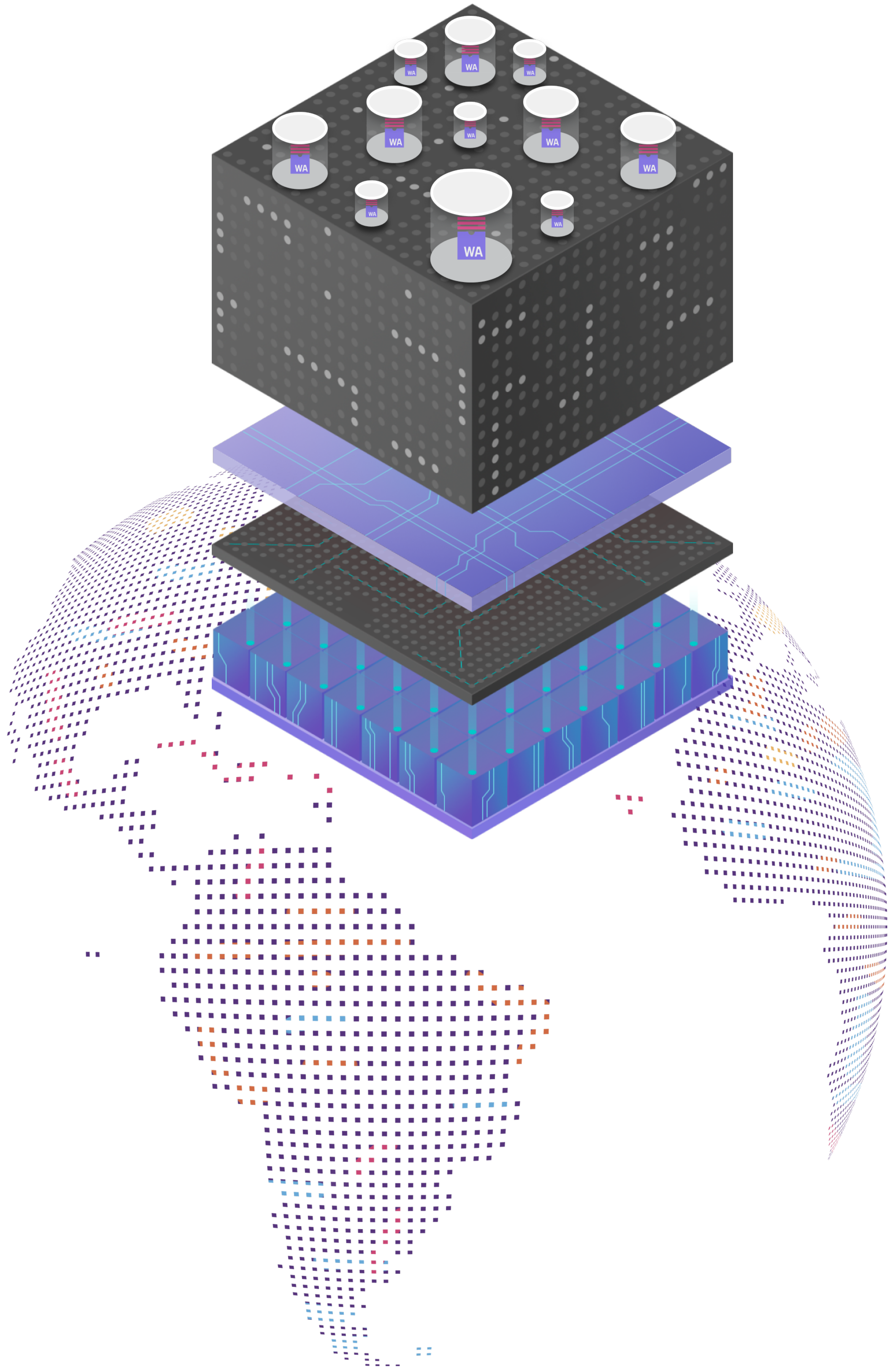
DFINITY

The Internet Computer
An Overview

Yvonne Anne Pignolet (yvonneanne@dfinity.org)
Thomas Locher (thomas.locher@dfinity.org)

Outline

- What is the Internet Computer?
- Consensus on the Internet Computer
- The Internet Computer Today



What is the Internet Computer?

What is the Internet Computer?

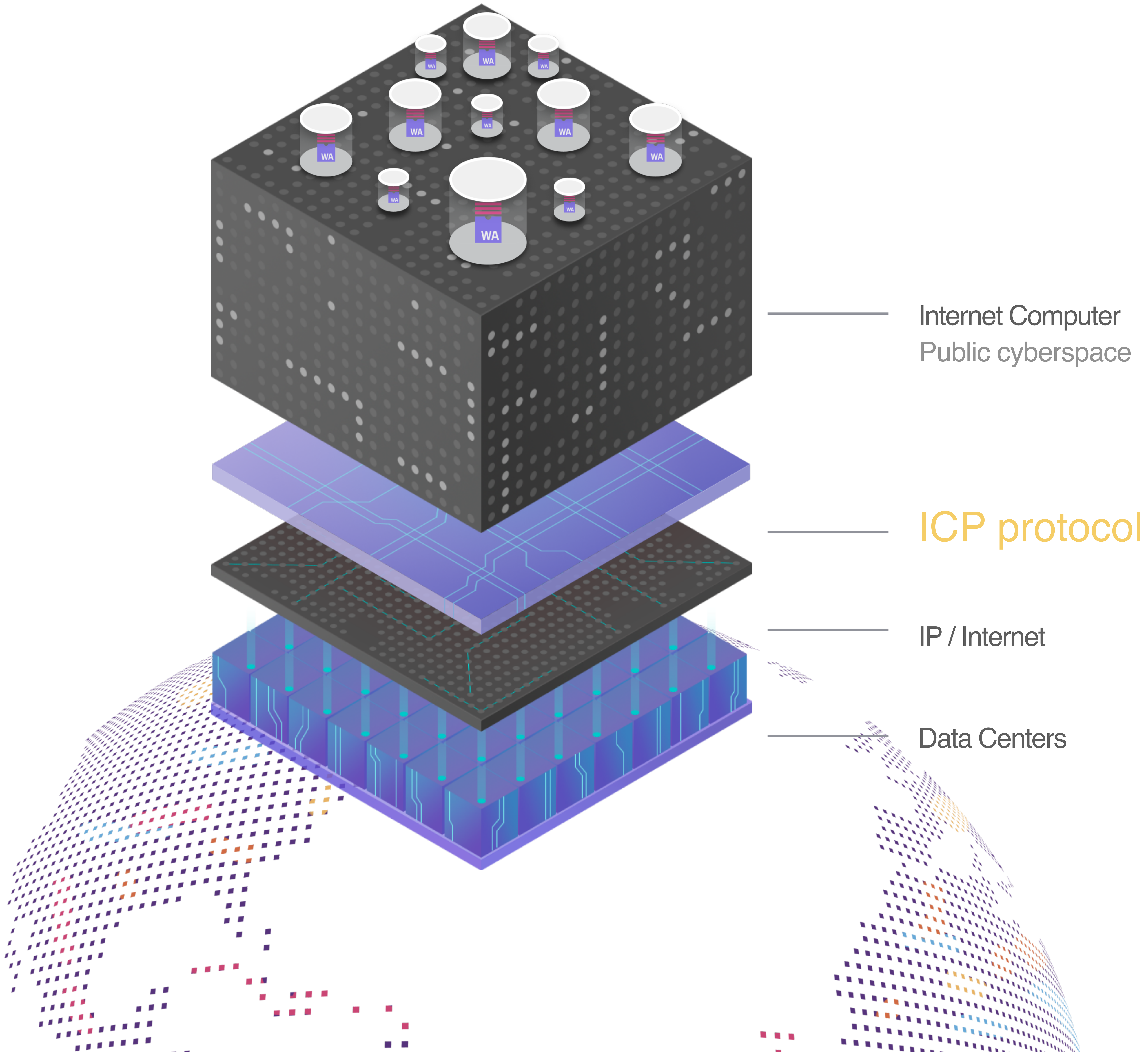
Platform to run any computation, using blockchain technology for decentralisation and security

Internet Computer Protocol (ICP)

Coordination of nodes in independent datacenters, jointly performing any computation for anyone

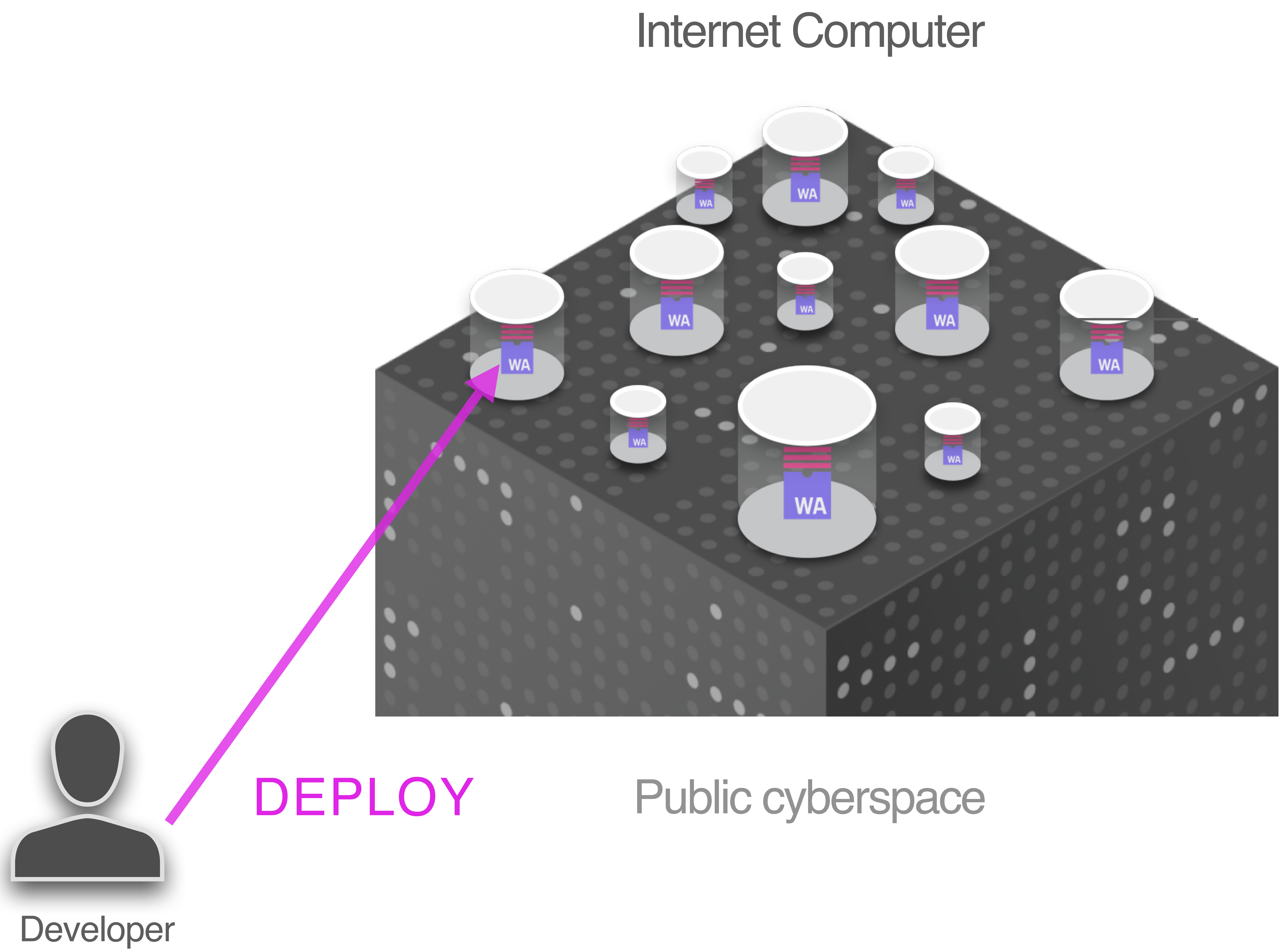
ICP creates the
Internet Computer blockchains

Guarantees safety and liveness of smart contract execution despite Byzantine participants

