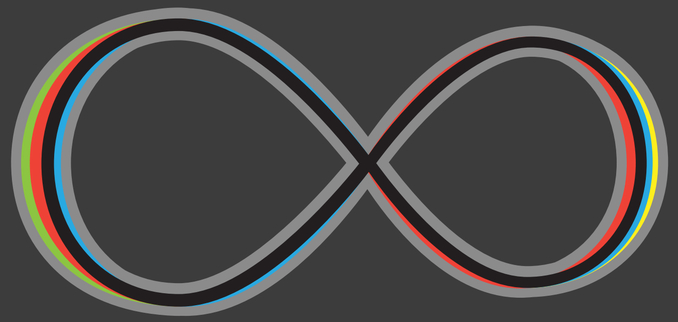


DFINITY

The Intelligent Decentralized Cloud

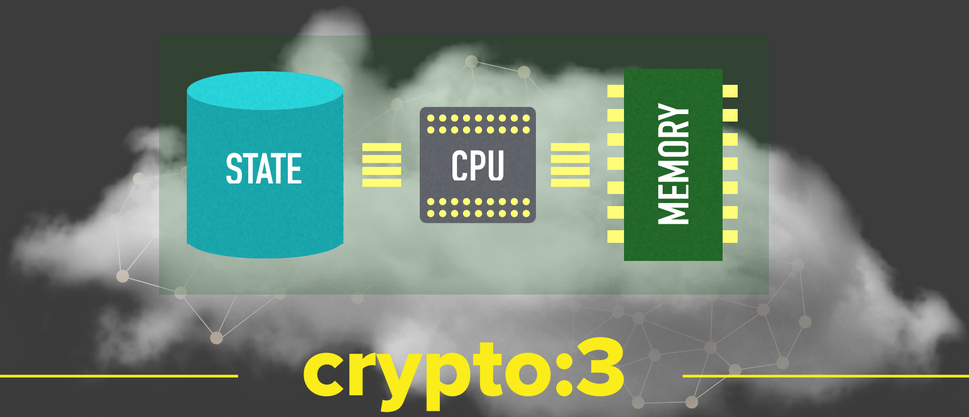
v1.3 - 2nd April 2017

DFINITY

Overview

Performant Blockchain Computer

FINALITY 3 - 7.5s



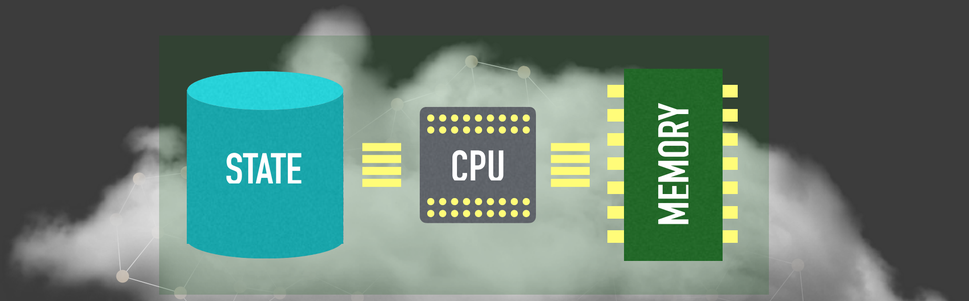
crypto:3

Threshold Relay: fast consensus + randomness

DFINITY

Infinite Blockchain Computer

SCALE-OUT WITH MINING POWER

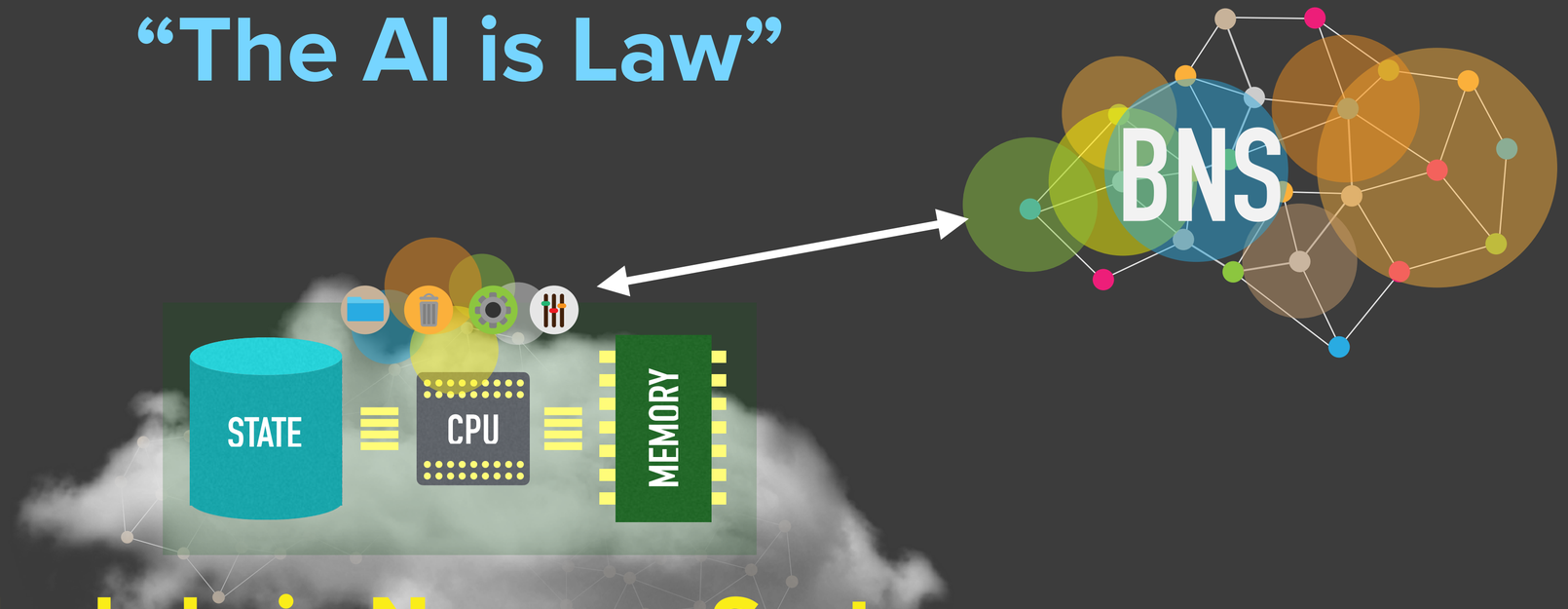


crypto:3

Apply randomness to make network scale-out...

DFINITY

“The AI is Law”



Blockchain Nervous System

Intelligent governance *without intermediaries*

DFINITY

Research began January 2015

"Create an *infinite* blockchain computer and address performance challenges...

USES OF DECENTRALIZED CLOUD...

D-uber, D-ebay, Social media, Web search...

"OPEN" TECH INTERMEDIARIES

CORPORATE IT RE-ENGINEERING

Lower Total Cost Enterprise IT Systems

DFINITY

Project Timeline

2014—

Pebble Project

CC for micropayments

Uses derivations BFT consensus

2015—

DFINITY Project

Infinite blockchain computer

New idea: apply “randomness”

July 2016

DFINITY Stiftung

Incubation by String Labs

Organizational build-out

Feb 2017

Seed Fundraising

$10M new funds for R&D

Build research SV & Zurich

July 2017

Test Network

Copper Release beta

Seeing is believing!

August 2017

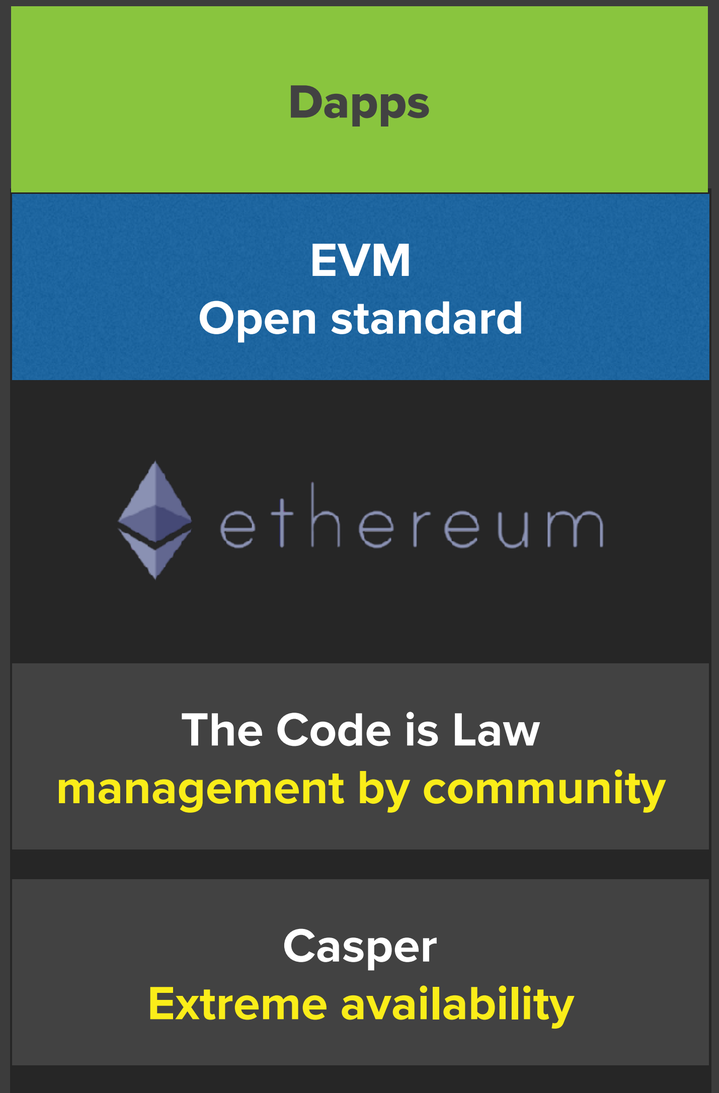
Main Fundraising

20M CHF hard cap

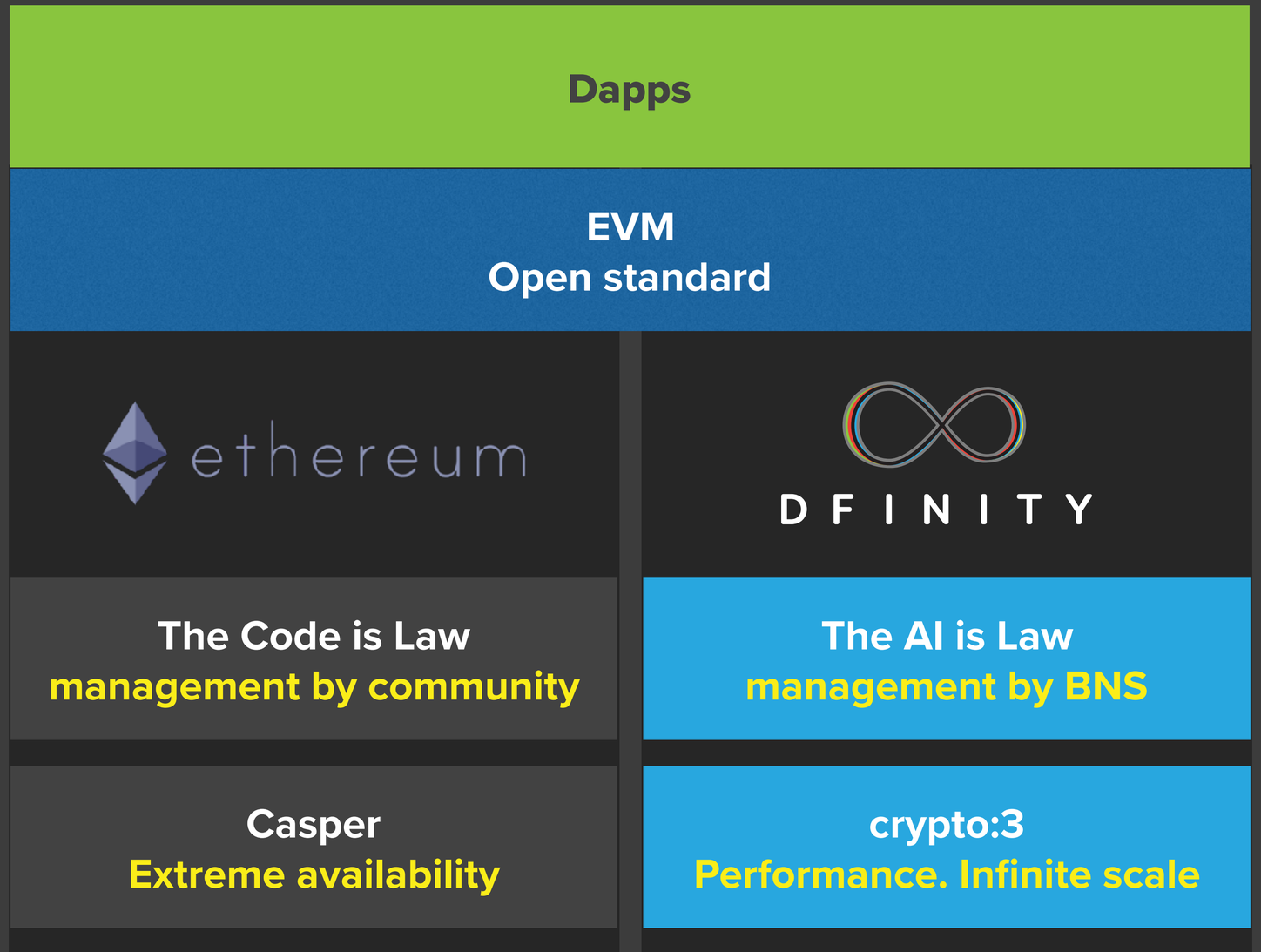
Then network launch...

DFINITY

The EVM ecosystem



Broaden stack with sister network



DRY — extend, do not imitate...

The Code is Law is the preferable paradigm for many applications

Extreme availability preferable for many fiduciary applications

Dapps

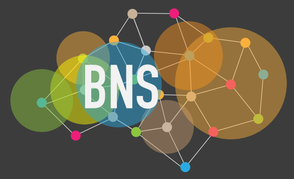
EVM
Open standard

ethereum

DFINITY

The Code is Law
management by community

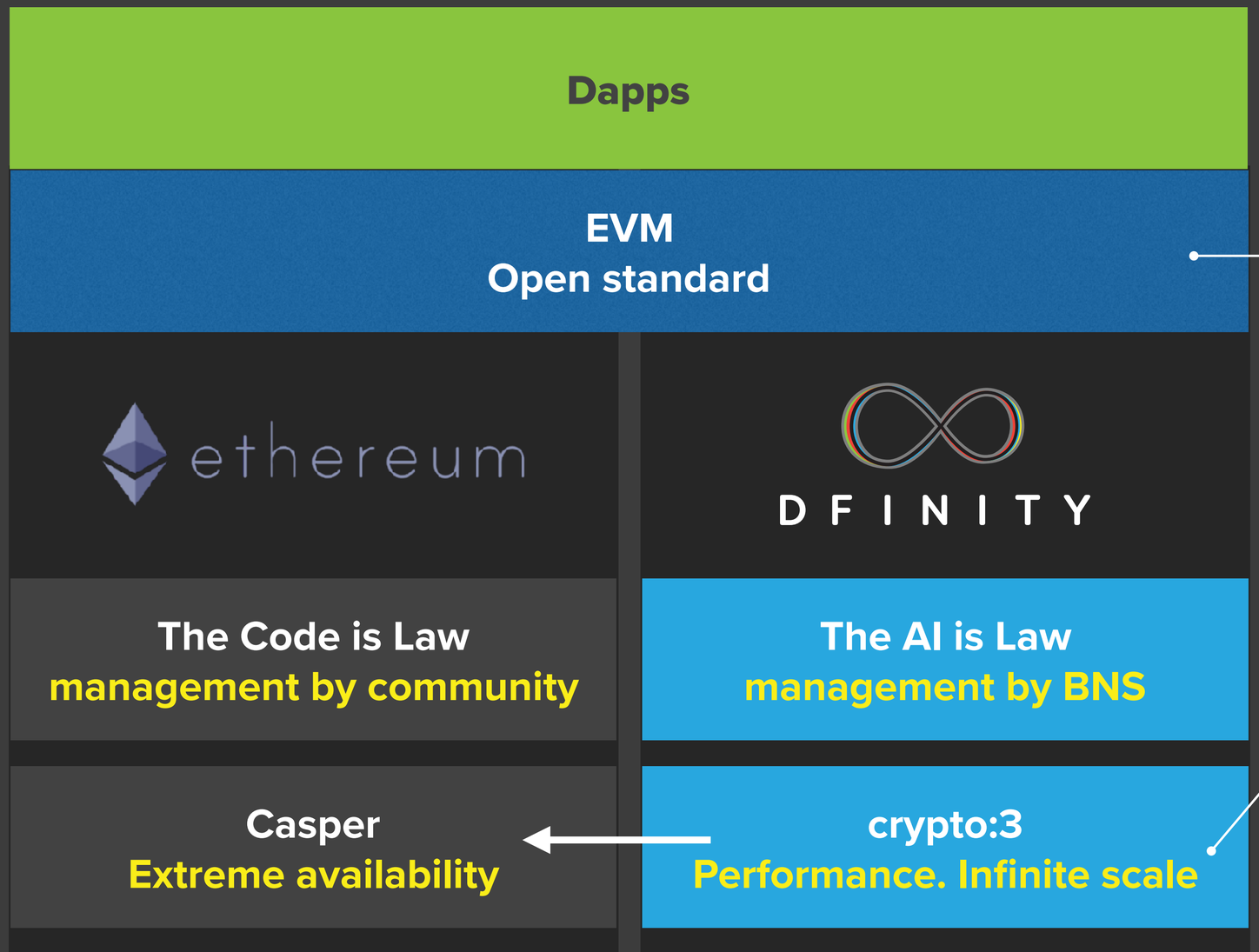
The AI is Law
management by BNS



Casper
Extreme availability

crypto:3
Performance. Infinite scale

Benefits of technology sharing



DFINITY working next gen. EVM & e.g. upgrading P2P networking

crypto:3 techniques reusable within Ethereum

Common open standards win out

Not compatible

Dapps

EVM
Open standard

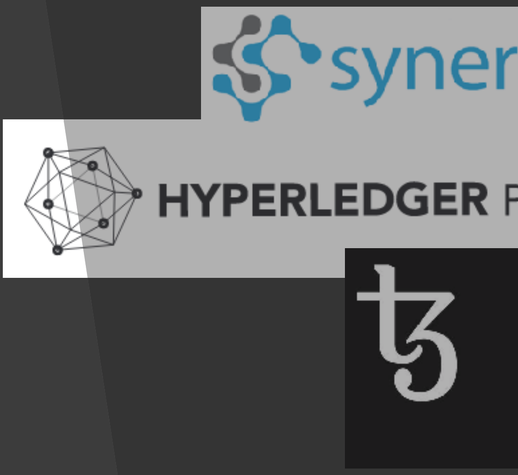
The Code is Law
management by community

The AI is Law
management by BNS

Casper
Extreme availability

crypto:3
Performance. Infinite scale

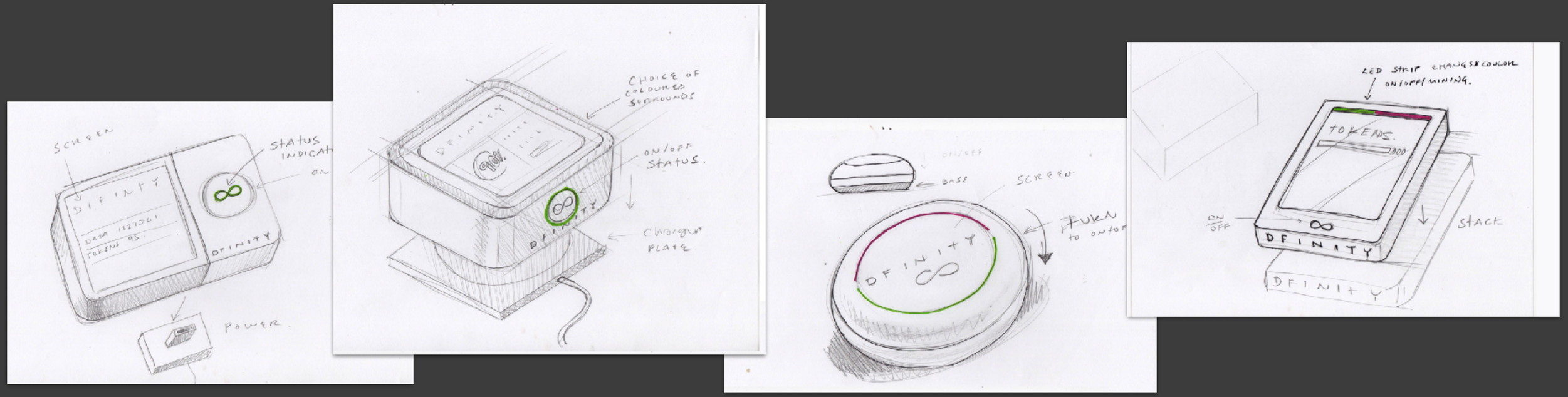
Not compatible



Decentralization vision

Decentralize/open The Cloud

Distribute across many hosts. Don’t just locate compute power in a few data centers



