

Elrond Network

Blockchain basics



Radu Chis

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

Elrond - Introduction

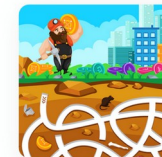
- Idea + Team
- Blockchain 1.0, 2.0 si 3.0
- Nodes/Protocol
- Consensus and Security
- Smart Contracts and Virtual Machine
- Future work

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



Open Finance



Gaming



IoT



Healthcare



Prediction Markets



Cross-Border Payments



Interoperability



Real Estate

Blockchain Trilemma

- Scalability

- } sharding

- } consensus

- } layer 2

- sidechains

- rollups

The Blockchain Trilemma

Decentralization

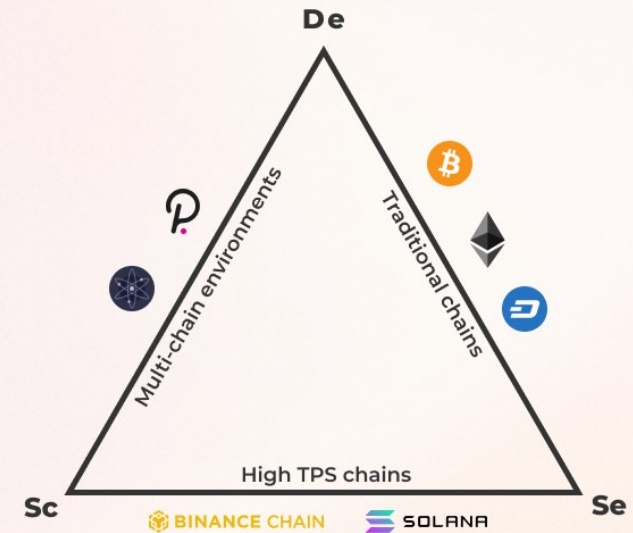
How many nodes?
How many node owners?
Can be hardforked easily?

Scalability

How many transactions per second?
Where is TPS bottleneck?
How it affects network fee?

Security







51% attackable?
Sybil attackable?
ISP level attackable?












Elrond - beginning

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

Advisors
People with relevant experience supporting the team.

 Alex Iskold BUSINESS ADVISOR Managing Director at Technics NYC. Also was founder/CEO at CardSpace. Founder/CEO of Information Laboratory. Chief Architect at Disruptive. Award winner and seasoned investor with experience in over 50 startups.	 Alex Tabarrok ECONOMICS ADVISOR Professor of economics at George Mason University. He holds the Bentley J. Muddan Chair in Economics at the Shenandoah Center. Co-founder of Marginal Revolution University. He is co-author of Modern Principles of Economics and co-author of the Marginal Revolution economics blog.	 Grigore Rosu TECHNICAL ADVISOR Grigore Rosu is a computer science professor at the University of Illinois at Urbana-Champaign (UIUC), where he leads the Formal Systems Laboratory (FSL). Previously, he was a scientist at Intel, where he worked on the term-time verification with his colleagues.
 Andrei Pitis BUSINESS ADVISOR CEO Simple Capital. Founder and CEO of Vector Health. Angel investor with several tech leadership positions.	 Fabio C. Ganesin TECHNICAL ADVISOR Co-founder of City of Zion and NEX, he holds a PhD in computational mechanics and variational multi-scale modeling, and is a research engineer in the petroleum industry.	 Ethan Fast TECHNICAL ADVISOR CS PhD from Stanford. Co-founder of City of Zion and NEX. Co-founder of Intel. Ethan is an entrepreneur and research scientist with a background in HD, AI, and blockchain.

elrond Technology Team Blog Docs Resources BUY EGLD

 CO-FOUNDER & CEO Benjamin Mincu Tech Visionary & Early Blockchain Pioneer in Europe. Previously Product & Business at Nem Core in 2014, Founder & CEO MetaChain Capital. Twitter LinkedIn	 CO-FOUNDER & COO Lucian Todea Tech Entrepreneur, Founder & CEO Soft32, 10M users/month, Partner mobilPay, Angel investor in Typing DNA & Smart Bill. Twitter LinkedIn	 CO-FOUNDER & CIO Lucian Mincu Self-taught Tech Whiz Kid. Previously Engineer at Uhrenwerk 24, Cetto, and Liebl Systems. Co-founder & CTO MetaChain Capital. Twitter LinkedIn
 HEAD OF RESEARCH Felix Crisan CTO of Netopia, co-founder of BTKO, Romania's first Bitcoin exchange platform. Twitter LinkedIn	 HEAD OF TECHNOLOGY Radu Chis Software Engineer NTT DATA, Olympiad champion, CS Teaching Assistant Lucian Blaga Sibiu, PhD CS. Twitter LinkedIn GitHub	 HEAD OF ENGINEERING Adrian Dobrita Software Engineer Intel, ST-Ericsson, Continental, AI Olympiad champion, MSc CS. Twitter LinkedIn GitHub
 CORE DEVELOPER Iulian Pascalau Software Engineer Compa, IoT specialization, BS CS.	 CORE DEVELOPER Sebastian Marian Software Engineer Compa, Multiple world AI RoboCup Olympiad champion.	 CORE DEVELOPER Robert Sasu Software Engineer Continental, Google summer code school, E-mobility

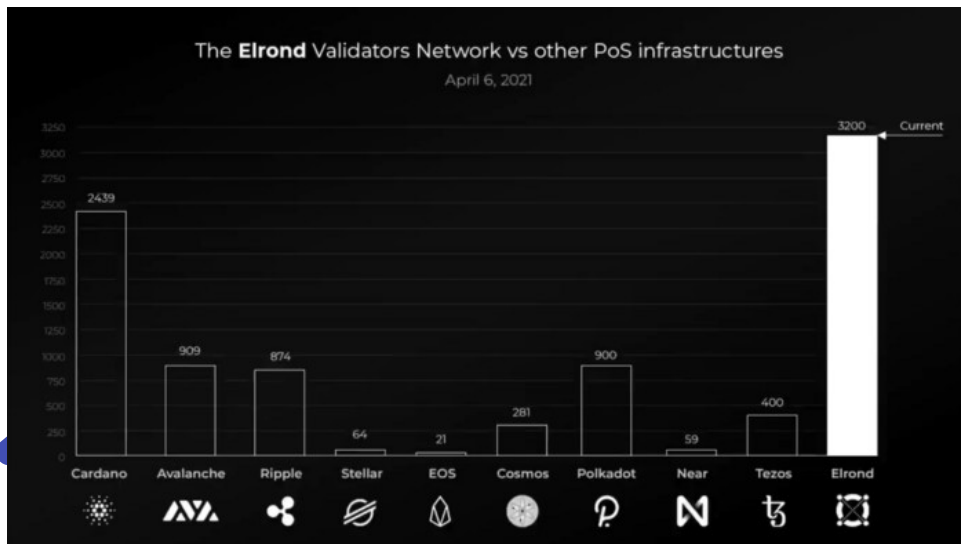
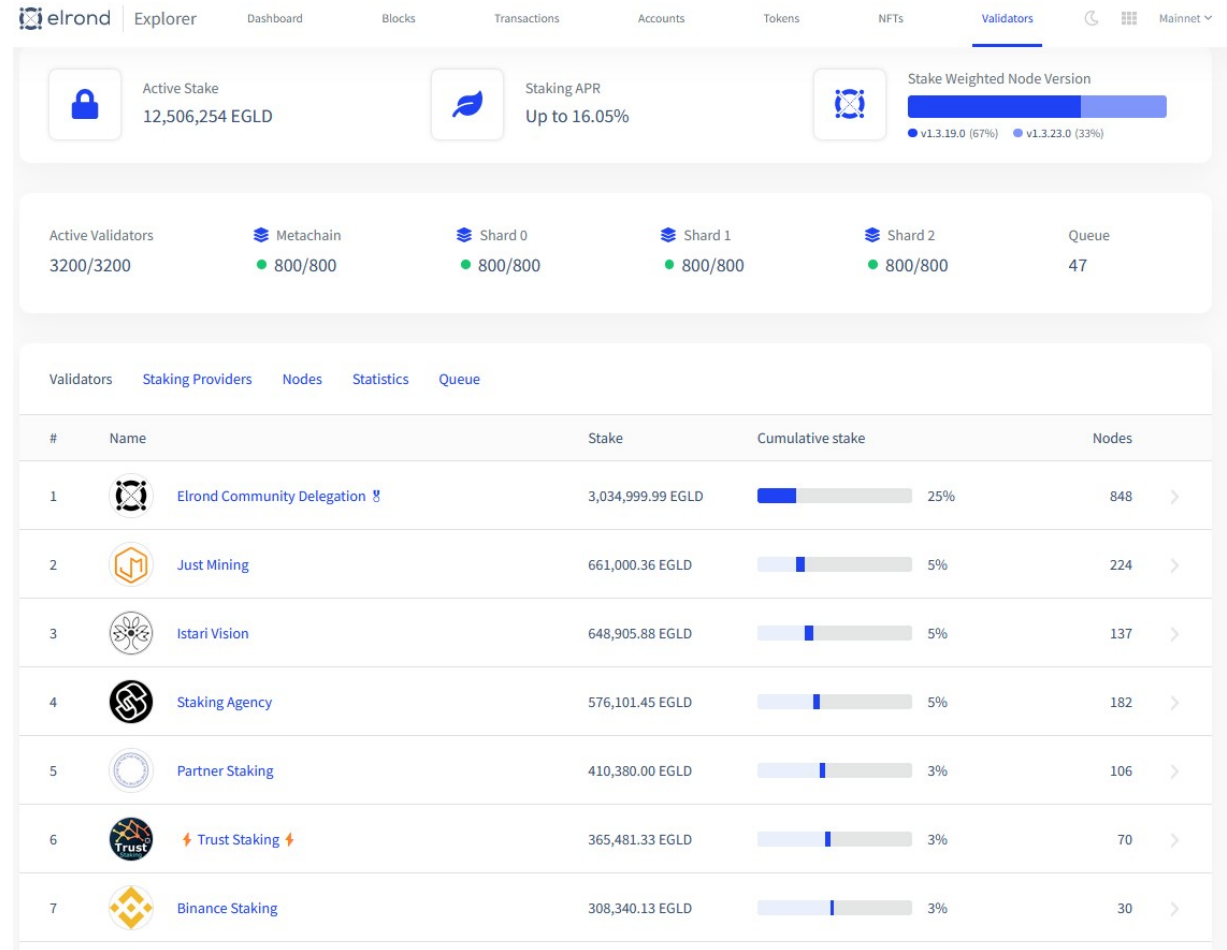
Elrond - The Internet Scale Blockchain