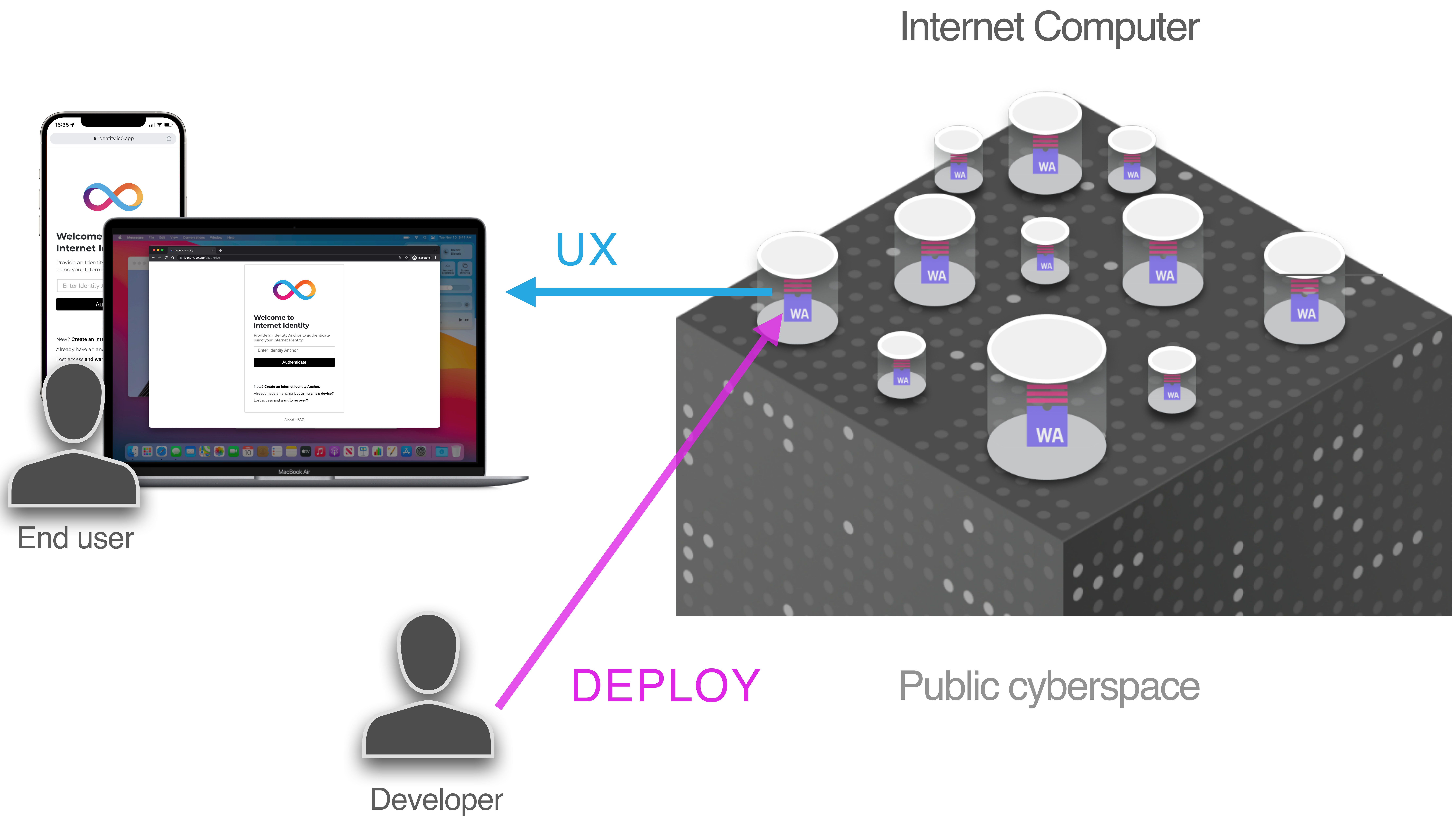


Canister Smart Contracts: Combination of Data and Code

Developers and users interact directly with Canisters on the IC



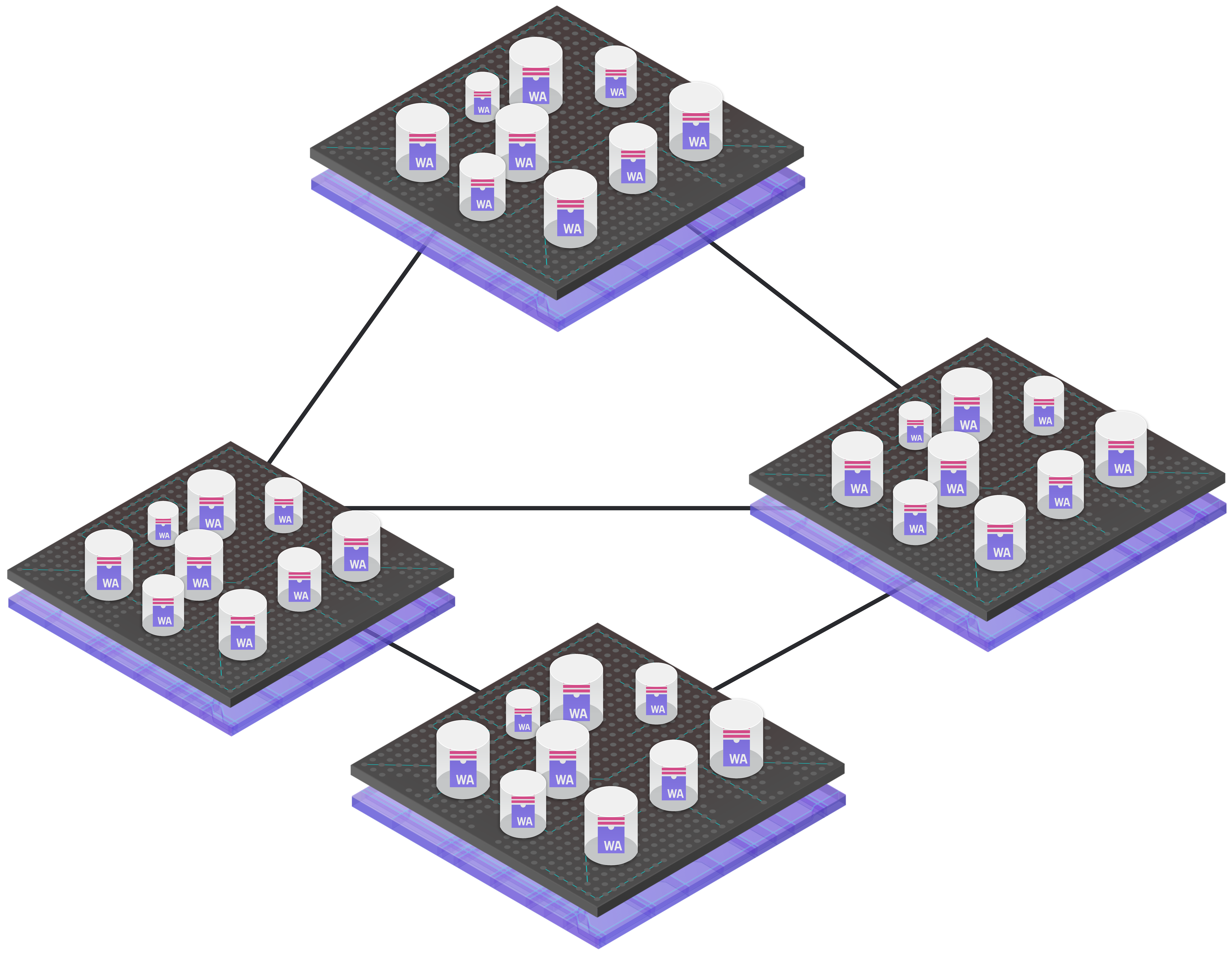
Developers and users interact directly with Canisters on the IC



Scalability: Nodes and Subnets

Nodes are partitioned into **subnets**

Canister smart contracts are assigned to different subnets



Scalability: Nodes and Subnets

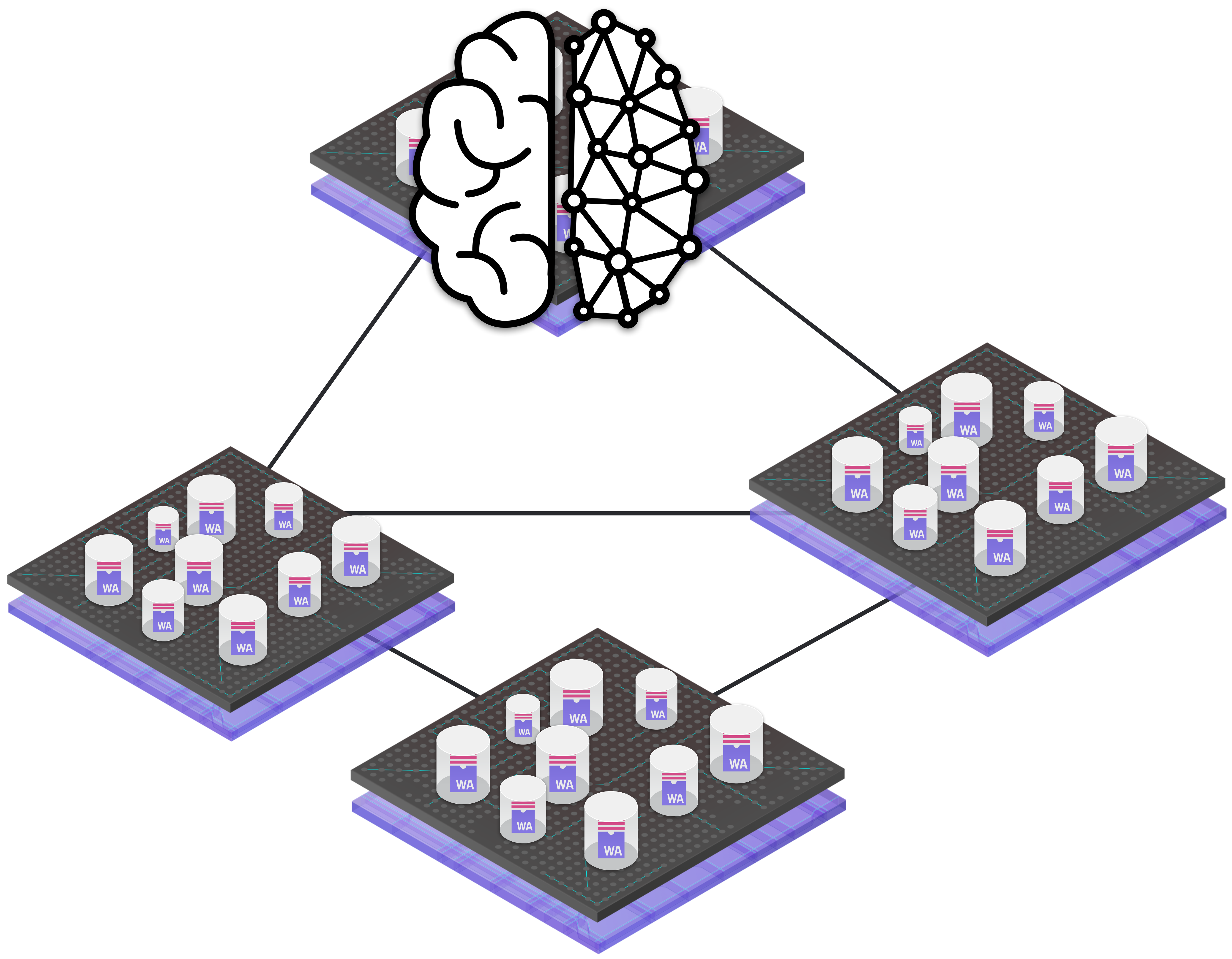
Nodes are partitioned into **subnets**

Canister smart contracts are assigned to different subnets

One subnet is special: it host the **Network Nervous System (NNS)** canisters which govern the IC

ICP token holders vote on

- Creation of new subnets
- Upgrades to new protocol version
- Replacement of nodes
- …

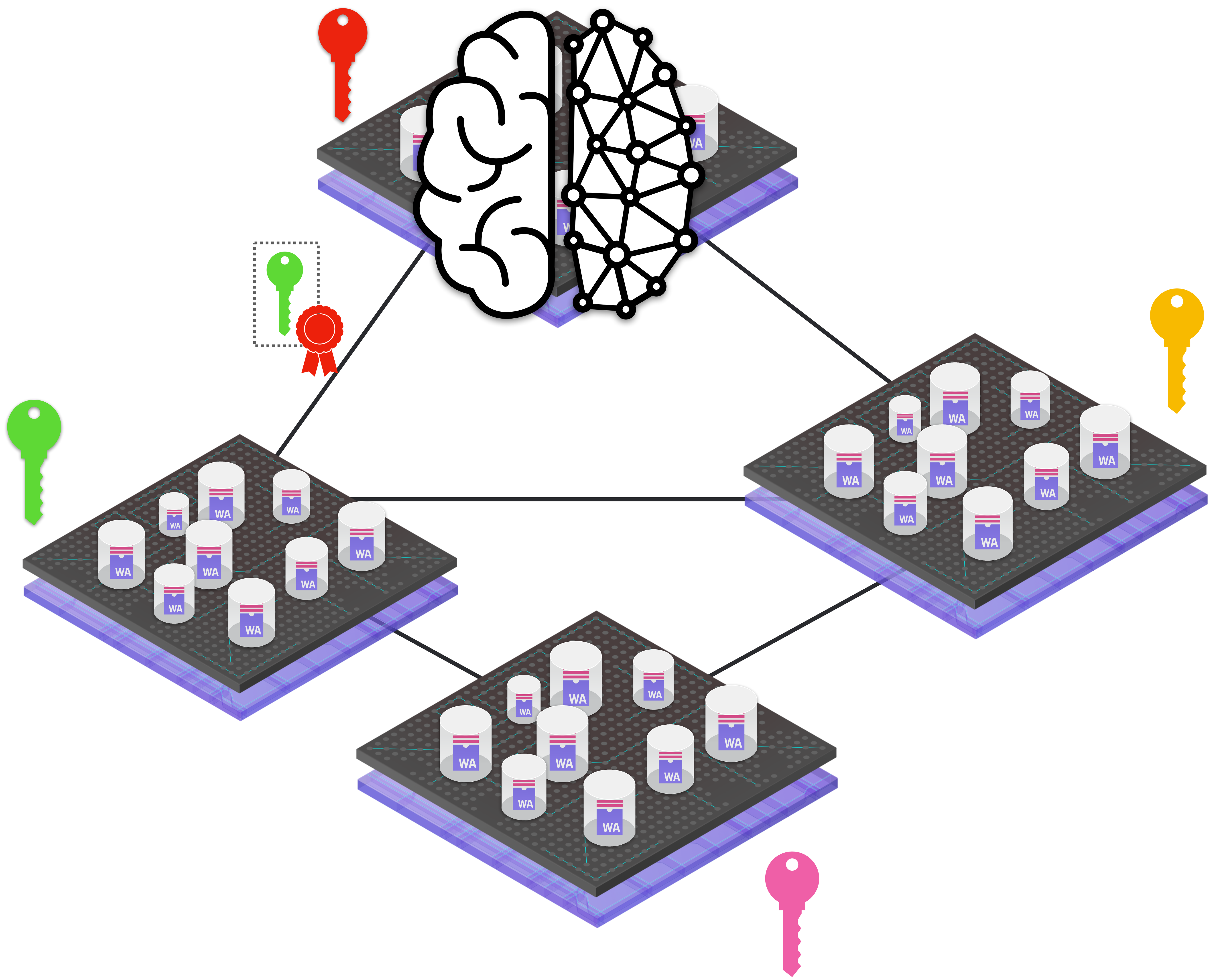


Chain Key Technology

- Public key of NNS never changes, nodes in NNS share private key

- NNS generates key of subnets and certifies them

- Node in subnets use these keys to secure communication



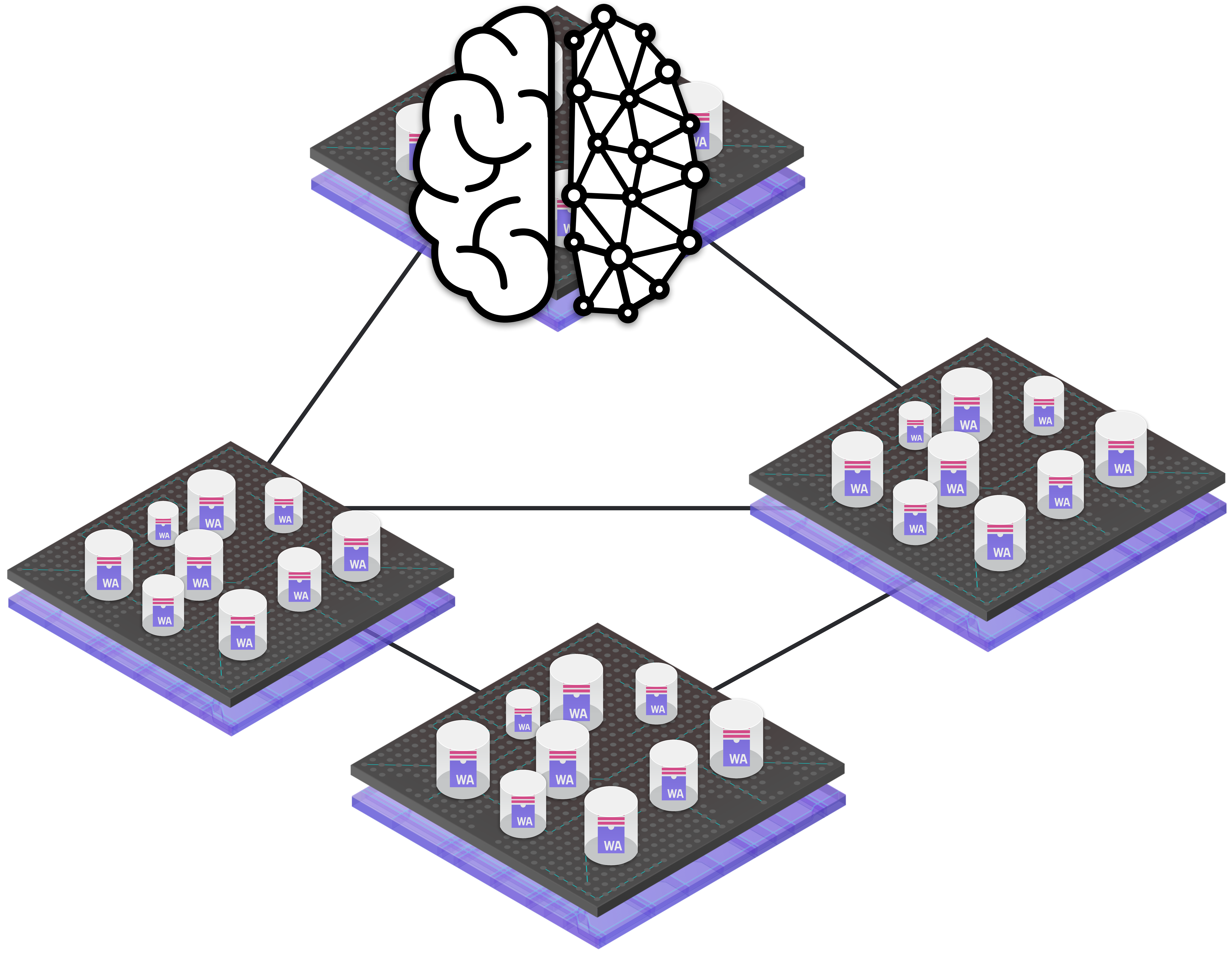
Each Subnet is a Replicated State Machine