Consumer DFINITY mining devices under development @ String Labs

Decentralize/open Core Public Services

DFINITY was originally founded to unlock the massive scalability needed

Sharing **Micro-blogging** **“Email”** **Search** **Storage**

Decentralize/open Core Public Services

Special features enable advanced services such as PHI

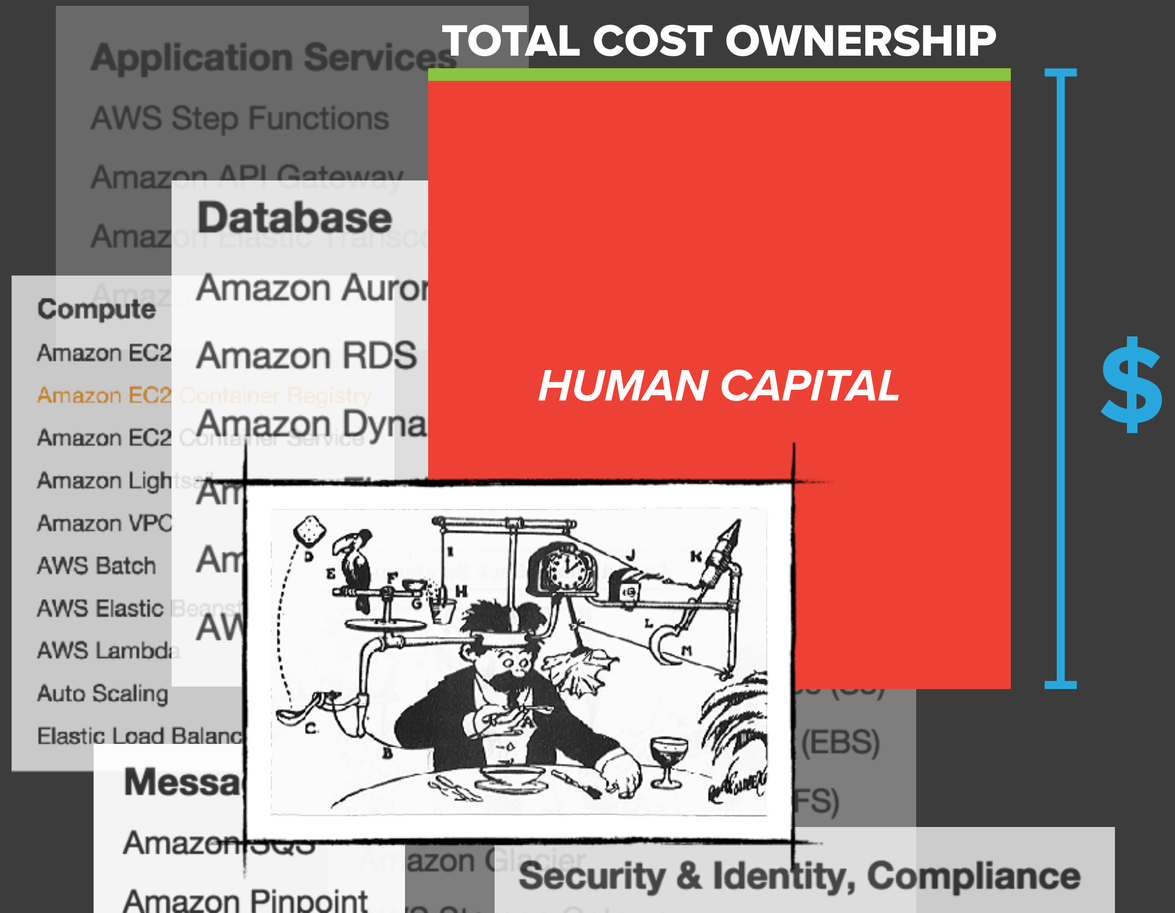
Decentralized Commercial Banking

PHI uses unmanipulable randomness
made available by DFINITY to
originate loans autonomously

Enterprise IT vision

Kill Enterprise IT Costs

Traditional IT → Decentralized Cloud



D F I N I T Y

The costs of owning enterprise IT systems are dominated by human capital. We can increase the cost of computation enormously but *save* money

Reimagine Enterprise IT

Blockchain properties make reinvention possible

rities & Trading | Supply chain & Trade finance | Intellectual property management | Logistics & Asset Tracking | Charity | Educati

Legal | Real Estate & Property | Internet of Things | Financial markets and exchanges | Electronic medical records | Digital rights

Smart property | Workforce | Collaborative economy | Voting & Governance Systems | Insurance | Global identity | Provenan

s-border finance | Customer Acquisition & Loyalty | Escrow & Custody services | Identity management | Auditing & Compliance

Autonomous
systems w/o intermediaries

Unstoppable
no servers to fail

Verifiable
know what code you execute

Cyberspace
no servers so no geography

Tamperproof
no servers to meddle with

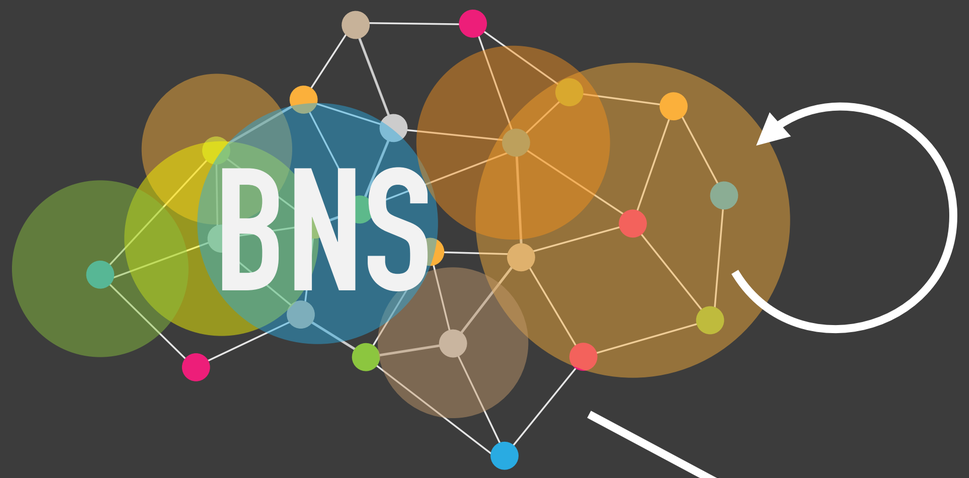
Shareable
Open code and governance

Simple
distribution abstracted away

Interoperability
no server boundaries

Blockchain Nervous System

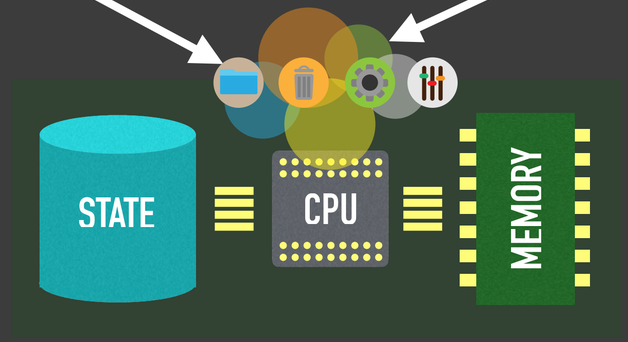
Proposal Processing



2. BNS evaluates proposal
- Process is type dependent
- Output is adopt | reject

1. Submit proposal
- Standard types of proposal
- A fee is paid in dfinities
- Deposit refunded on adoption

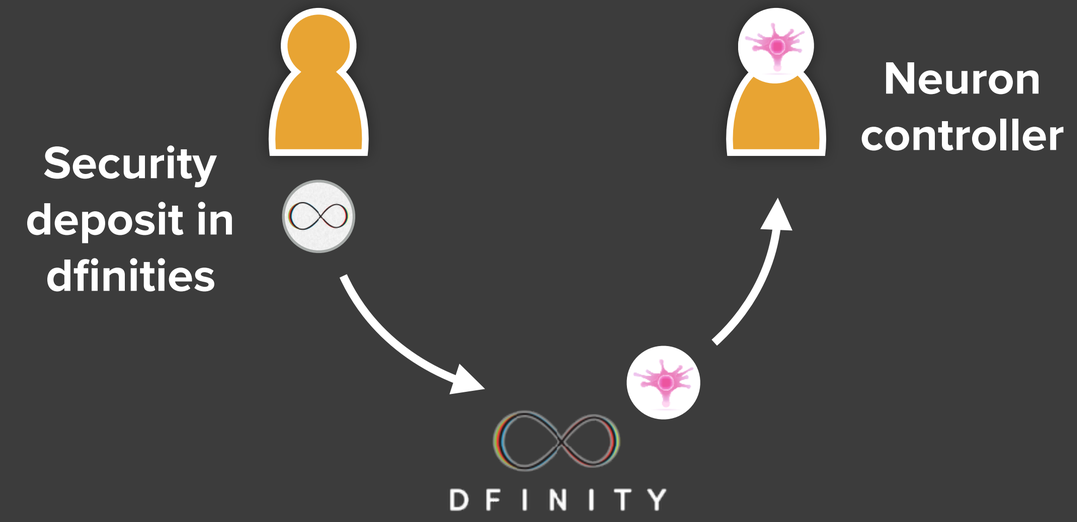
3. Voting triggers decision
- Exec. privileged EVM op codes
- Freeze contracts, move tokens
- Run arbitrary privileged code
- Change economic parameters
- Upgrade the protocol



People Create Neurons

Users create neurons to earn “decision” mining rewards

Neuron’s rewards proportional to dfinities deposited and votes

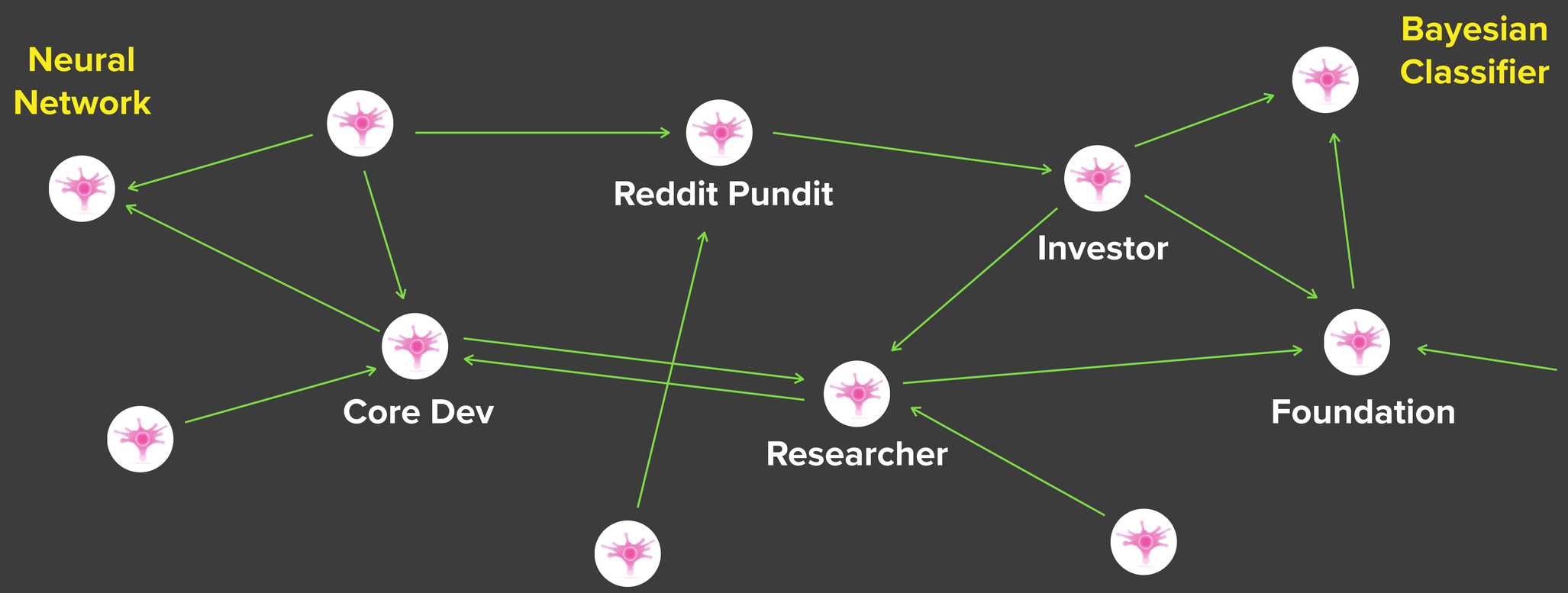


Neuron voting key configured into laptop or smartphone client

Neuron’s voting power equals dfinities deposited

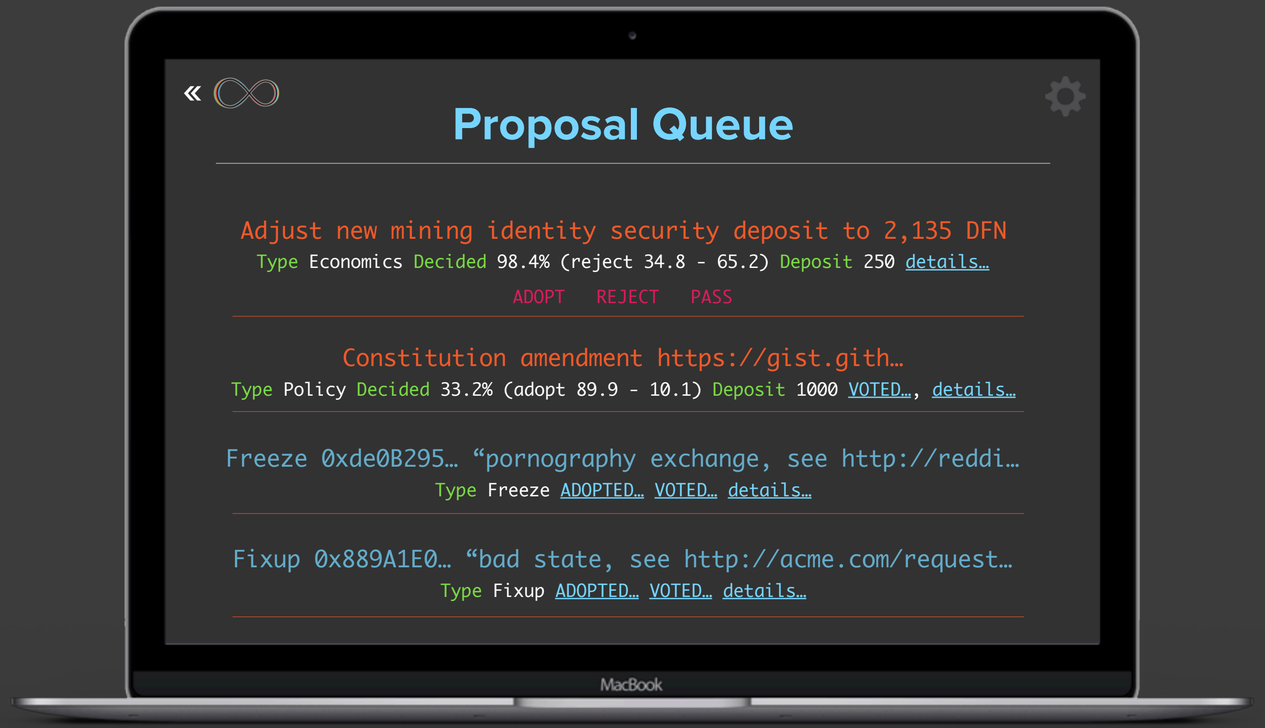
Create a neuron by depositing DFN/dfinities with the BNS. Try and ensure BNS adopts good decisions the markets reward since it takes months to dissolve your neuron and recover the DFN

Neurons Follow Neurons...



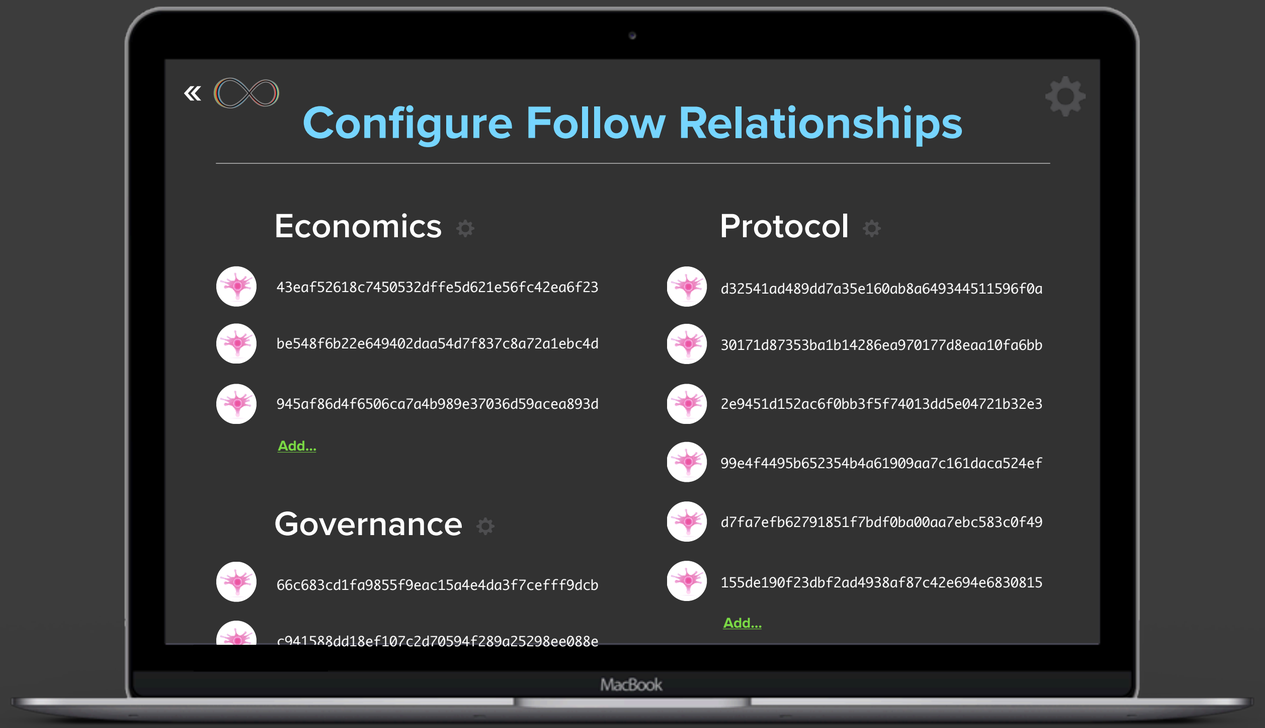
Neurons “follow” other neurons (relationships can be arbitrarily complex) to vote automatically using the output of other neurons. People can advertise the address of their neuron

Neuron Client Software



Proposals are submitted with a non-refundable fee and deposit that is refunded if the proposal is adopted. Before the timeout, the neuron controller (owner) can vote manually on proposals...