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



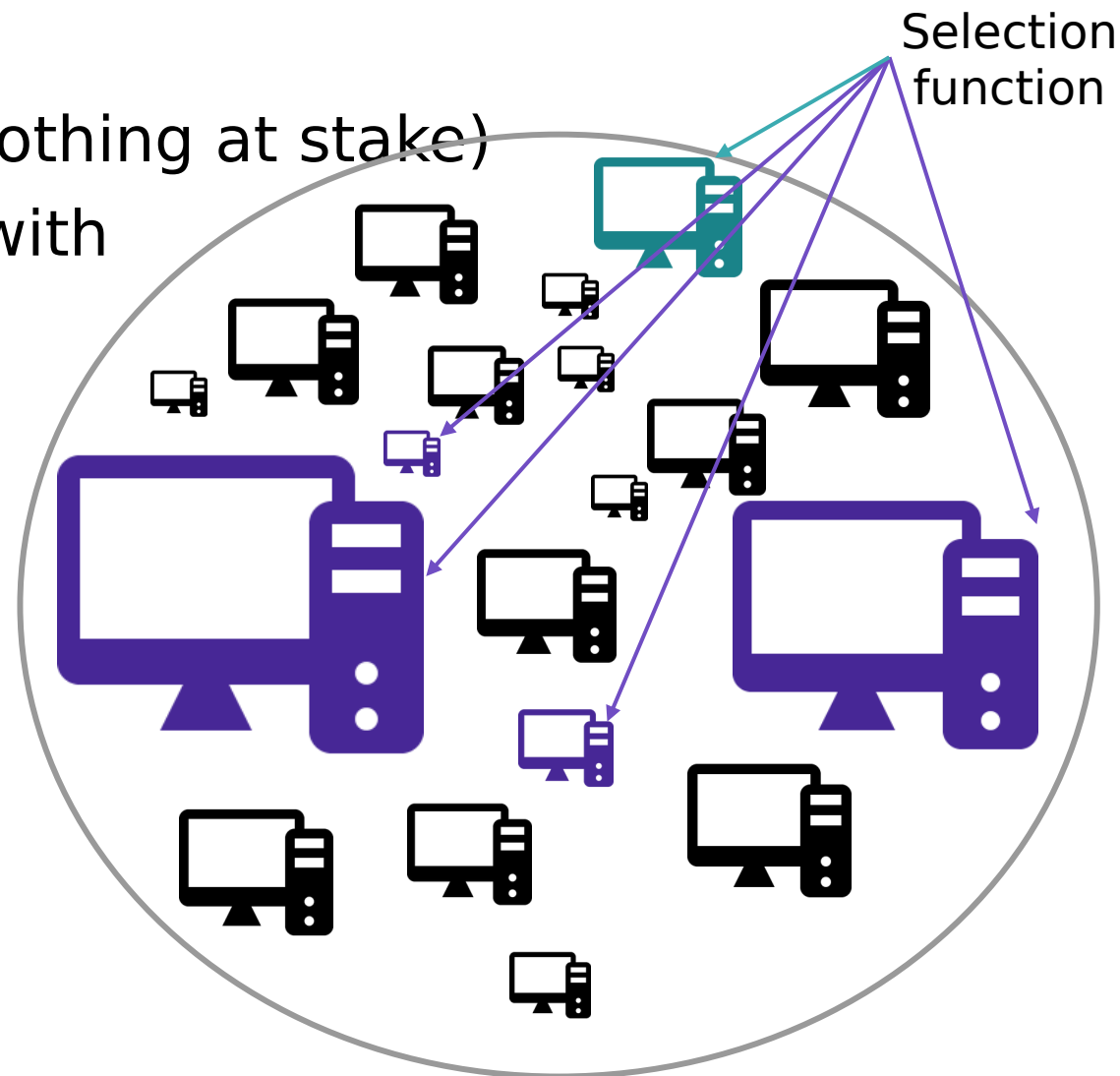
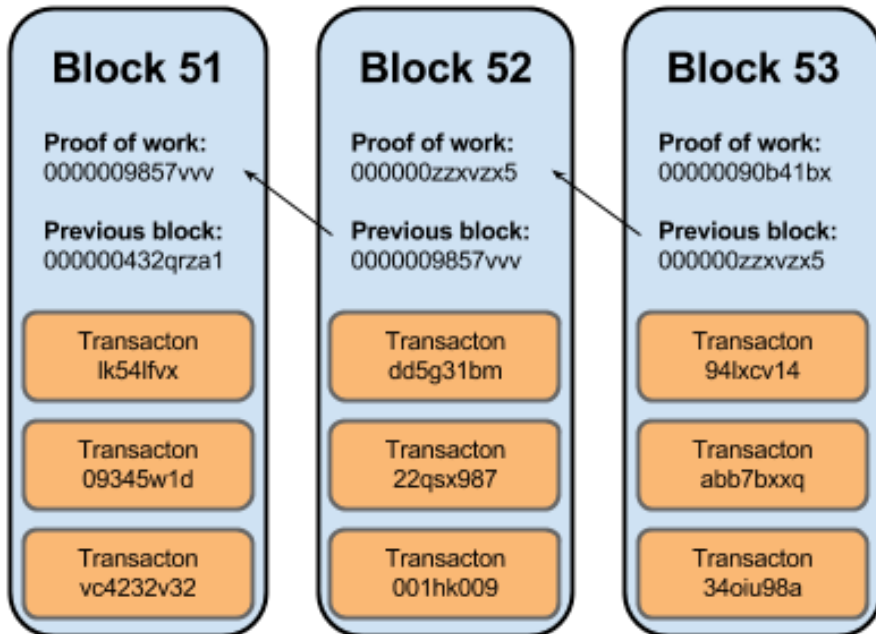
Elrond - 3200 nodes

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

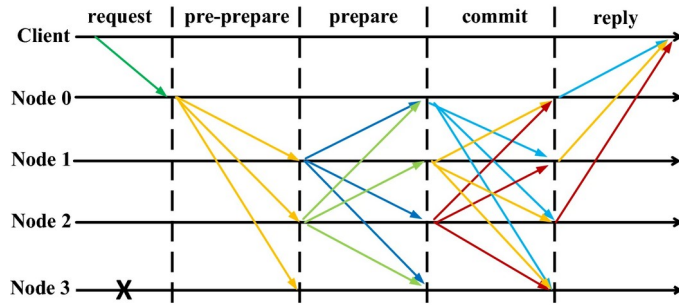


Consens - Proof of Stake

- 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

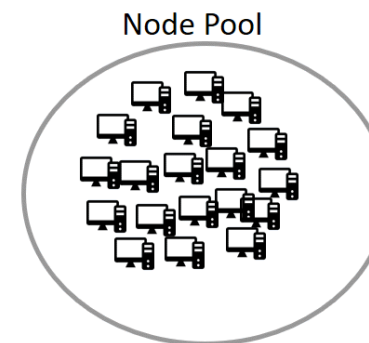
Elrond - Adaptive State Sharding - 2

Step 1:
Node to shard assignment



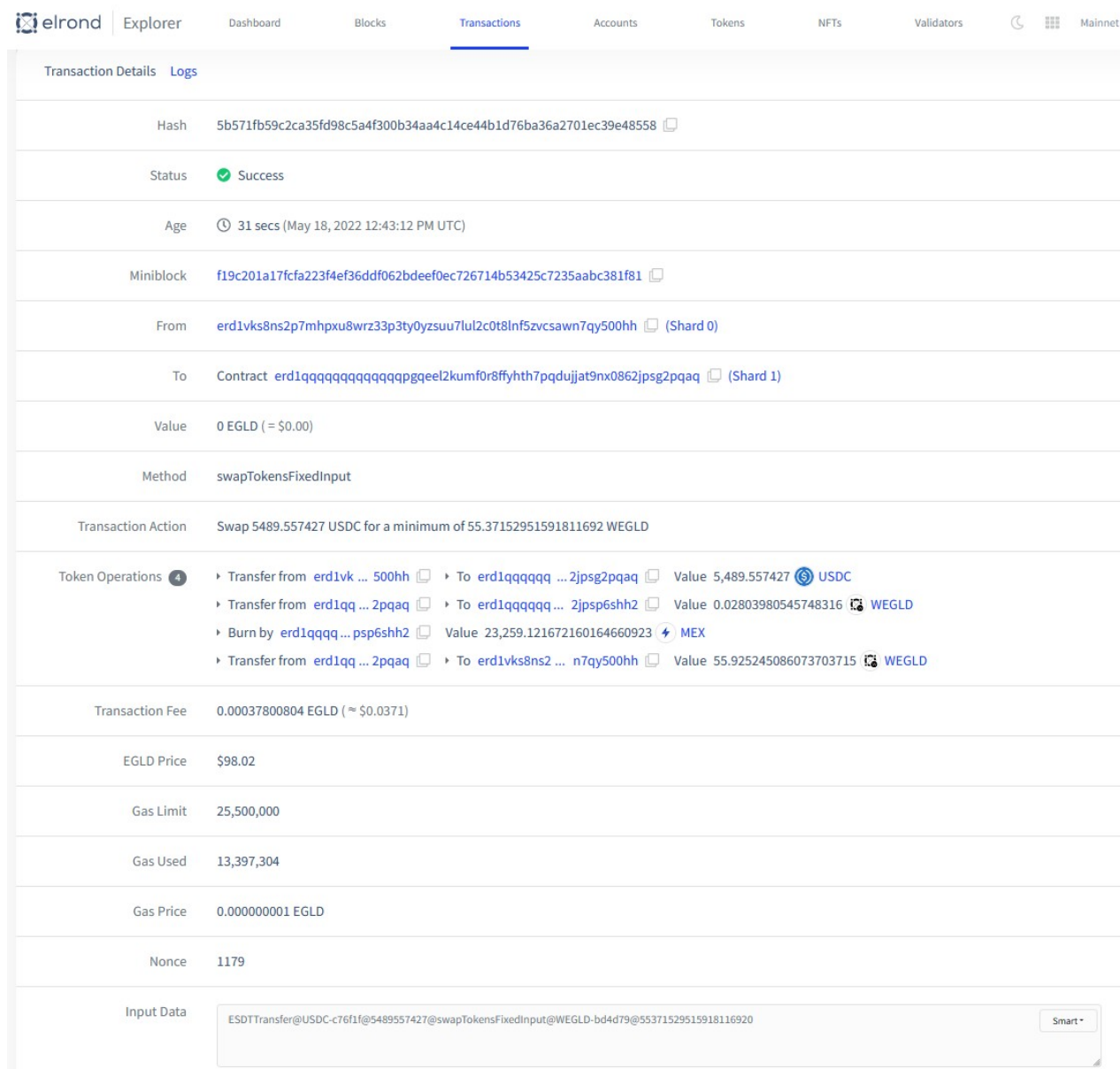
3bit Addresses			Shard
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	0
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	0