State:
- canisters and their queues

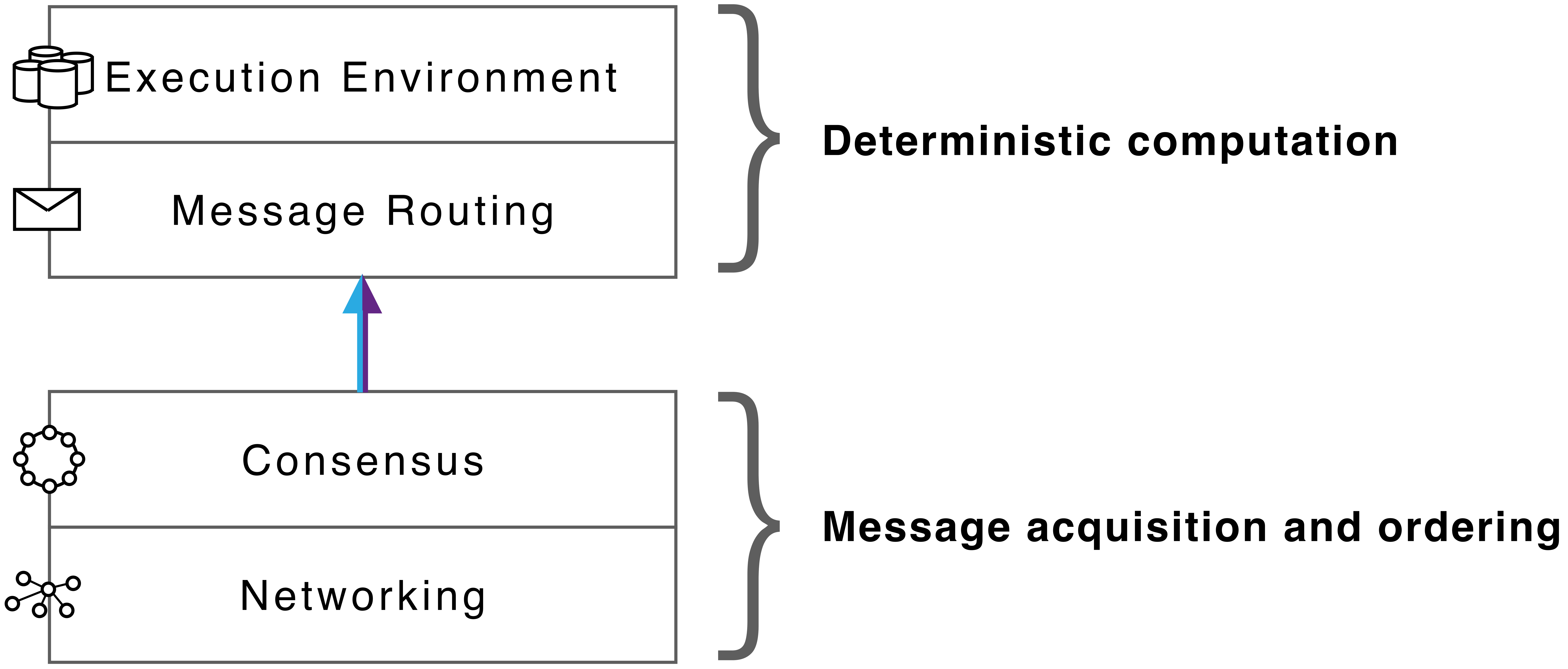
Inputs:
- new canisters to be installed,
- messages from users and other canisters

Outputs:
- responses to users and other canisters

Transition function:
- message routing and scheduling
- canister code

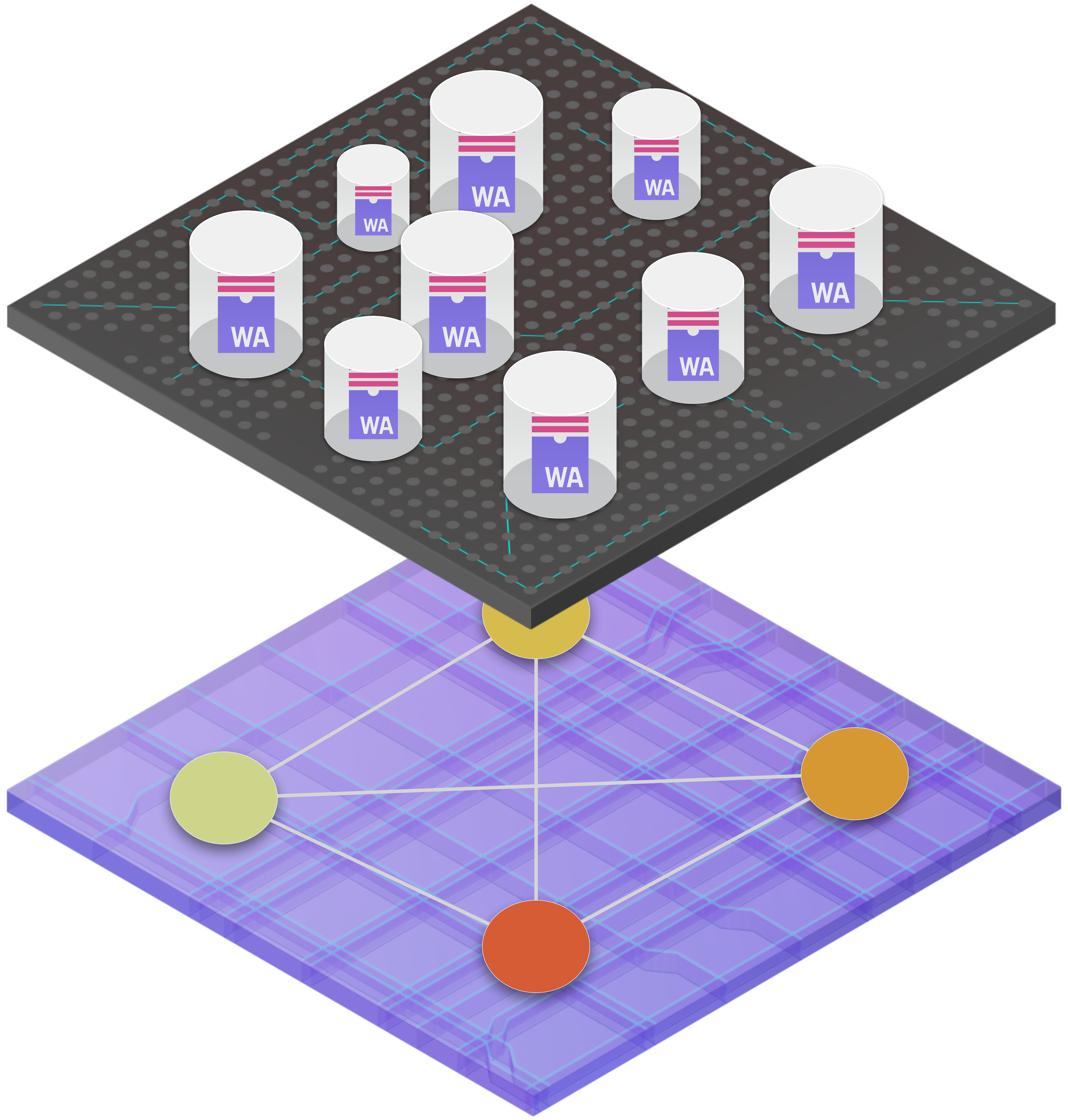


The Layers of the Internet Computer Protocol



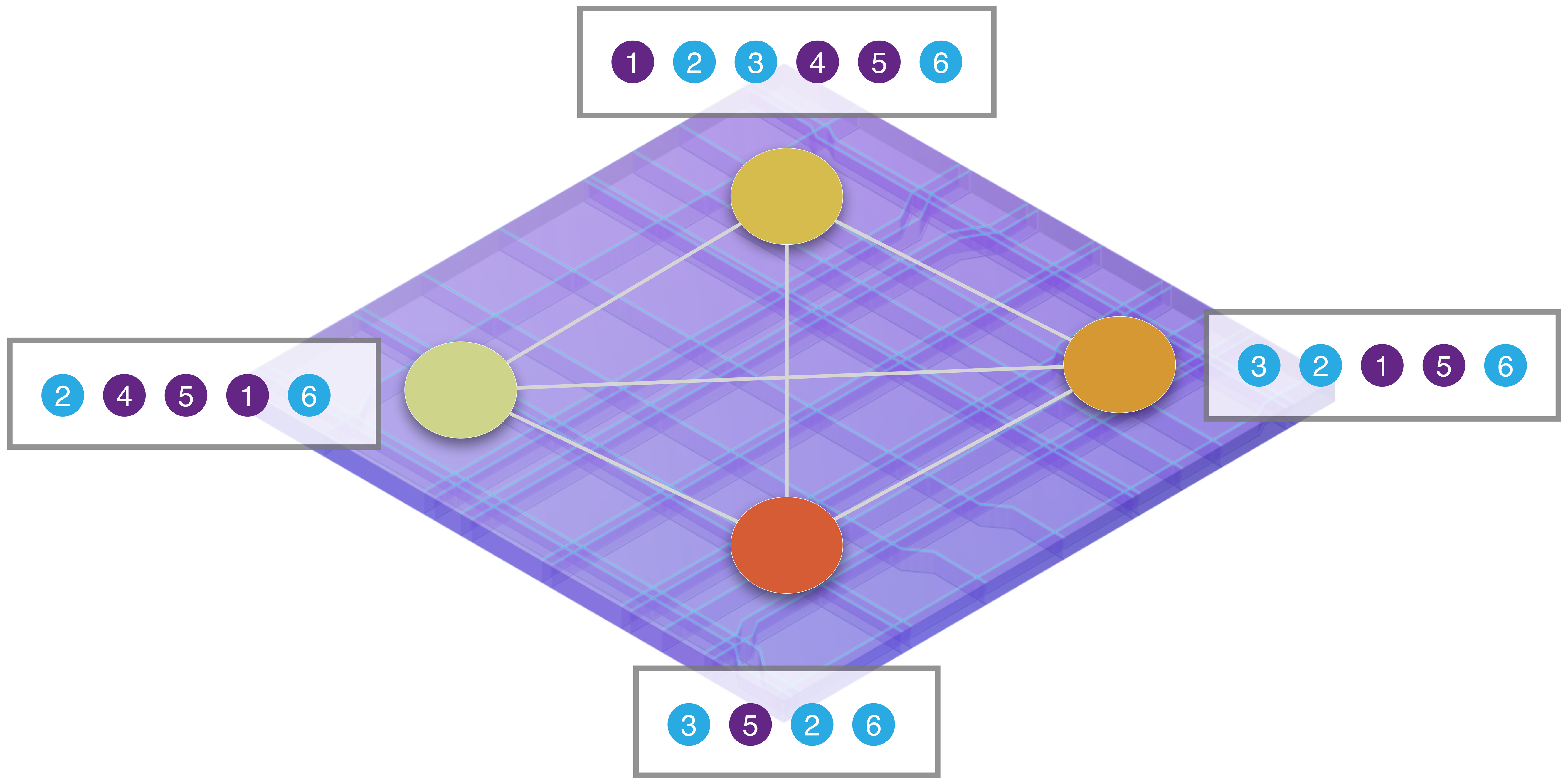
Consensus on the Internet Computer

Consensus Orders Messages



Consensus Orders Messages

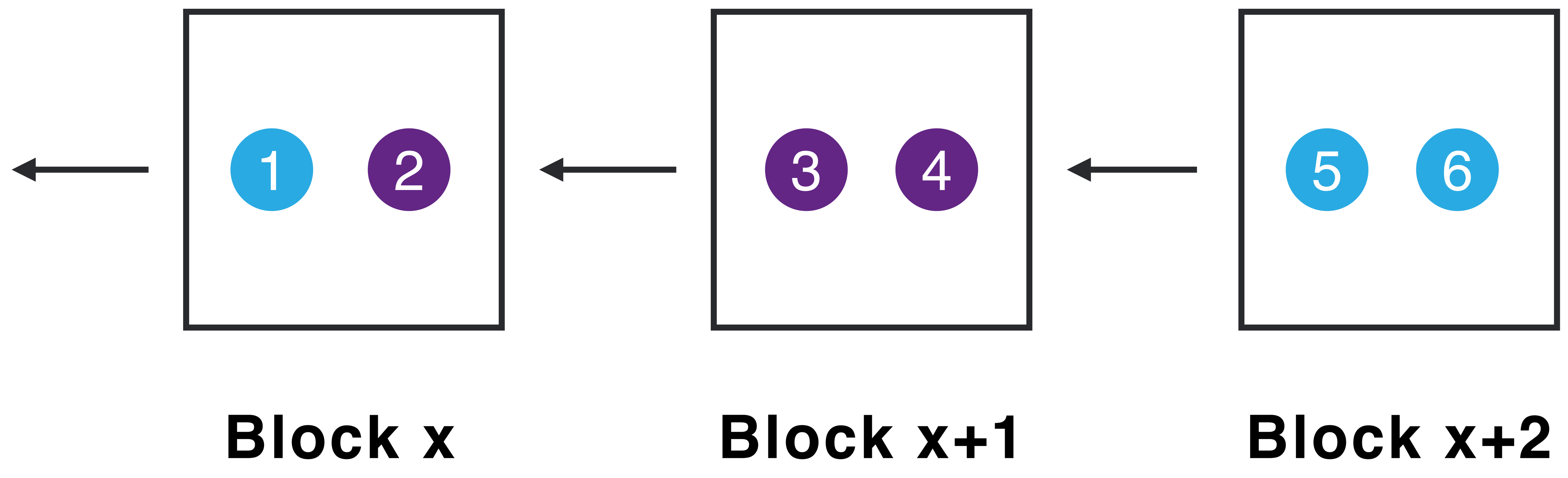
● Message (user → canister) ● Message (canister → canister)



Replicas may receive input messages in different orders, but must process them in the same order, for example 1 2 3 4 5 6

Consensus Properties

Messages are placed in **blocks**. We reach agreement using a blockchain.

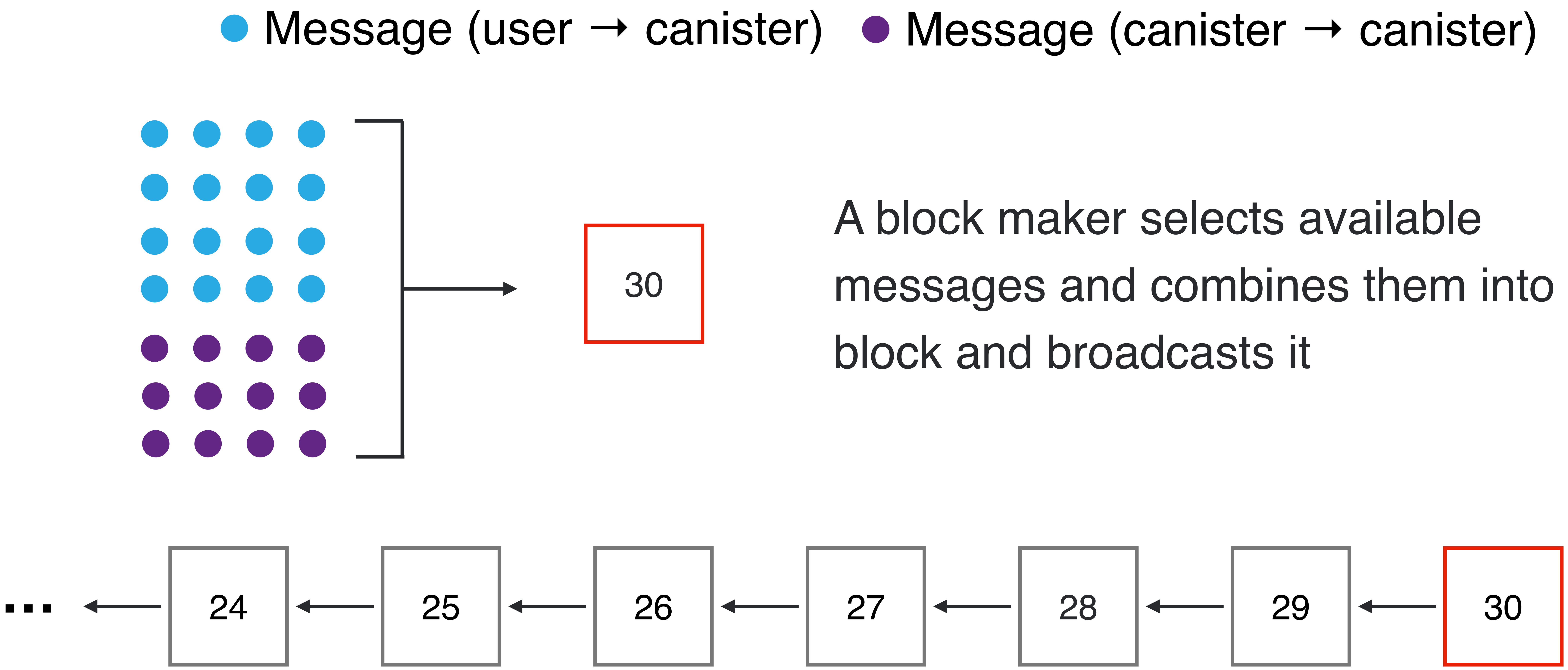


We use ***n*** **= 4,** ***f*** **= 1** in examples

The following properties must hold even if up to $f < n/3$ nodes misbehave

- **Safety**: For any *i*, If two (honest) replicas think that the *i*-th block is agreed upon, they must have the same block
- **Liveness**: For any *i*, at some point every (honest) replica will think that the *i*-th block is agreed upon
- **Validity**: all agreed upon blocks are valid

Block Maker



A block maker selects available messages and combines them into a block and broadcasts it

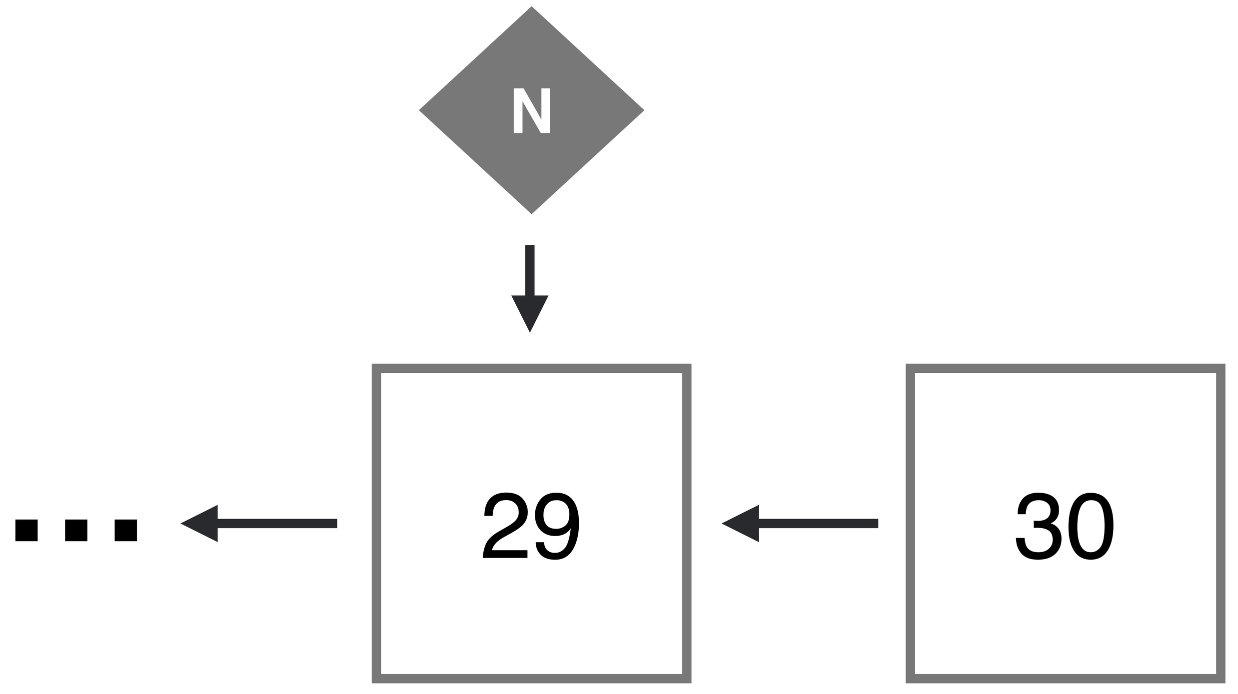
Note: We need more than one block maker in each round, otherwise the IC would not be fault tolerant!