Neuron Client Software



When the neuron's controller (owner) doesn't vote on a proposal before the timeout, the neuron client software examines the "follow" relationships configured for the proposal's type...

BNS Factoids

Distributed “Hybrid” AI

Wisdom of Crowds processed algorithmically

Traditional AI integrated via neurons & “followed”

Neurons cascade to make decisions on proposals

Objective: drive market value of DFN/dfinities

Dopamine: is market reaction to decisions made

Learning: relationships updated after market feedback

Security

Follow relationships on edges and *unknowable*

Impossible blackmail, extort, bribe key neuron holders

Impossible sue or prosecute owners neurons “trip” decisions

BNS Factoids

Read in-depth articles on our blog

---

https://medium.com/dfinity-network-blog

See technical FAQ on website

---

https://dfinity.network/faq

crypto:3

EXAMPLE TECHNIQUES

1

Threshold Relay randomness

Relay between groups of clients and produce randomness unmanipuably

The world's *first* decentralized "random beacon"

2

Probabilistic Slot Protocol blockchain

Threshold groups select forgers and notarize blocks produced

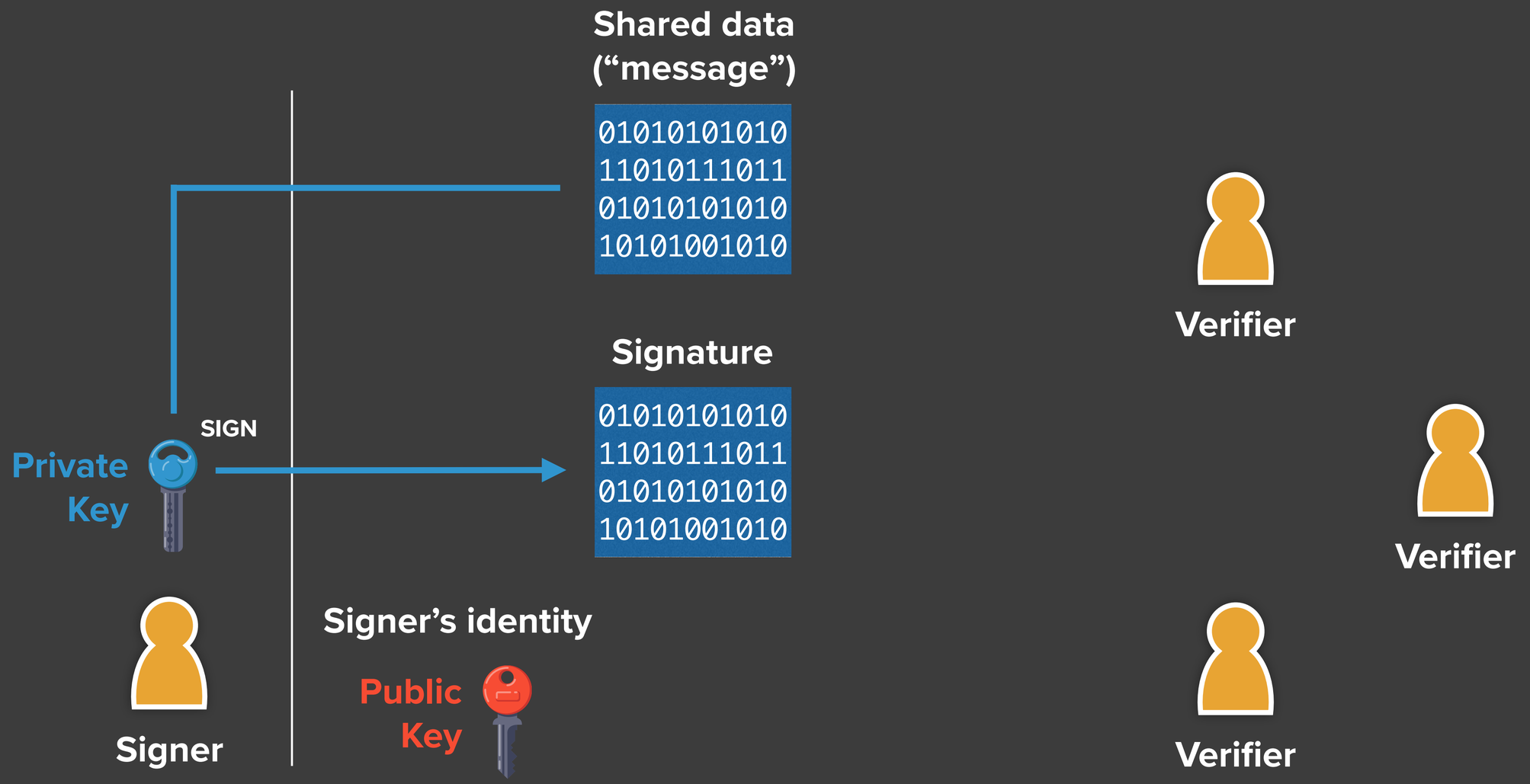
50X+ faster finality (speed) plus 50X+ more gas available vs today's Ethereum

Threshold Relay

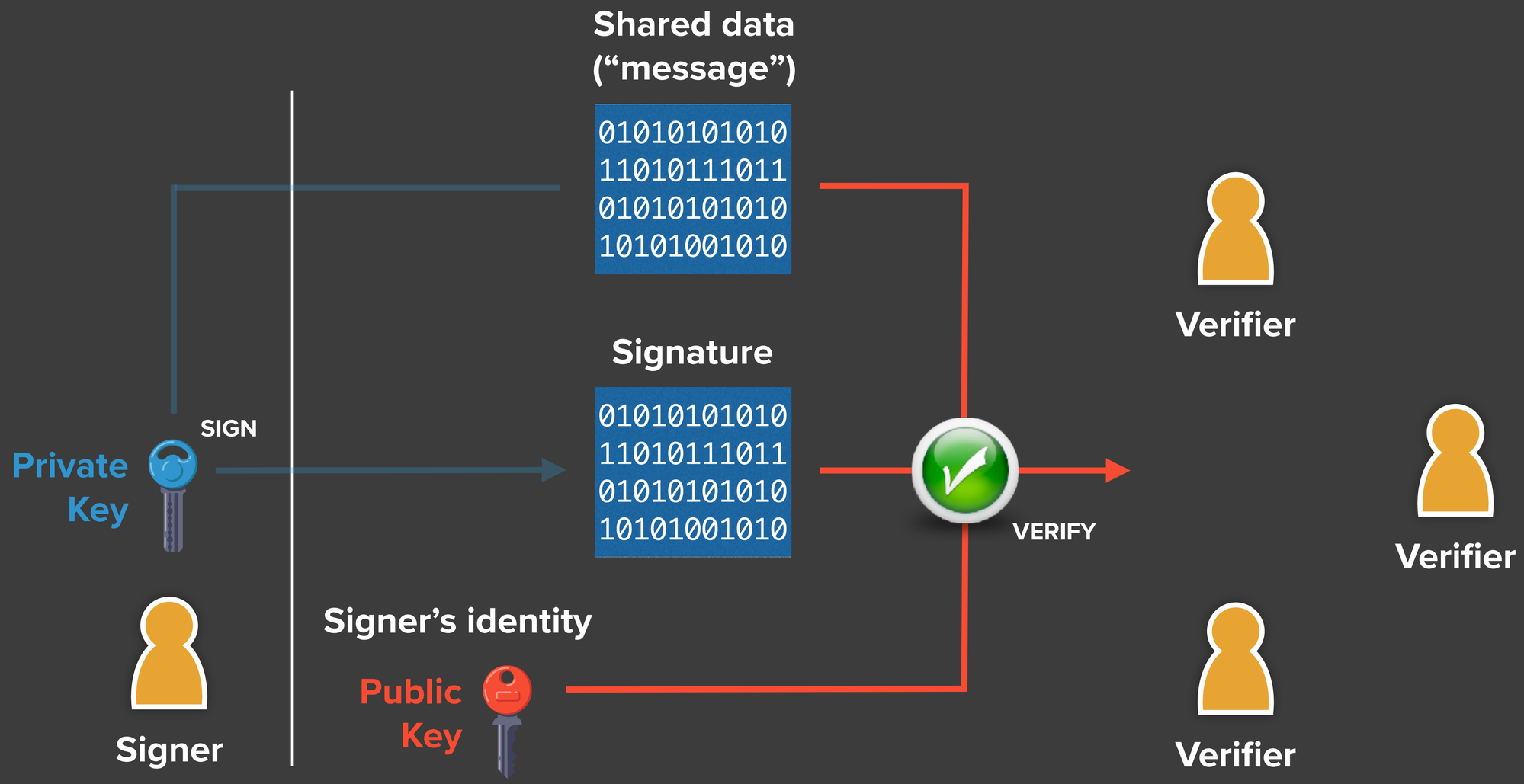
Produce randomness that is incorruptible,
unmanipulable and unpredictable

Explain “unique deterministic” threshold signatures...

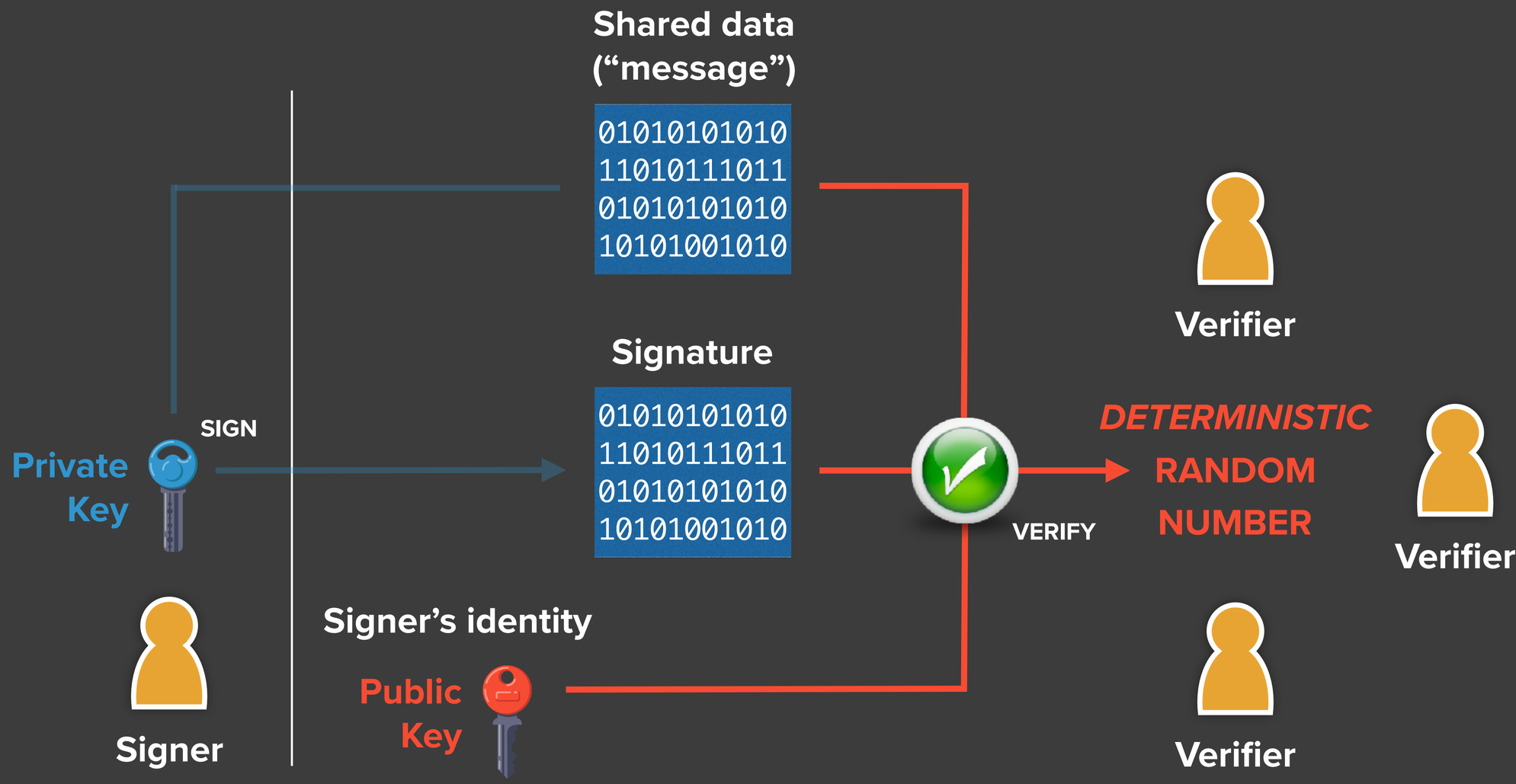
Usually a signer creates a signature on message data



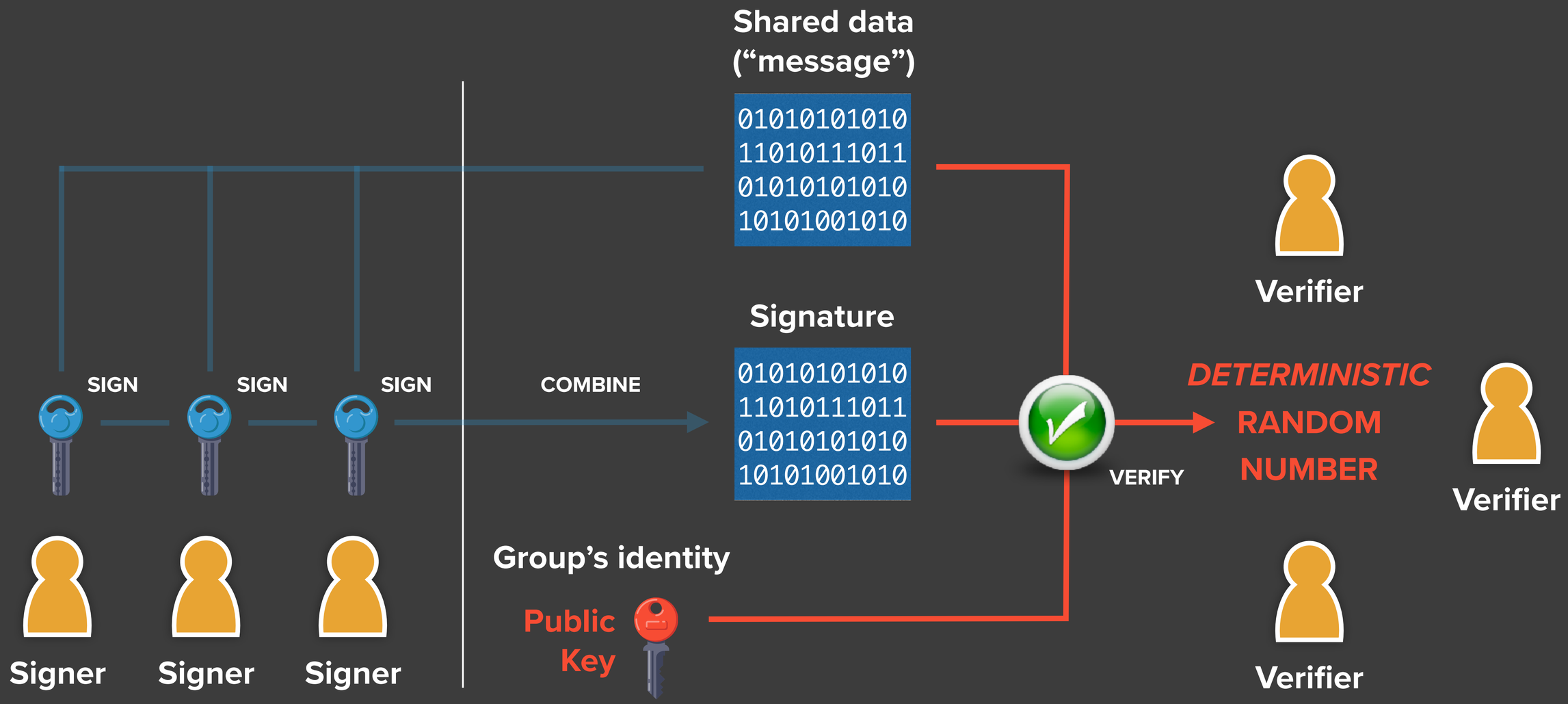
That can be verified using the signer's public key



