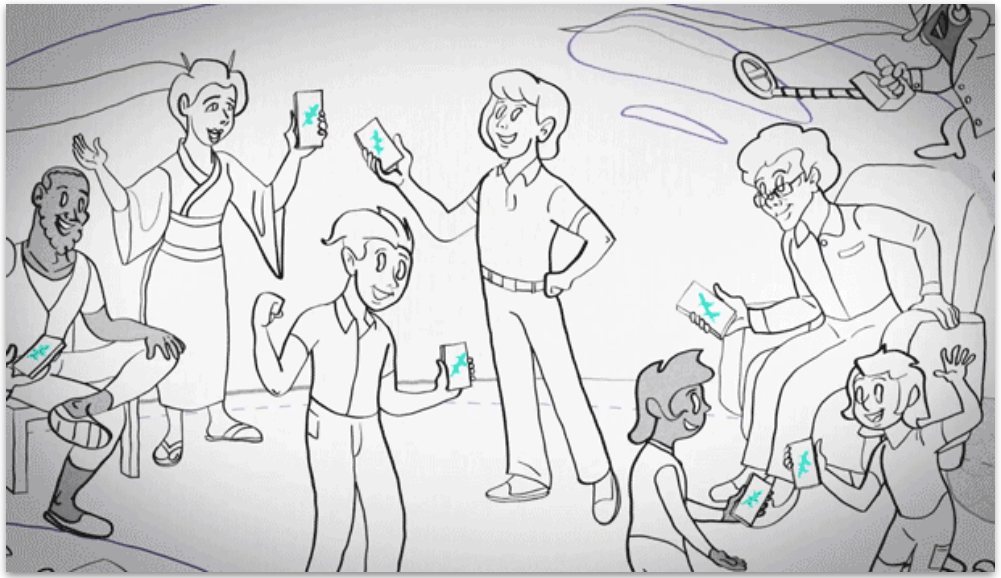
Our Freedom

Metadata is the meta issue

A New Vision

We need a new type of platform, a protected digital sphere, allowing users to:

- Share ideas
- Exchange value in a secure and private manner.



What's Needed?

All three are needed,
yet nobody has even one:

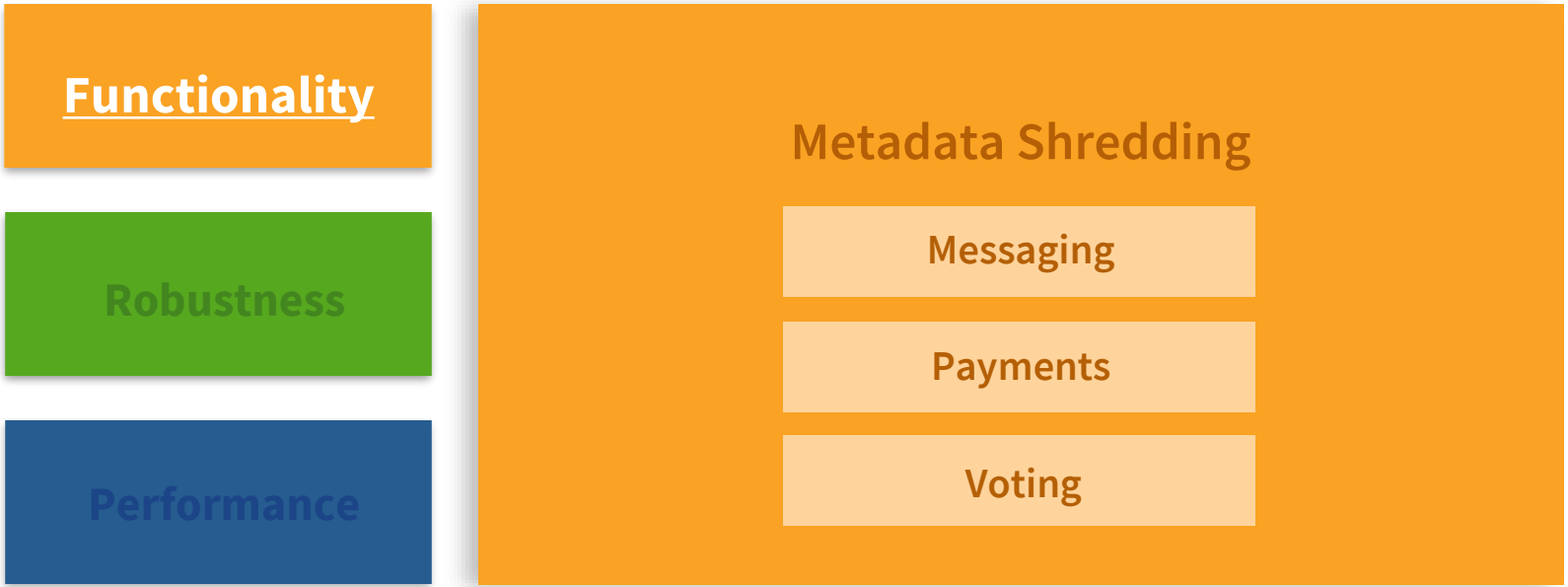
Functionality

Robustness

Performance

What's Needed?

All three are needed, *yet nobody has even one:*



What's Needed?

All three are needed, *yet nobody has even one:*

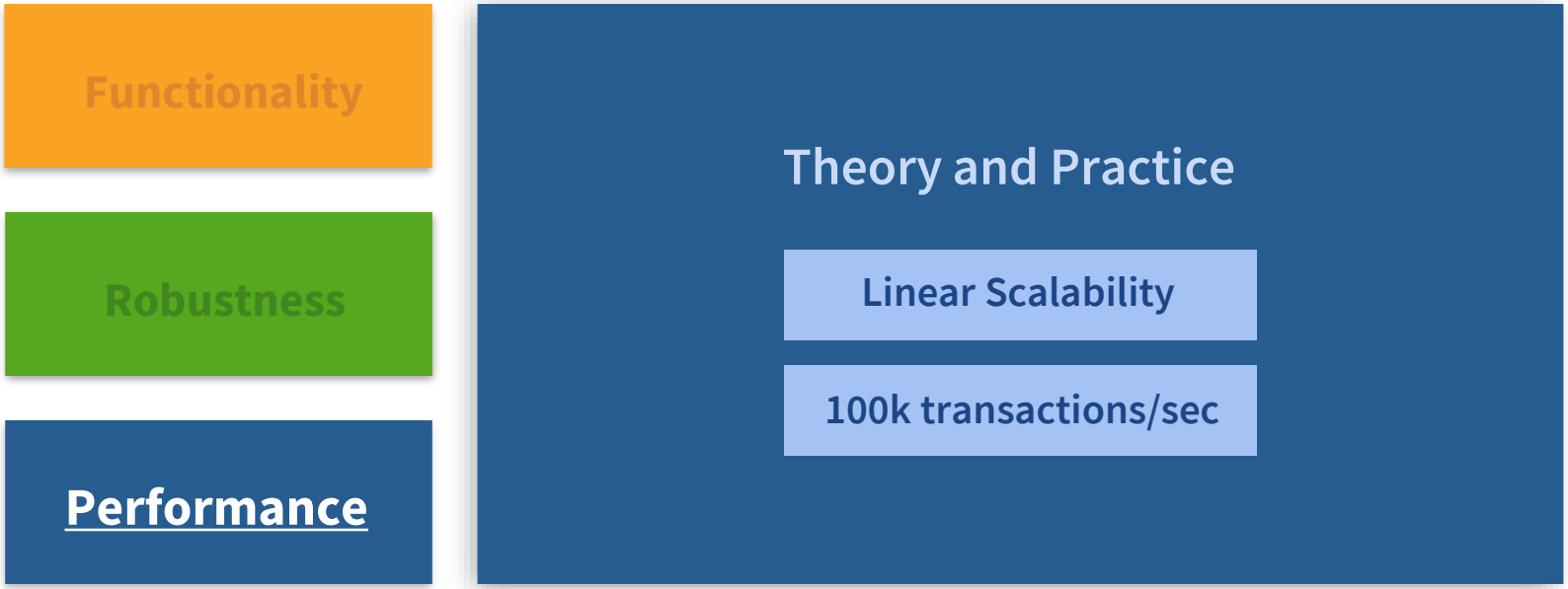
- Functionality
- **Robustness**
- Performance

Weak Link Phenomena - Need All Four

1. Quantum resistance/computational attack
   (all current blockchains/proof of work)
2. Resist money attack *(proof of stake)*
3. Resist sybil attack *(think click farm)*
4. Resist voting/control attack
   (all current polling and blockchains)

What's Needed?