400 < Total Nodes < 800



Elrond - Transaction

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

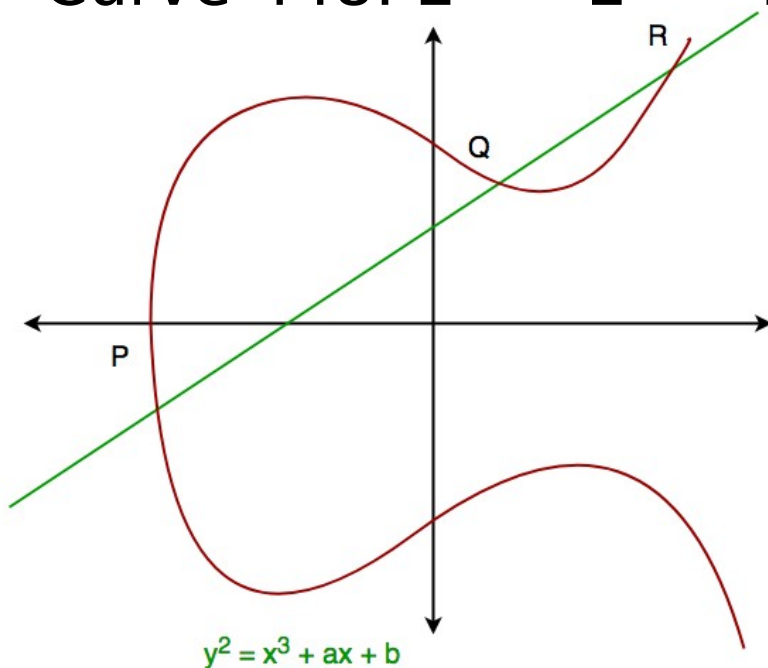


The screenshot displays the Elrond Explorer interface, specifically the Transactions page. The transaction details are as follows:

Field	Value
Hash	5b571fb59c2ca35fd98c5a4f300b34aa4c14ce44b1d76ba36a2701ec39e48558
Status	Success
Age	31 secs (May 18, 2022 12:43:12 PM UTC)
Miniblock	f19c201a17cfa223f4ef36ddf062bdeef0ec726714b53425c7235aac381f81
From	erd1vks8ns2p7mhpXu8wrz33p3ty0yzsuu7lul2c0t8Inf5zvcawn7qy500hh (Shard 0)
To	Contract erd1qqqqqqqqqqqqqqeel2kumf0r8ffyhth7pqdujjat9nx0862jpsg2pqaq (Shard 1)
Value	0 EGLD (= \$0.00)
Method	swapTokensFixedInput
Transaction Action	Swap 5489.557427 USDC for a minimum of 55.37152951591811692 WEGLD
Token Operations	<ul style="list-style-type: none">Transfer from erd1vk ... 500hh to erd1qqqqqq ... 2jpsg2pqaq Value 5,489.557427 USDCTransfer from erd1qq ... 2pqaq to erd1qqqqqq ... 2jpsp6shh2 Value 0.02803980545748316 WEGLDBurn by erd1qqqq ... psp6shh2 Value 23,259.121672160164660923 MEXTransfer from erd1qq ... 2pqaq to erd1vks8ns2 ... n7qy500hh Value 55.925245086073703715 WEGLD
Transaction Fee	0.00037800804 EGLD (≈ \$0.0371)
EGLD Price	\$98.02
Gas Limit	25,500,000
Gas Used	13,397,304
Gas Price	0.000000001 EGLD
Nonce	1179
Input Data	ESDTTransfer@USDC-c76f1f@9489557427@swapTokensFixedInput@WEGLD-bd4d79@95371529515918116920

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 $\{P, a, b, G, n, h\}$

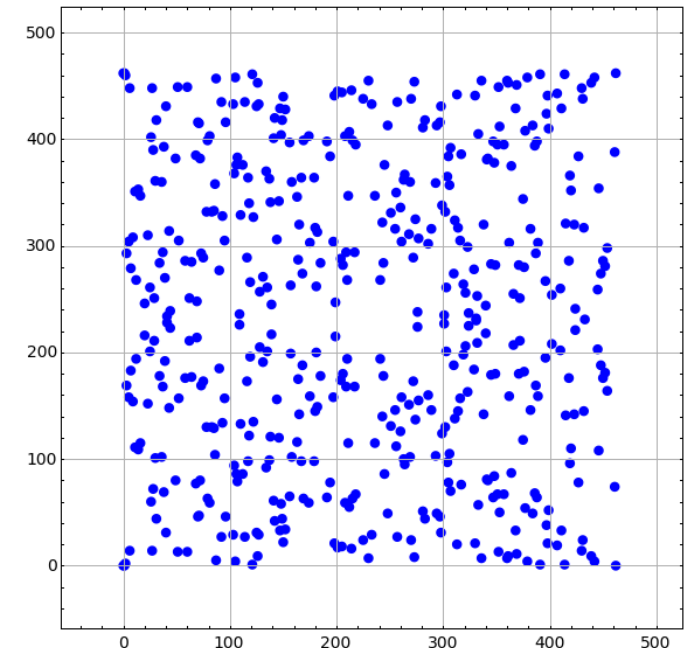
P = Field that the curve is define over

G = Generator point

a, b = Values define the curve

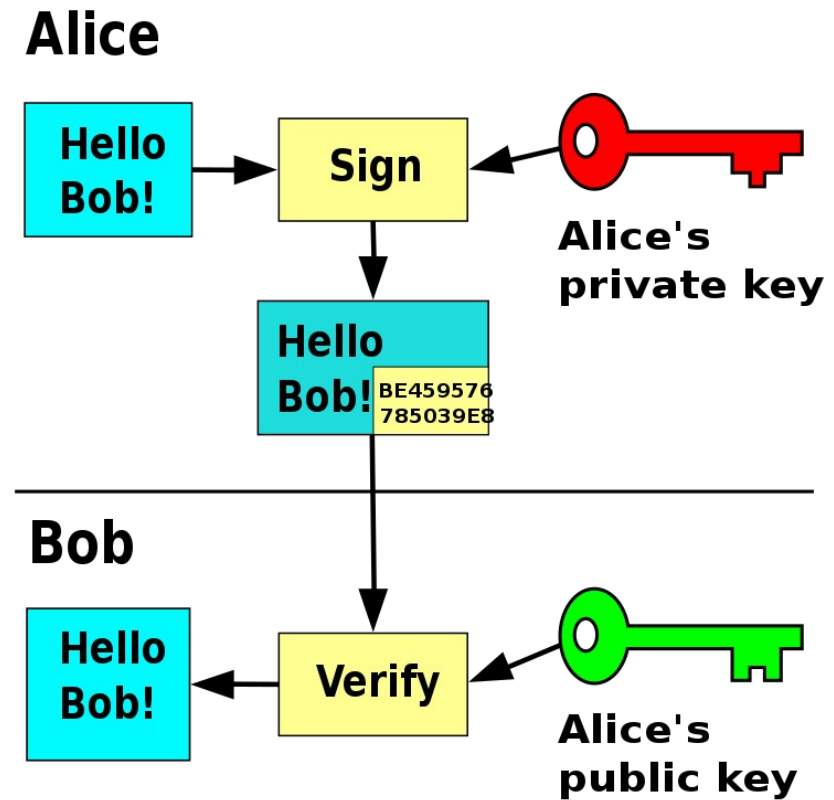
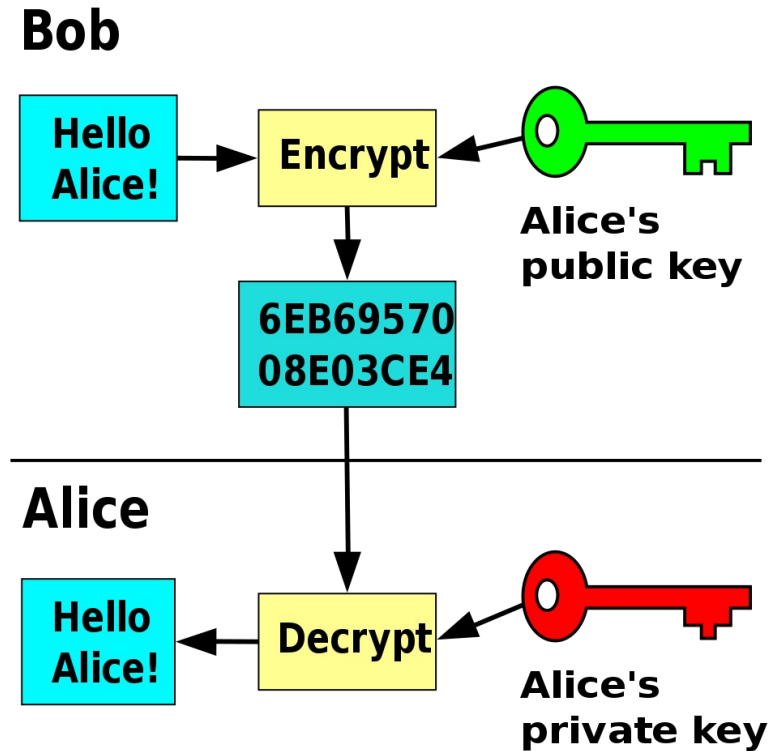
h = Co- factor