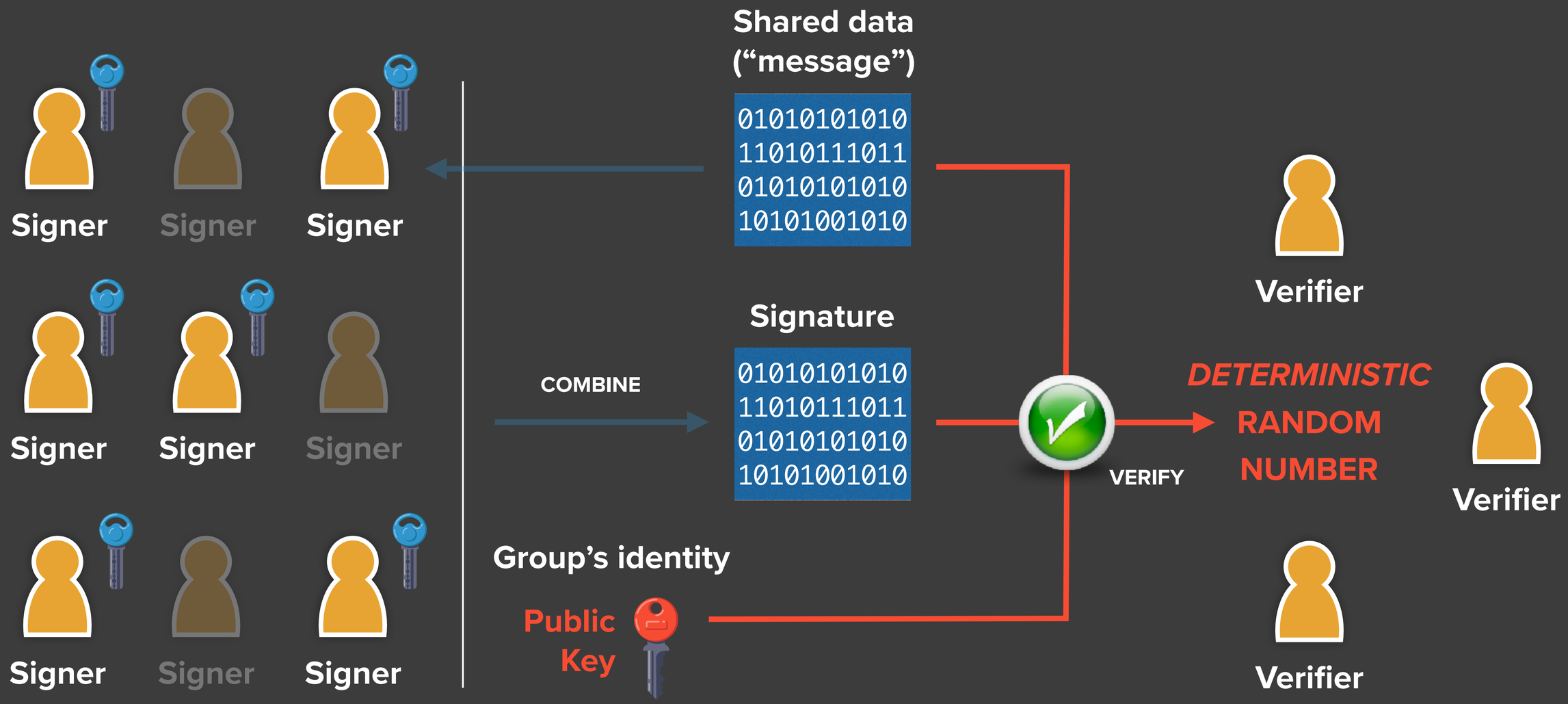
If unique and deterministic scheme then only 1 correct signature



Unique and deterministic threshold signature scheme possible



Whatever subset (threshold) of group sign signature stays same



Unique Deterministic Scheme
Boneh-Lynn-Strachan signatures (BLS)

Parameters

- Two groups G_1, G_2 of prime order r (on two elliptic curves)
- Generators $Q_1 \in G_1, Q_2 \in G_2$
- Bi-linear pairing $e : G_1 \times G_2 \mapsto G_T$

Key Generation

- Secret key: $x \bmod r$
- Public key: $P = xQ_2 \in G_2$

Signing

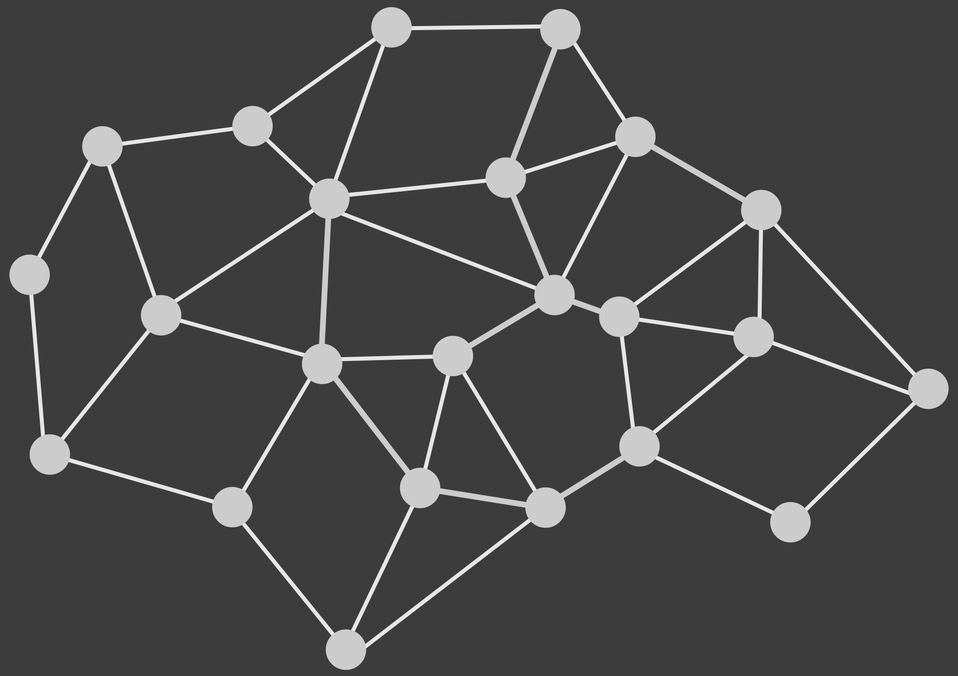
- Message hashed to $H(m) \in G_1$
- Signature: $s = xH(m) \in G_1$

Verification $e(s, Q_2) = e(H(m), P)$?

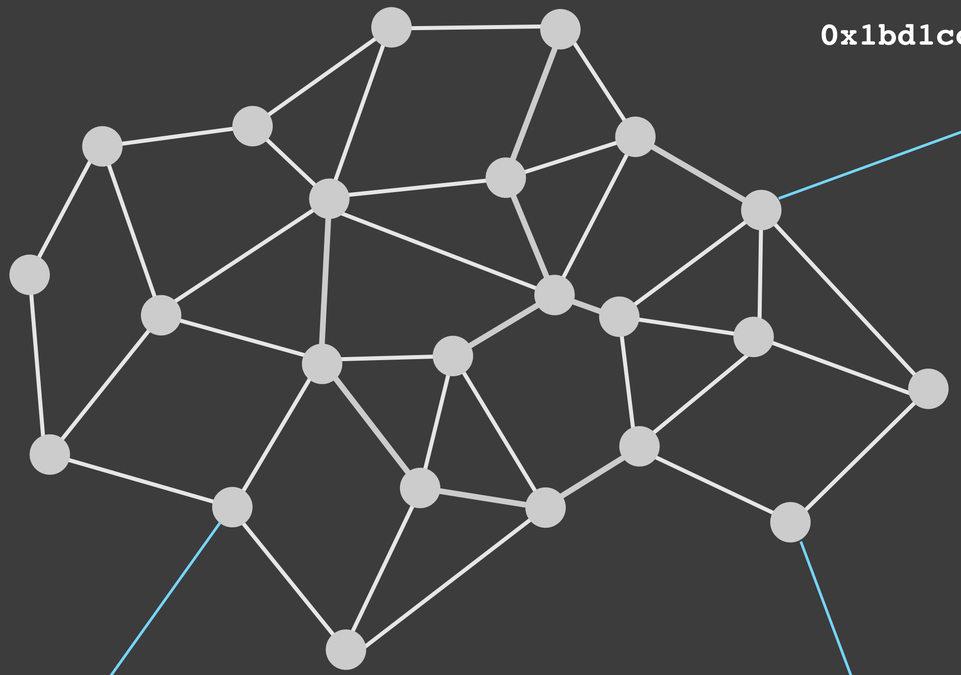
BLS, 2003 (Stanford University)

Relay between groups of signers...

A vast peer-to-peer broadcast network of mining clients...



That are registered on the ledger



0x1bd1ccf169d755306e077b38cb9aeae28e245351

DEPOSIT: 1000 DFN

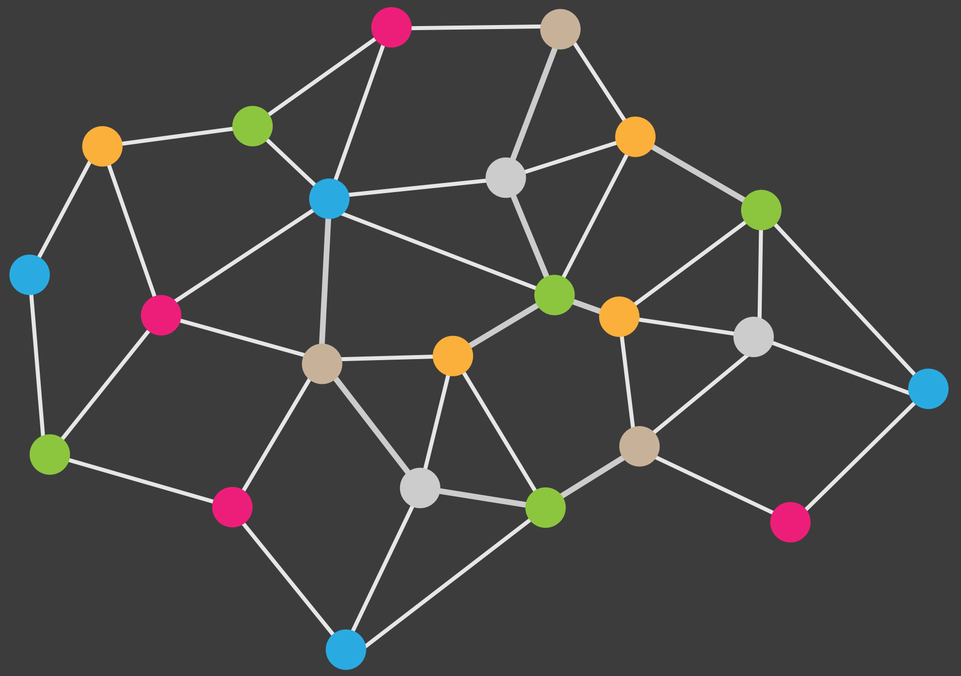
0x2b197453dcfabe85be2fbe31c8cc19bd30576ed0

DEPOSIT: 1000 DFN

0x2b197453dcfabe85be2fbe31c8cc19bd30576ed0

DEPOSIT: 1000 DFN

Are randomly assigned to groups that...



GROUP

GROUP

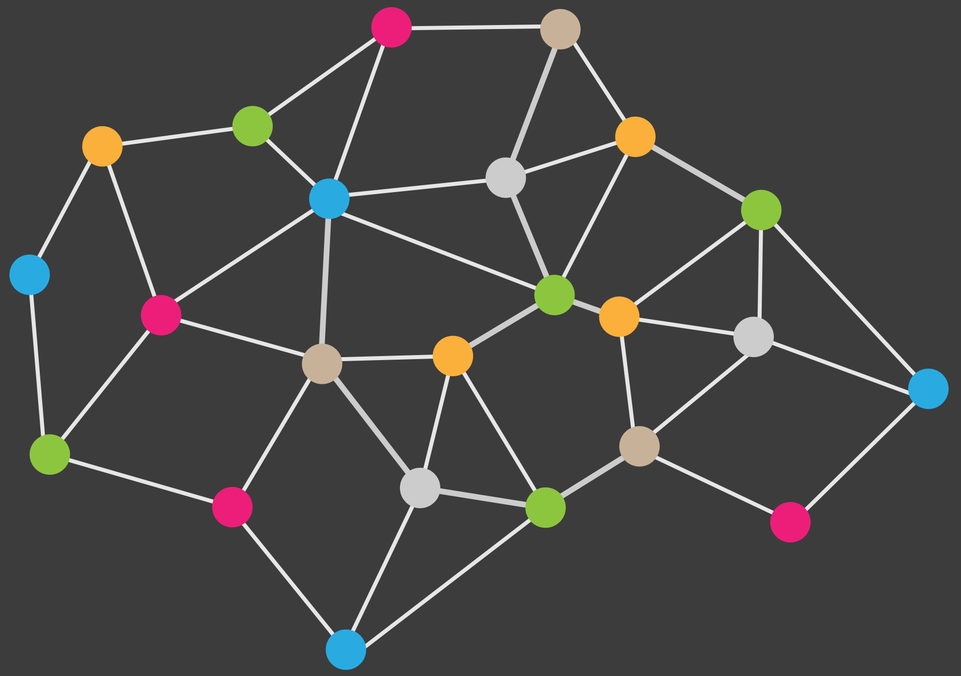
GROUP

GROUP

GROUP

...

Try to setup a “BLS threshold” scheme using DKG...



GROUP

GROUP

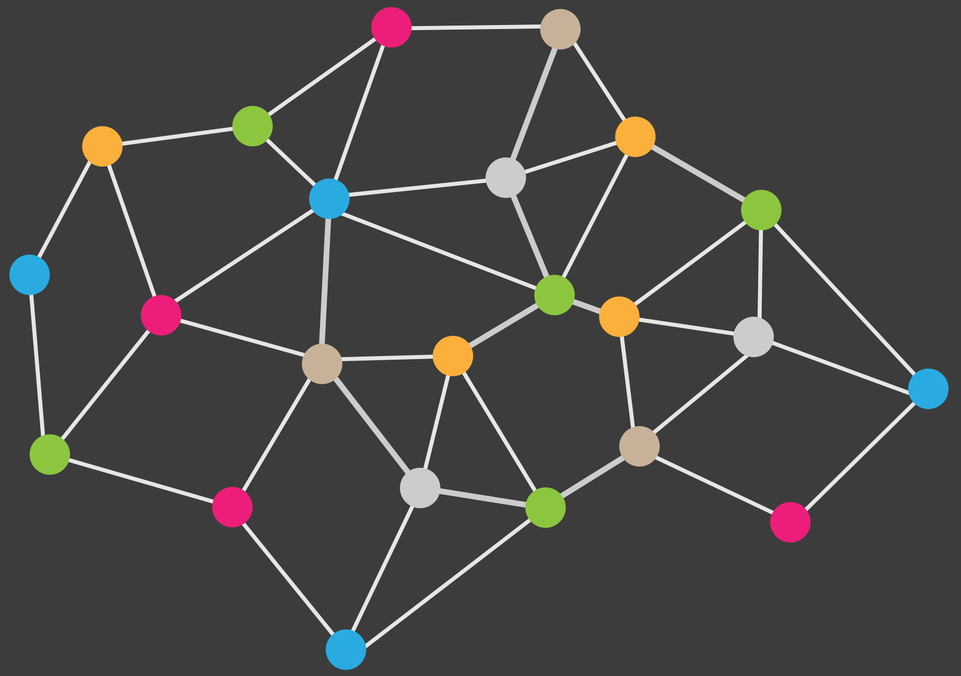
GROUP

GROUP

GROUP

...

And register their PubKey on the ledger too



GROUP
–

GROUP
–

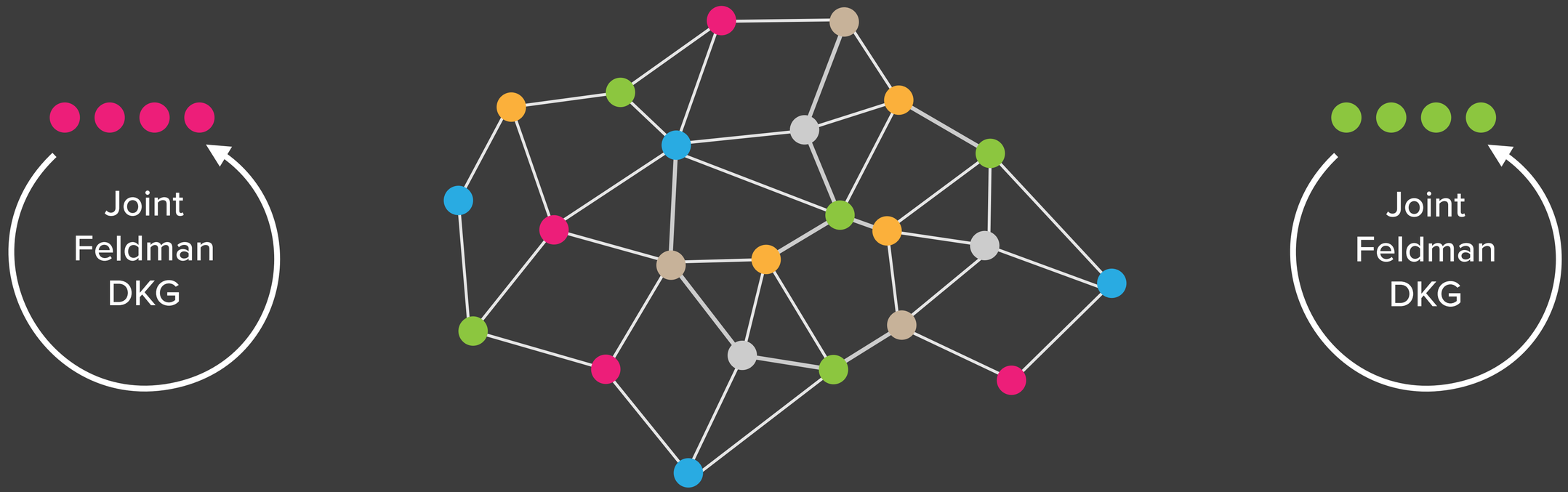
GROUP
–

GROUP
0x2b197453...

GROUP
–

...

Setup is independent of blockchain progression...



GROUP
–

GROUP
–

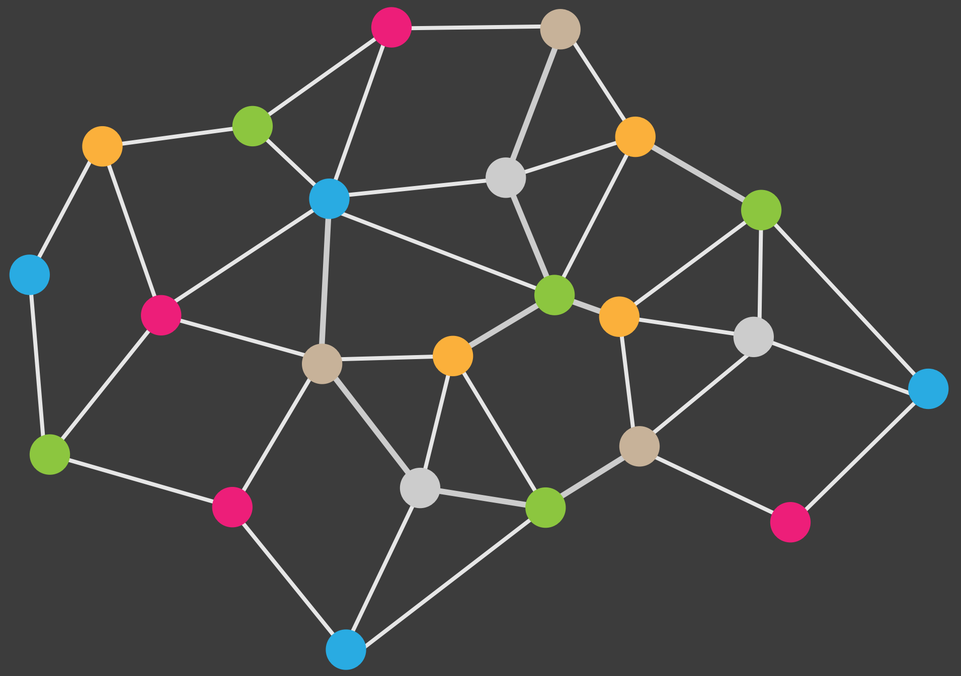
GROUP
–

GROUP
0x2b197453...

GROUP
–

...

And occurs asynchronously



GROUP
0x7de4ac5...

GROUP
0x8fb251b...