All three are needed, *yet nobody has even one:*



Introducing the xx network

Introducing the xx network!

Elixxir's cMix

The only technology which not only protects the data being sent, but also the metadata.

Secure Election Technology

Verifiably secure elections using random sample voting and decoy ballots.

Praxxis' Blockchain and Currency

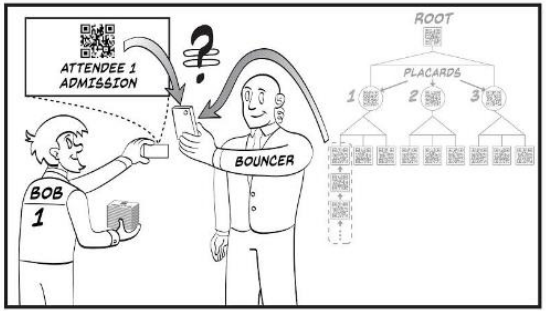
The fastest and most secure distributed consensus and privacy-enabled currency.

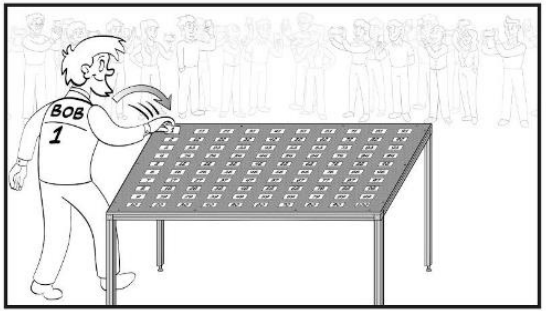
Praxxis Blockchain + Payments

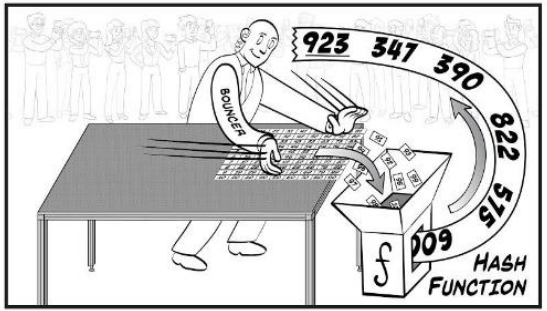
- NodeCon
- Block Producers
- Validators
- Fallback
- Payments
- Compact Endorsement

NodeCon

A **quantum-secure** way to initialize the network and establish a secure random seed and authenticated channels between all nodes.

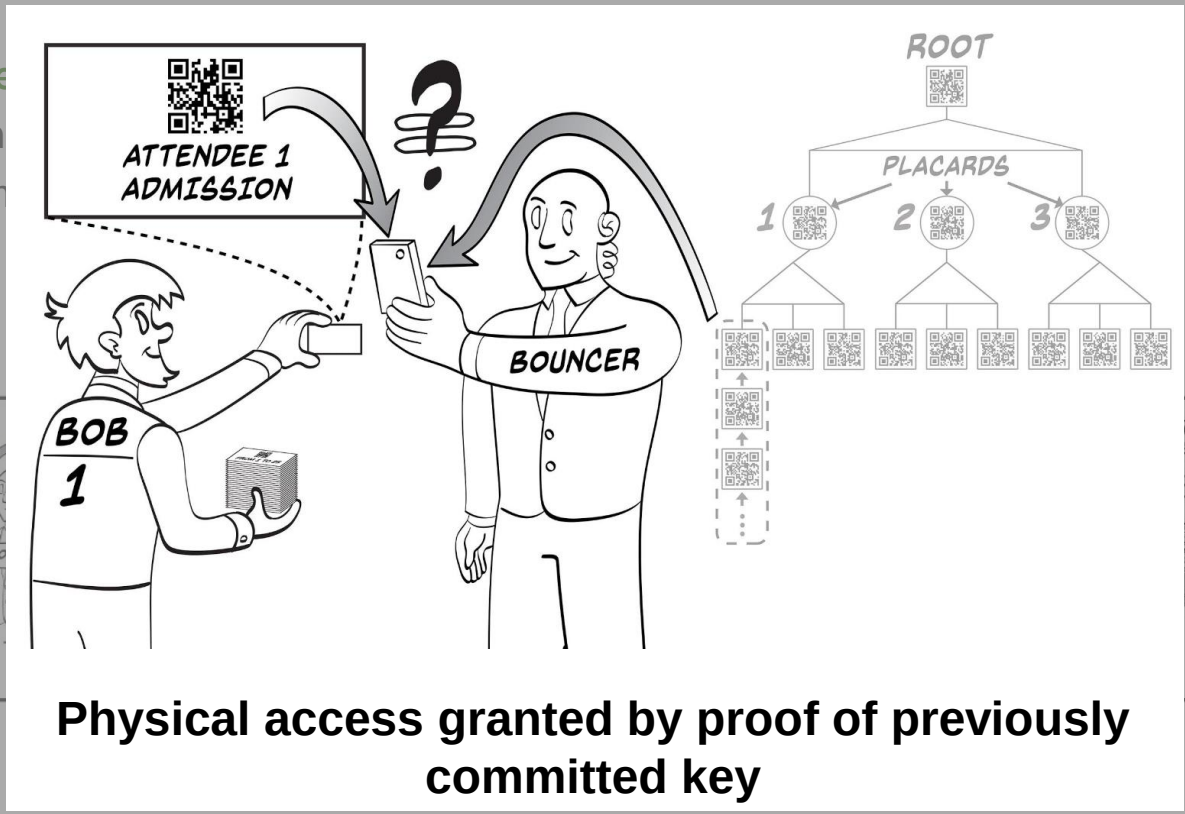






NodeCon

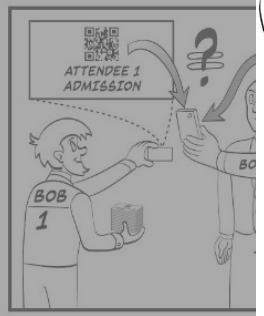
A **quantum-se**
the network a
seed and auth
all nodes.

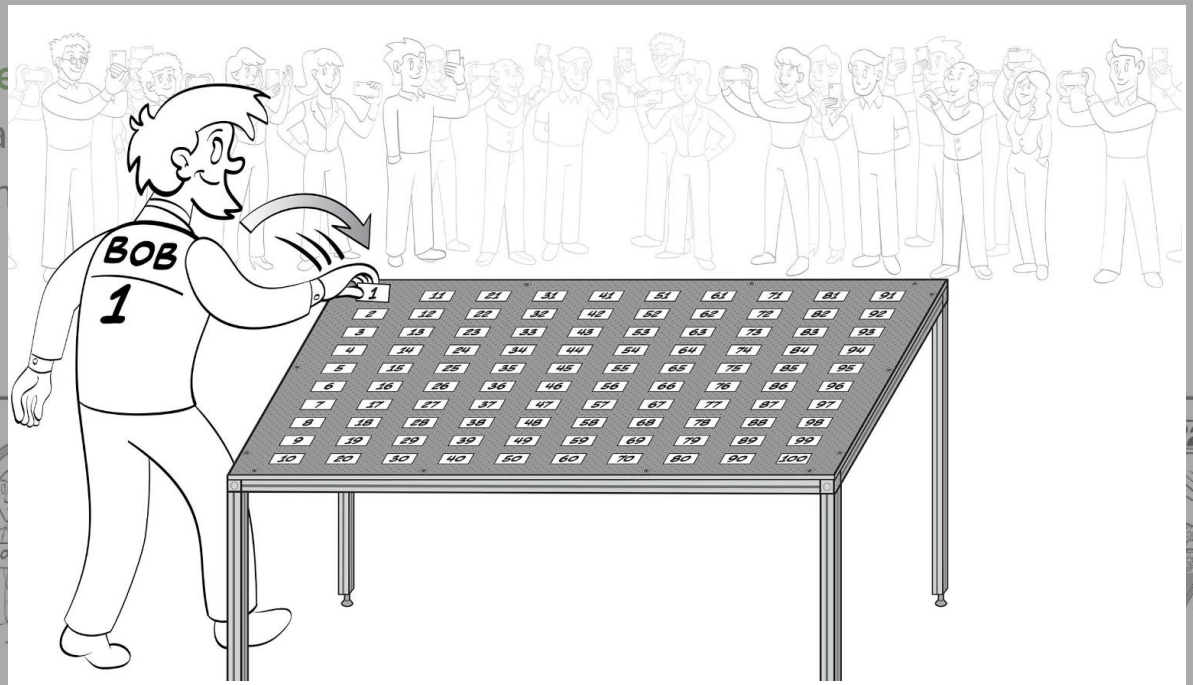


Physical access granted by proof of previously committed key

NodeCon

A **quantum-se**
the network a
seed and auth
all nodes.