Notarization

The notarization process ensures that a *valid* block proposal is published for every round

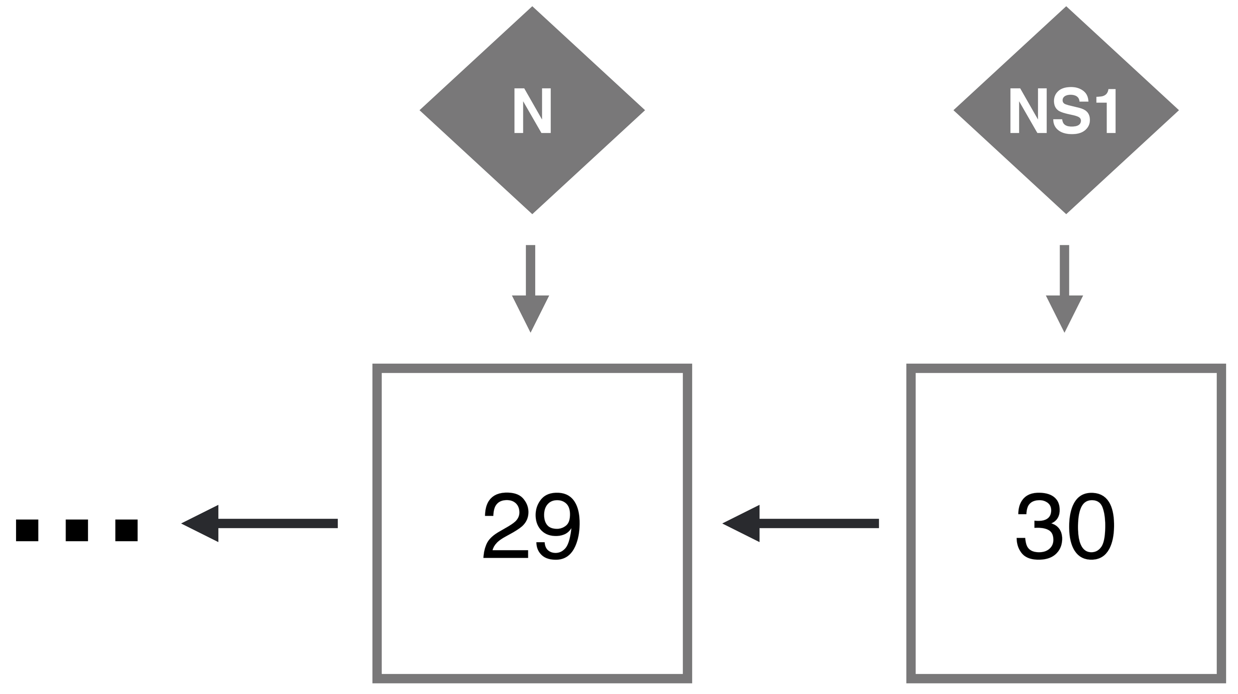
Step 1

Replica 1 receives a block proposal for height 30, building on some notarized height 29 block



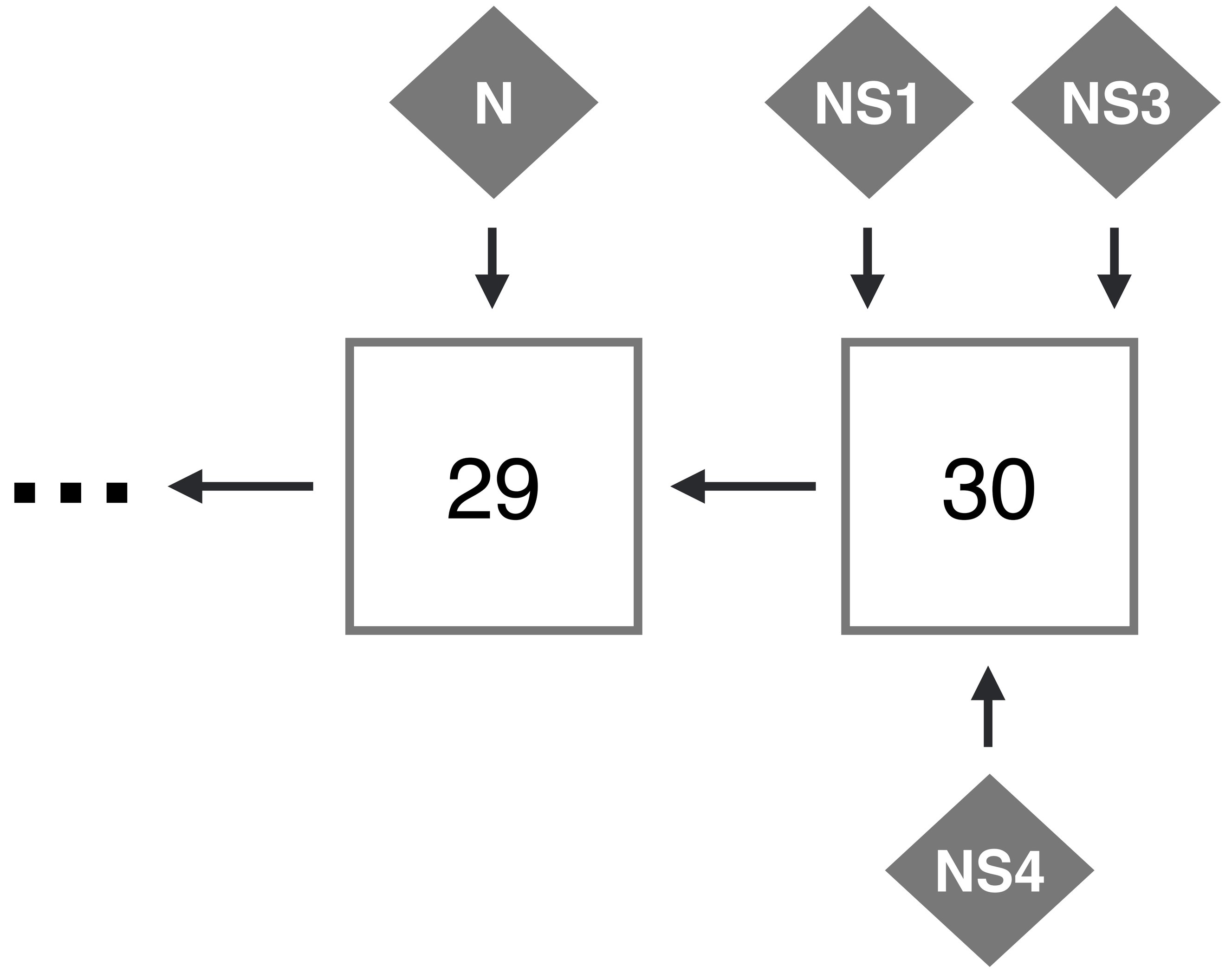
Step 2

Replica 1 sees that the block is valid, signs it, and broadcasts its *notarization* share



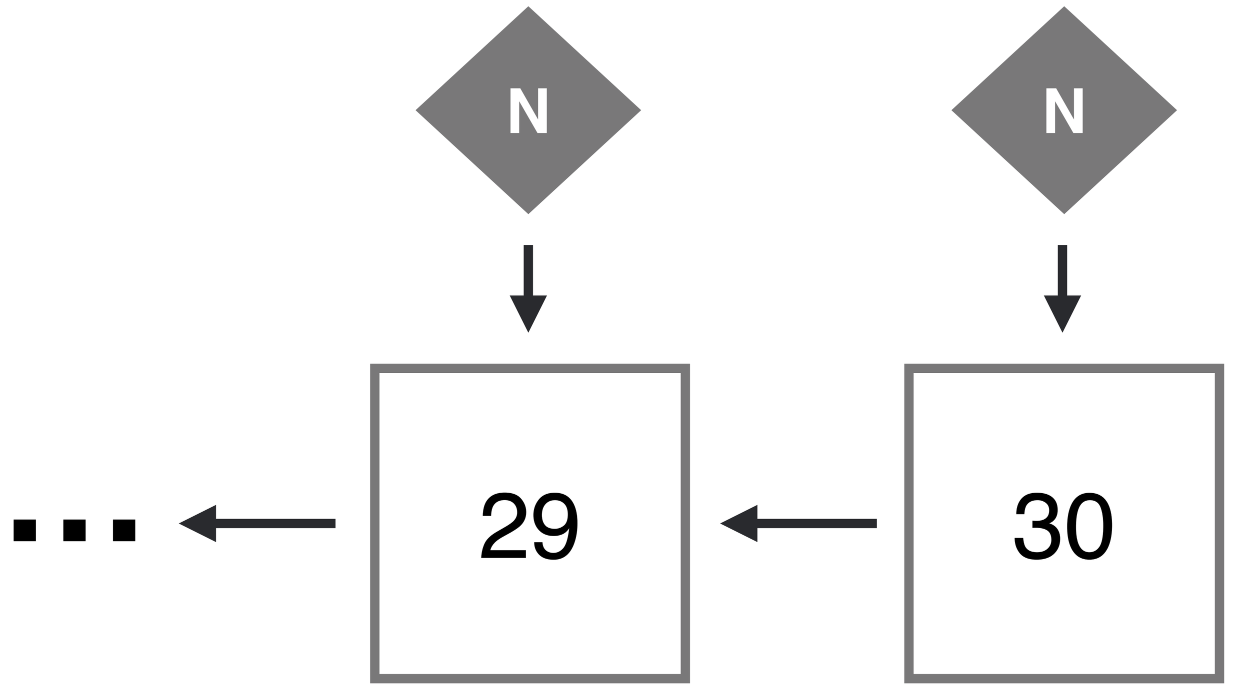
Step 3

Replica 1 sees that replicas 3 and 4 also published their notarization shares on the block



Step 4

3 notarization shares are sufficient approval: the shares are aggregated into a single full notarization. Block 30 is now notarized, and notaries wait for height 31 blocks

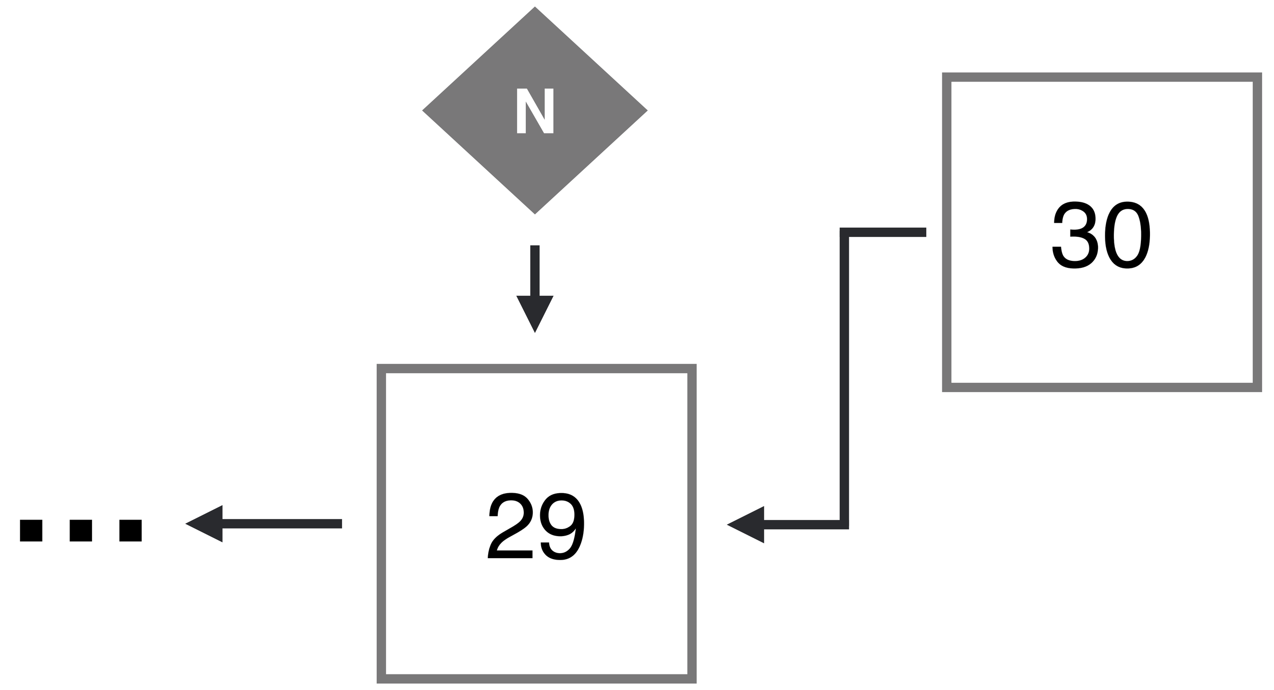


Notarization

Replicas may notary-sign multiple blocks to ensure that at least one block becomes fully notarized