n = Prime order of G



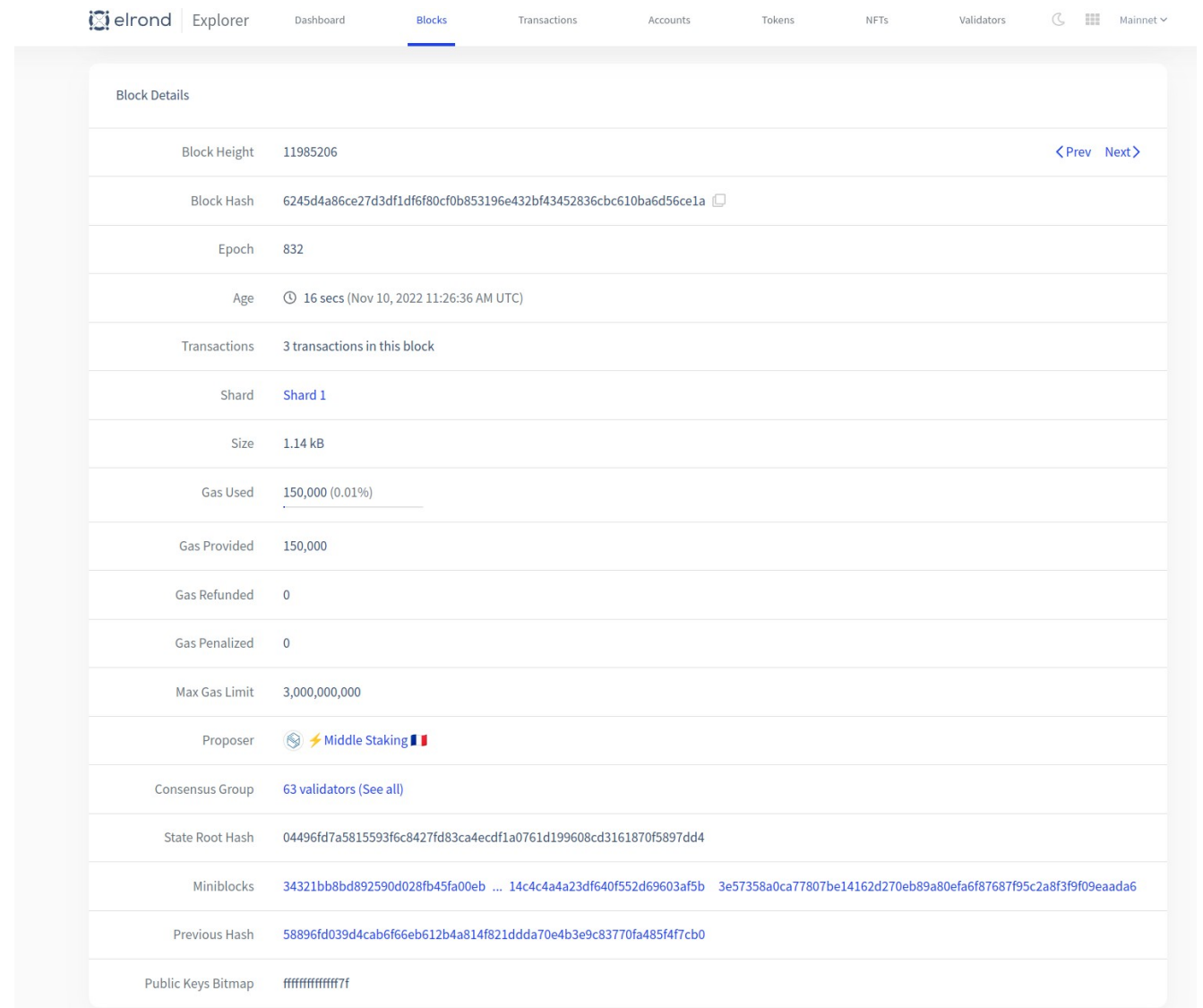
Elrond - Transaction signing - 2

Elliptic curve cryptography - asymmetric



Elrond - Blocks

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



The screenshot shows the 'elrond Explorer' interface with the 'Blocks' tab selected. The main content area displays 'Block Details' for a specific block. The details are as follows:

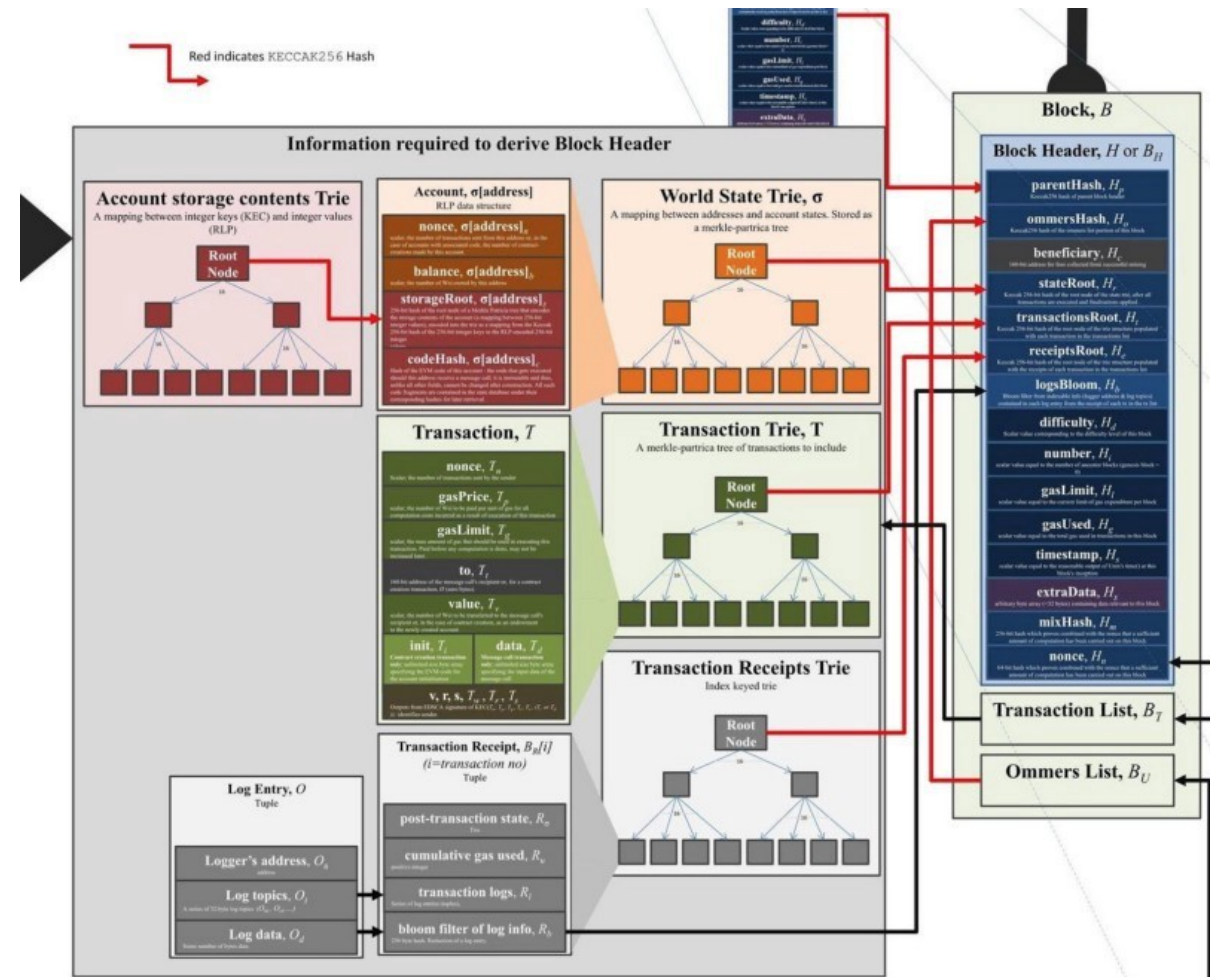
Block Details	
Block Height	11985206 < Prev Next >
Block Hash	6245d4a86ce27d3df1df6f80cf0b853196e432bf43452836cbc610ba6d56ce1a 📄
Epoch	832
Age	🕒 16 secs (Nov 10, 2022 11:26:36 AM UTC)
Transactions	3 transactions in this block
Shard	Shard 1
Size	1.14 kB
Gas Used	150,000 (0.01%)
Gas Provided	150,000
Gas Refunded	0
Gas Penalized	0
Max Gas Limit	3,000,000,000
Proposer	👤 ⚡ Middle Staking 🇫🇷
Consensus Group	63 validators (See all)
State Root Hash	04496fd7a5815593f6c8427fd83ca4ecdf1a0761d199608cd3161870f5897dd4
Miniblocks	34321bb8bd892590d028fb45fa00eb ... 14c4c4a4a23df640f552d69603af5b 3e57358a0ca77807be14162d270eb89a80efa6f87687f95c2a8f3f9f09eaada6
Previous Hash	58896fd039d4cab6f66eb612b4a814f821ddda70e4b3e9c83770fa485f4f7cb0
Public Keys Bitmap	ffffffffffff7f