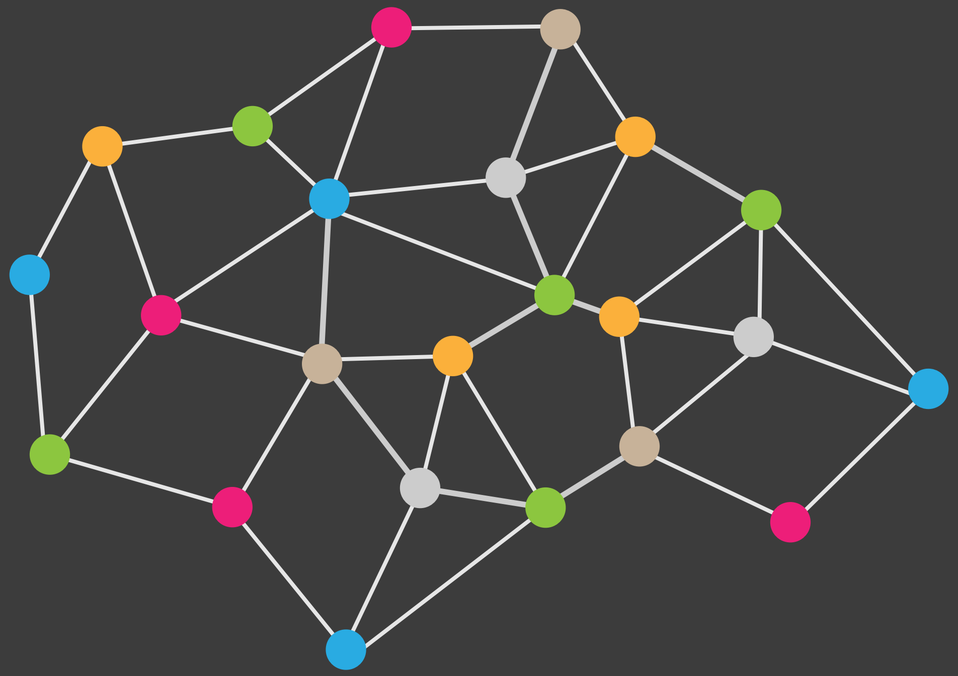
GROUP
–

GROUP
0x2b197453...

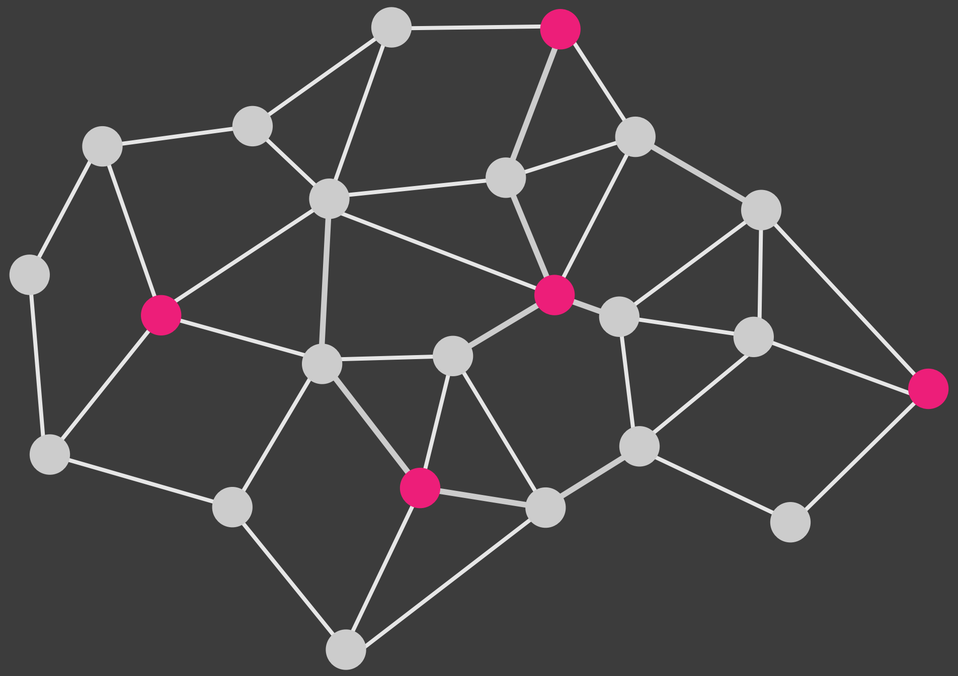
GROUP
–

...

As regards the blockchain itself...

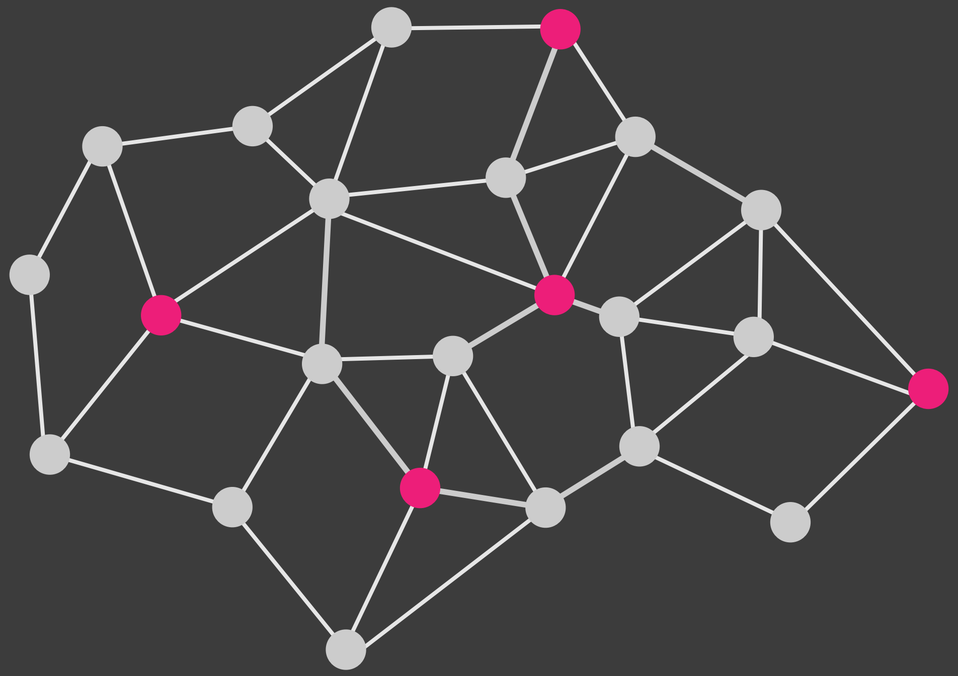


There is always a current group...



h

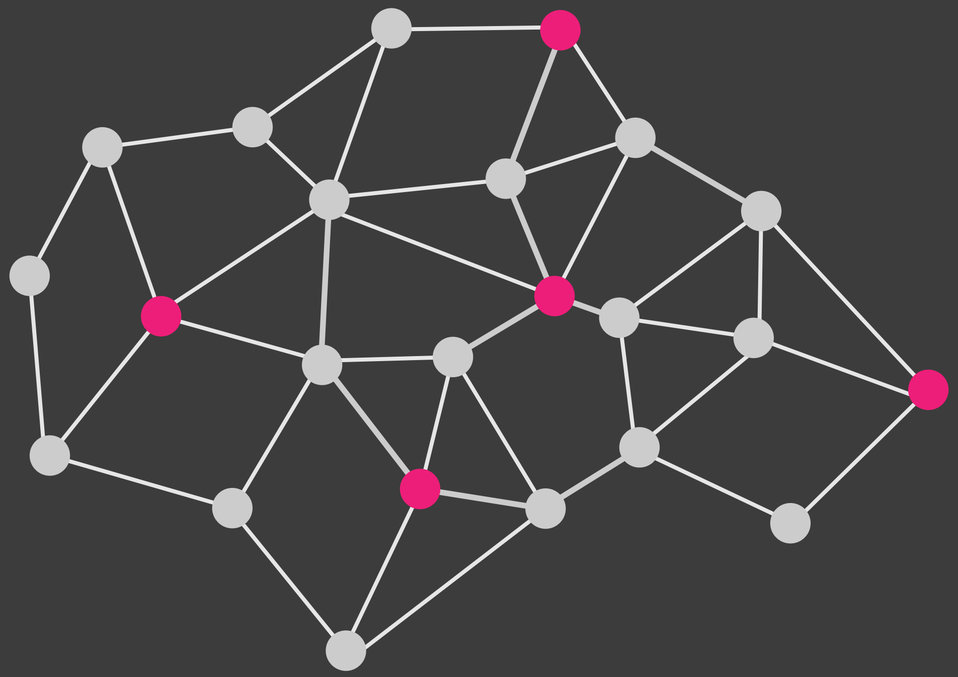
That signs the previous group's signature...



$$e(\sigma, g) = e(H(m), g^x)$$

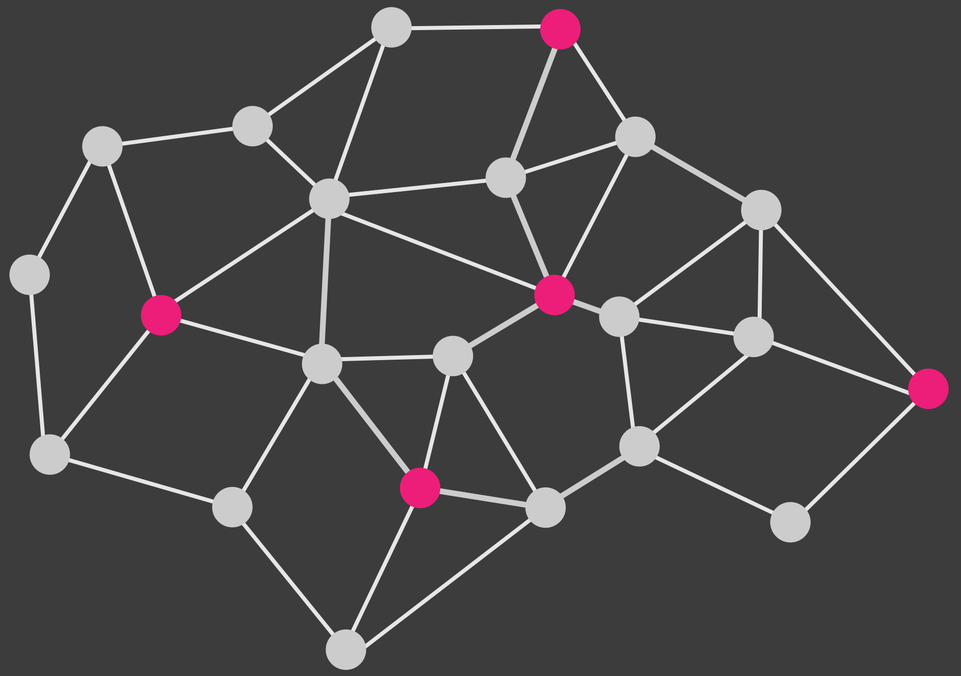
BLS Signature Scheme

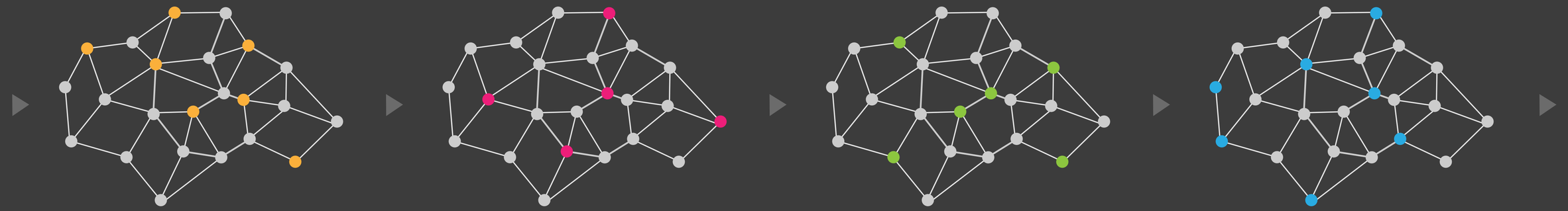
To select the next group and “relay”



$$G^{h+1} = \mathcal{G}[\sigma^h \bmod |\mathcal{G}|]$$

To select the next group and “relay”