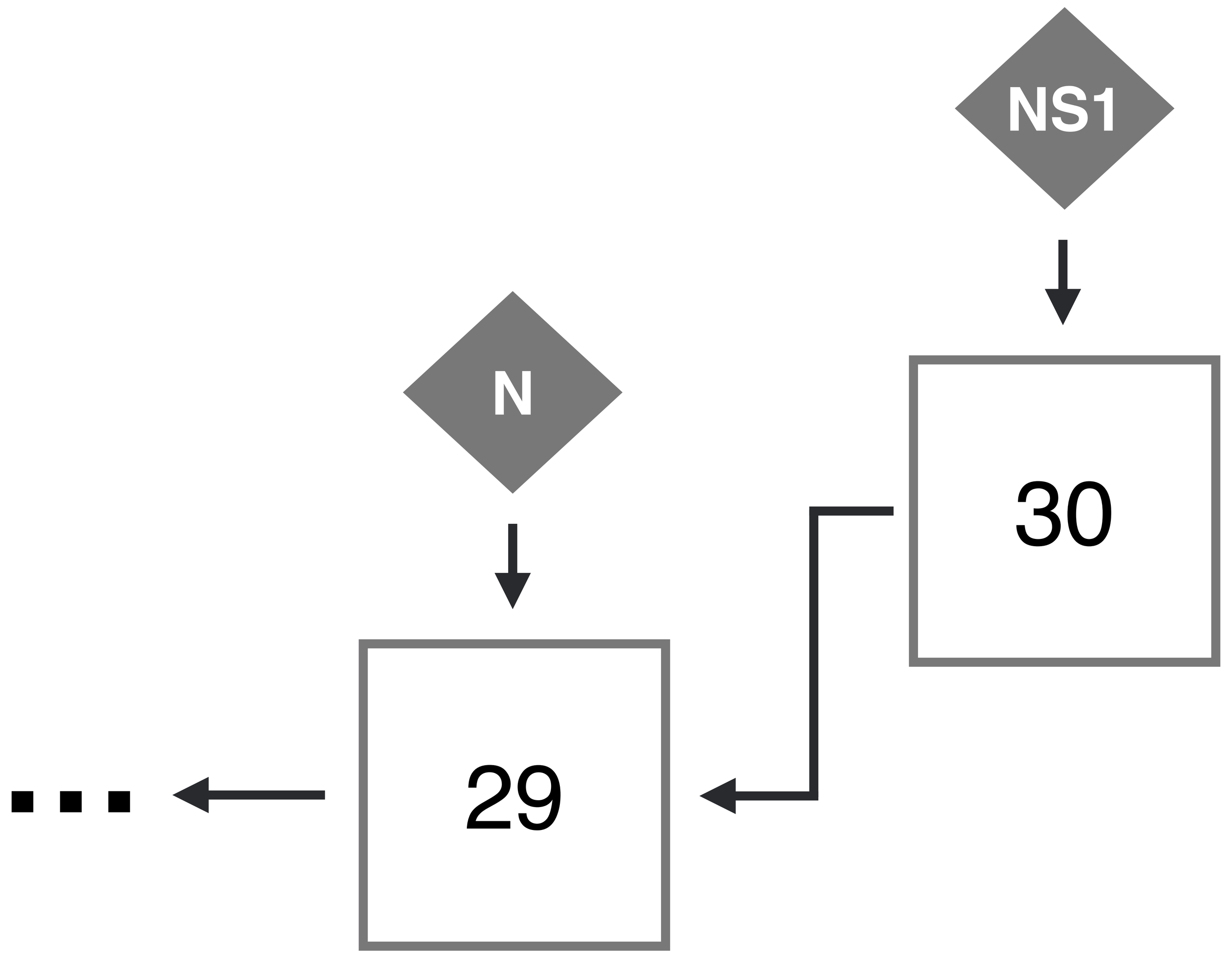
Step 1

Replica 1 receives a block proposal for height 30, building on some notarized height 29 block



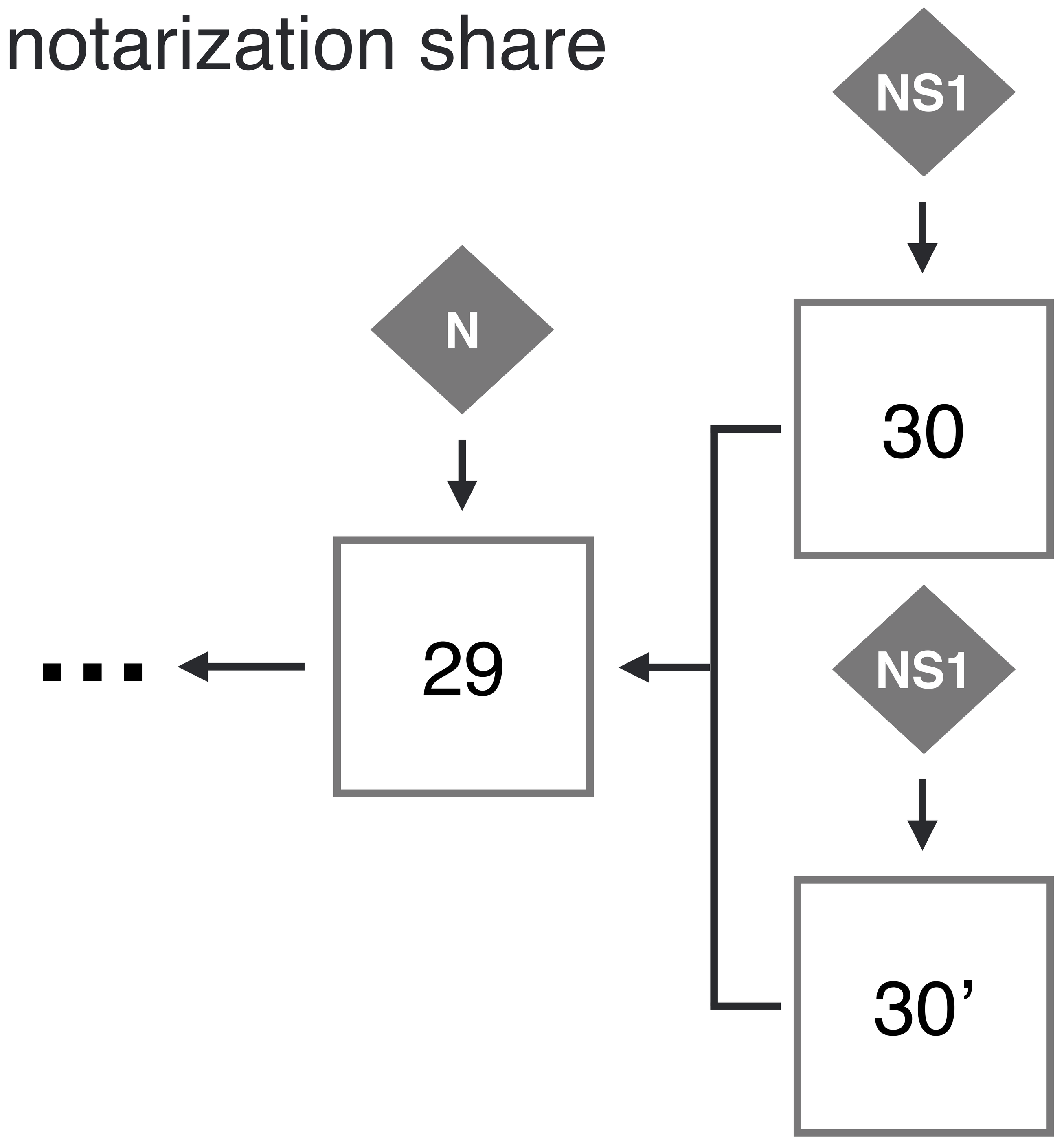
Step 2

Replica 1 sees that the block is valid, signs it, and broadcasts its *notarization* share



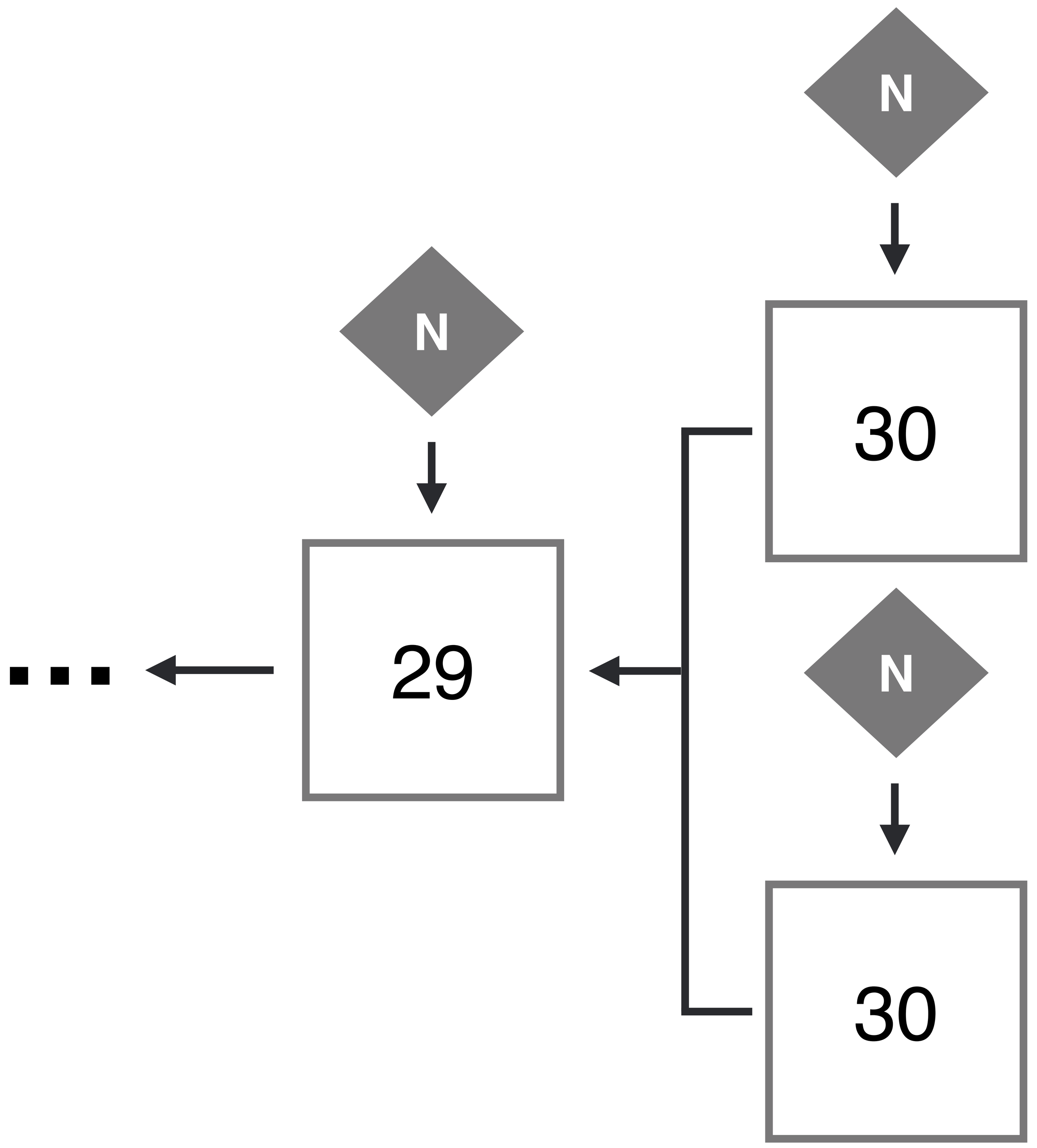
Step 3

Replicas 1 sees another height 30 block, which is also valid, and it broadcasts another notarization share



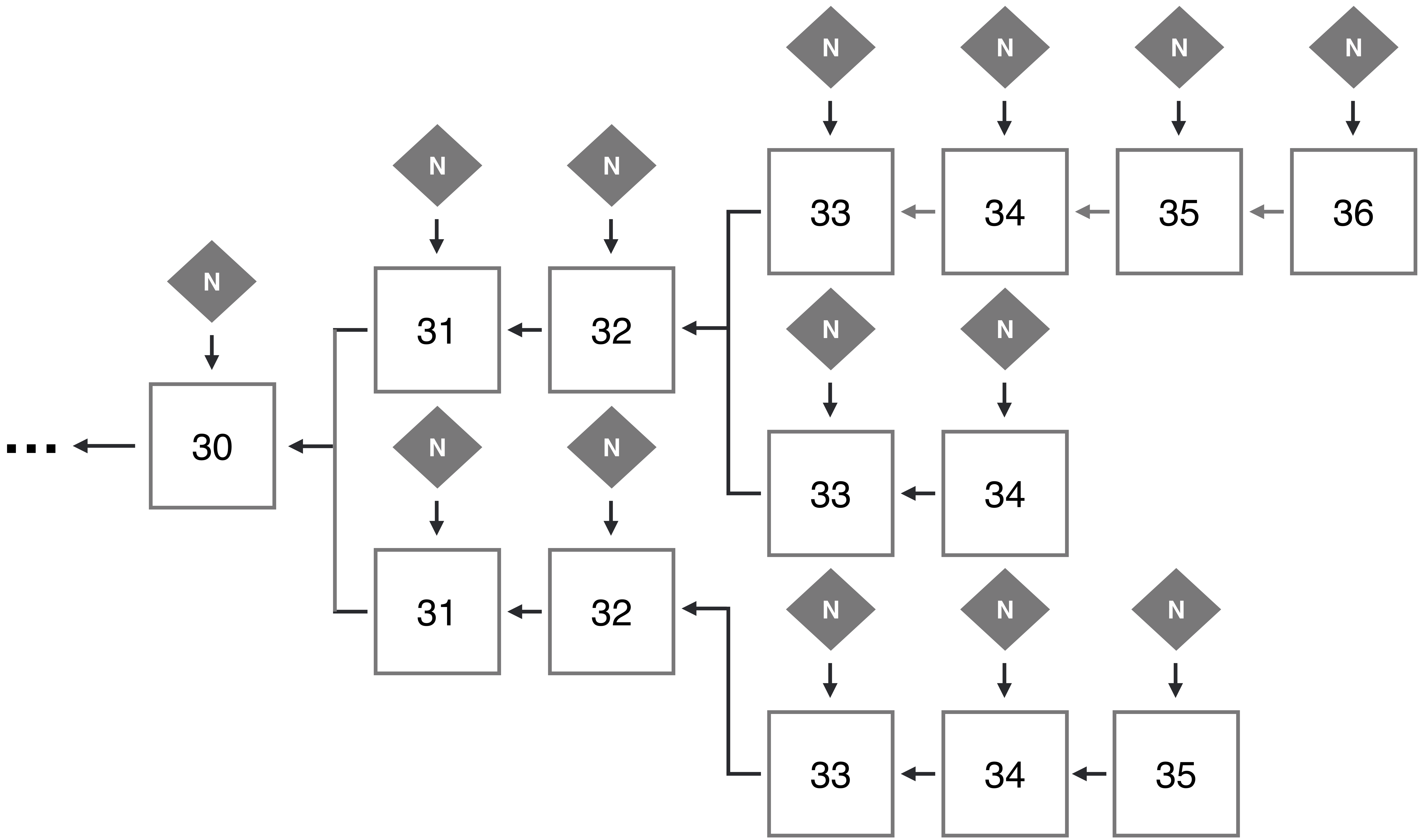
Step 4

Both height 30 blocks get enough support to become notarized



Notarization

Multiple notarized blocks may exist at the same height



Random Beacon

At every height, there is a Random Beacon, an unpredictable random value shared by the replicas

Step 1

Replica 1 has Random Beacon 29 and wants to help constructing Random Beacon 30

Step 2

Replica 1 signs RB29 using a threshold signature scheme, yielding a share of random beacon 30

Step 3

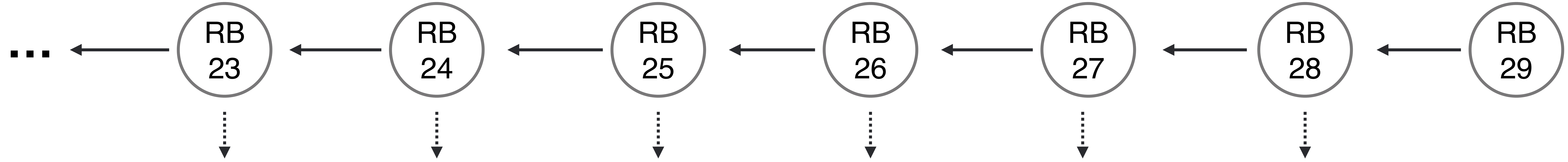
Replicas 1 sees that replica 2 also published a share of Random Beacon 30

Step 4

2 random beacon shares are sufficient to reconstruct a full threshold signature, which is Random Beacon 30

Block Maker Ranking

The Random Beacon is used to rank block makers



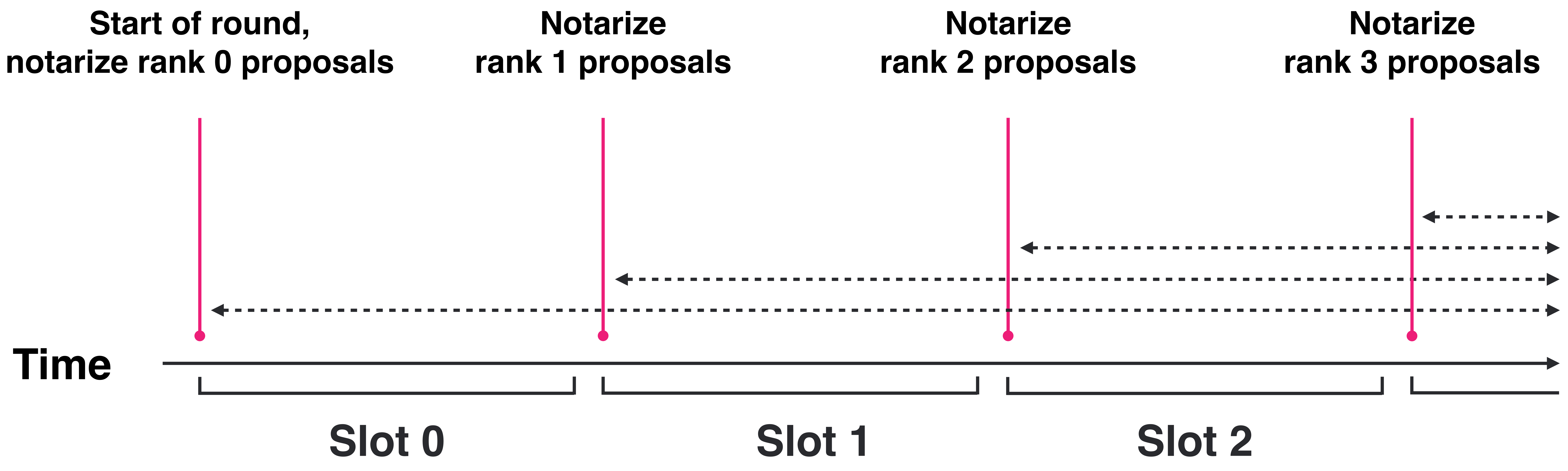
High Priority

	Round 24	Round 25	Round 26	Round 27	Round 28	Round 29
Rank 0	Replica 1	Replica 4	Replica 2	Replica 3	Replica 4	Replica 2
Rank 1	Replica 4	Replica 3	Replica 3	Replica 1	Replica 2	Replica 1
Rank 2	Replica 3	Replica 1	Replica 4	Replica 4	Replica 1	Replica 3
Rank 3	Replica 2	Replica 2	Replica 1	Replica 2	Replica 3	Replica 4

