Internet Computer Protocol: democratic evolution of a web3 platform

DEBS Keynote, June 29, 2023

Yvonne-Anne Pignolet
Director of Research, yvonneanne@dfinity.org
DFINITY

- Not-for-profit organisation developing for the Internet Computer
- Roots in early Ethereum community
- DFINITY Foundation established in 2016
- Headquarter: Zurich, Switzerland
- RnD enters in Zurich and San Francisco
- Staff: +250
Outline

• What is the Internet Computer?
• Apps, numbers and stats
• How does the IC evolve?
What is the vision of the Internet Computer?
The Internet Computer does to computation what the Internet does to communication
Autonomous public cloud to run general purpose applications using blockchain technology for decentralisation and security
Internet Computer Protocol (ICP)

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

ICP creates the Internet Computer blockchains

Guarantees safety and liveness of smart contract execution despite Byzantine participants
Deploying and Using Canister Smart Contracts

- Multi-chain
- Scalable
- Energy-efficient
- Low-cost
- Fast
- Serve HTTP directly
ICP Tokens are used...

- To facilitate *participation* in network *governance*.

- To *reward participants* that participate in governance and operate the node machines.

- To produce the *cycles*, i.e., the fuel used to power computation.

besides ICP, the other native token on the IC
Canisters are pre-charged with “cycles” that fuel their computation. Users don’t need to pay for transaction gas.

This “reverse gas” model is the opposite of Ethereum’s where end users must pay for each transaction.
Architecture and Governance
Nodes in Independent Data Centers
Assumption: \( n > 3f \)

Guarantees **agreement** even under asynchrony

Guarantees **termination** under partial synchrony
Chain Key Cryptography

Single 48-byte public key

for a secret-shared private key

https://internetcomputer.org/how-it-works(chain-key-technology)
Chain Key Cryptography

Single 48-byte public key

for a secret-shared private key

\text{verify}(\text{Email}, \text{Key})

https://internetcomputer.org/how-it-works/chain-key-technology
Subnets for Scalability

• Each canister is assigned to one subnet

• Each subnet is a **replicated state machine**

• A canister can call canisters on other subnets

• Subnets make the Internet Computer **scalable**!
Governance: Network Nervous System

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
- …

[https://internetcomputer.org/nns](https://internetcomputer.org/nns)
Governance: Network Nervous System

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
- ...
Execution layer

Systems challenges:

• statefulness (orthogonal persistence)
• scalability (caching, time slicing)
• determinism (scheduling)
• security (sandboxing, accounting)

=> Alternative and improvement upon current centralized & stateless serverless paradigm
The Internet Computer Today
Live Since May 2021!

https://dashboard.internetcomputer.org
## Comparison with other Blockchain Systems

<table>
<thead>
<tr>
<th></th>
<th>Ethereum</th>
<th>Cardano</th>
<th>Solana</th>
<th>Avalanche</th>
<th>Algorand</th>
<th>Internet Computer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avg # TX/s</td>
<td>14.4</td>
<td>2.95</td>
<td>381</td>
<td>49.52</td>
<td>15.5</td>
<td>5000</td>
</tr>
<tr>
<td>Avg finality</td>
<td>15min</td>
<td>-</td>
<td>5-12.8s</td>
<td>2.3s</td>
<td>3.5s</td>
<td>1.4s</td>
</tr>
<tr>
<td>Wh / TX</td>
<td>-</td>
<td>51.59</td>
<td>0.166</td>
<td>4.76</td>
<td>2.7</td>
<td>0.008</td>
</tr>
<tr>
<td>1GB storage</td>
<td>15M$</td>
<td>17-113k$</td>
<td>48k$</td>
<td>200k$</td>
<td>off-chain storage</td>
<td>5$</td>
</tr>
</tbody>
</table>


see also [https://wiki.internetcomputer.org/wiki/L1_comparison](https://wiki.internetcomputer.org/wiki/L1_comparison)
Internet Computer Ecosystem

See dapps running on ICP
Evolution
IC has an governance system that controls every aspect of it:

- **Tokenized DAO**
- **Operational governance**
- **Strategic governance**: evolution of the IC protocol

We increasingly decentralize decisions on evolution by letting the community vote on so-called motion proposals. Also involve the community through workshops; upcoming workshop with community on Bitcoin.