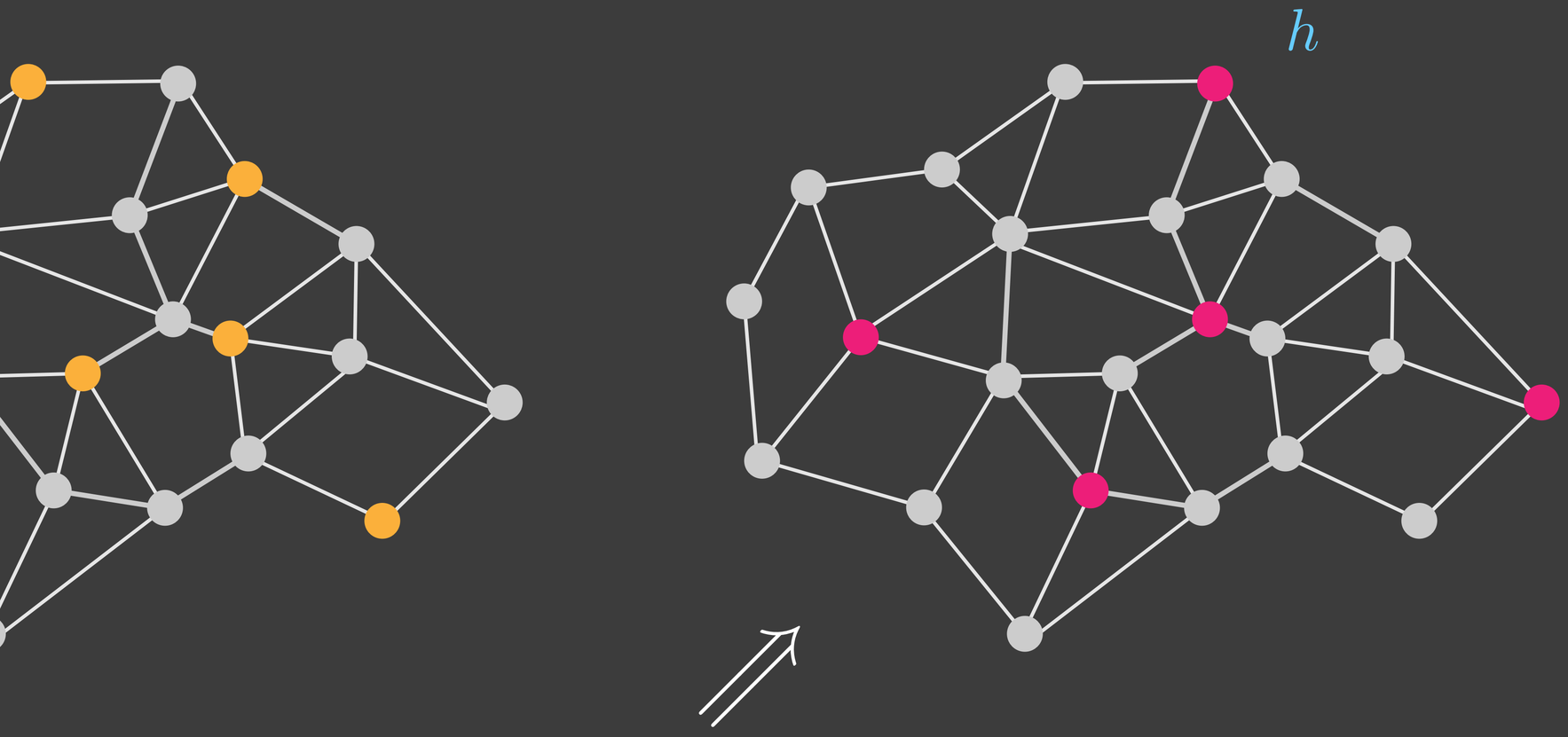


This is what Threshold Relay looks like

SIGNATURE

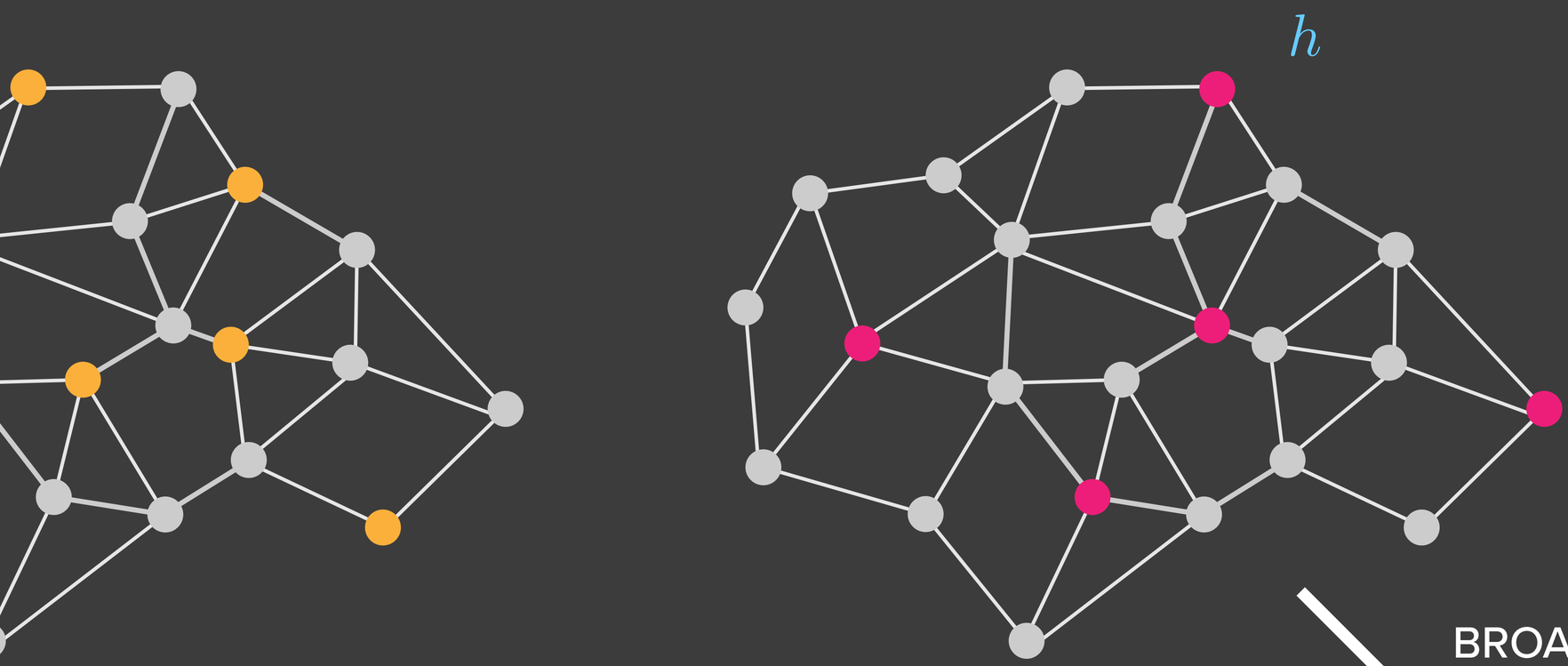
σ^{h-1}

The signature created at *h-1* selects the group at *h*

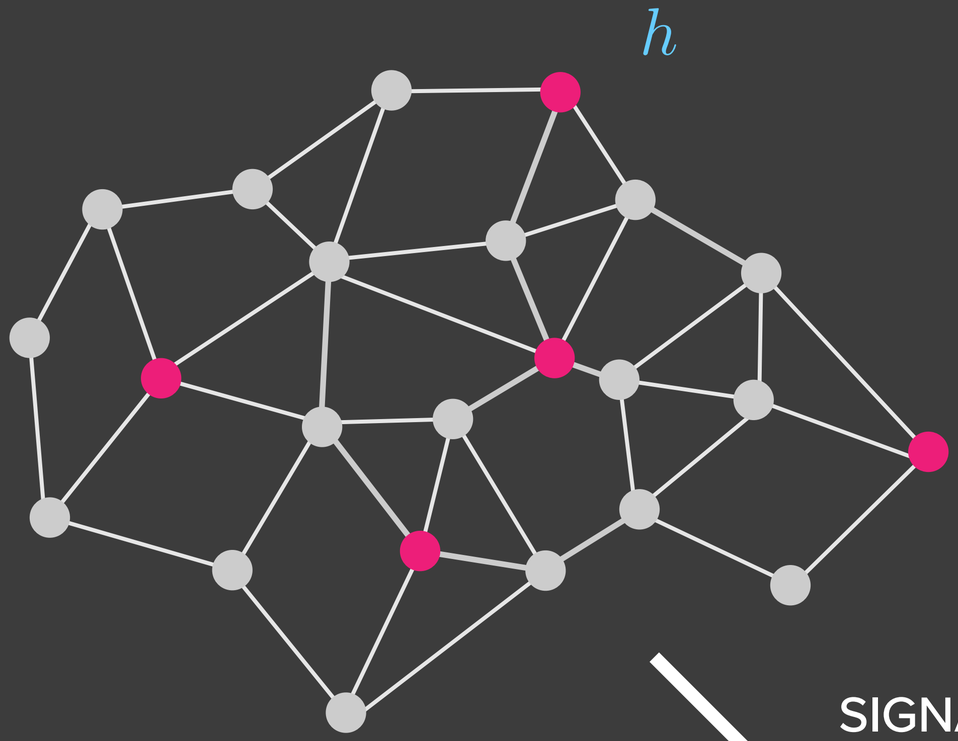


$$G^h = \mathcal{G}[\sigma^{h-1} \bmod |\mathcal{G}|]$$

Group members at *h* broadcast signature shares



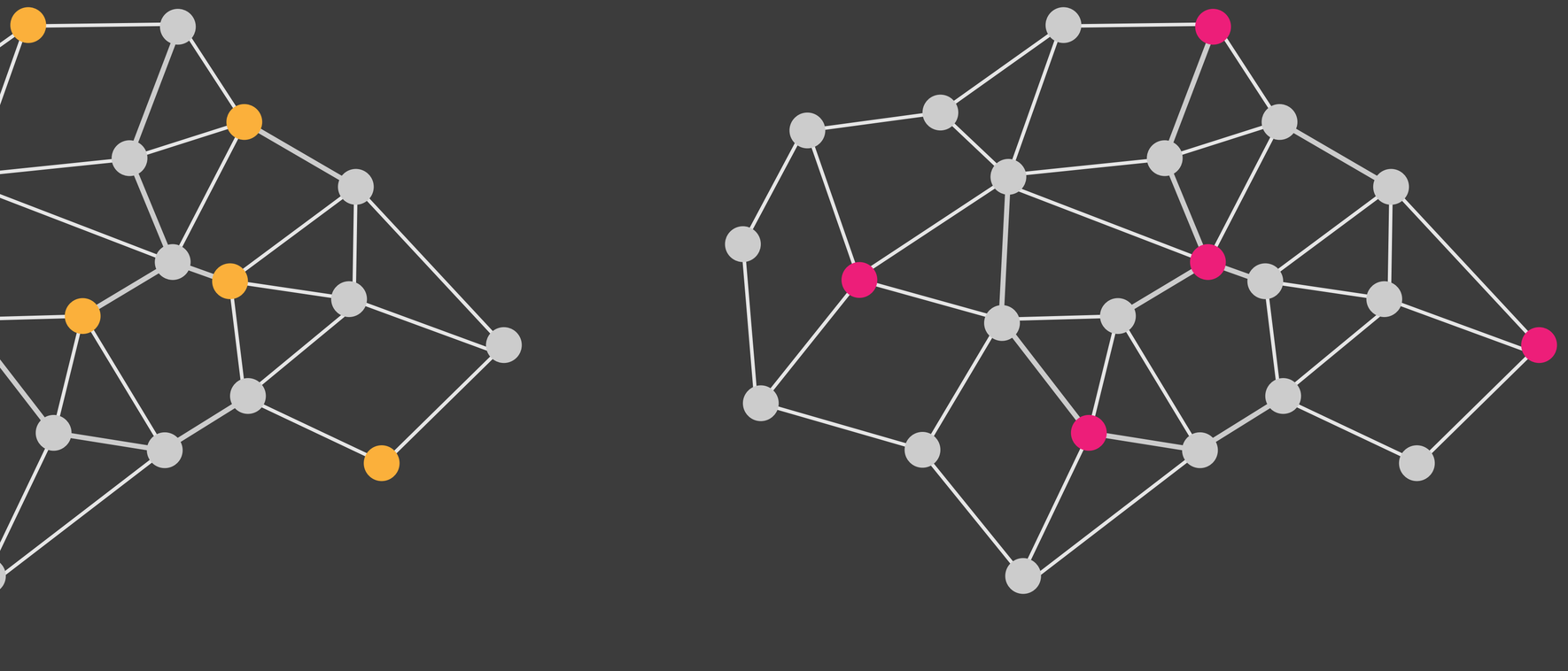
Collect threshold of shares & create only possible group sig...



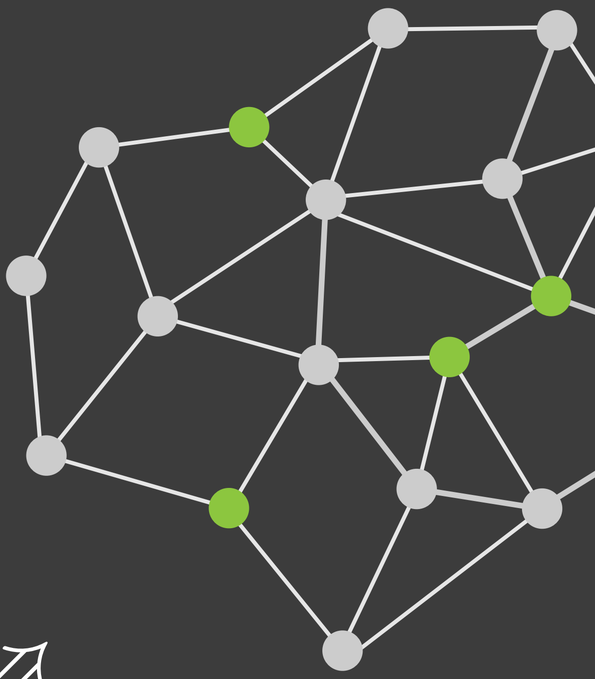
SIGNATURE

$$\sigma^h = bls(\{\sigma_p^h, p \in G^h\})$$

That selects the next group, ad infinitum



$h+1$



$$G^{h+1} = \mathcal{G}[\sigma^h \bmod |\mathcal{G}|]$$

This creates a decentralized VRF

$\sigma^{h-7}, \quad \sigma^{h-6}, \quad \sigma^{h-5}, \quad \sigma^{h-4}, \quad \sigma^{h-3}, \quad \sigma^{h-2}, \quad \sigma^{h-1}, \quad \sigma^{h}$ 

A sequence of random numbers that is...

Deterministic • **Verifiable** • **Unmanipulable**

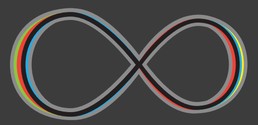
Next value released on agreement a threshold of the current group...

Unpredictable

> Random numbers should not be generated with a method chosen at random
>
> - Donald Knuth

TLDR; unmanipulable randomness is v useful...

Scale-out Decentralized Network Protocols



DFINITY

PSP Blockchain Designs

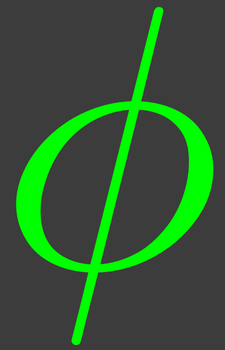
Validation Towers

Validation Trees

USCIDs

Lottery Charging Lazy Validation

Advanced Decentralized “Applications”



Autonomous loan issuance and crypto “fiat”

Financial exchanges

Data harvesting

Fault Tolerance Example

NETWORK METRICS

Processes	10,000
Faulty	3,000
(Correct)	7,000
Group Size	400
Threshold	201

Note: in practice the probability 30% of professionally run mining processes "just stop" is very low. Miners will generally deregister IDs to retrieve deposits when exiting.

$$P(Faulty \geq 200)$$

$$1e{-}17$$

Probability that a sufficient proportion of the group are faulty that it cannot produce a signature

Calculated using hypergeometric probability.
http://www.geneprof.org/GeneProf/tools/hypergeometric.jsp

Note: groups should expire to thwart "adaptive" adversaries

Communications Overhead Example

MESSAGE FORMAT

Process ID	20 bytes
Signature share	32 bytes
Signature on comms	32 bytes
Total	84 bytes

In order for a group to produce a threshold signature, its members must broadcast “signature shares” on the message that can be combined. Here is a typical packet carrying a signature share.

GROUP SIZE

Group size	400
Threshold	201

COMMUNICATION OVERHEAD

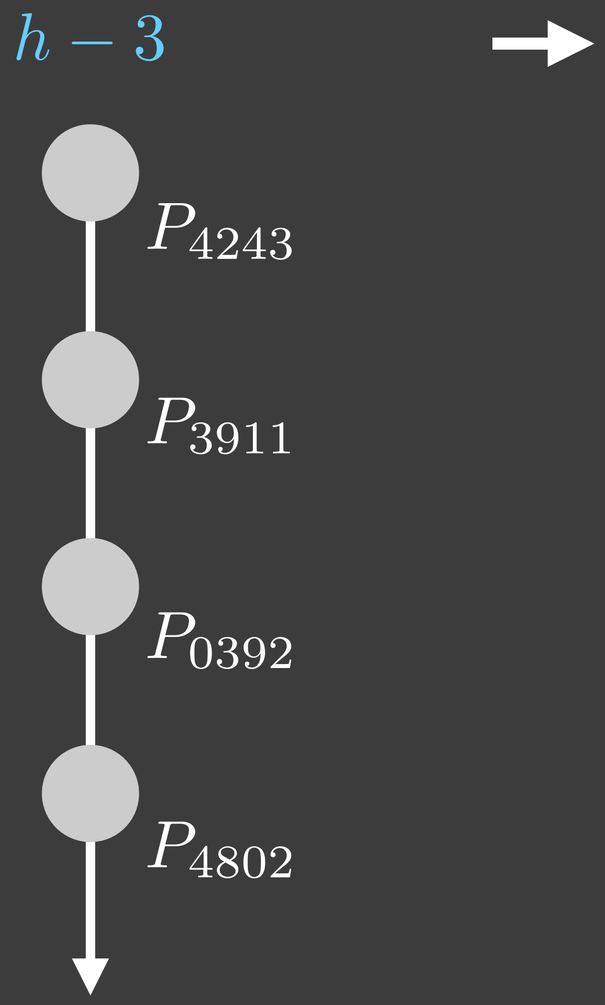
Maximum	34 KB

400 messages involve 34 KB of data transfer. However, only 17 KB (half the messages) are required to construct the signature. Thereafter signature shares are not relayed, so a more typical overhead is 22 KB.

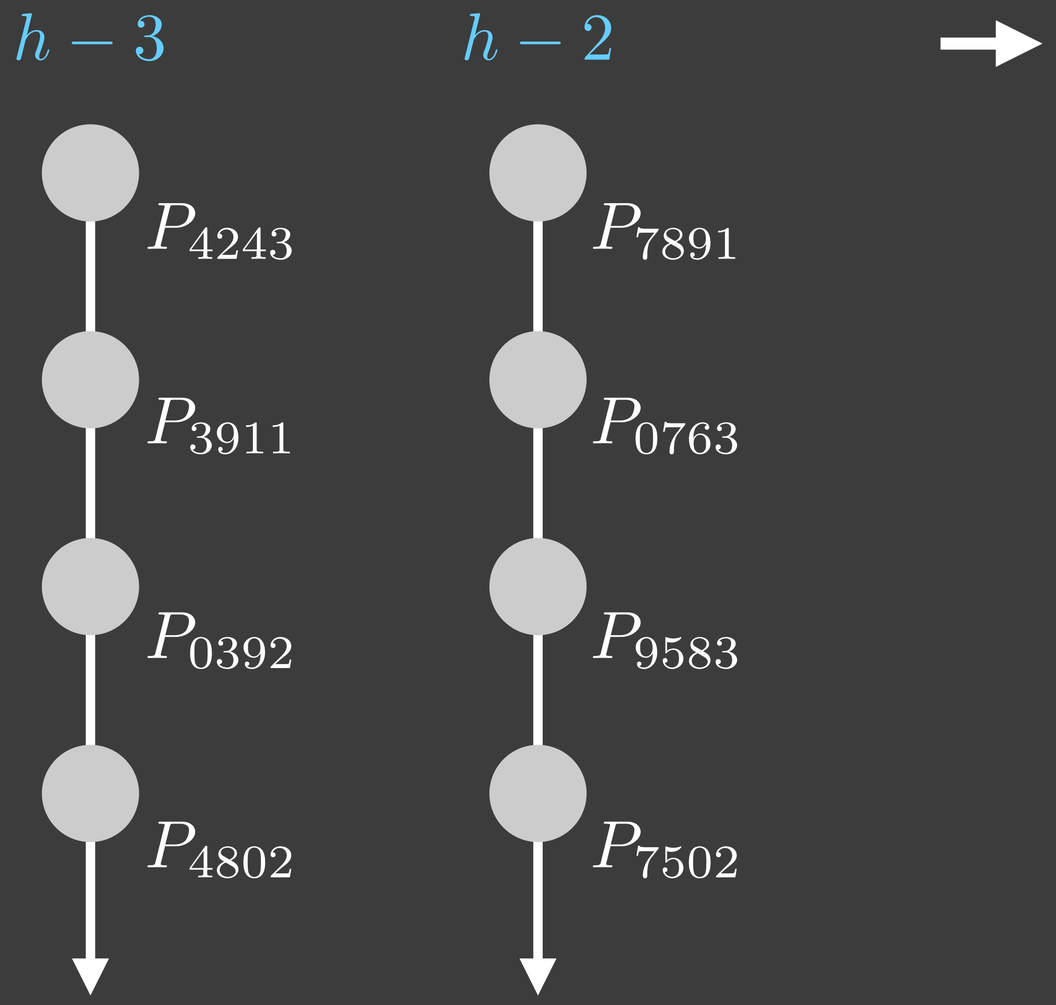
Probabilistic Slot Protocol

Derive from Threshold Relay a blockchain that securely increases speed and capacity 50X+

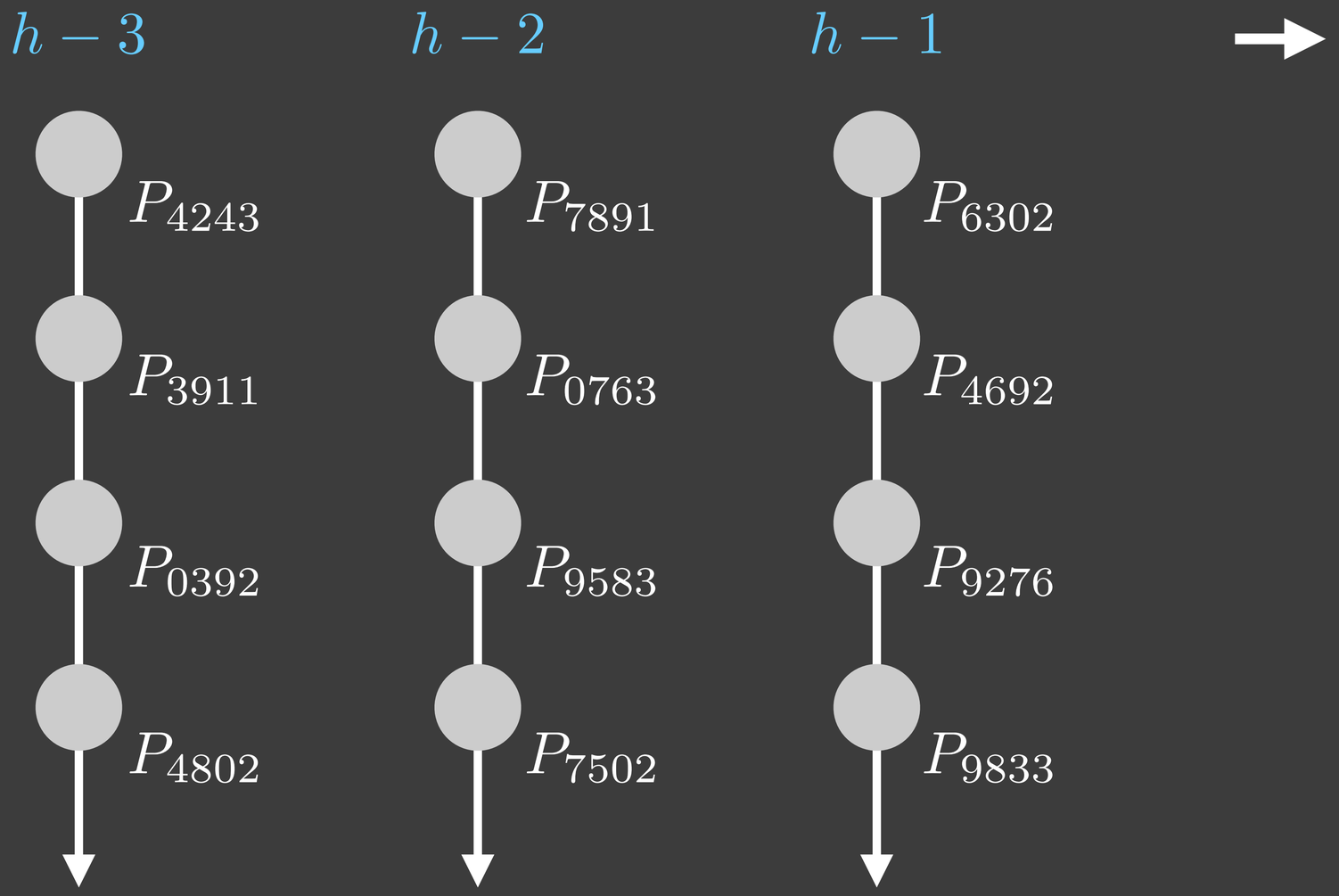
At each height, the randomness orders the processes...