Low Priority

Notarization with Block Maker Ranking

Rounds are divided into time slots defining when block maker proposals are considered

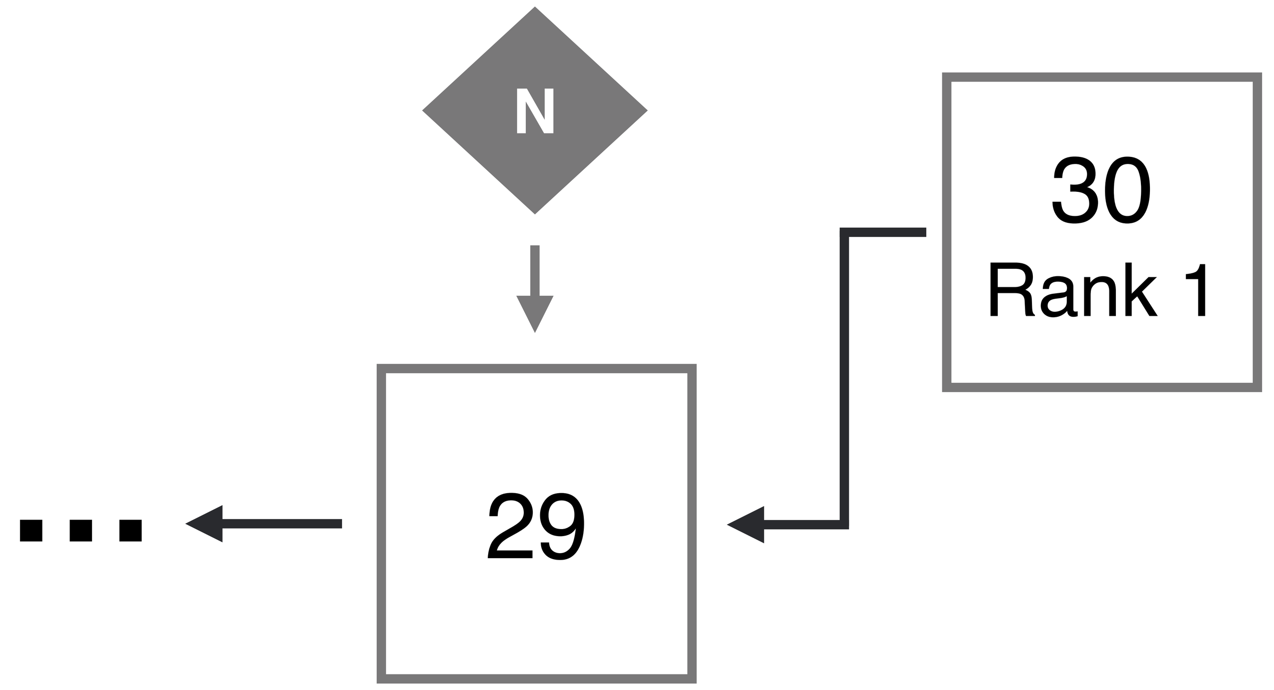


Notarization with Block Maker Ranking

The block ranks can reduce the number of notarized blocks

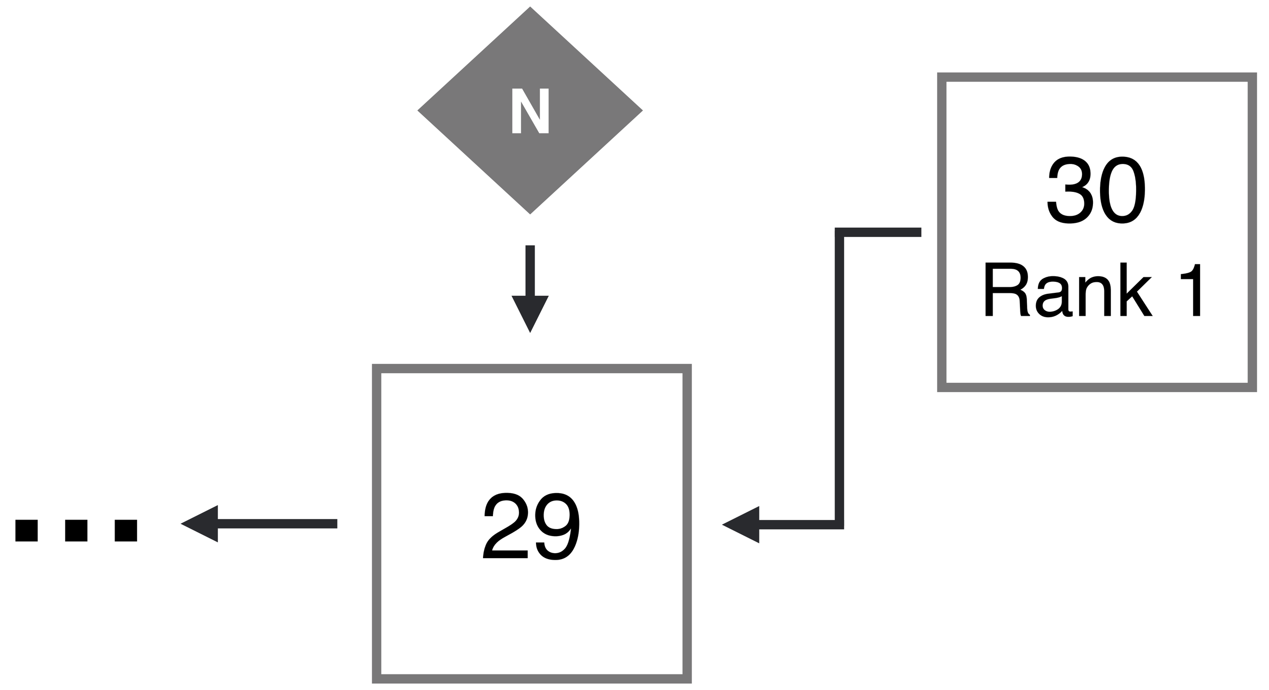
Step 1

Replica 1 receives a rank-1 block proposal for height 30, building on some notarized height 29 block



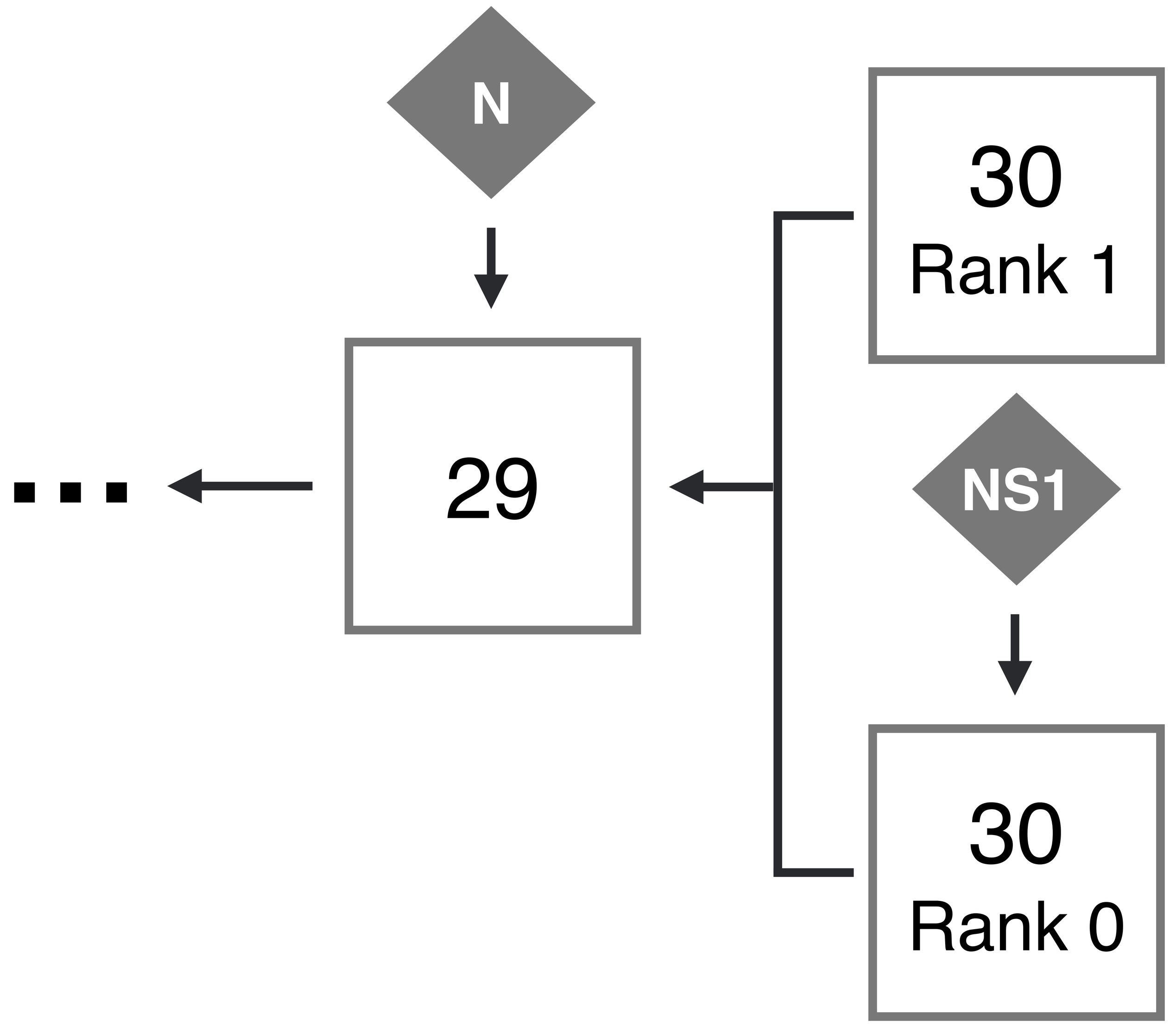
Step 2

Replica 1 is still in time slot 0, so not willing to notary-sign a rank-1 block yet



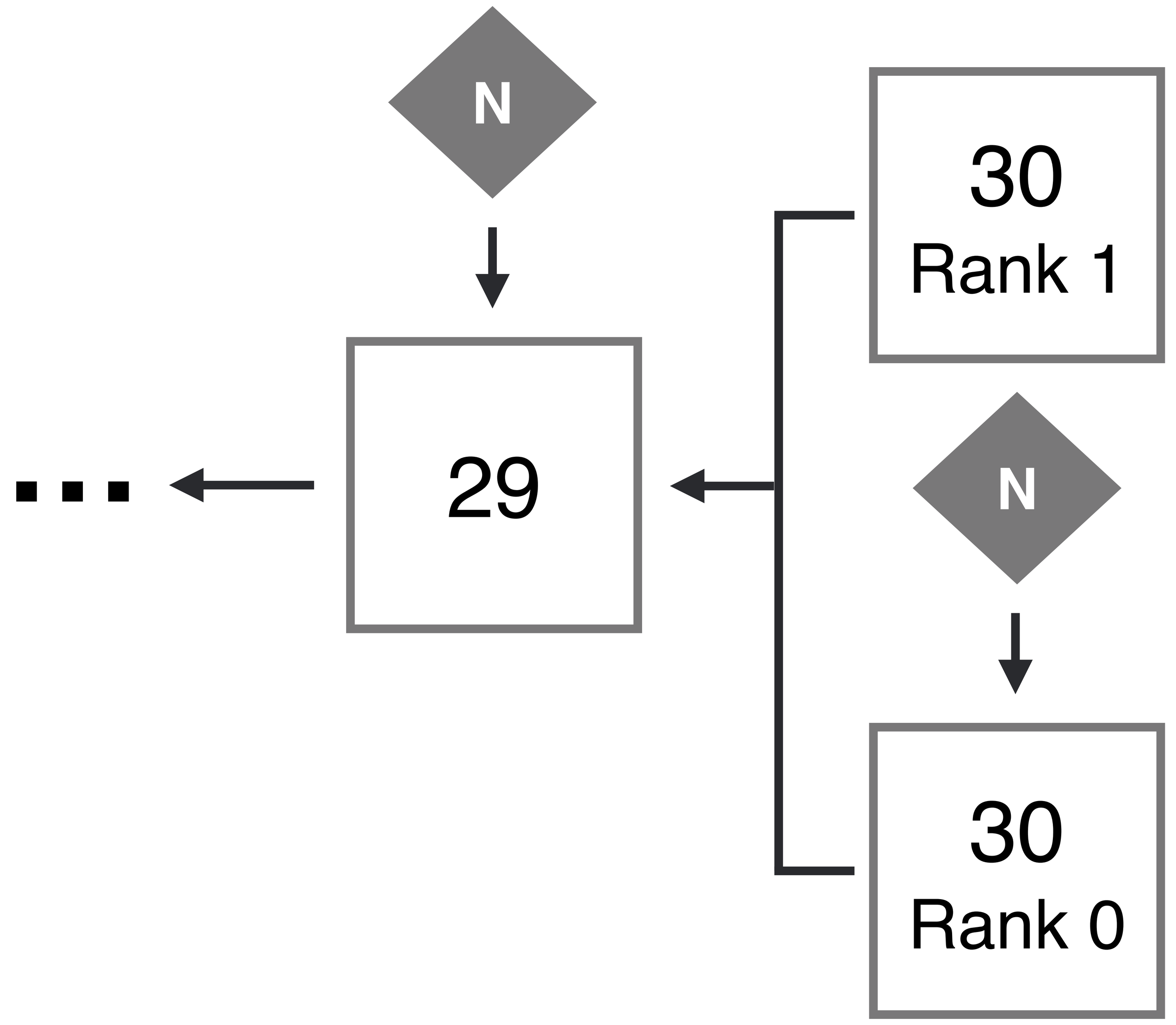
Step 3

Replicas 1 sees a valid rank-0 height 30 block, and it broadcasts a notarization share