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 → $2/3+1$

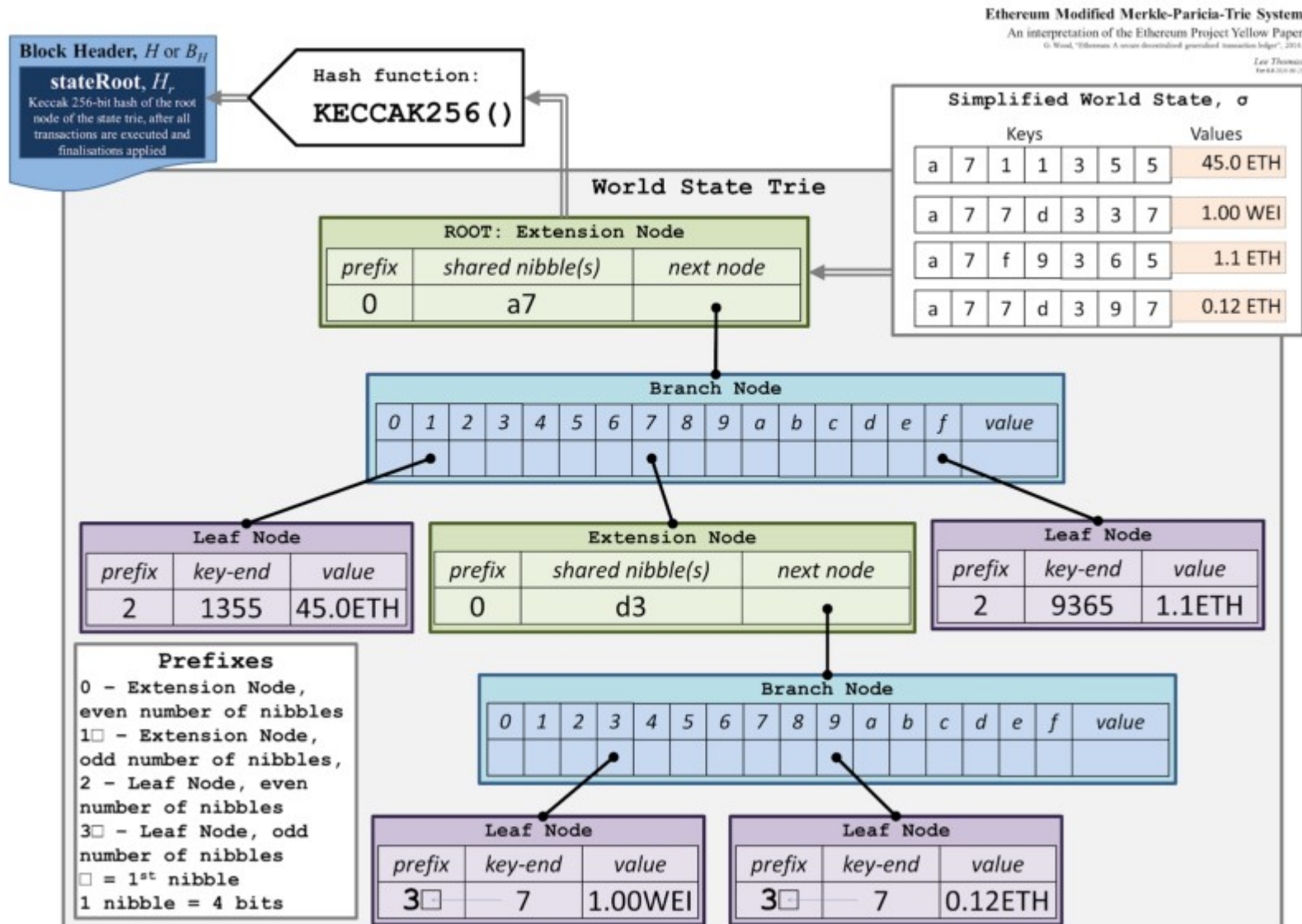
Elrond - Consensus (63/400)

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



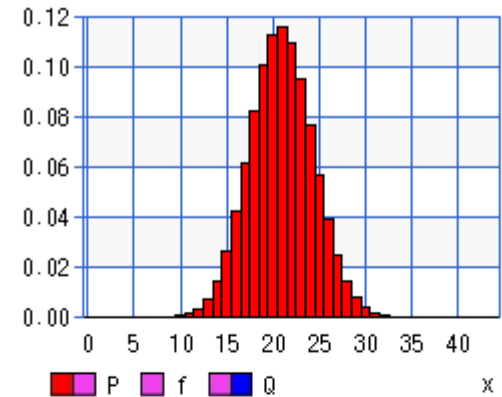
Elrond - Trie

- 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

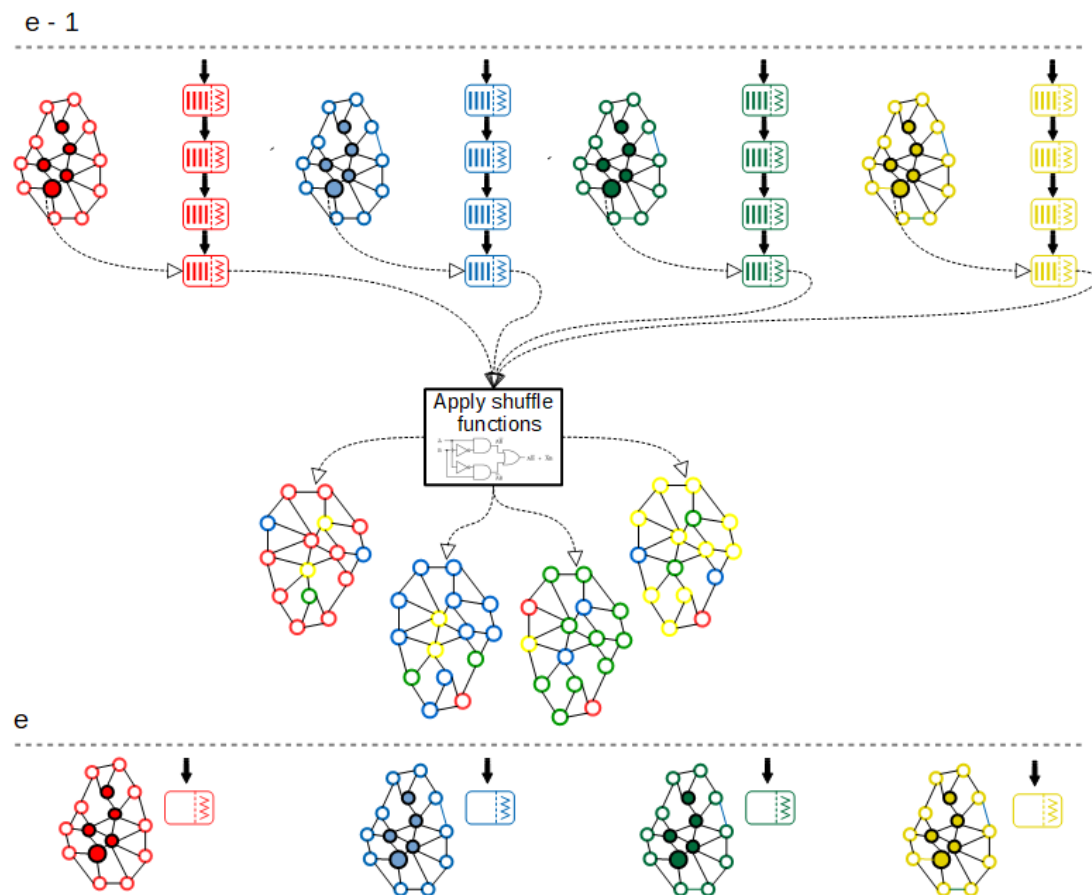


successes of sample x x=0,1,2,... x≤n
 sample size n n=0,1,2,... n≤N
 successes of lot M M=0,1,2,... x≤M
 lot size N N=0,1,2,... M≤N

hypergeometric distribution	value
■ probability mass f	4.5125292571885902679E-10
lower cumulative P	0.9999999999125636288
upper cumulative Q	5.386892969171805282269E-10
mean	20.9475