- In-depth use case discussion; ensure use cases are captured by what we implement.
- Getting new requirements.

Further decentralization of our governance is exciting:

- Adding datacenters
- Adding node providers
- Adding / removing nodes to / from subnets

**Evolution of the protocol**

**Features to build / roadmap** (facilitated through forum discussions and community workshops)

**Liquid democracy**

- Token holders can vote on their own or follow others (e.g., for selected topics).

Accepted proposals are automatically executed on the IC or shape the roadmap.
IC has a governance system that controls every aspect of it: Tokenized DAO - Operational governance - Strategic governance: evolution of the IC protocol.

We increasingly decentralize decisions on evolution by letting the community vote on so-called motion proposals. Also involve the community through workshops; upcoming workshop with the community on Bitcoin - In-depth use case discussion; ensure use cases are captured by what we implement - Getting new requirements.

Further decentralization of our governance is exciting.

- Adding datacenters
- Adding node providers
- Adding / removing nodes to / from subnets

Evolution of the protocol - Features to build / roadmap (facilitated through forum discussions and community workshops).

Liquid democracy - Token holders can vote on their own or follow others (e.g., for selected topics). Accepted proposals are automatically executed on the IC or shape the roadmap.
IC has an governance system that controls every aspect of it:

- **Tokenized DAO** - Operational governance
- **Strategic governance** - Evolution of the IC protocol

We increasingly decentralize decisions on evolution by letting the community vote on so-called motion proposals. Also, involve the community through workshops; upcoming workshop with the community on Bitcoin.

An in-depth use case discussion ensures use cases are captured by what we implement.

Further decentralization of our governance is exciting:

- Adding data centers
- Adding node providers
- Adding/removing nodes to/from subnets

Evolution of the protocol:

- Features to build/roadmap (facilitated through forum discussions and community workshops)

**Liquid democracy**:

- Token holders can vote on their own or follow others (e.g., for selected topics)

Accepted proposals are automatically executed on the IC or shape the roadmap.
Decentralised Upgrade Challenges

How to

• Select version to upgrade to?
• Ensure all nodes in a subnet know about new version?
• And switch to the new version at the same time?
• And minimise time without processing messages?
• And minimise compatibility risks?
Vote on Proposals

**Type**  
Add or Remove Node Provider

**Topic**  
Participant Management

**Proposer**  
62985...00623

"Add node provider: niw4y-aseue-l3qvz-sozsi-tfkvb-cxcx6-pzs1g-5dqd-oudp-hsui-xae"

**Status**  
1 day, 3 hours remaining

**Type**  
NNS Canister Upgrade

**Topic**  
System Canister Management

**Proposer**  
59

"Upgrade Nns Canister: qoctq-giaaa-aaaaa-a3aee-cai to wasm with hash: 87743bc2a9ed4c7739bd2073fcb54574ed2 db2fe1022a3e7a945fb803bafa72f"

**Status**  
Executed

**Type**  
Bless Replica Version

**Topic**  
Replica Version Management

**Proposer**  
46

"Elect new replica binary revision (commit 8487a2be2a0e105843d03f07079d97e8 82d440)"

**Status**  
Executed

**Type**  
NNS Canister Upgrade

**Topic**  
System Canister Management

**Proposer**  
70

"Upgrade Nns Canister: mqygn-kiaaa-aaazar-qaadq-cai to wasm with hash: 9525c491b534a85d31624ac36d15b5ef6d 2acc607fae53167f5027c70a351f"