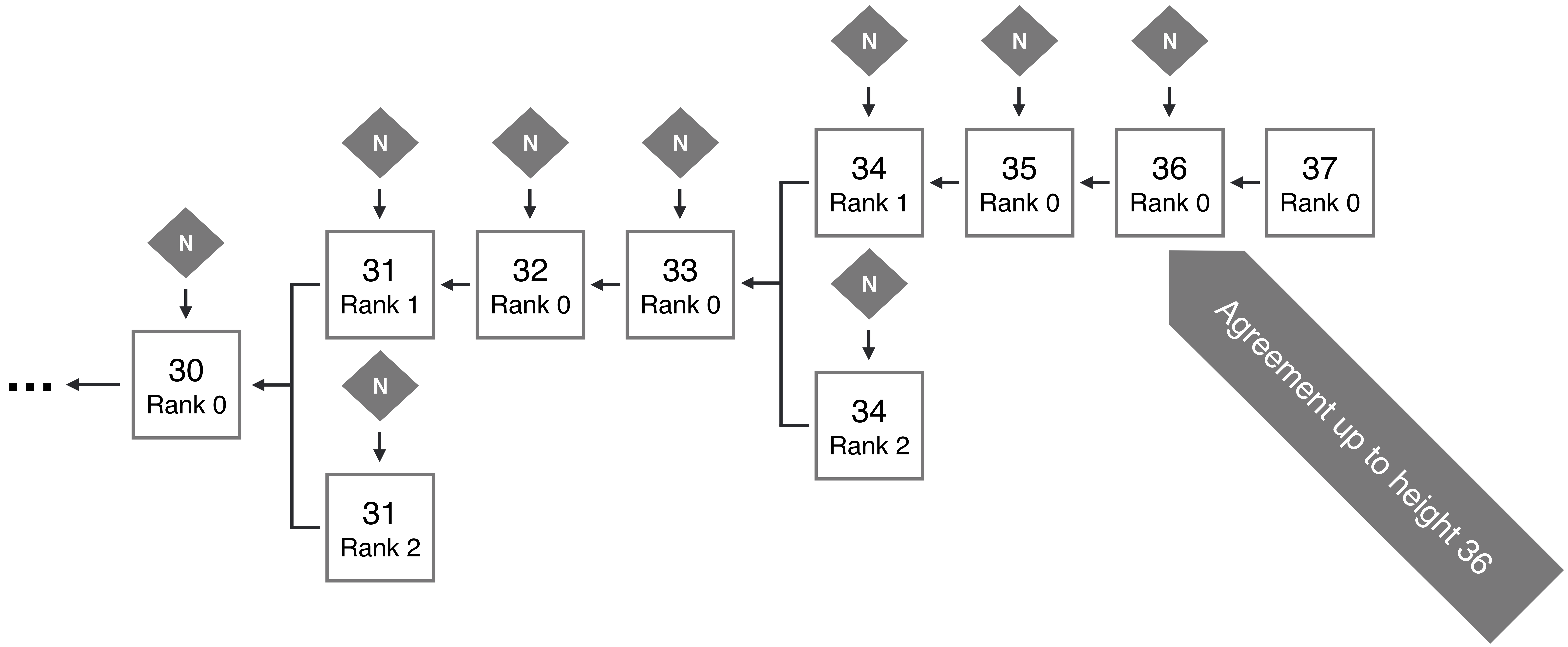
Step 4

Eventually, only the rank 0 block becomes notarized



Notarization with Block Maker Ranking

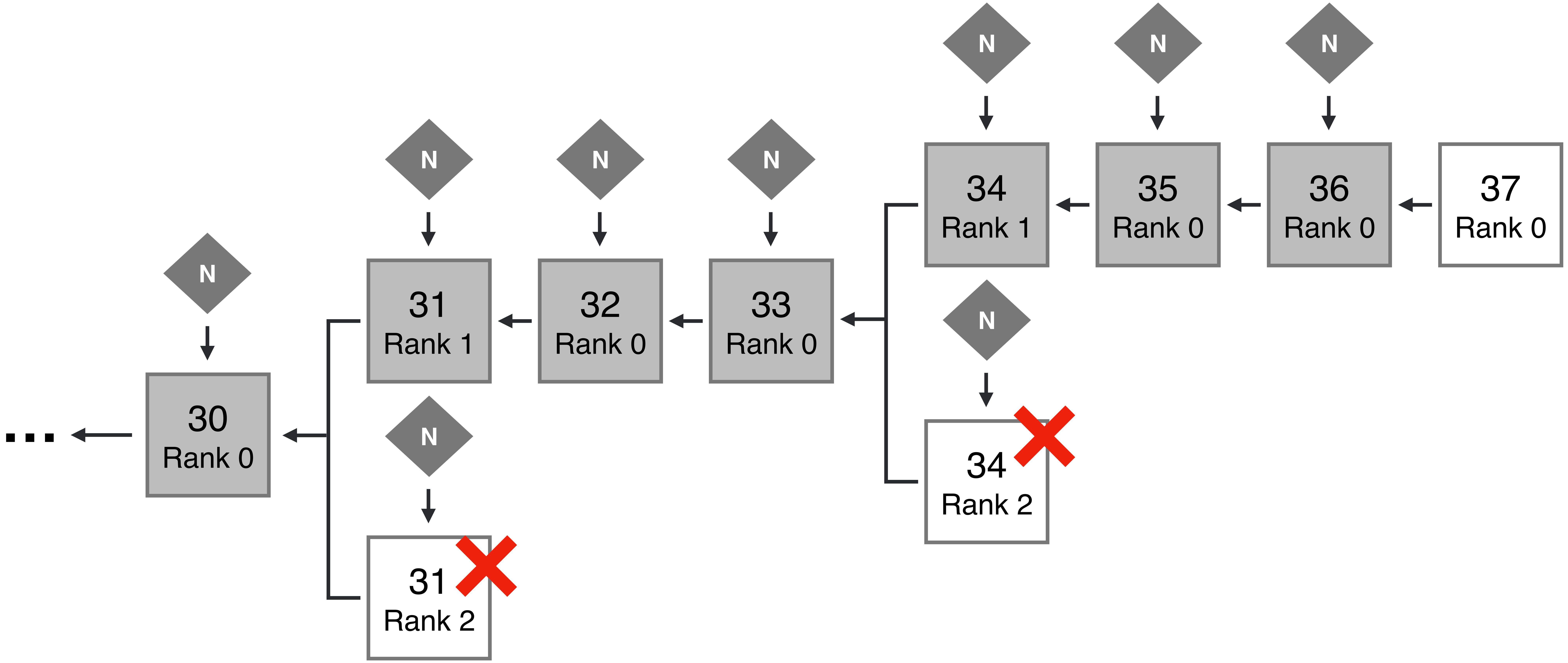
One notarized block *b* at a height *h* = Agreement up to *h*



How can we detect this…?

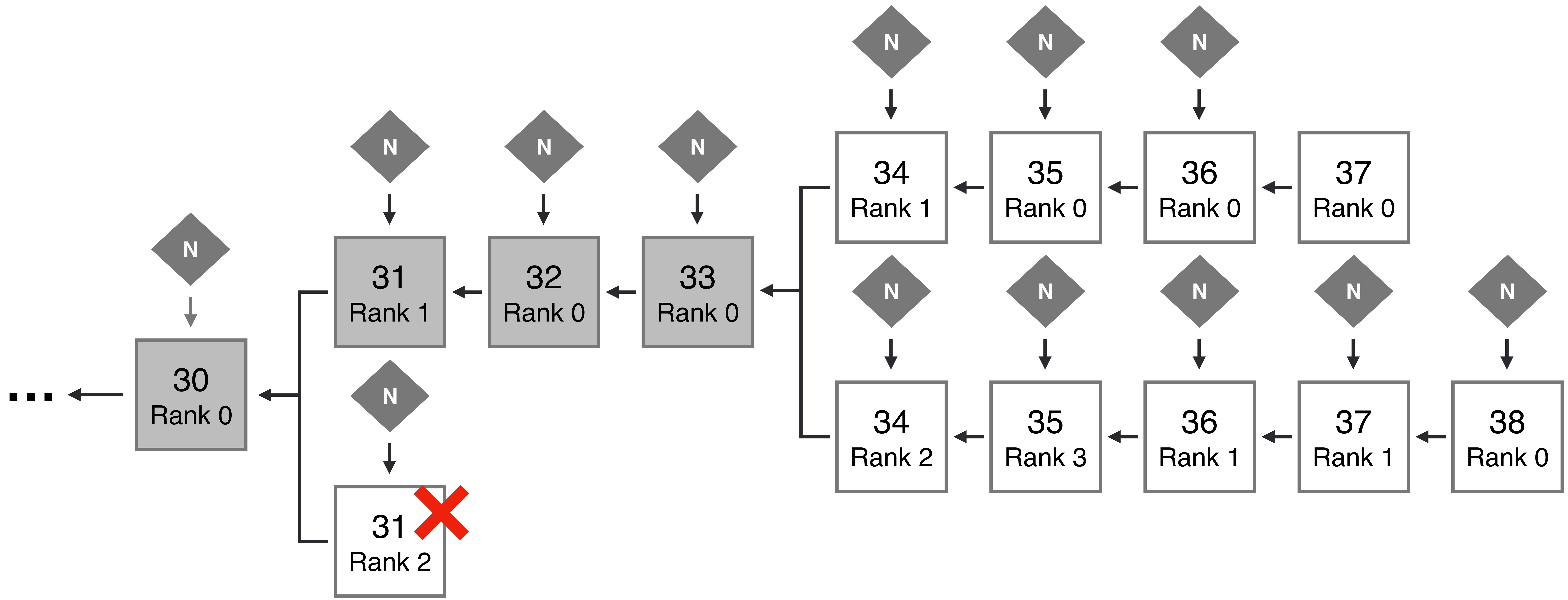
Notarization with Block Maker Ranking

Synchronous communication → Forks can be removed



Notarization with Block Maker Ranking

Partially synchronous communication → Forks cannot be removed!



Finalization

Replicas create finalization shares if they did not sign any other block at that height

Step 1

Replica 1 notary-signs block *b* at height 30

Step 2

Replica 1 observes that block *b* is fully notarized and will no longer notary-sign blocks at height ≤ 30

Step 3

Since replica 1 did not notary-sign any other block than block b, it signs block *b*, creating a finalization-share on *b*

Step 4

Replicas 2 and 4 also cast finalization shares on block *b*

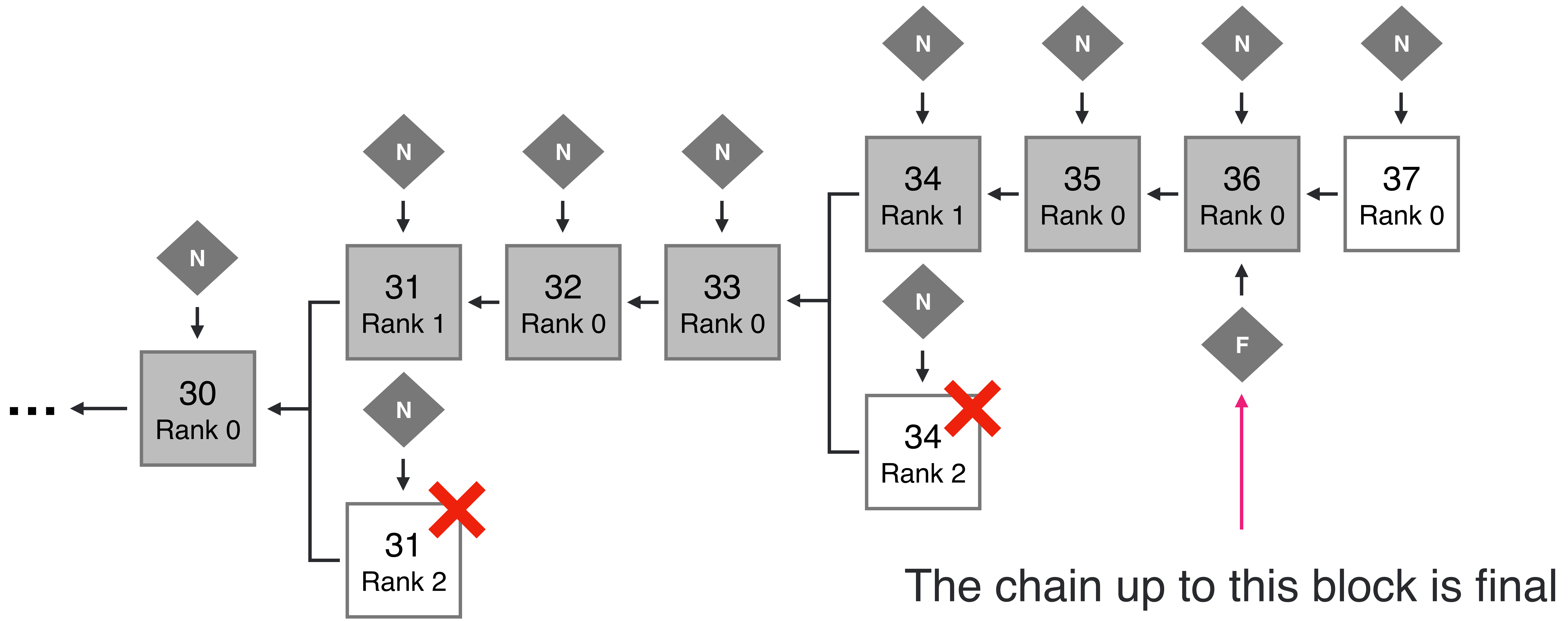
Step 5

3 finalization-shares are sufficient approval: the shares are aggregated into a single full finalization

Replica 1 did not notary-sign any height 30 block other than b

Finalization

Finalization on block *b* at height *h* = Proof that no other block is notarized at height *h*



Safety of Finalization

If block *b* at height *h* is finalized, then there is no finalized block $b' \neq b$ at height *h*.

Proof:

1. A full finalization on *b* requires ***n-f*** replicas to finality-sign (by construction)
2. At least ***n-2f*** of the **n-f** replicas that finality-signed *b* must be honest (by assumption that ≤ ***f*** replicas are corrupt)
3. An honest replica that finality-signed *b* did not notary-sign any other block at height *h* (by construction)
4. At least ***n-2f*** replicas did not notary-sign any height *h* block other than *b* (by 2. & 3.)
5. A full notarization requires ***n-f*** notarization-shares (by construction)
6. The ***n-(n-2f) < n-f*** remaining replicas that may have notary-signed a block *b'* are not sufficient to reach the notarization threshold of ***n-f*** (by 4. & 5.)

The Internet Computer Today

Live Since May 2021!

Currently 375 machines by 53 node providers

https://dashboard.internetcomputer.org/

Many distributed systems problems

- Disseminating messages among all nodes in the same subset
- Exchanging canister and control messages between subnets
- Scheduling and concurrent execution of canister messages
- Catching up after a node has been offline for a while
- Handling churn (adding and removing nodes)
- Guaranteeing consistency (different users need a consistent view of data and operations)
- Upgrading to next protocol version
- Creating new subnets
- Load balancing
- …

Fast Growing Blockchain Ecosystem

Toniq Labs | Fleek | DSCVR | Distrikt | Origyn | OpenChat | Plug | Internet Identity | IC Rocks | NNS Dapp | Dank | Motoko Playground

Agryo | Sudograph | Reversi | DFINITY Explorer | NNS Calculator | Stoic Wallet | ICME | Saga Tarot | IC Drive | DeckDeckGo | Aedile

The Wall | Uniswap Front End on the IC | DFinance | Rise of the Magni | Welcome Into the Metaverse | HexGL | ICPunks | Entrepot | Departure Labs | Axon

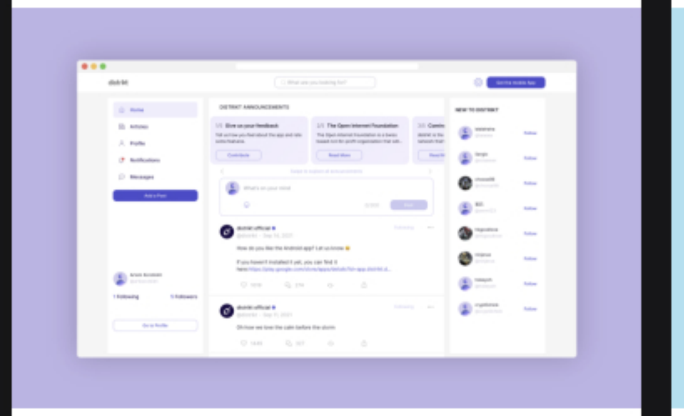
FLEEK

Fleek brings decentralized web-hosting to the Internet Computer. With thousands of webpages deployed, Fleek enables anyone to deploy their content on Web3.0

fleek.co

#Infrastructure #Tools

DISTRIKT



Distrikt is a completely decentralized, community-owned professional network. Users of the platform will vote on upgrades, and no user data will ever be mined or sold. Create your account, secured by Internet Identity today.

19 000 users

#Social #Dapp

ORIGYN

The Origyn Foundation is blending luxury goods, with NFTs by providing digital verifications for physical objects. Only possible on the Internet Computer.

www.origyn.ch

#Enterprise #NFT

OPENCHAT

Decentralized messaging has been a pipe-dream for decades. With the advent of the Internet Computer, real-time messaging is now possible on a blockchain.

50 000 users

7e6iv-biaaa-aaaaf-aaada-cai

#Social #Dapp

INTERNET IDENTITY

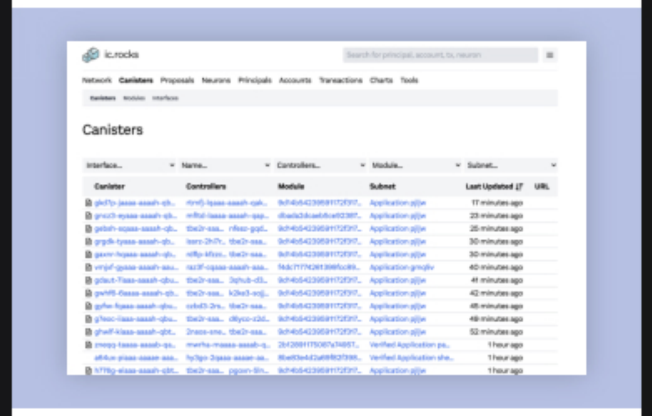
Internet Identity guarantees that your data isn't visible, tracked, or mined. The blockchain authentication system enables users to sign in to dapps on the Internet Computer and sites across the web anonymously and securely.

