiler
precompiled contract code
WASM contract bytecode
compiled contract code for caching

Heartbeat v2 improvements



Trie sync improvements

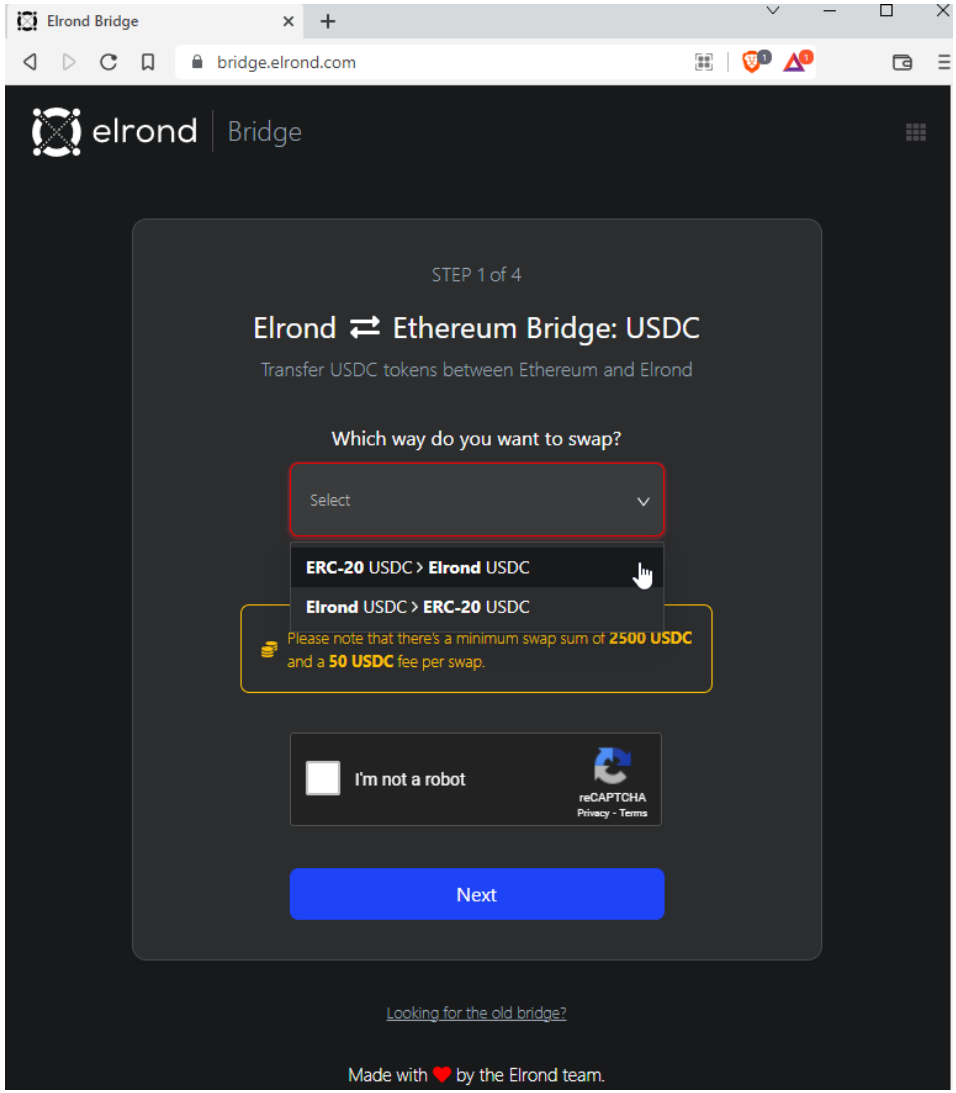


Further improvements

- 16K TPS per shard with “only scheduled-transactions”
- Faster TX Finality: increase consensus size on shards to 400
- 2FA-like mechanism with open source co-signers
- Light Clients, zk-SNARKs
- Sovereign Chain Creation Kit (layer 2 scaling)

Bridge

- Not yet fully automated transfer USDC from/to Ethereum
  - Wrapped USDC on Elrond
  - Stablecoin
  - DEX
- Bridge 2.0
  - Multiple tokens => ESDT (wBTC, wETH)
  - Safe contract
- Largest Crypto Hack: Axie Bridge $750 million



Elrond - Audit

- Blockchain (protocol)– Trail of Bits (Apple, Facebook & DARPA)
- EGLD Economics – Prysm Group
- Smart Contracts – Runtime Verification (Grigore Rosu)
- Bridge Audit – internal, solidity external team and Runtime Verification

Beware of scammers!

- Audit => maybe no bugs in the code
- Social engineering for the 24 words
- Thousands of EGLD lost
  - Lottery
  - Impersonations
  - Fake websites, ads etc
  - ...
- You own your tokens!