Elrond - random shuffling

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

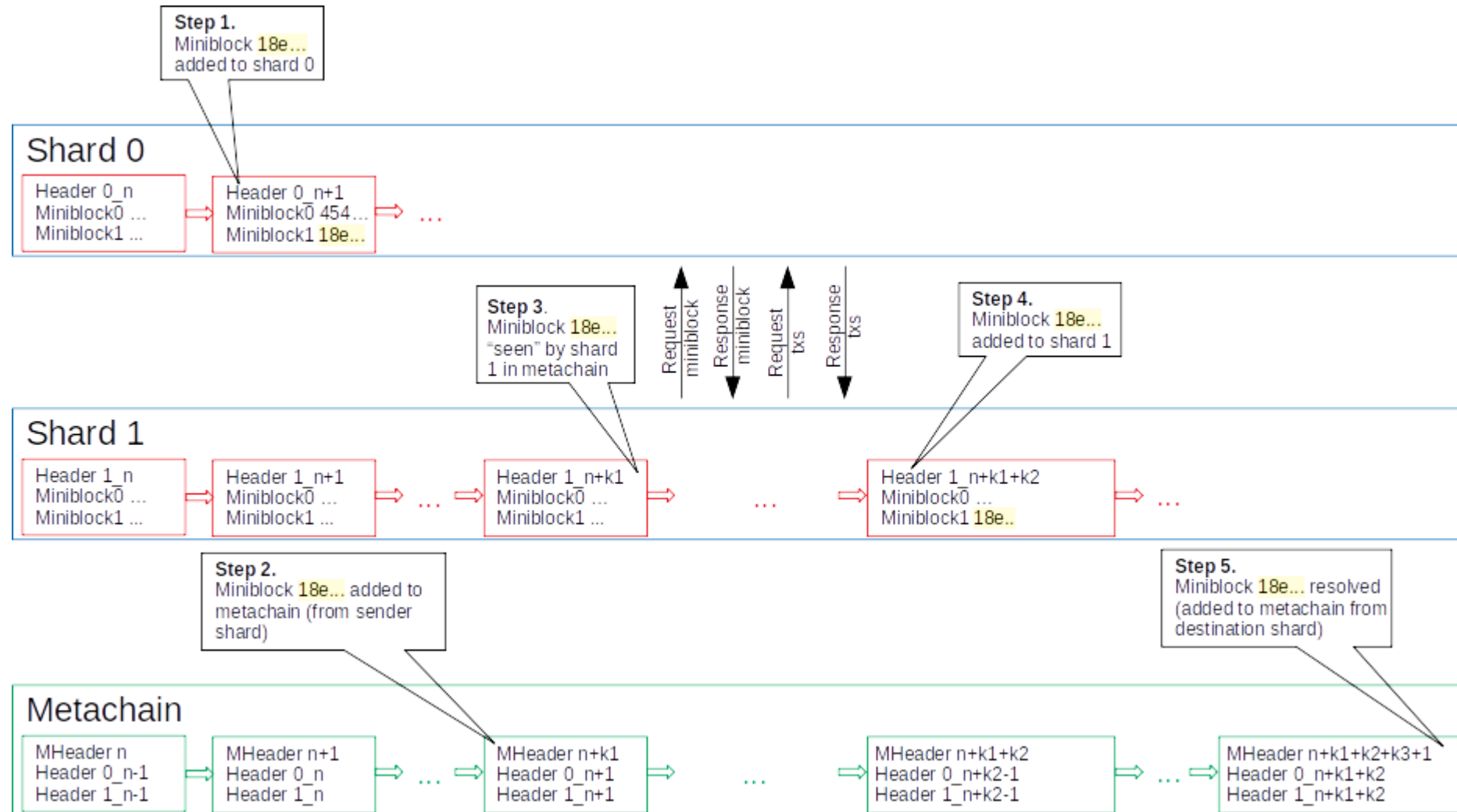


Elrond - Peer rating

- 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

```
11
12 [General]
13     StartRating = 5000001
14     MaxRating = 10000000
15     MinRating = 1
16     SignedBlocksThreshold = 0.01
17     SelectionChances = [
18         { MaxThreshold = 0, ChancePercent = 5},
19         { MaxThreshold = 1000000, ChancePercent = 0},
20         { MaxThreshold = 2000000, ChancePercent = 16},
21         { MaxThreshold = 3000000, ChancePercent = 17},
22         { MaxThreshold = 4000000, ChancePercent = 18},
23         { MaxThreshold = 5000000, ChancePercent = 19},
24         { MaxThreshold = 6000000, ChancePercent = 20},
25         { MaxThreshold = 7000000, ChancePercent = 21},
26         { MaxThreshold = 8000000, ChancePercent = 22},
27         { MaxThreshold = 9000000, ChancePercent = 23},
28         { MaxThreshold = 10000000, ChancePercent = 24},
29     ]
30
31 [ShardChain.RatingSteps]
32     HoursToMaxRatingFromStartRating = 72
33     ProposerValidatorImportance = 1.0
34     ProposerDecreaseFactor = -4.0
35     ValidatorDecreaseFactor = -4.0
36     ConsecutiveMissedBlocksPenalty = 1.10
37
38 [MetaChain.RatingSteps]
39     HoursToMaxRatingFromStartRating = 55
40     ProposerValidatorImportance = 1.0
41     ProposerDecreaseFactor = -4.0
42     ValidatorDecreaseFactor = -4.0
43     ConsecutiveMissedBlocksPenalty = 1.10
44
```