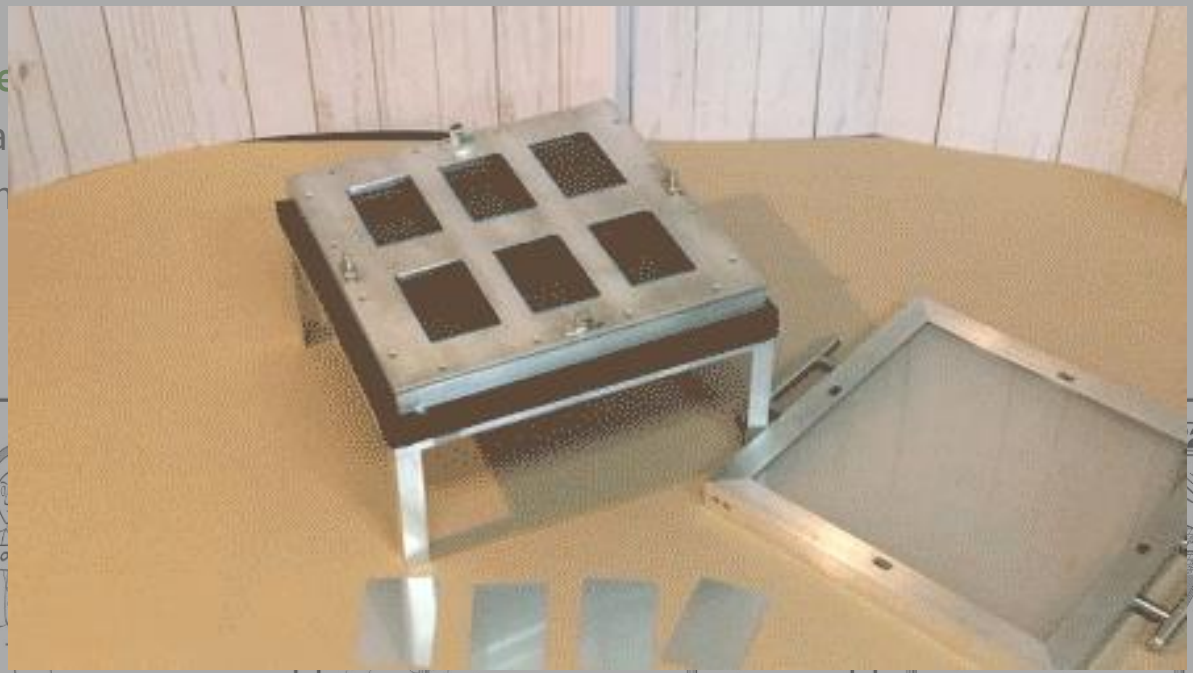




All attendees submit a secret commitment

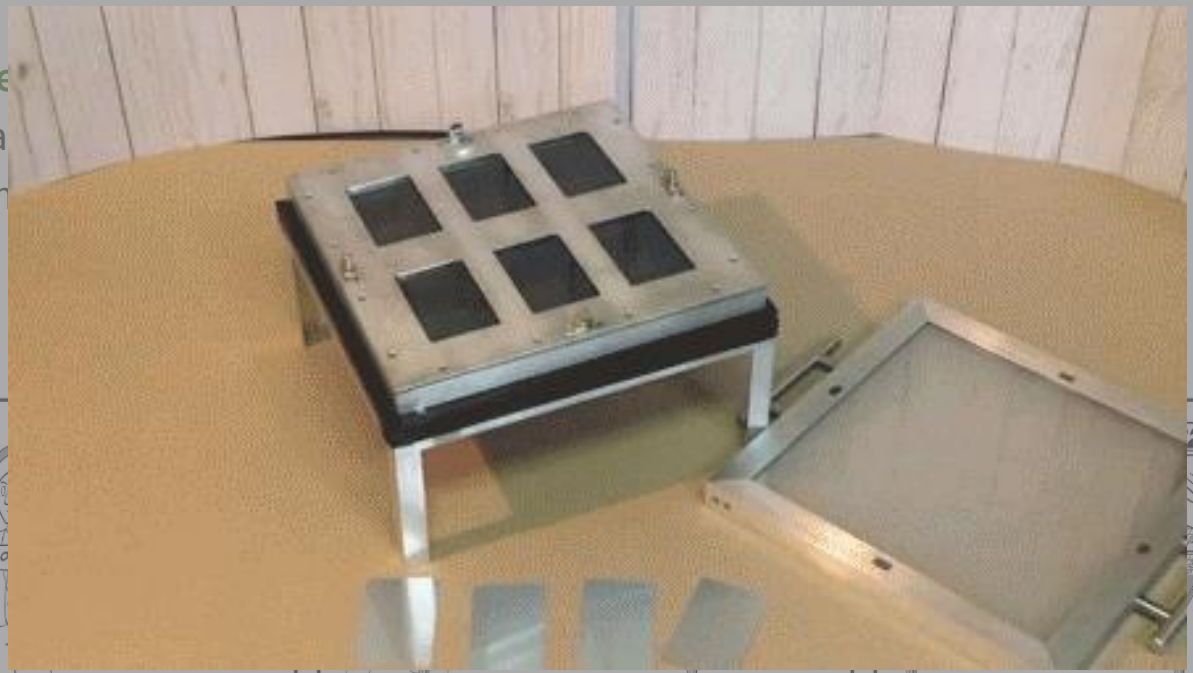
NodeCon

A **quantum-se**
the network a
seed and auth
all nodes.



NodeCon

A **quantum-se**
the network a
seed and auth
all nodes.

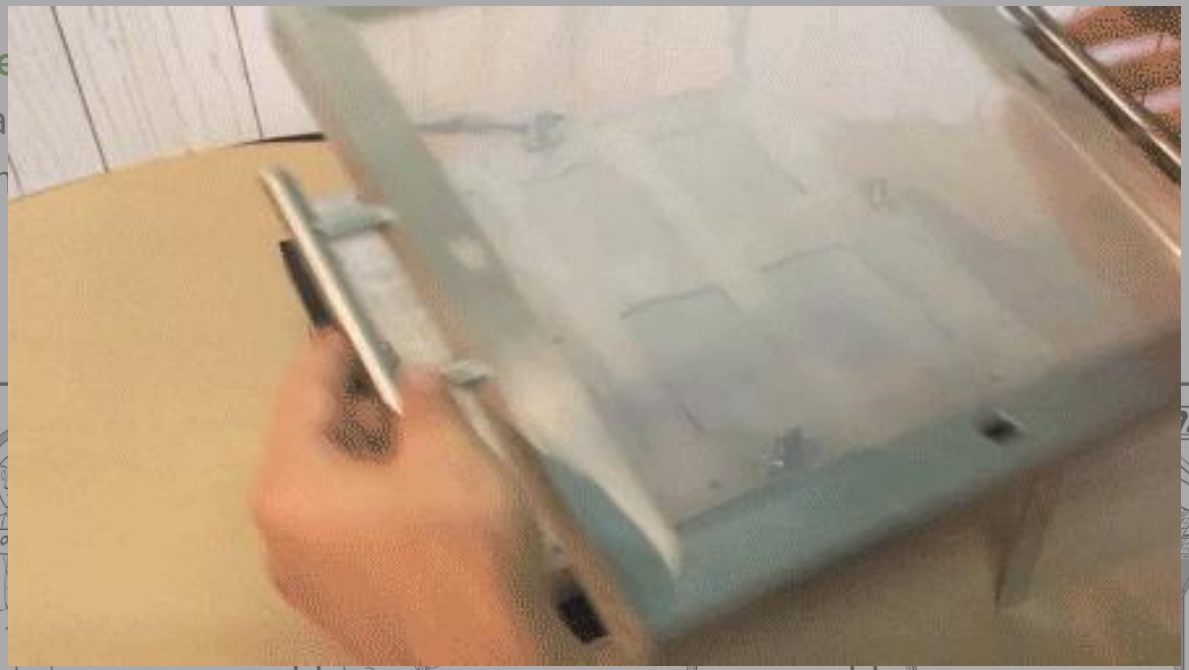


NodeCon

A **quantum-se**
the network a
seed and auth
all nodes.