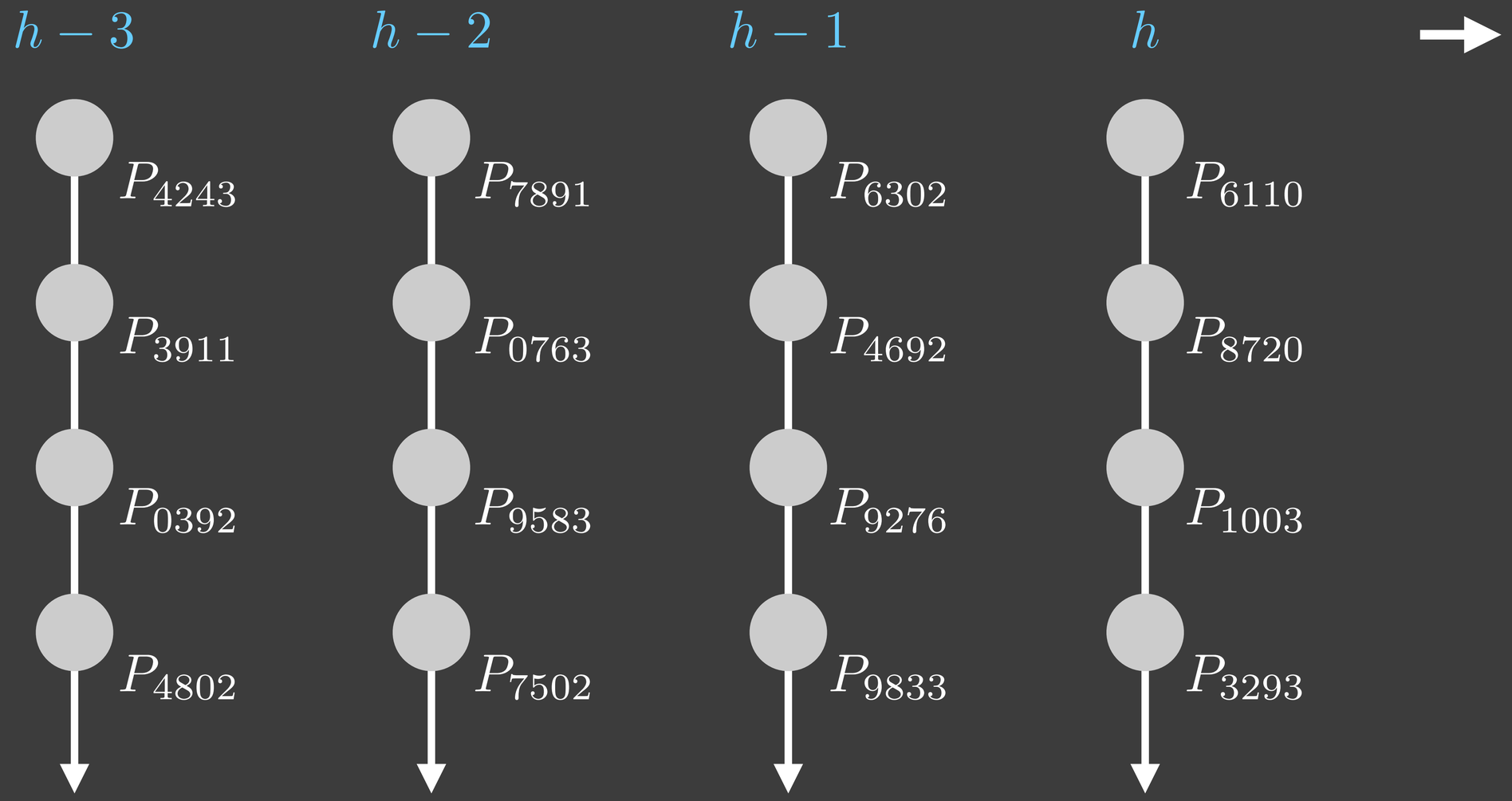
At each height, the randomness orders the processes...



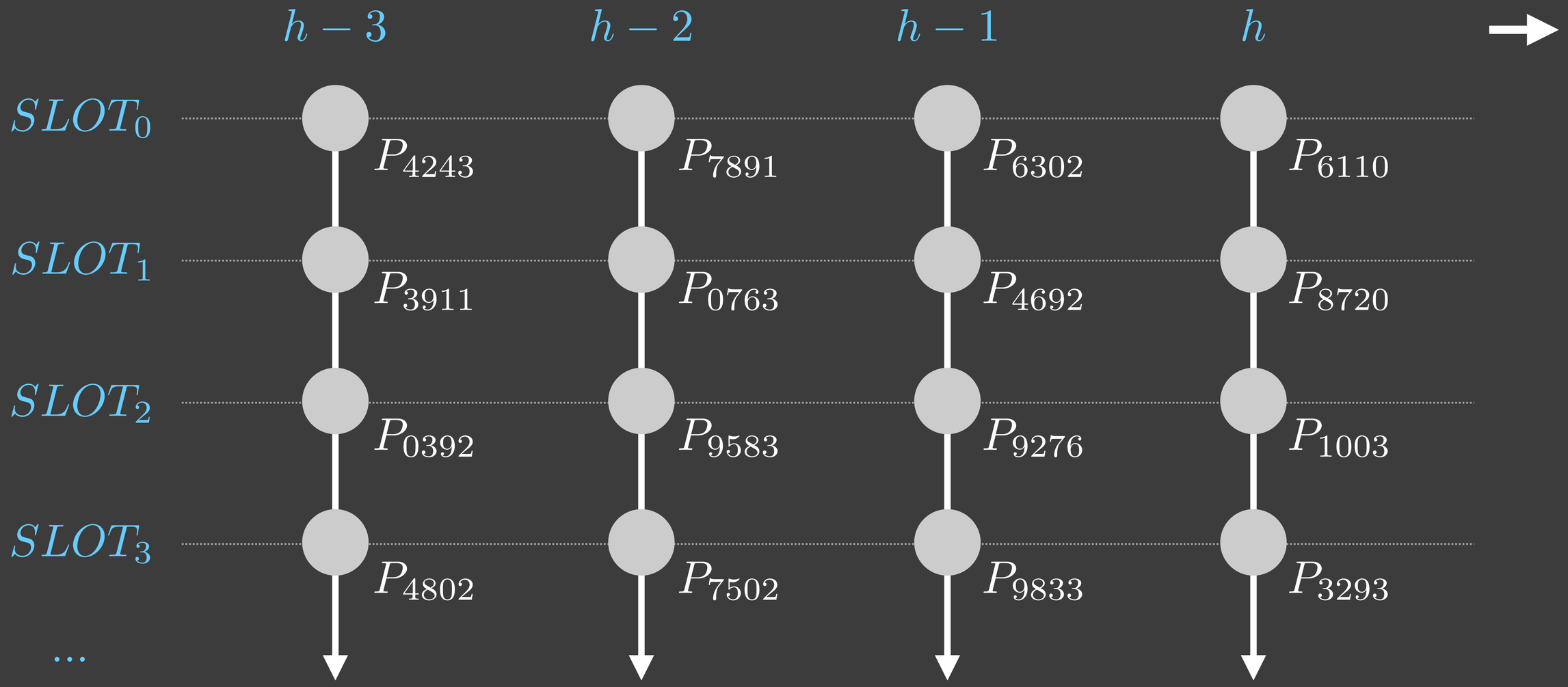
At each height, the randomness orders the processes...



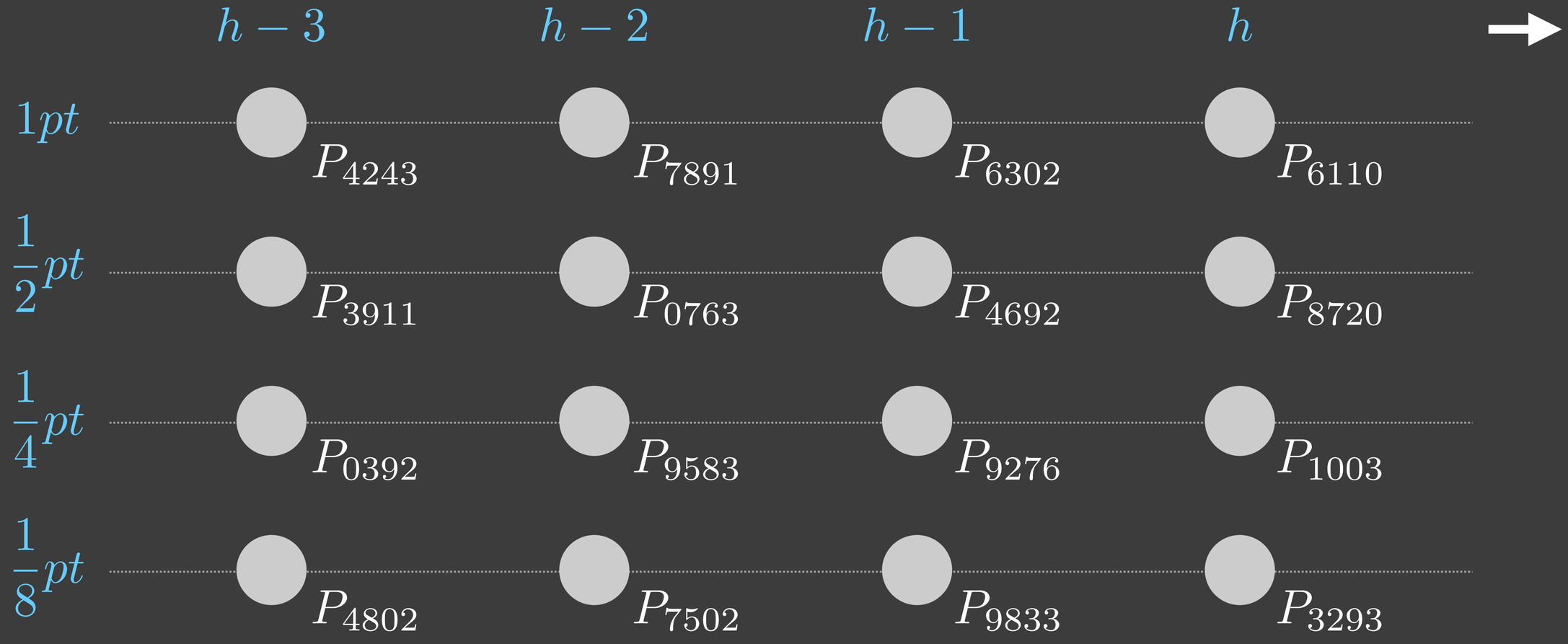
At each height, the randomness orders the processes...



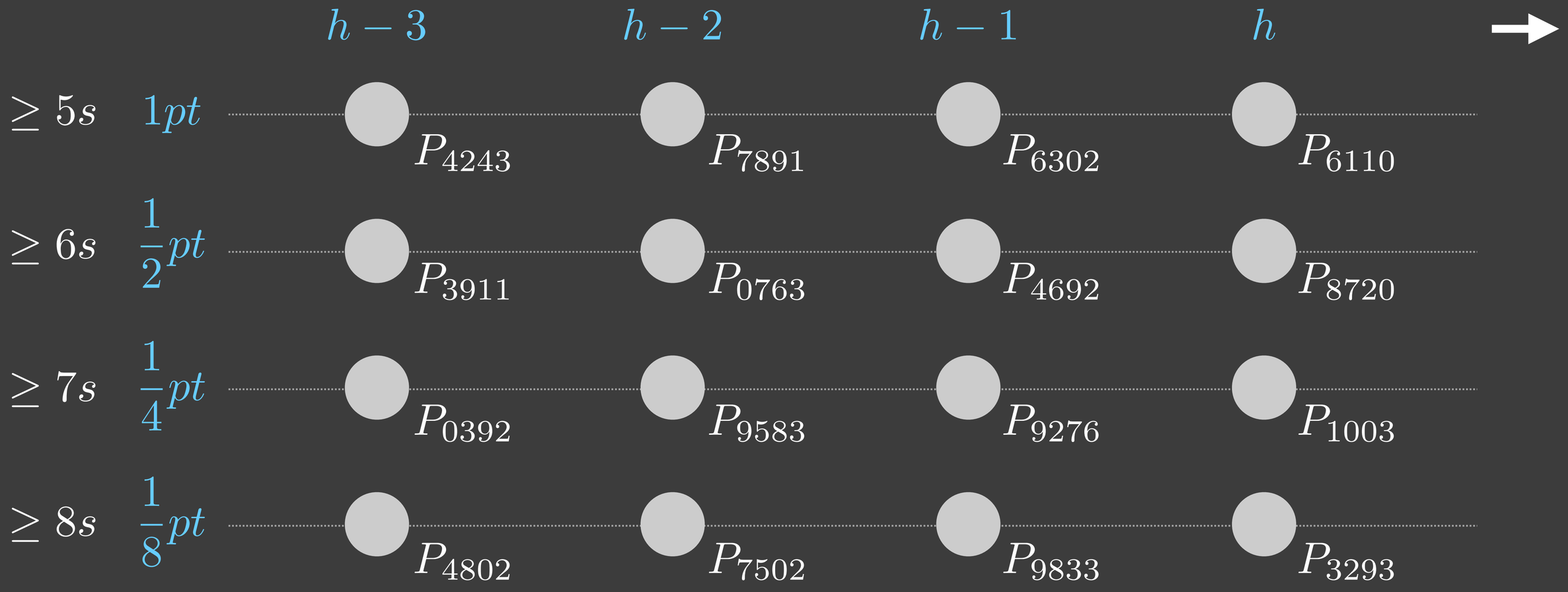
Indexes are priority “slots” for forging (zero highest)



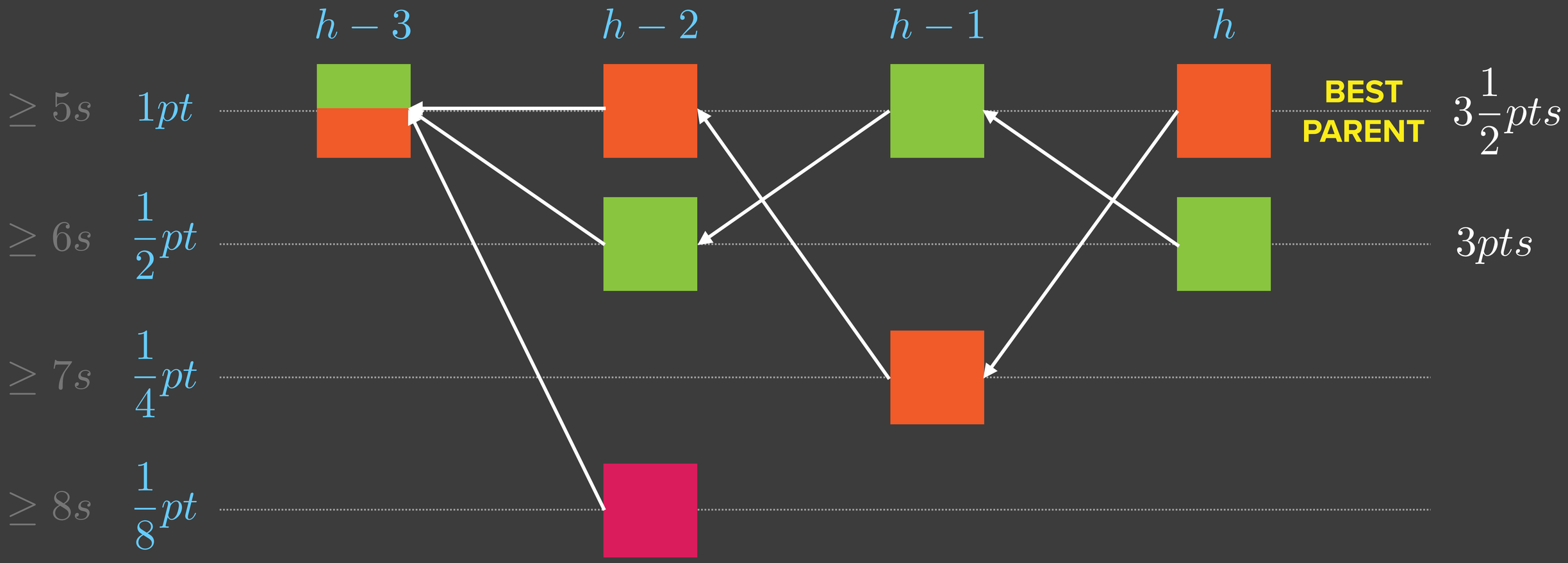
Value of candidate blocks scored by author's slot...



First publish/relay delay too (an optimization)...



We can create & score blockchains that converge



Very nice. But usual limitations. O no...

SELFISH MINING ATTACKS

The adversary can withhold blocks to gain an advantage over honest processes.

Selfish mining attacks increase the confirmations necessary for finality.

NOTHING AT STAKE

The adversary can go back in time and create forks from below *h* to Double Spend.

He only needs to be lucky and be granted a sequence of zero slots.

Solution?

Threshold groups “notarize” (sign) at least one block at their height before relaying...