Elrond - Cross shard execution

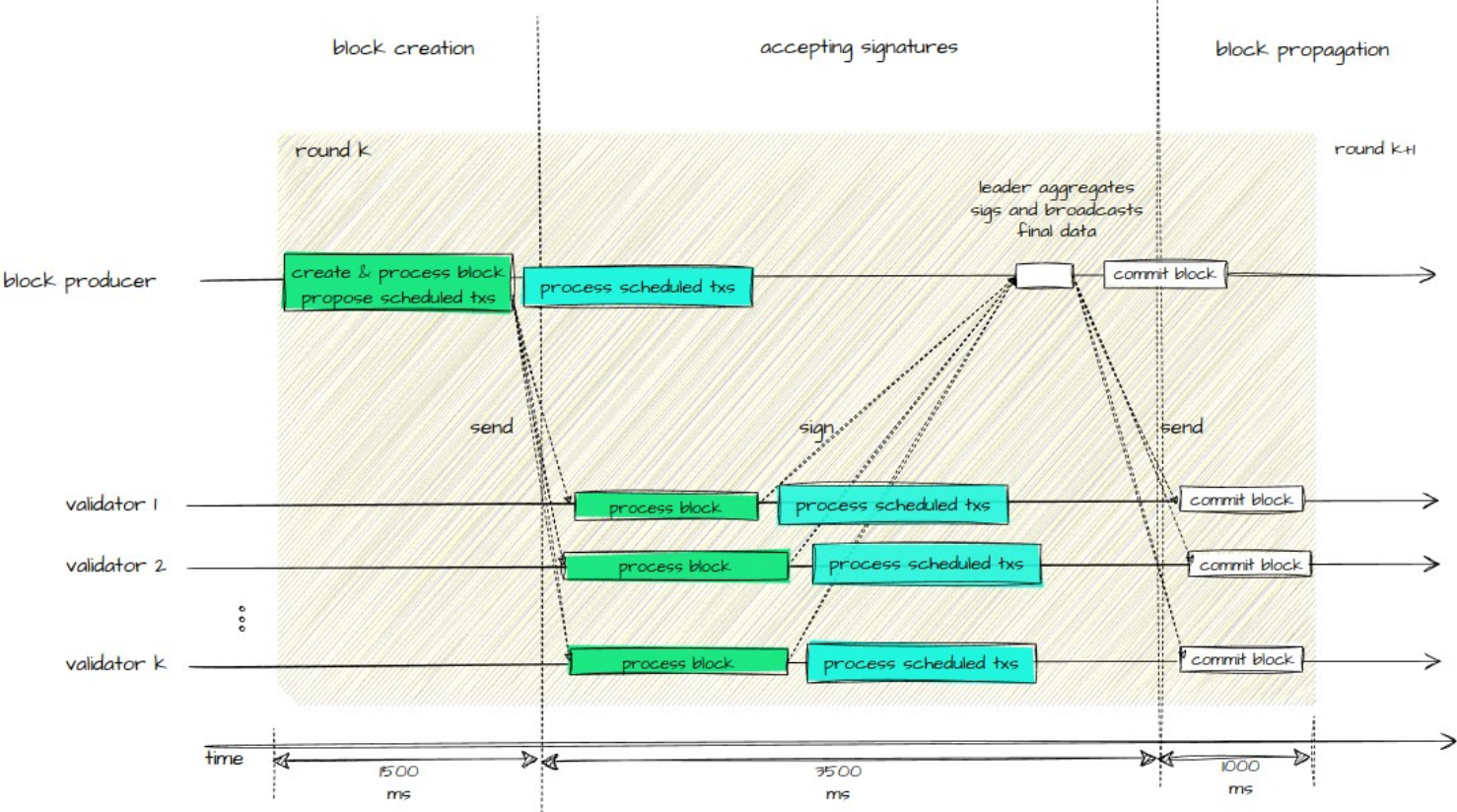


1000x improvement over existing architectures

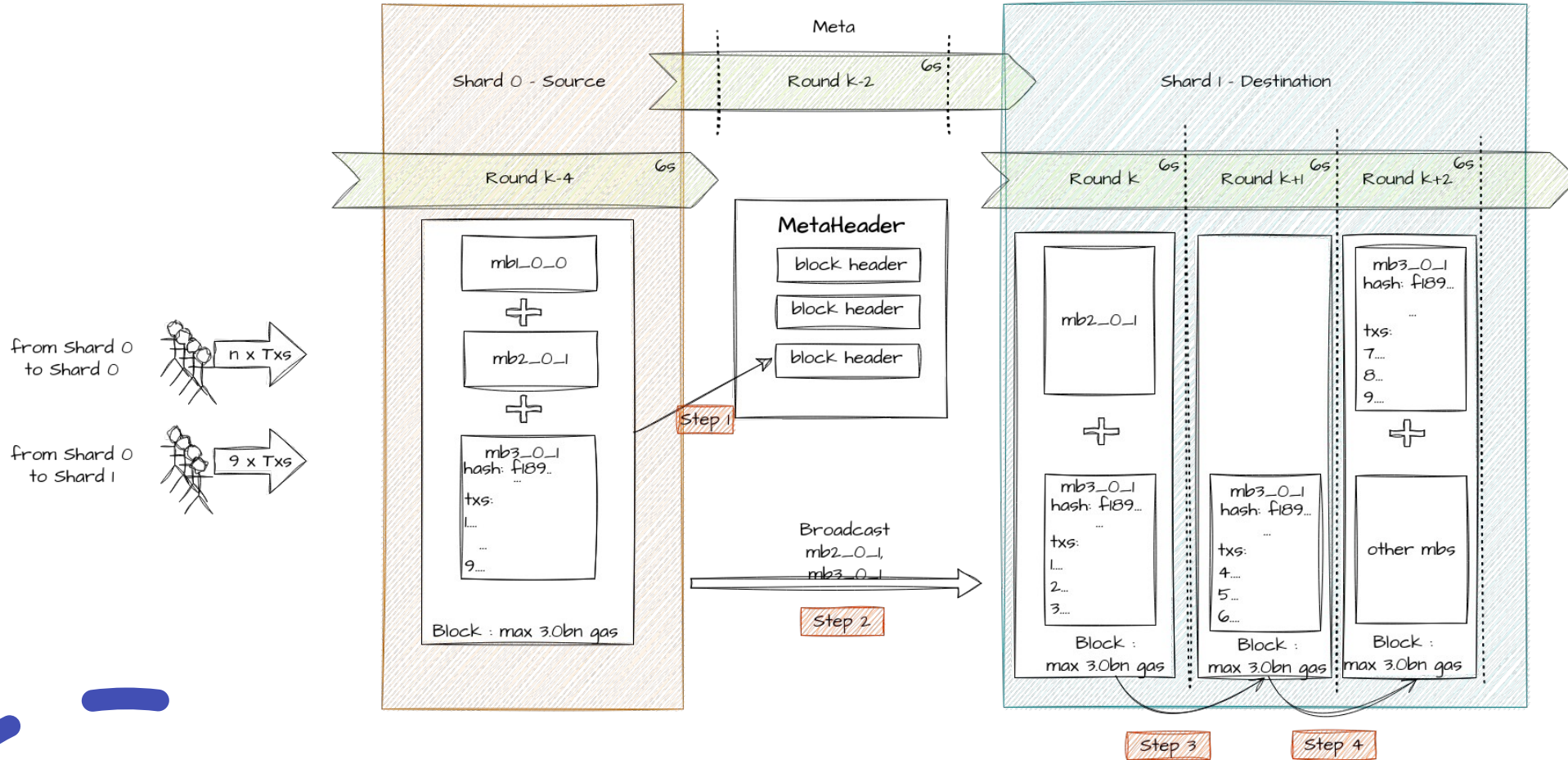
- 15000 TPS with 3 shards (max 1.5 Bil gas)
- Scheduled Transactions
- Partial Miniblocks Execution
- 2x → 30000 TPS
- New Target: 50000 TPS

Scheduled Transactions

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



Partial Miniblocks Execution

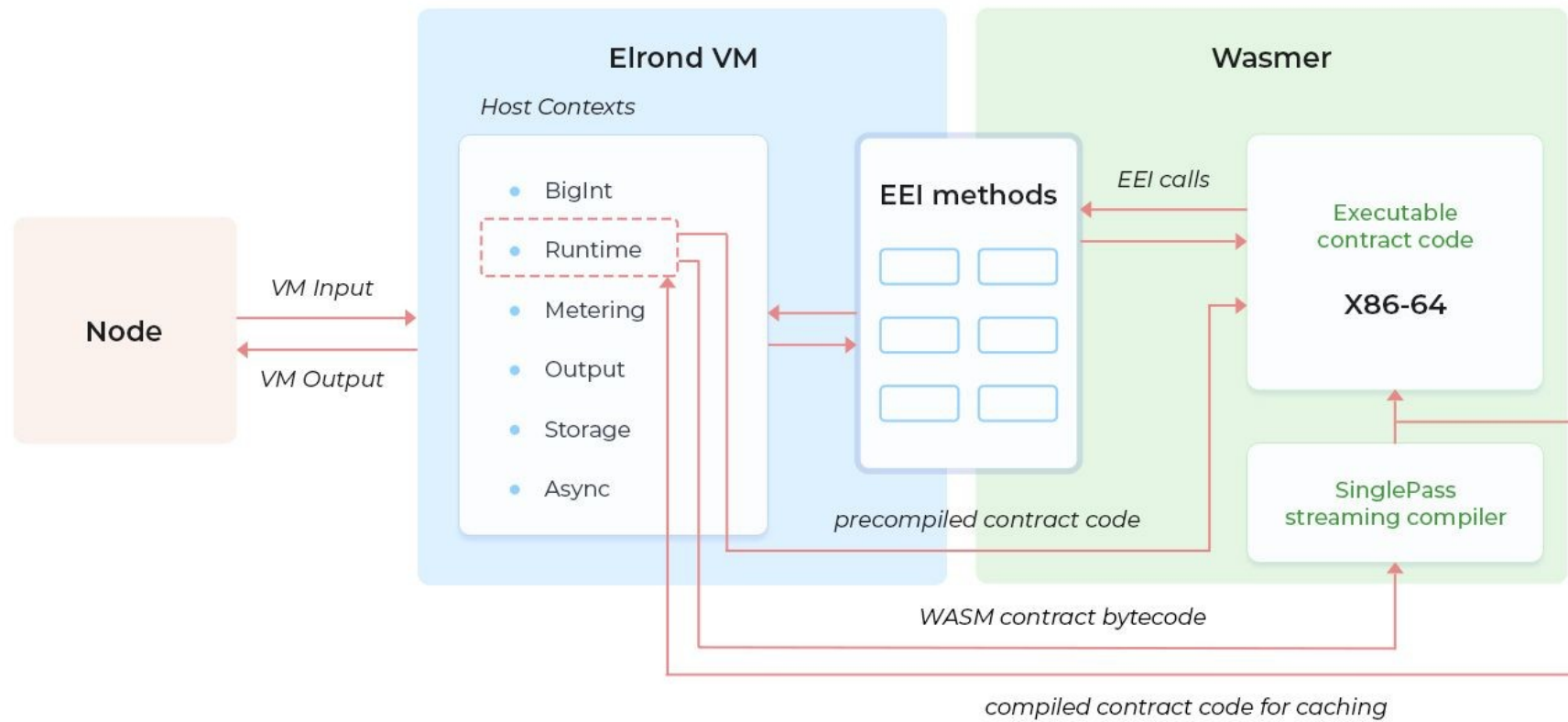


Elrond – ESDT

- Custom tokens at native speed and scalability, without ERC20
- NFT/SFT/MetaESDT:
- metadata and attributes

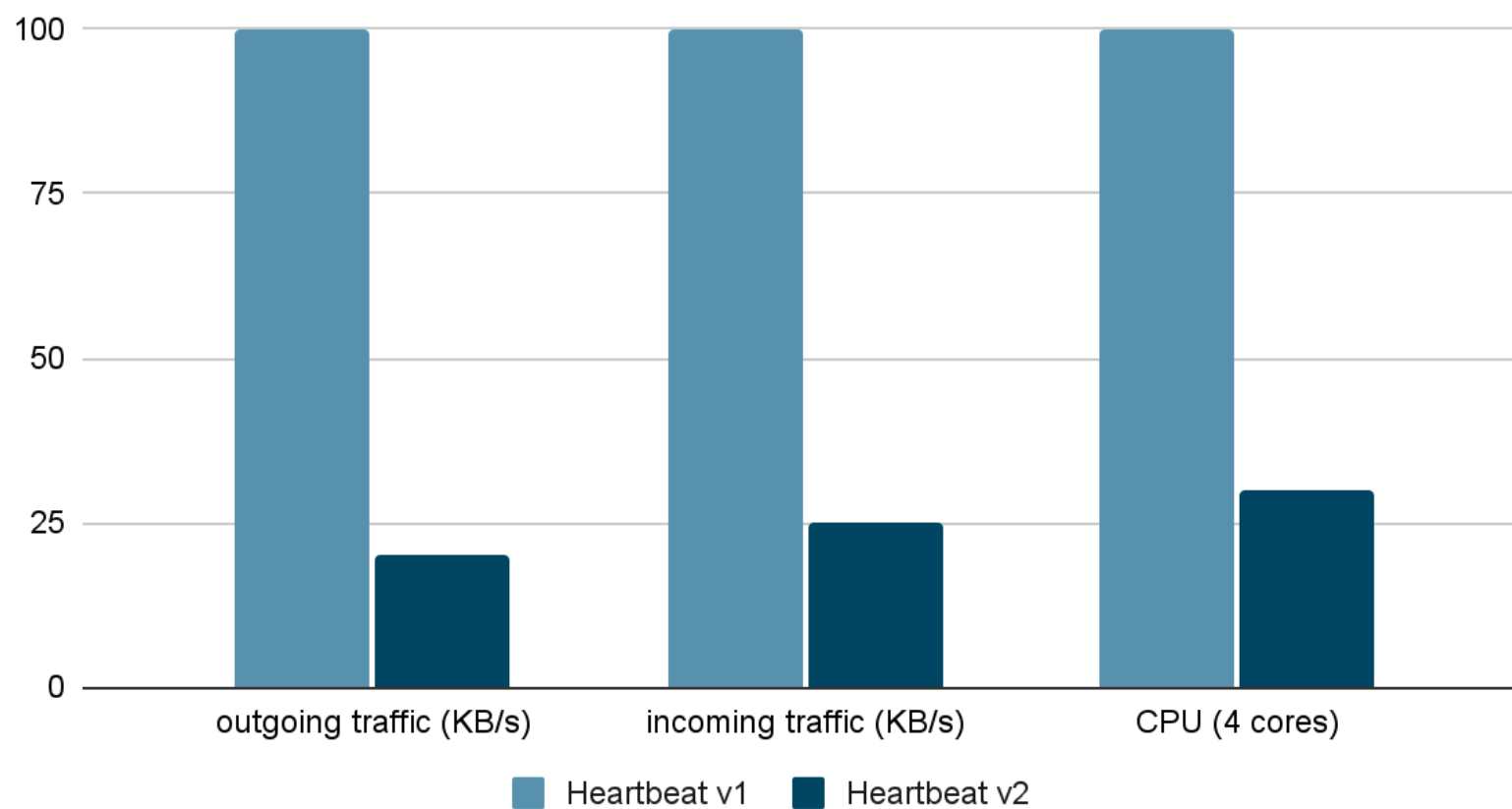
```
IssuanceTransaction {
  Sender: <account address of the token manager>
  Receiver: erd1qqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqqzllls8a5w6u
  Value: 50000000000000000 # (0.05 EGLD)
  GasLimit: 60000000
  Data: "issue" +
    "@" + <token name in hexadecimal encoding> +
    "@" + <token ticker in hexadecimal encoding> +
    "@" + <initial supply in hexadecimal encoding> +
    "@" + <number of decimals in hexadecimal encoding> +
    "@" + <"canFreeze" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encoded>
    "@" + <"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 encoded>
    "@" + <"canUpgrade" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encoded>
    "@" + <"canAddSpecialRoles" hexadecimal encoded> + "@" + <"true" or "false" hexadecimal encoded>
}
```