NodeCon

A **quantum-se**
the network a
seed and auth
all nodes.

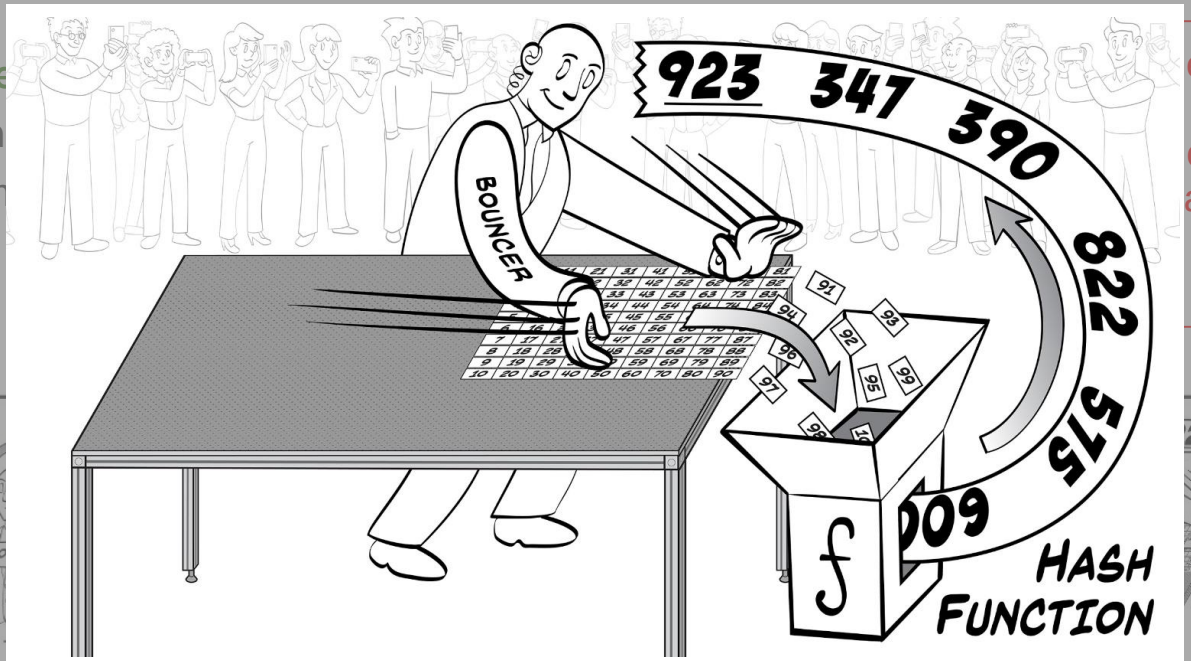


NodeCon

A **quantum-se**
the network a
seed and auth
all nodes.

ere

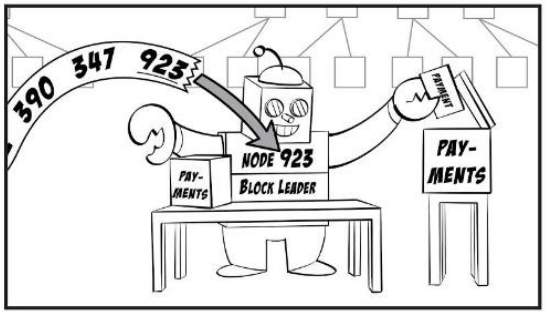
of entire
able? *v

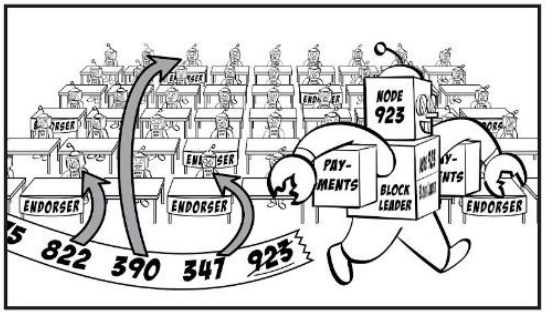


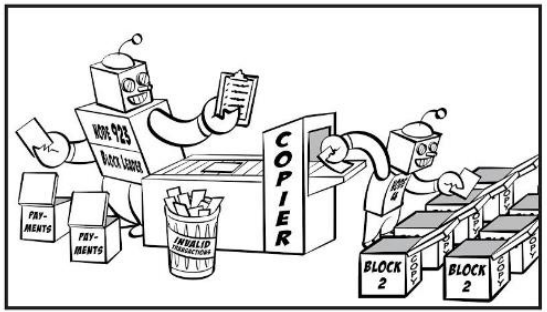
Hash function of QR codes determine unpredictable sequence of nodes

Block Producers

Unmanipulatably and unpredictably select a random node to lead each round of consensus.