**Status**  
Executed

**Type**  
Bless Replica Version

**Topic**  
Replica Version Management

**Proposer**  
40

"Elect new replica binary revision (commit 9fde647b04e9994c11207a652914d5f9d5 ae895)"

**Status**  
Executed

**Type**  
NNS Canister Upgrade

**Topic**  
System Canister Management

**Proposer**  
73

"Upgrade Nns Canister: rdmx6-jaaaa-aaaaa-aaadq-cai to wasm with hash: 38b54cbcb8b8c6e7e3c0c028461f535f8 0fad23dd43b605c036f46ba2a01"

**Status**  
Executed
NNS Canister Upgrade

Type
Topic
Status
Reward Status
Created
Decided
Executed
Proposer

NNS Canister Upgrade
System Canister Management
Executed
Ready to Settle
Mar 13, 2023 11:19 AM
Mar 13, 2023 11:29 AM
Mar 13, 2023 11:29 AM
59

Voting Results

Adopt
437303219.45
Reject
60193

Proposal Summary
Upgrade Nns Canister: qoctq-giiaa-aaaaa-aaaaa-cai to wasm with hash: 87743bc2e1ed4c739bd207f3c54674ed2db2fe1022e3e7a945fb803bafa72f

Upgrade frontend NNS Dapp canister to commit
0733e335ec64001e8904497a388ce4516e57e1304

Wasm sha256 hash: 87743bc2e1ed4c739bd207f3c54674ed2db2fe1022e3e7a945fb803bafa72f (https://github.com/dfinity/nns-dapp/pull/2076/checks)

Change Log:
- Do not allow increasing stake for CF SNS neurons.
- Improve validations in address inputs.
Background: State Machine Replication

State $h - 2$ → State $h - 1$ → State $h$

Input Block $h - 1$ → Input Block $h$

Agreement on input by Consensus
IC Versions Have Non-Overlapping Responsibilities

Responsibility of V1

State $h - 2$ → State $h - 1$ → State $h$ → State $h + 1$ → State $h + 2$

Responsibility of V2

State $h - 2$ → State $h - 1$ → State $h$ → State $h + 1$ → State $h + 2$

Agree what the state here is and create a "snapshot"
Decentralised Upgrade Challenges

• Select version to upgrade to?
  ✓ NNS-based community voting

• Ensure all nodes in a subnet know about new version?
  ✓ Store version in NNS canister, nodes poll this canister

• And switch to the new version at the same time?
  ✓ consensus on next version to use and at which height to switch

• And maximise time processing messages?
  ✓ state snapshot on previous version, read-only until finalization of state from last block with old version
  A/B partition reboot, persist state

• And minimise compatibility risks?
  ✓ simplicity > performance, extensive automated testing
IC has a governance system that controls every aspect of it: Tokenized DAO operational governance - strategic governance: evolution of the IC protocol.

We increasingly decentralize decisions on evolution by letting the community vote on so-called motion proposals. Also involve the community through workshops; upcoming workshop with community on Bitcoin - in-depth use case discussion; ensure use cases are captured by what we implement - getting new requirements.

Further decentralization of our governance is exciting: adding datacenters, adding node providers, adding or removing nodes from subnets, evolution of the protocol, features to build / roadmap (facilitated through forum discussions and community workshops).

Liquid democracy - token holders can vote on their own or follow others (e.g., for selected topics). Accepted proposals are automatically executed on the IC or shape the roadmap.

DAOize your dapp.
Game changer: DAO Factory

1. Proposal to turn dapp into DAO
2. ICP creates dapp token
3. ICP initiates decentralisation swap
4. Anyone who buys tokens becomes DAO participant
5. DAO fully controls dapp

Hot or Not DAO creation is ongoing right now
Take aways

The Internet Computer can

• Run rich canister smart contracts
• Serve requests at web speed
• Upgrade itself based on community votes
• DAOize apps

IC code: https://github.com/dfinity/ic
Dashboard: https://dashboard.internetcomputer.org/
Dataset API: https://ic-api.internetcomputer.org/api