Elrond - VM

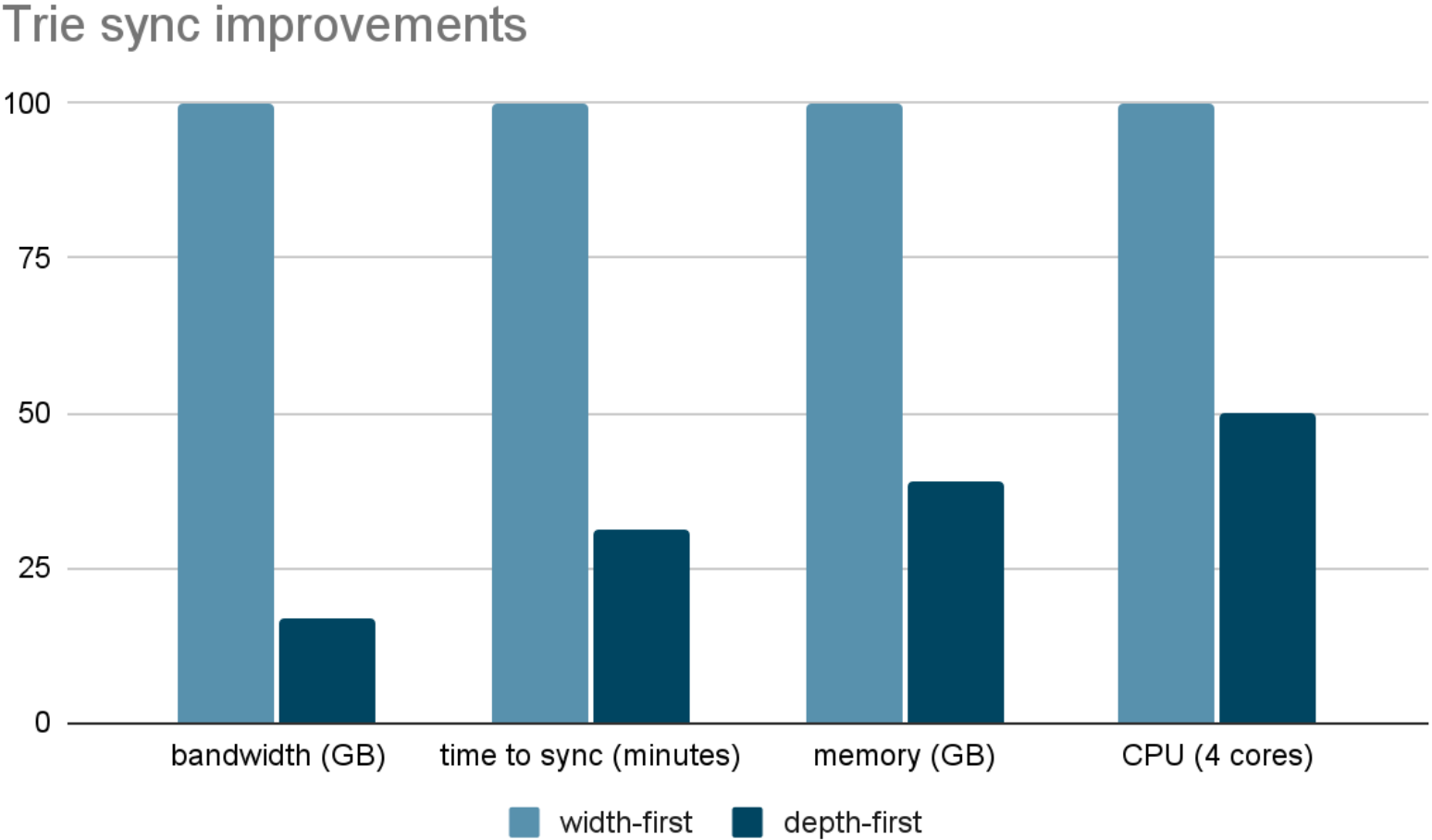


Heartbeat v2 improvements

Heartbeat V2 improvements



Trie sync improvements

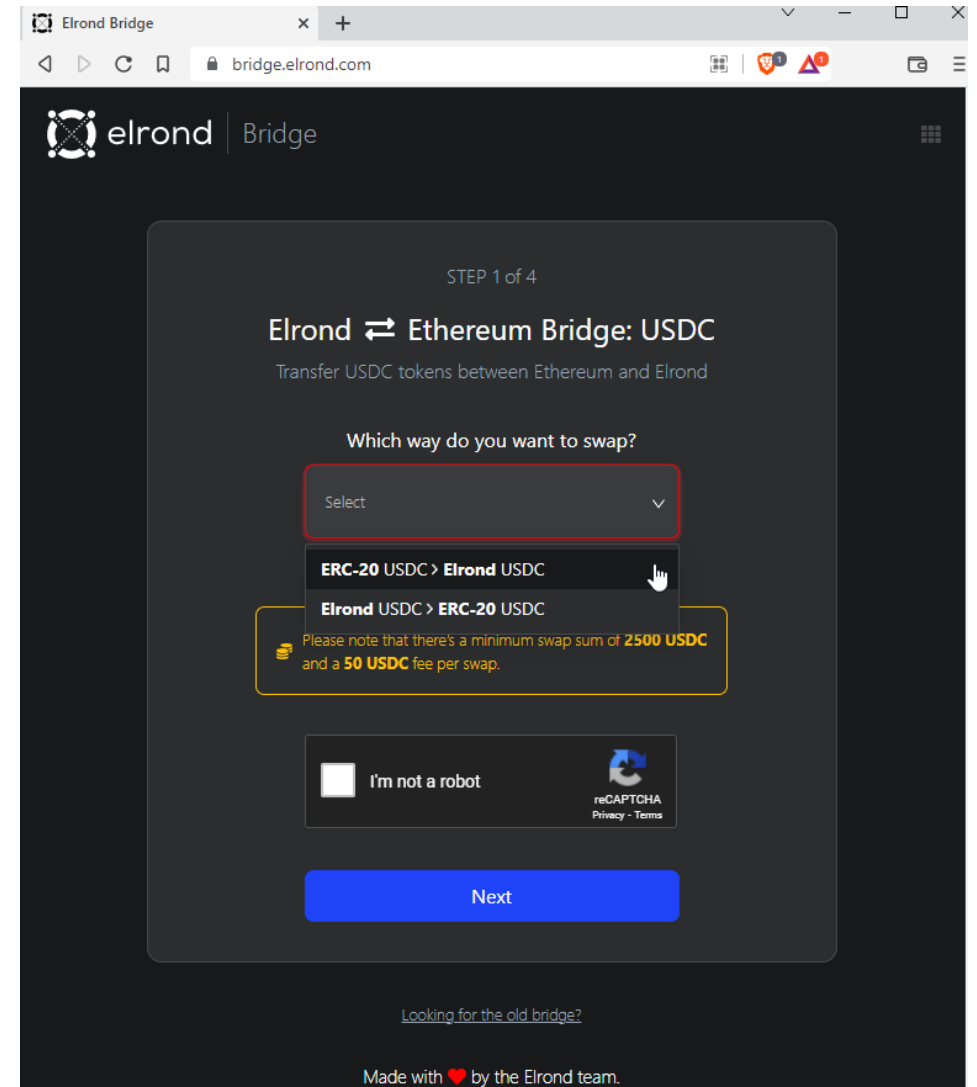


Further improvements

- 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

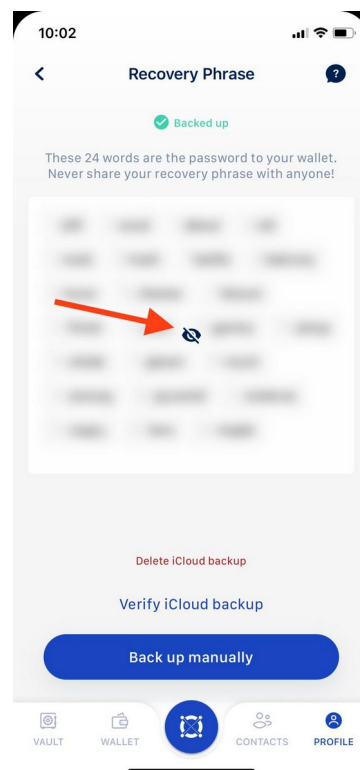


Elrond - Audit

- 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!**



Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.



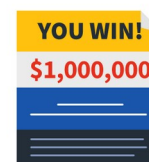
Your 'friend' sends you a strange message.



Your emotions are heightened.



The request is urgent.



The offer feels too good to be true.



You're receiving help you didn't ask for.



The sender can't prove their identity.