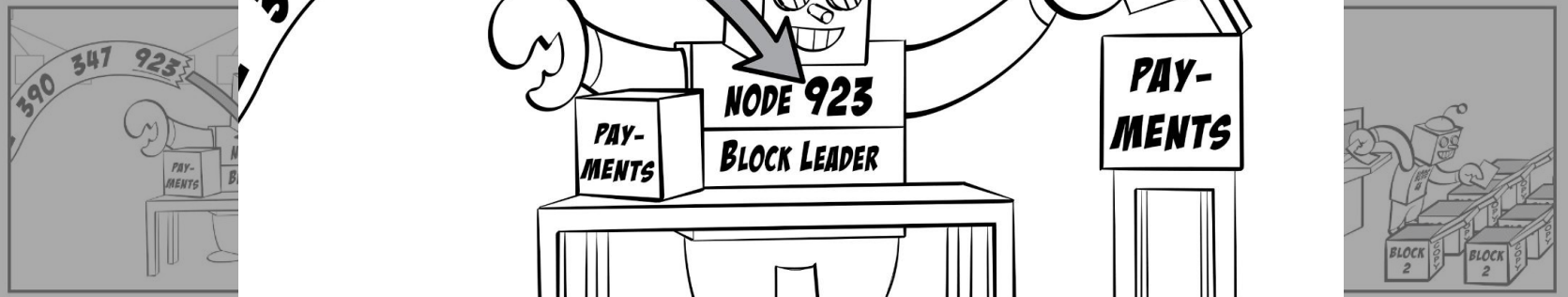






Block Producers

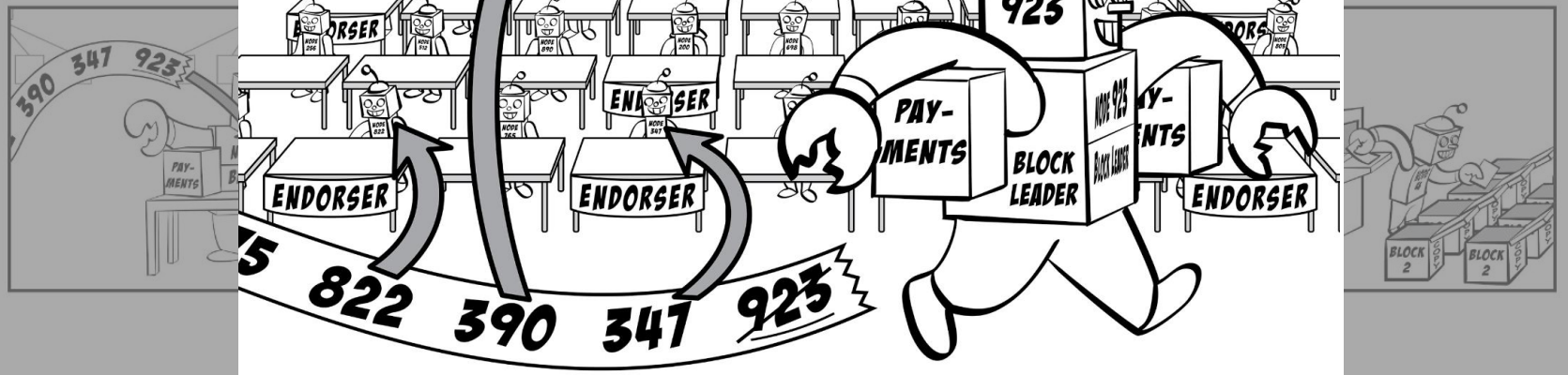
Unmanipulata f consensus.



Block leader (first on tape) creates a block

Block Producers

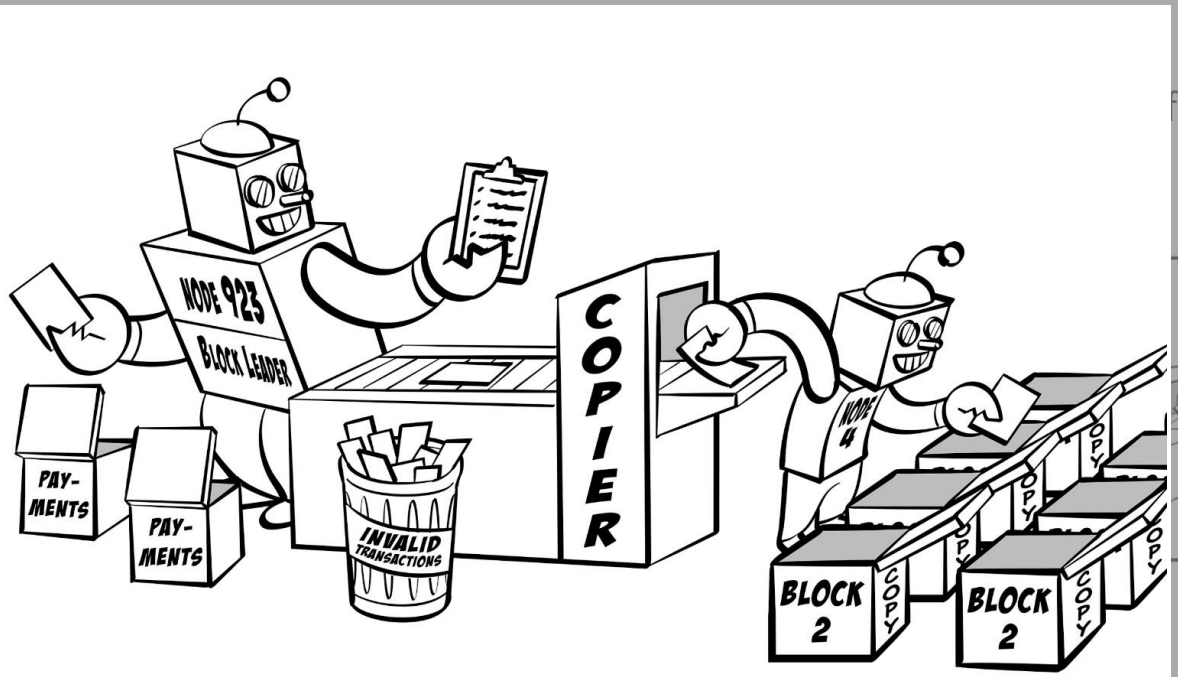
Unmanipulata consensus.



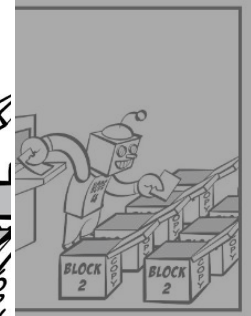
Endorsers selected by subsequent values

Block Producers

Unmanipulata consensus.

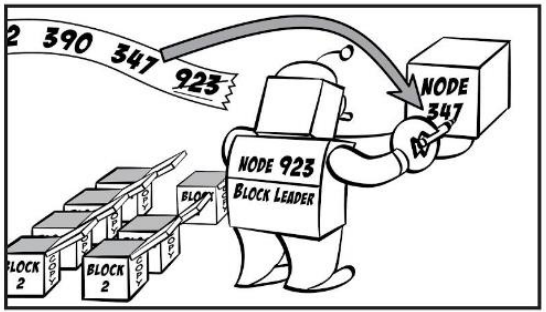


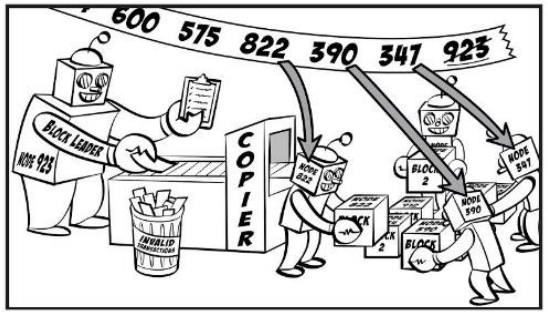
Block leader prepares copies of block

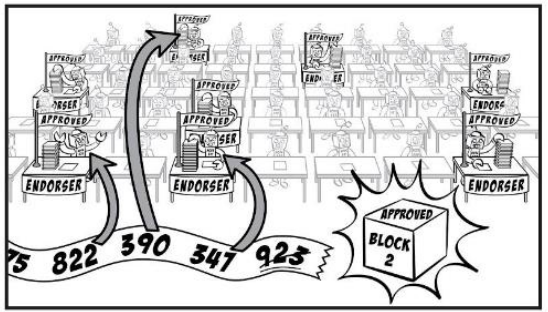


Validators

Execute a scalable, optimistic consensus decision by sampling a constant-sized subset of the network to verify and endorse each block.