1 000 000+

identity.ic0.app

#Authentication #Dapp #Infrastructure

IC ROCKS



IC.Rocks is a complete "block explorer" for the Internet Computer – built by the community. Tracking everything from transactions, to network upgrades, to cycles, IC.Rocks enables anyone to explore the inner-workings of the Internet Computer.

ic.rocks

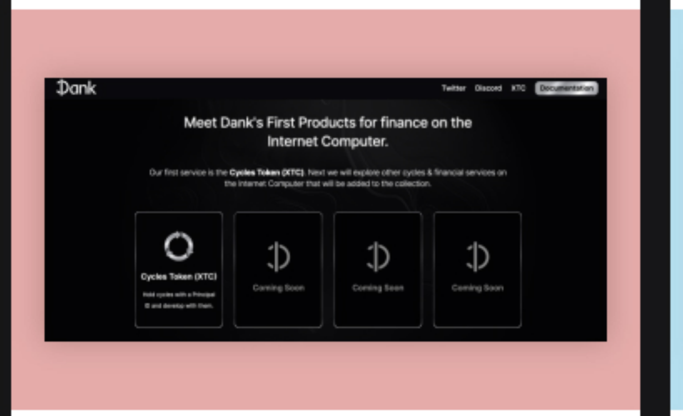
#Infrastructure #Explorer

NNS DAPP

The NNS front-end dapp allows anyone to interact with the Internet Computer's Network Nervous System with a user-friendly UI. Served completely end-to-end through blockchain, this dapp allows you to manage ICP, stake neurons, participate in voting, and earn rewards.

#Dapp #Infrastructure #Wallet #NNS

DANK



Dank is the first Decentralized Bank built on the Internet Computer, developed by Fleek. Through a collection of Open Internet Services for users and developers, Dank makes cycles management seamless.

dank.ooo

#Infrastructure #DeFi

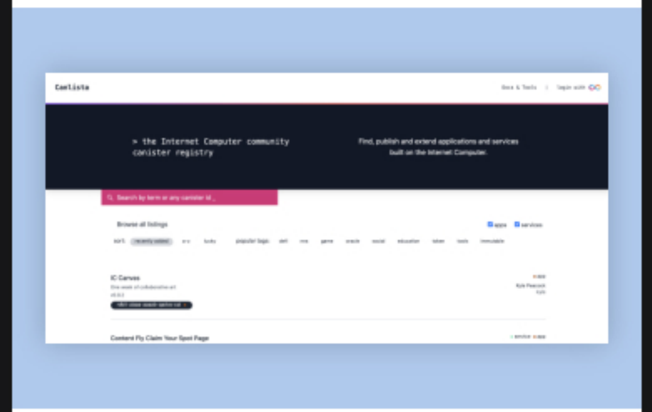
TONIQ LABS

Toniq Labs is the creator of Entrepot NFT marketplace, Stoic Wallet, Exponent, and Rise of the Magni, Cronic NFTs and more. Try out their projects that range from NFTs to wrapped cycles to games built on, and for, the Internet Computer blockchain.

igpeu-waaaa-aaaad-qaava-cai

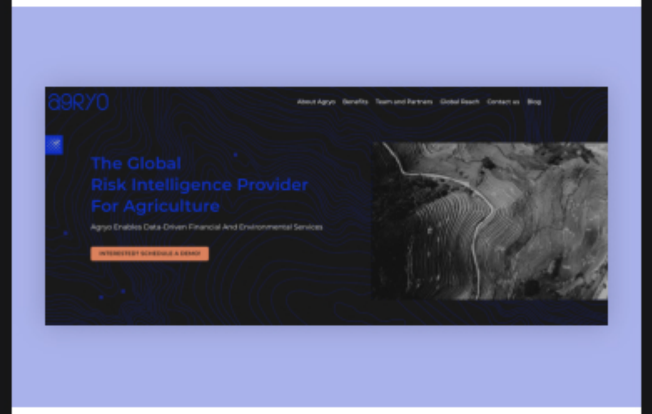
#Infrastructure #Dapp

CANLISTA



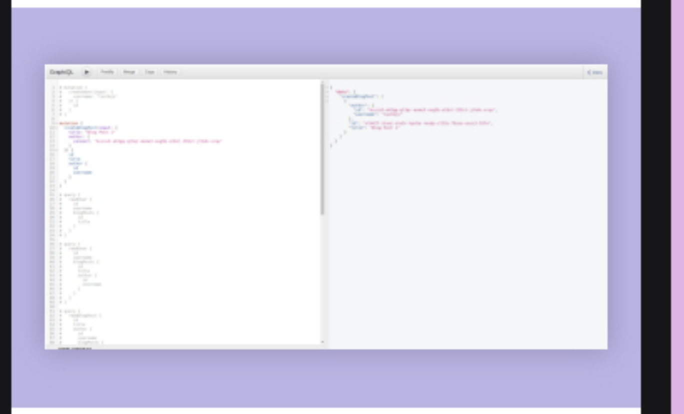
The Internet Computer community canister registry. Find, publish and extend applications

AGRYO

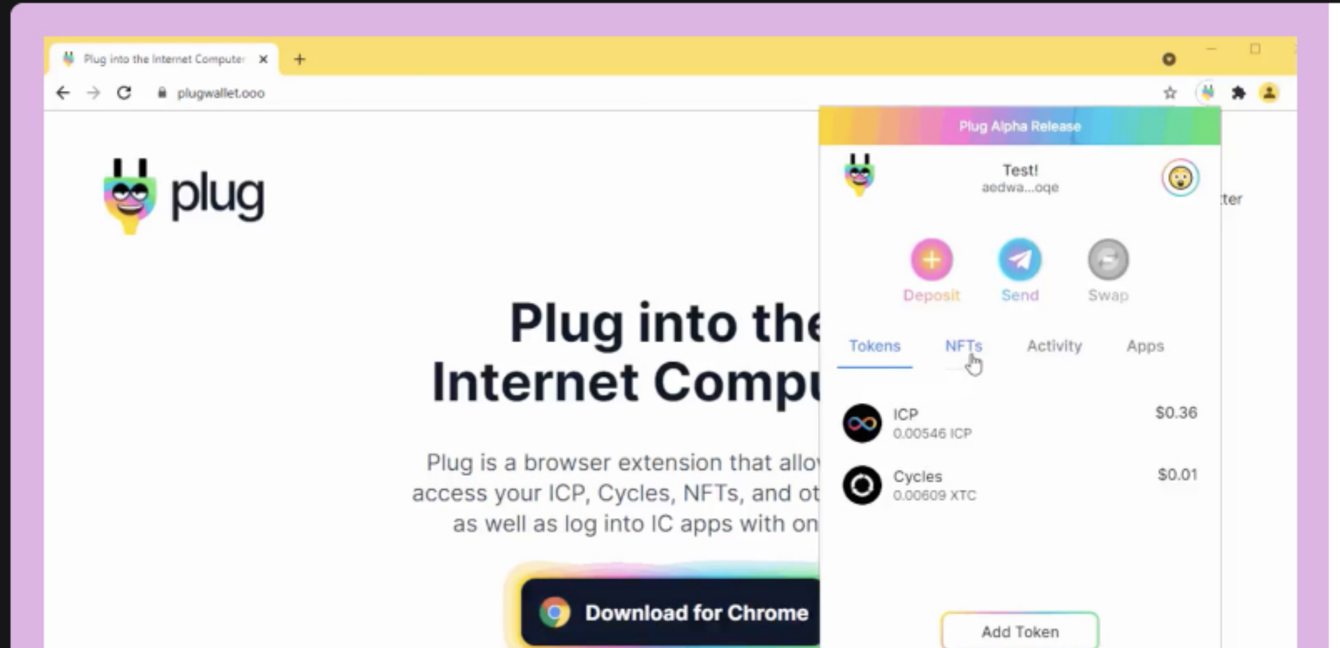


Agryo is the global risk intelligence provider that enables financial institutions to assess and

SUDOGRAPH



Sudograph is a GraphQL database for the Internet Computer. Its goal is to become the



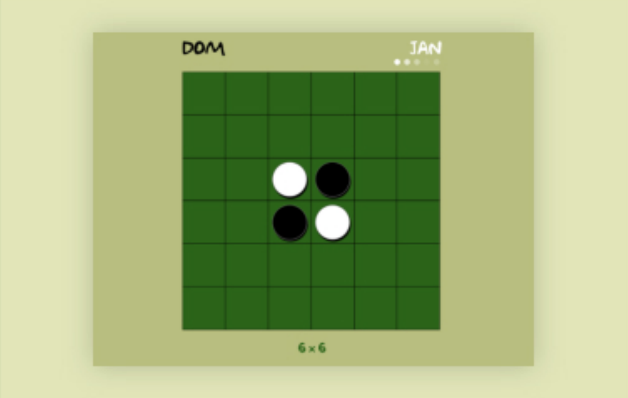
PLUG

Plug Wallet, built and open sourced by Fleek, is a browser extension that allows you to access your ICP, Cycles and other tokens – as well as log into Internet Computer dapps with one click. Download it here.

100 000 users

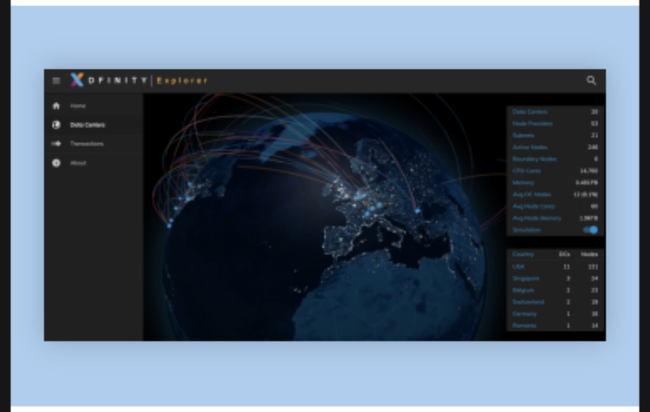
plugwallet.ooo

REVERSI



Reversi is one of the first canister smart contracts deployed to the Internet Computer

DFINITY EXPLORER



DFINITY Explorer, a project started in 2018, is

NNS CALCULATOR

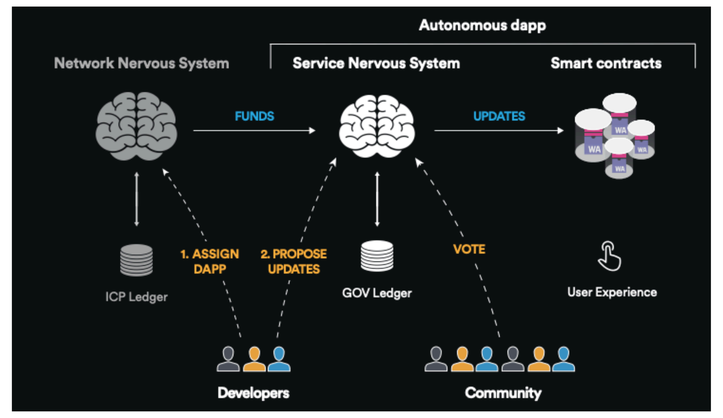
The Network Nervous System Calculator is a

Internet Computer vs. …

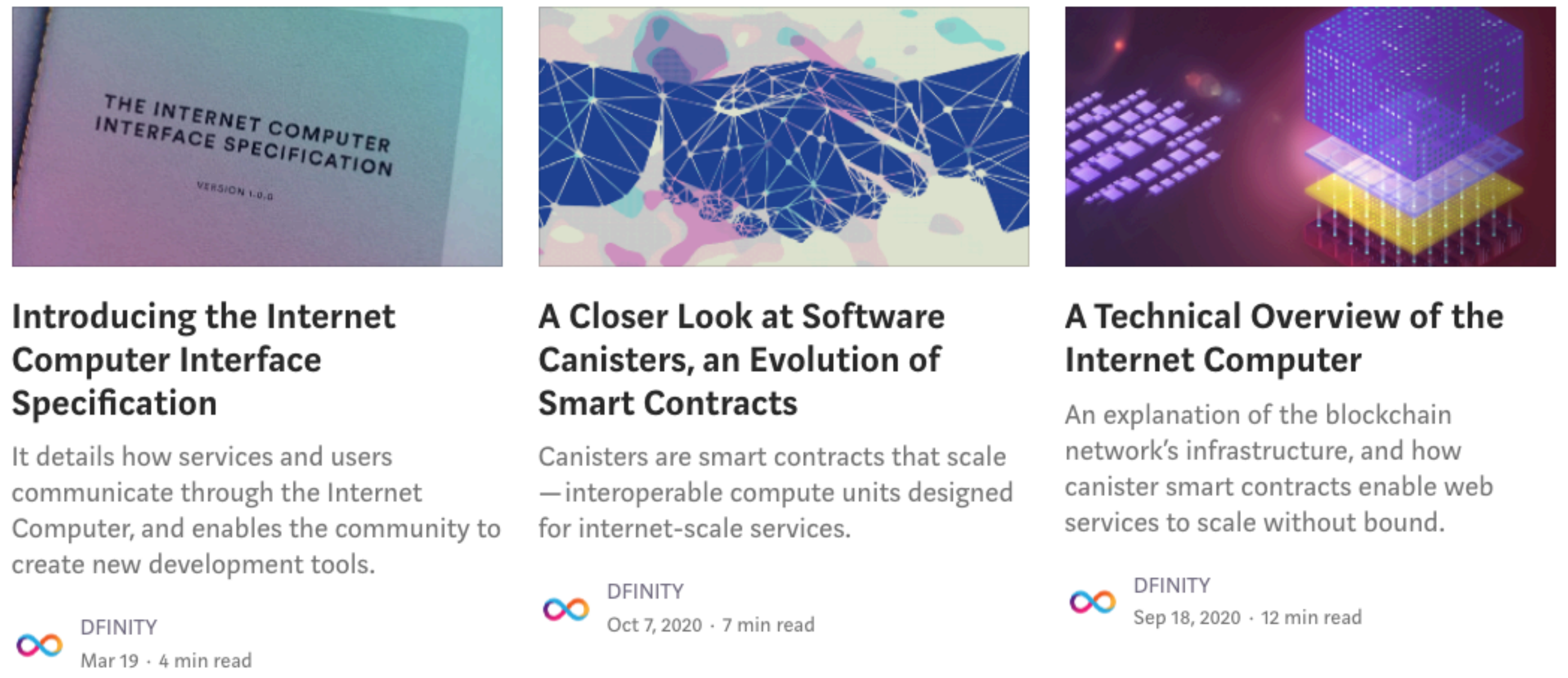
	Bitcoin	Ethereum	Internet Computer
Average block time:	1 block / 10 minutes	1 block / 15 seconds	30 blocks / second
Finality:	1 hour	3 minutes	1-3 seconds
TX per second:	7	15	11,500 (write) / 250,000 (read)
Validation data:	380 GB	550 GB	48 bytes

More information

- Infographic: here



- Technical Library: here (videos of talks) and here (blogposts)

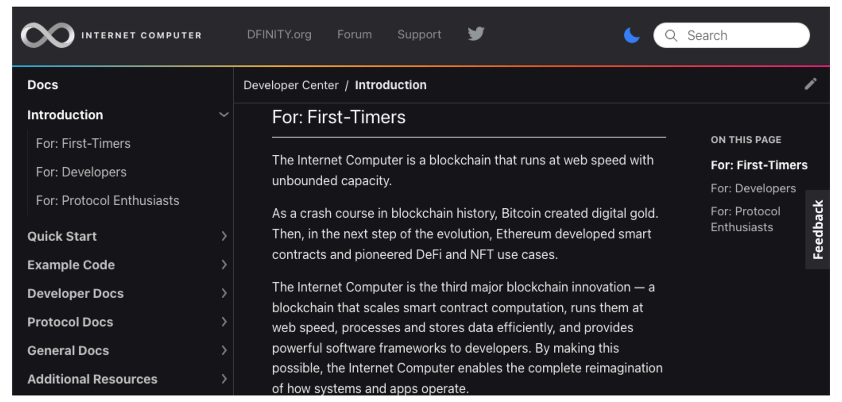


- 200,000,000 CHF Developer Grant Program here

102 GRANTEES

Grantee	Grant Commitment
AEDILE Project management dapp	$25,000
AGRYO Global risk intelligence for agriculture	$25,000
ASTROX Dart developer tools and "mini apps" framework	$25,000
B9 LABS Developer onboarding documentation	$25,000
BAUCTION Decentralized and transparent auction platform	$25,000
BEBENTURE	$5,000

- DFINITY SDK: here




DFINITY