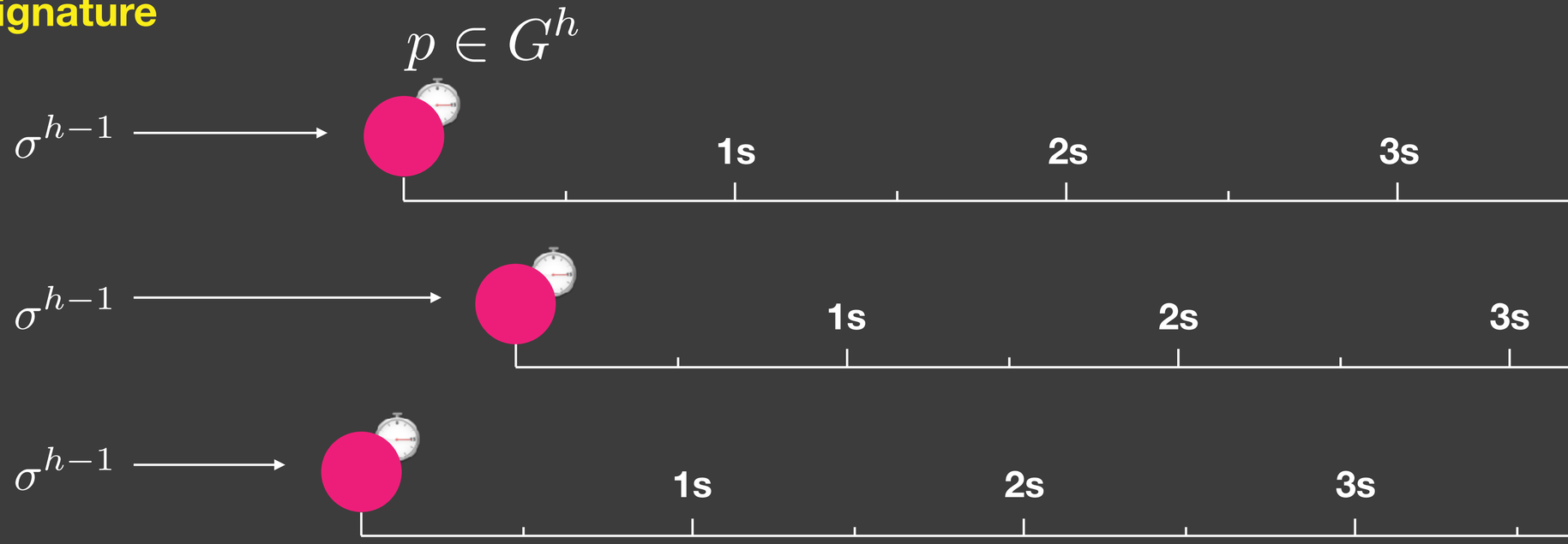
A valid block proposed at *h* must reference a block that was notarized at *h-1*

Thus, blocks must be published in good time or have no chance of notarization

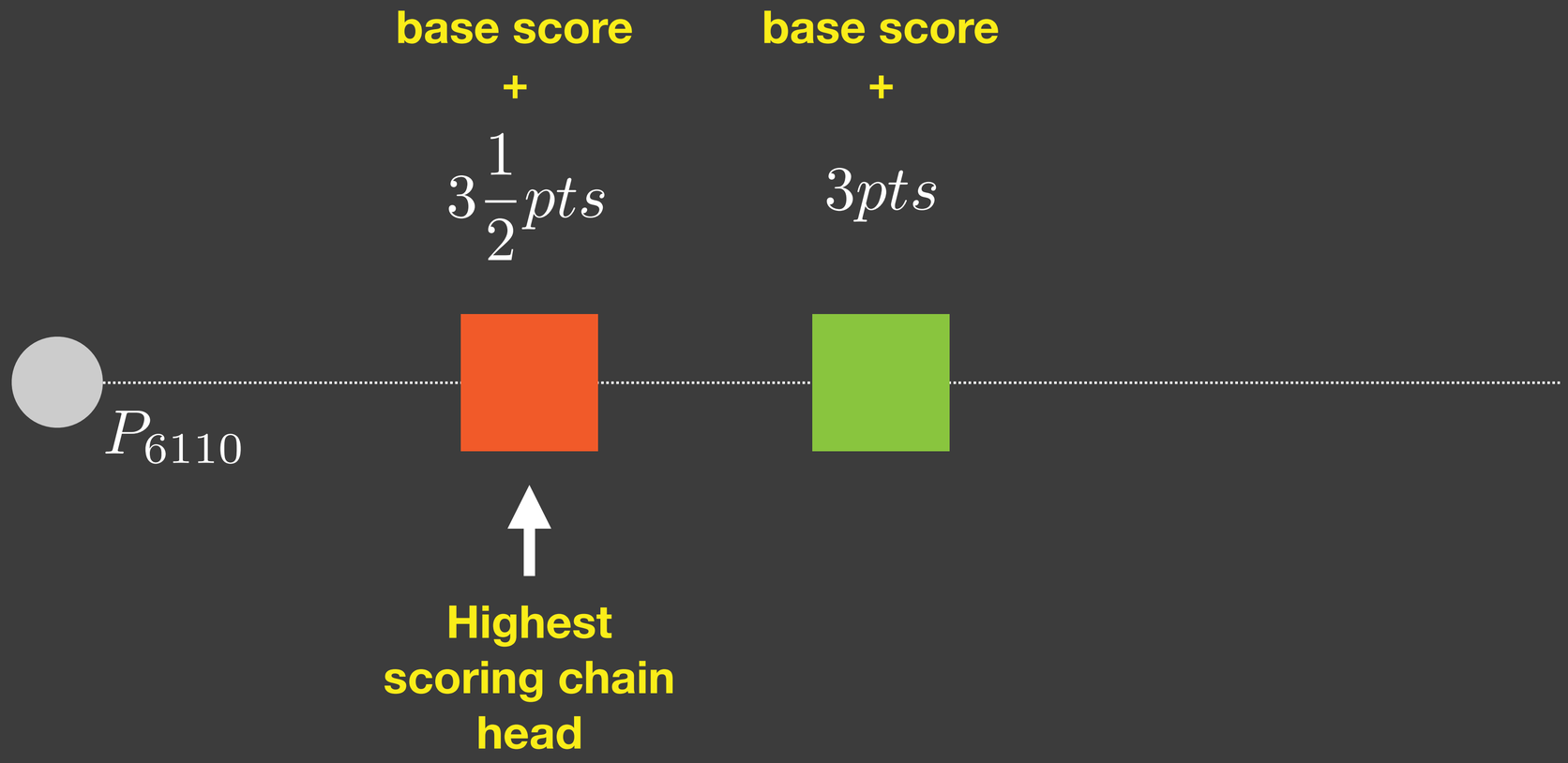
When group selected, its members start their timers...

Triggered by propagation threshold signature

Members start processing blocks after expiry BLOCK_TIME. Clocks will be slightly out-of-sync, but that's OK!

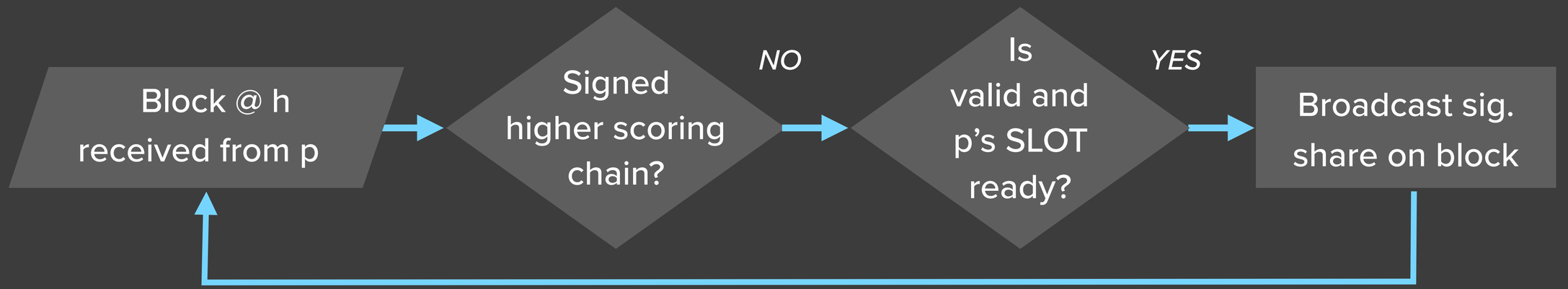


Queue blocks score order while waiting BLOCK_TIME

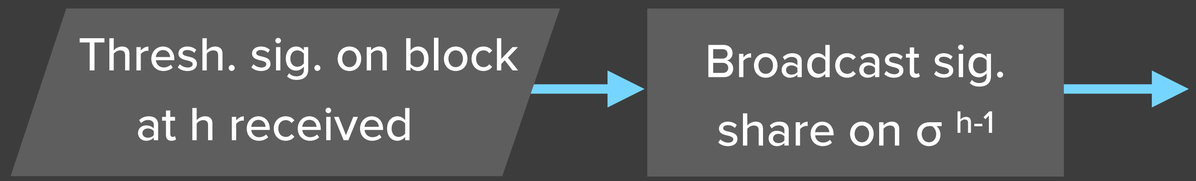


When BLOCK_TIME expires, start notarizing...

Group members sign until ≥1 blocks receive threshold signature

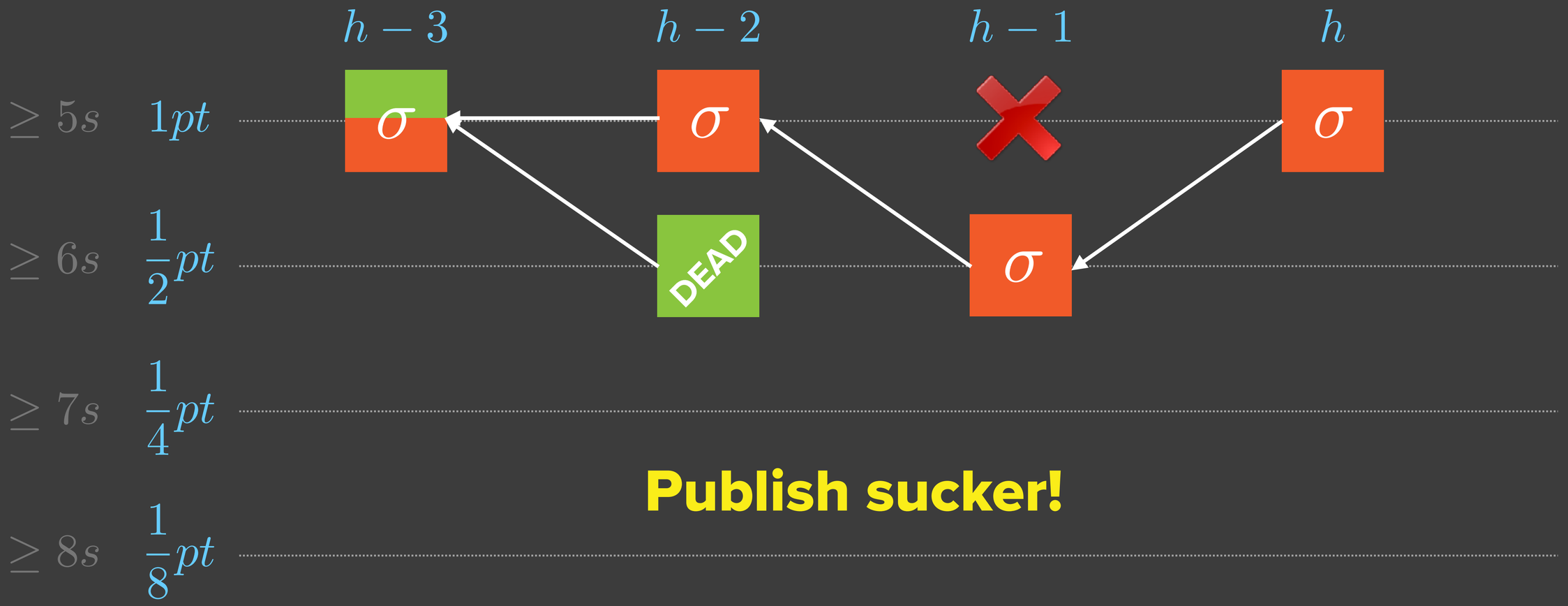


Sign best or equal best blocks



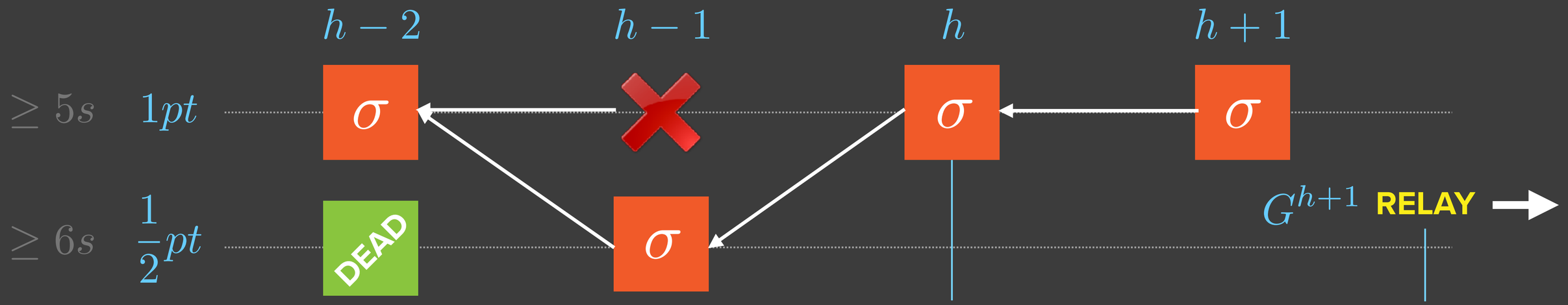
Relay and halt

Fair mining and very fast convergence



Publish sucker!

Optimal case. Overwhelming finality in 2 blocks + relay



No alternative chain head or even partially signed chain head is visible. Yet, for a viable chain head to exist, it must have been shared with some correct processes to collect signatures, and they would have propagated (broadcast) it…

The trap shuts! Now group ***h+1*** has relayed it will not notarize/sign any more blocks. Too late for any alternative chain head at ***h*** to "appear" and get notarized…

Gains from Notarization

Fast Optimal Avg. Finality

$$BLOCK\_TIME = 5s$$

$$\Longrightarrow$$

$$7.5s$$

Addresses Key Challenges

- Selfish Mining
- Nothing At Stake
- Equivocation

Quantifiable risk

Hooks make possible calculate probabilities more meaningfully

SPV

Light client needs only Merkle root of groups

Relative Performance Copper Release

			
Block Time	Average 10 mins *varies wildly*	Average 20 secs *varies wildly*	Average 5 secs *low variance*
“TX finality” (speed)	6 confirmations avg. 1 hr	37 confirmations avg. 10 mins	2 confirmations+relay ***avg. 7.5 secs*** ***Optimal case normal operation***
Gas available	- - -	Low due to Poisson distribution	**50X+ Ethereum** ***Unlimited scale-out achieved by applying randomness in following techniques…***

Miscellanea

Death By Poisson Process

The Simplest Flaws Are The Worst...

50% of Ethereum blocks are empty !

Miners prefer to build on empty blocks

since no need validate/delay

= more profitable

An empty block has more chance being

confirmed....

Duh !

Bitcoin Could Consume as

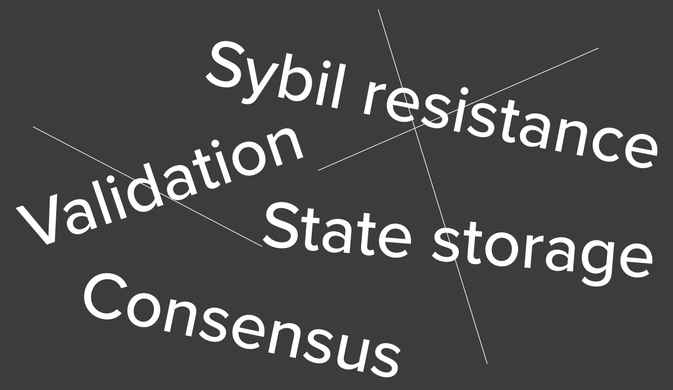
Much Electricity as Denmark

by 2020, Motherboard

3/29/2016

Separate and decouple concerns

Proof-of-Work Blockchain



DFINITY

Consensus

Validation

State storage

Sybil resistance

Computer Science should not go out of fashion

TCP/IP

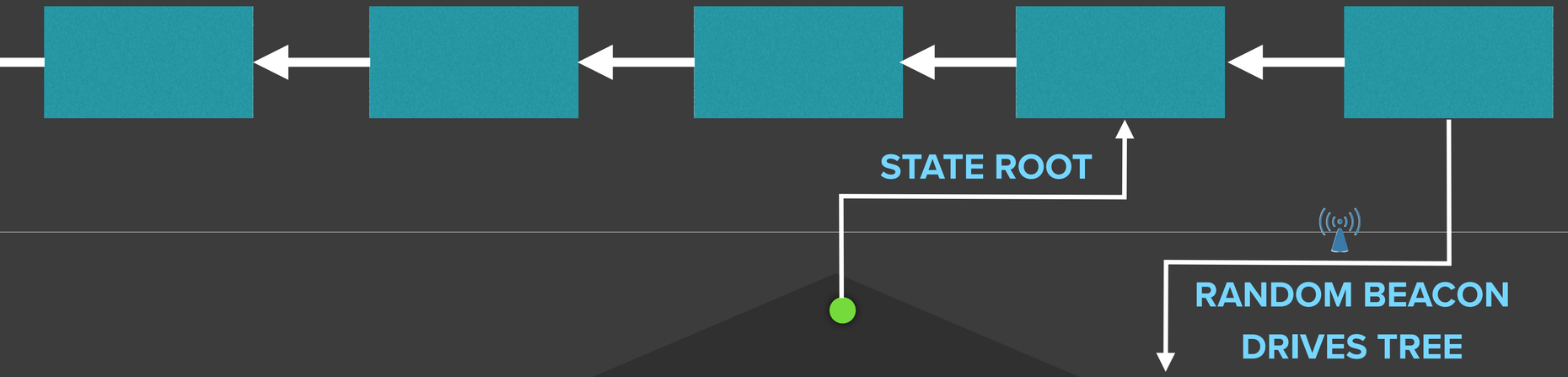
Application

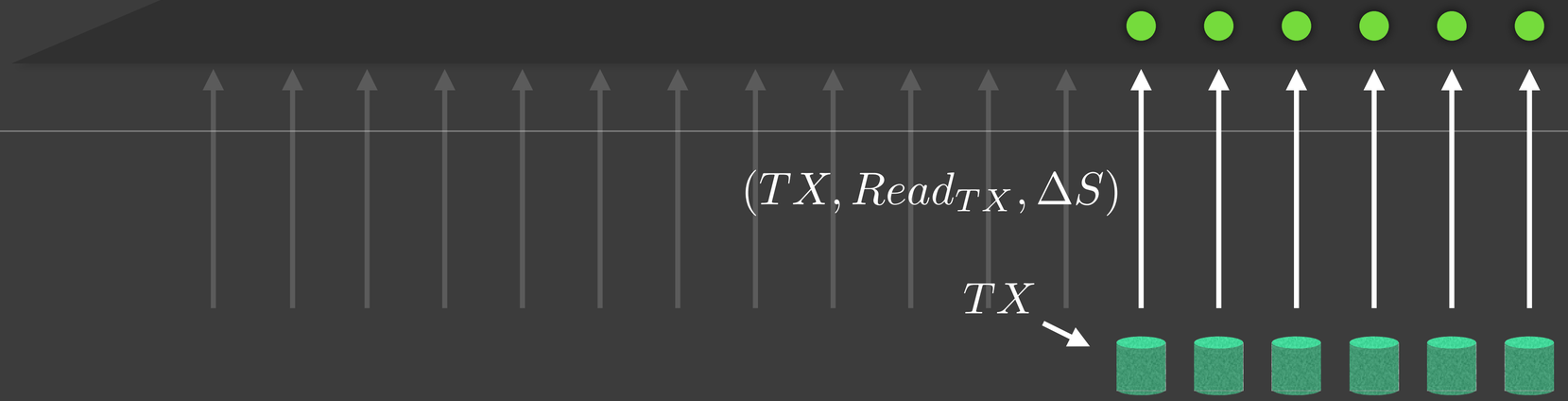
Transport

Internet

Network Access

“Scale-out” using 3-layer architecture





CONSENSUS

Threshold relay chain generates randomness, records network metadata & validation tree “state root”.

VALIDATION

Scalable “Validation Tree” composed “Validation Towers”. Does for validation what Merkle does for data.

STORAGE

State and updates to state stored on shards. State transitions passed to Validation Tree.

Near Term Client Releases

1 COPPER

- Threshold Relay + PSP
- Blockchain Nervous System (BNS)
- Security deposits
- State-root-only-chain (transaction logging not necessary)

2 ZINC

- Special features enabling creation robust *and* high performance private networks using unlimited host computers
- Single *atomic* call from smart contract on private cloud into smart contract on public cloud network

3 TUNGSTEN

- State sharding (basic)
- Validation Towers (basic)
- Asynchronous model for cross-shard programming
- USCIDs (Unique State Copy IDs)
- Advancements in BNS

BLS Implementation

BLS Signature based on optimal Ate-pairing, C++/ASM

Shigeo Mitsunari, https://github.com/herumi/bls

Distributed Key Generation via Joint-Feldman Verifiable Secret Sharing, Go

Timo Hanke [about to be released, follow Twitter @timothanke]

Threshold-Relay Simulator, Go

Timo Hanke [about to be released, follow Twitter @timothanke]

President/CTO String Labs

President/Chief Scientist DFINITY Stiftung

http:// twitter.com /dominic_williams

http:// linkedin.com /in/thedwilliams/

Decentralized Commercial Banking