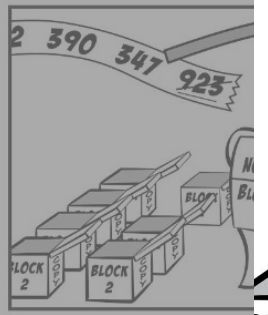


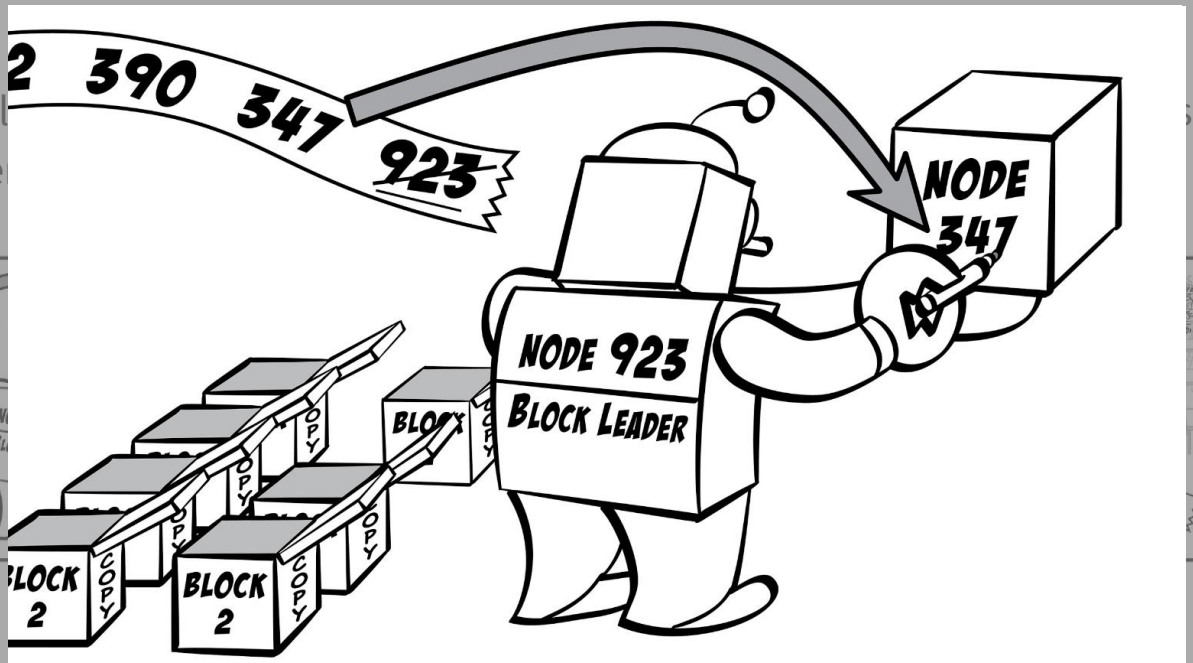




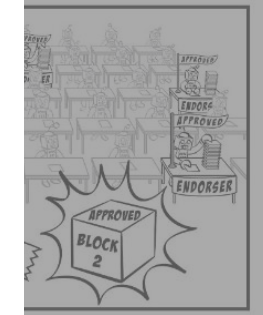
Validators

Execute a scal subset of the network to ve



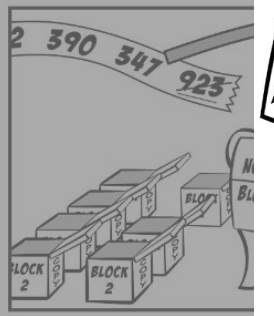


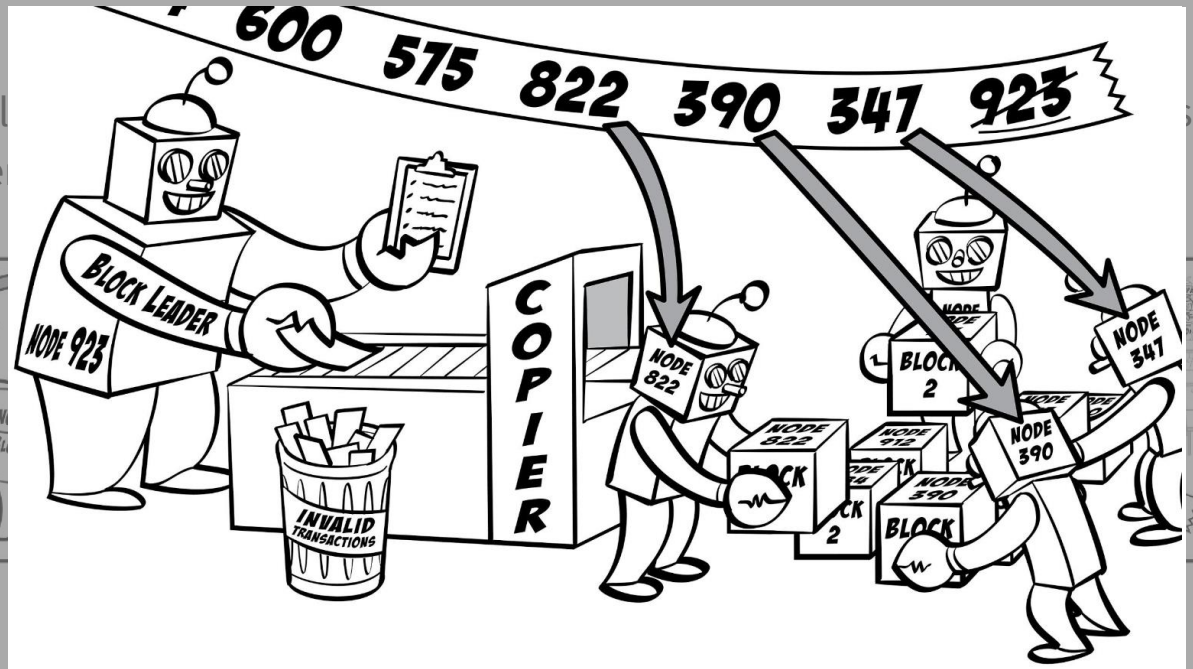
Block leader distributes full copies of blocks to endorsers



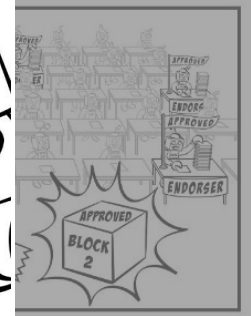
Validators

Execute a scal … subset of the network to ve…



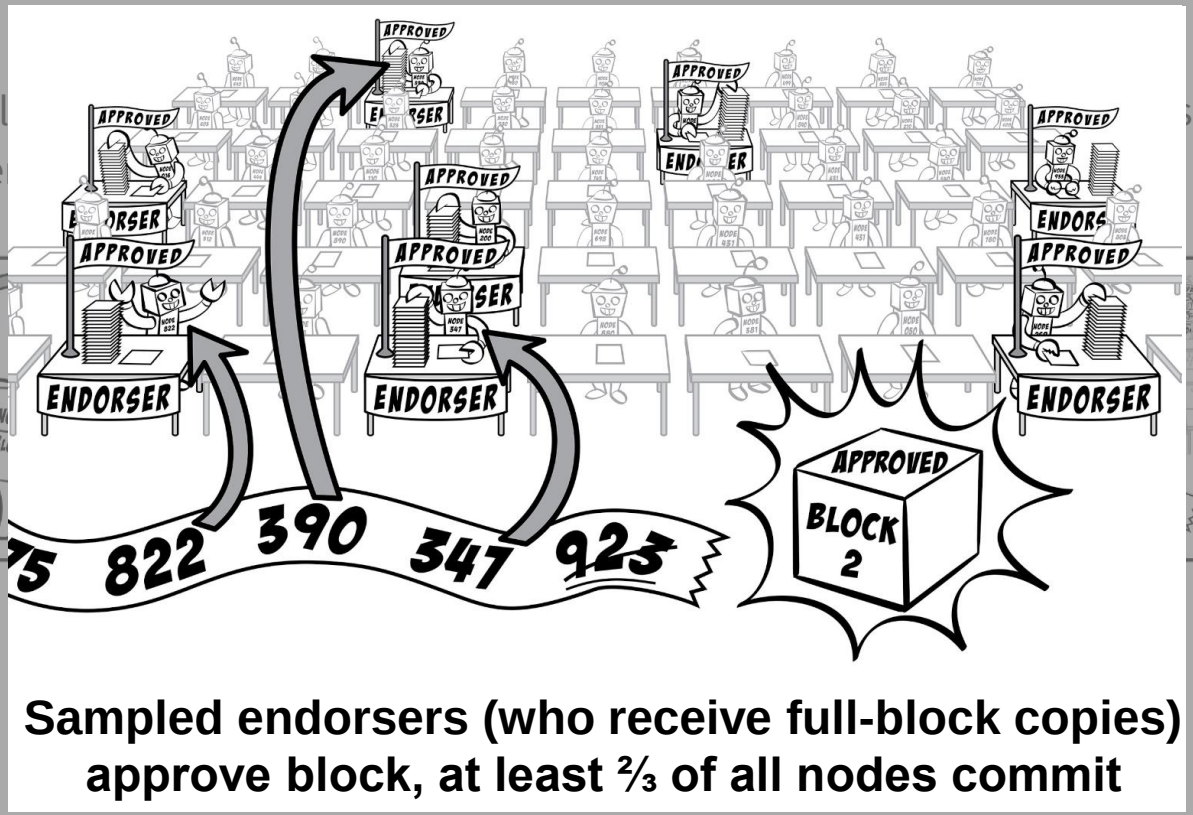


Block leader generates block summaries for non-endorsers



Validators

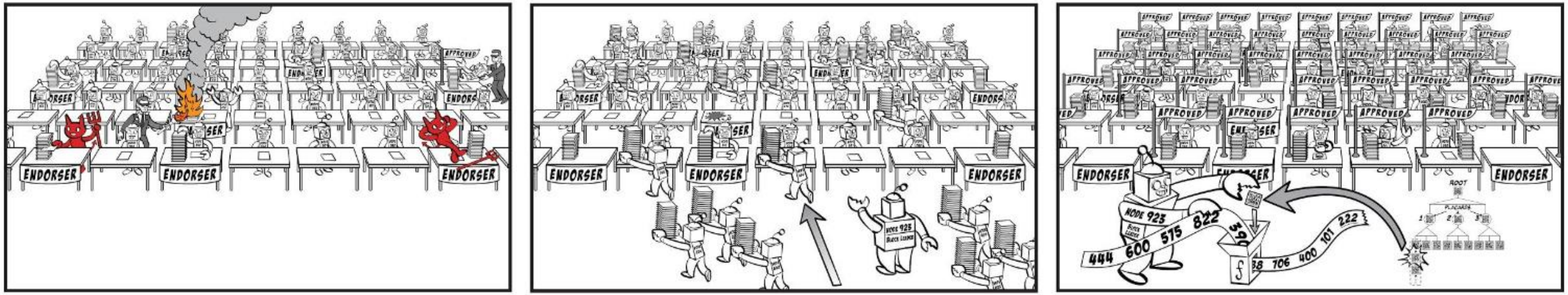
Execute a scal subset of the network to ve



Sampled endorsers (who receive full-block copies) approve block, at least ⅔ of all nodes commit

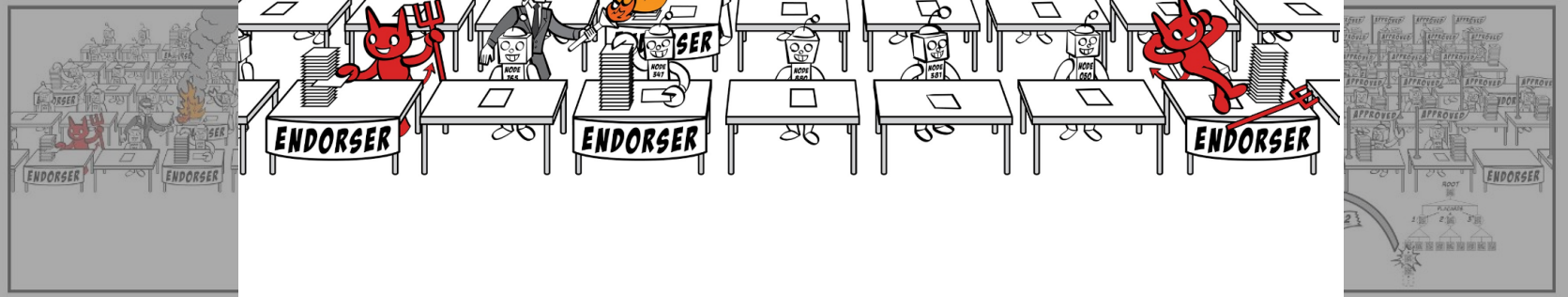
Fallback

Efficient fallback mechanism in the event that an optimistic consensus decision fails due to significant byzantine behavior.



Fallback

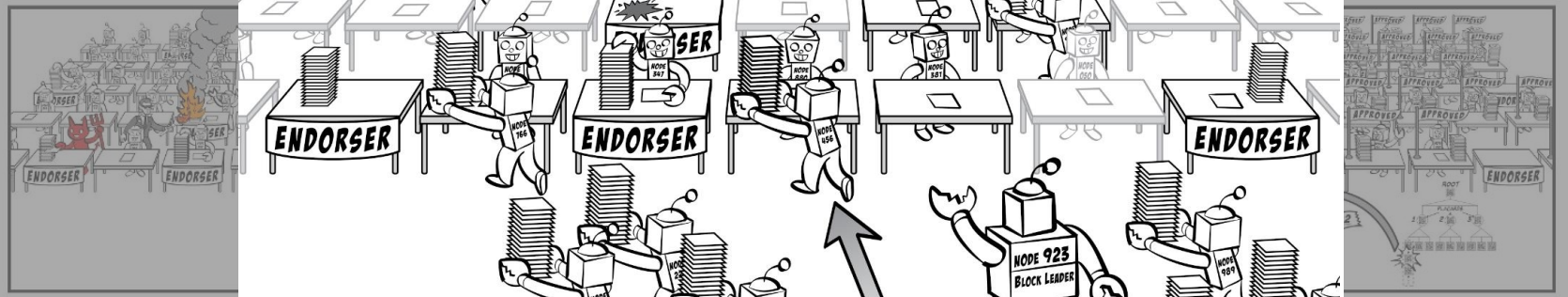
Efficient fallba ails due to
significant byz



Optimistic path may be disrupted

Fallback

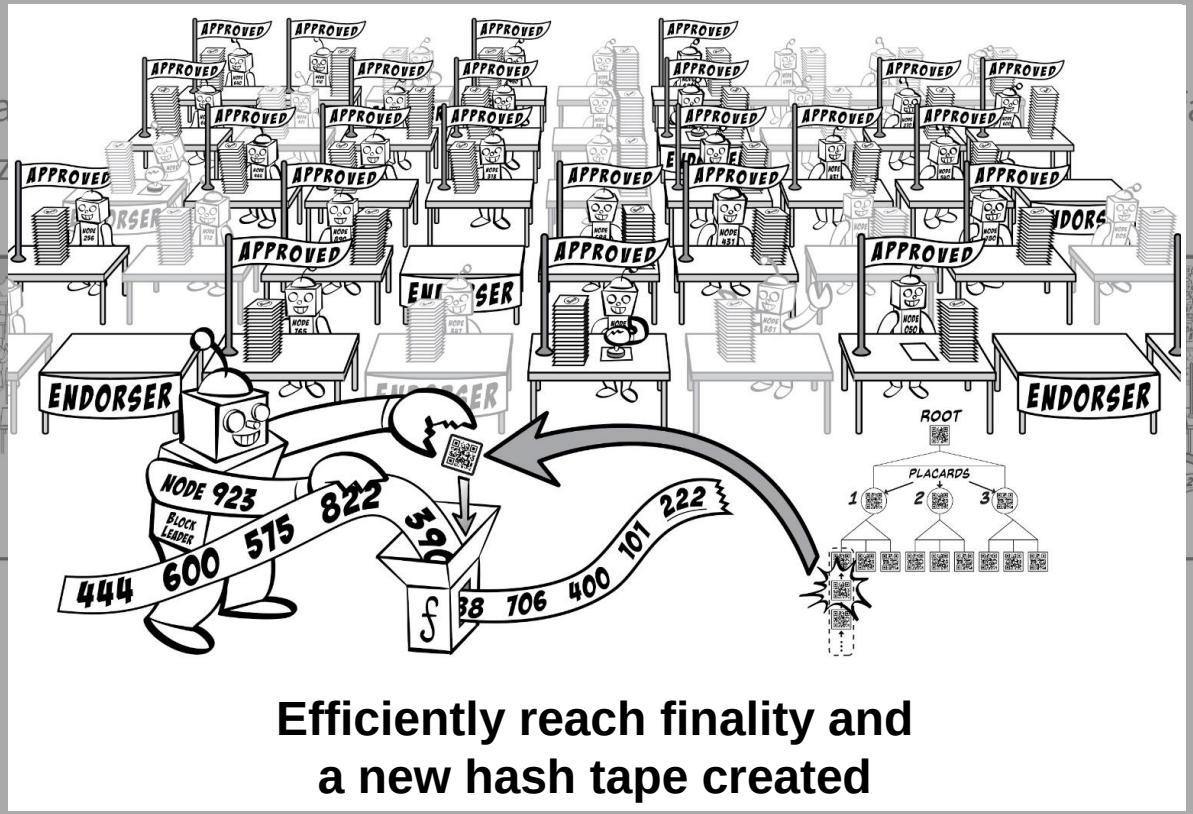
Efficient fallba ails due to
significant byz



A new sample of endorsers is chosen

Fallback

Efficient fallba ails due to
significant byz



Efficiently reach finality and a new hash tape created

Payments

(1) A coin is created and (2) its value is paid to another user:

(1a.) Create a random secret pre-image **x** that will be the "bearer instrument."

(1b.) Provide nodes with pre-image **x** under a one-way function **f(x)** -- along with the funding (e.g., say, by defunding another coin **w**).

(2a.) Payer makes payment by providing the pre-image **x** to the recipient.

(2b.) Nodes verify payment by applying the one-way function to **x** and recovering **f(x)** .

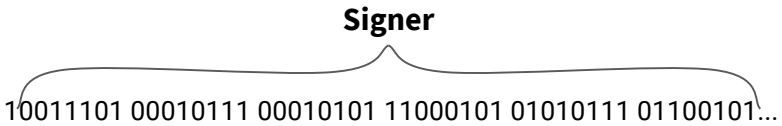
(2c.) Recipient uses **x** to fund creation of a new coin **y**.

Compact Endorsement

Single Signature

Message digest must be large enough to be unforgeable

Signer divides hashed message into 32 8-bit chunks and signs each one with 256 bit hash



= 32 * 256 = **8,196 bits per signature**
256 bit hash = **unforgeable**

For 100 endorsers: 8,196 * 100 = **819,600 bits**
100 x 256 bit hashes = **unforgeable**

Compact Endorsement Signature

The combined size of message digests of the group must be large enough to be unforgeable

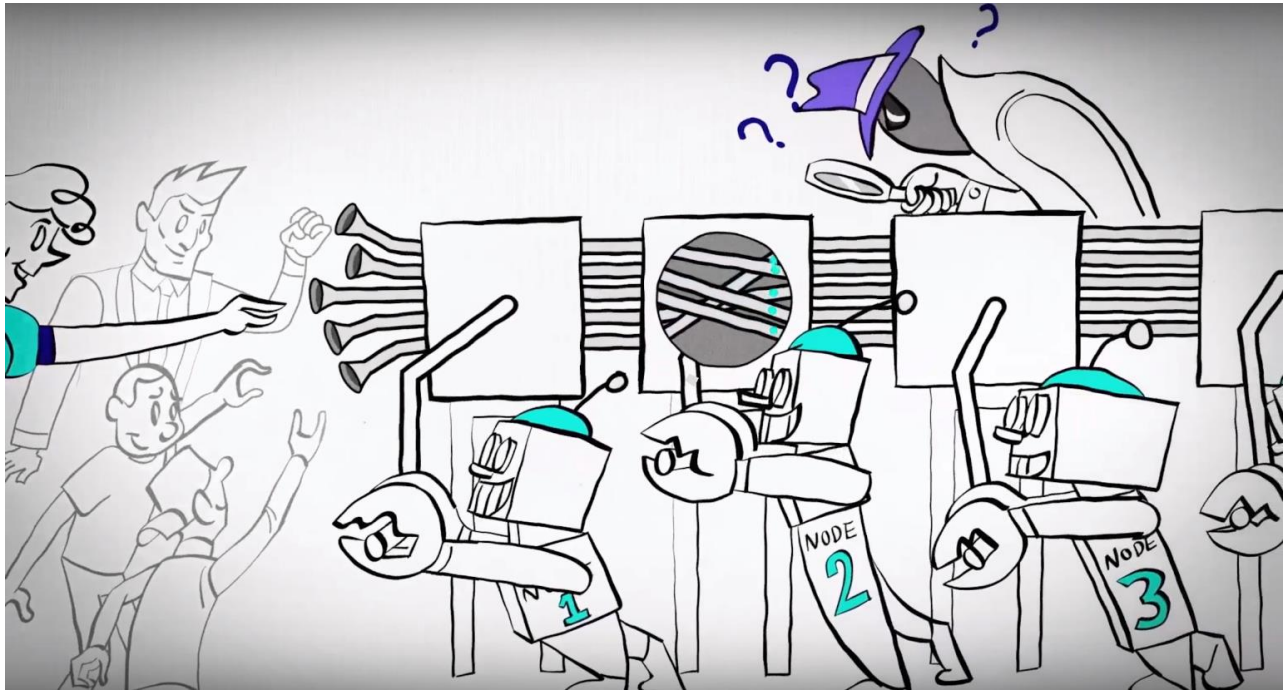
Each signer creates a separate hash of the message and signs 2 8-bit chunks

= 2 * 256 = **512 bits per signature**
16 bit hash = **forgeable**

For 100 endorsers: 512 * 100 = **51,200 bits**
100 x 16 bit hashes (with same message) = **unforgeable**

What’s Been Built

Messaging



Messaging

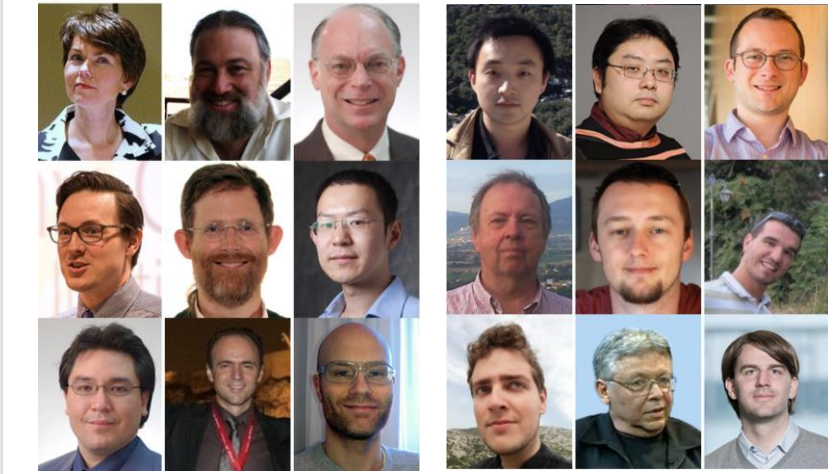

6:15
Back
Lee
Me too!
Wanna grab some lunch
Sure
How about in 15 min?
Sounds great!
Let's do sushi
Hey
The
It's
Back
Jenny
Sure
How about in 15 min?
Sounds great!
Let's do sushi
Hey
I
The
123
space
return

Sample Voting

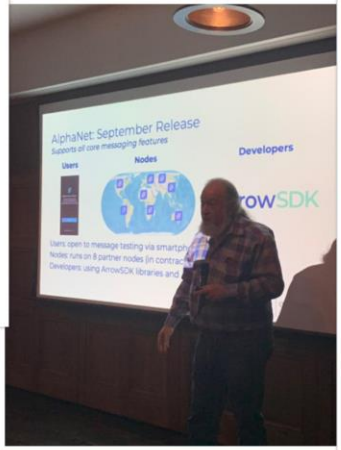
Council of Europe
World Forum for Democracy

The **Random-Sample-Voting Project** ran its first binding polls (and 4th public trial) at the World Forum for Democracy 2017, which was held in Strasbourg, France.

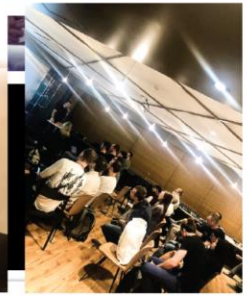
Team

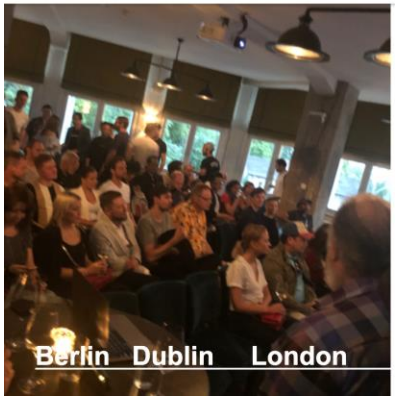


Work-In-Progress


AlphaNet: September Release
Supports all core messaging features
Users
Nodes
Developers


praxis




Berlin Dublin London


Seoul Tokyo Osaka


Shanghai Barcelona


Athens Singapore

Work-In-Progress

(but no promises here)

- “cMix with large payload: messaging and feeds”
- “Off-chain distributed dapps: secure and easy”
- “Direct democracy for exceptional tracing”
- “Who needs stable coins; a far better alternative”
- “Guerilla democracy: proving a majority would sign on to petition language”

Thank You!

Thank You!

Thank You!