AION

Blockchain 3.0

1

Generations of Blockchain

GENERATION OF BLOCKCHAIN

First Generation Blockchain

Blockchain 1.0

Bitcoin led the way in the creation of numerous alternative currency platforms as the first generation of blockchain technology. These first-generation blockchains provided a solution to conventional transaction limitations by implementing cryptographically-secure, peer-to-peer, digital transactions that are verified by a decentralized global network and recorded into an immutable public ledger.

Second Generation Blockchain

Blockchain 2.0

With the second generation of blockchain, Ethereum introduced the ability to build application-specific logic upon a blockchain network. This enabled new capabilities beyond transactions to incorporate state, business logic, and multi-party contracts to be stored and executed on a blockchain and written to an immutable ledger. These concepts have been incorporated into other distributed ledger technologies and have led to the distinction of building a blockchain and building upon a blockchain.

Third Generation Blockchain

Blockchain 3.0 (AION)

In the future, blockchains will federate data and value allowing different blockchains to communicate with one another. The future of mainstream blockchain adoption will be achieved by the development of a networked, federated blockchain which will operate in a manner similar to the internet. That integrated blockchain network is Aion.

The Third Generation Blockchain Network

A multi-tier blockchain system designed to address unsolved questions of scalability, privacy, and interoperability in blockchain networks.

What exactly is the AION network ?

The Aion network functions like a computer network and is based on blockchain technology. The network passes value and logic among the users. It also passes liquid assets freely where transactions are carried out without intermediaries.

The Aion network is focused on third-generation blockchain which is publicly known as the Aion-1. It is designed to link other blockchains and aid in managing its applications. Aion-1 also offers interoperability in the ecosystem.

MULTI-TER BLOCKCHAIN NETWORK

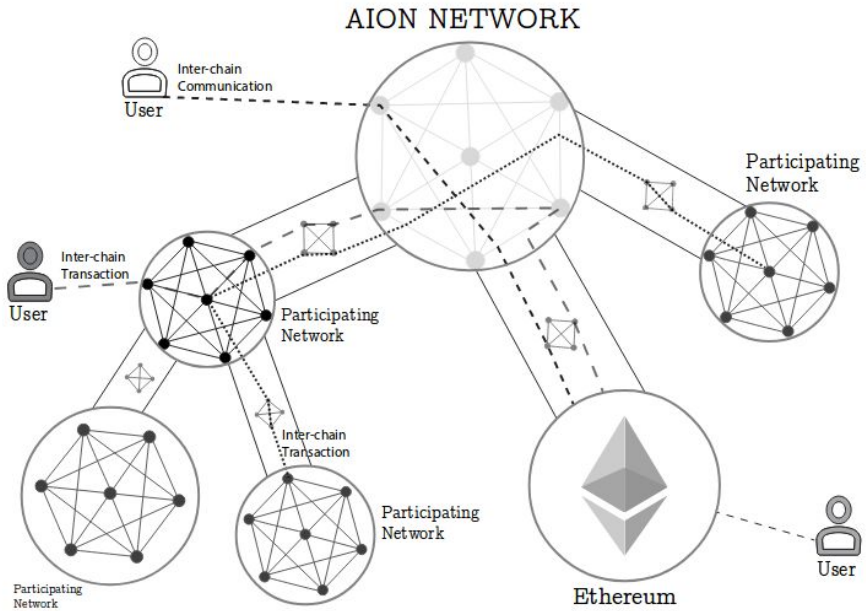


Figure 1: Example of a simple Multi-Tier Blockchain Network network, consisting of all the major actors

2

Architecture

MULTI-TIER BLOCKCHAIN NETWORK

The Aion multi-tier blockchain network provides protocol and standard for dissimilar systems to communicate.

- ➔ The Aion network will pass logic and value among participating blockchains to create a contiguous value chain where every transaction occurs on-chain, with logic and value passing among chains.
- ➔ The value of these technologies is that they enable one blockchain to transact with another blockchain, as well as one blockchain to transact with every connected blockchain.

MULTI-TIER BLOCKCHAIN NETWORK

Connecting Networks

Connecting networks are networks that facilitate interchain communication and interchain transactions between multiple private or public blockchain networks

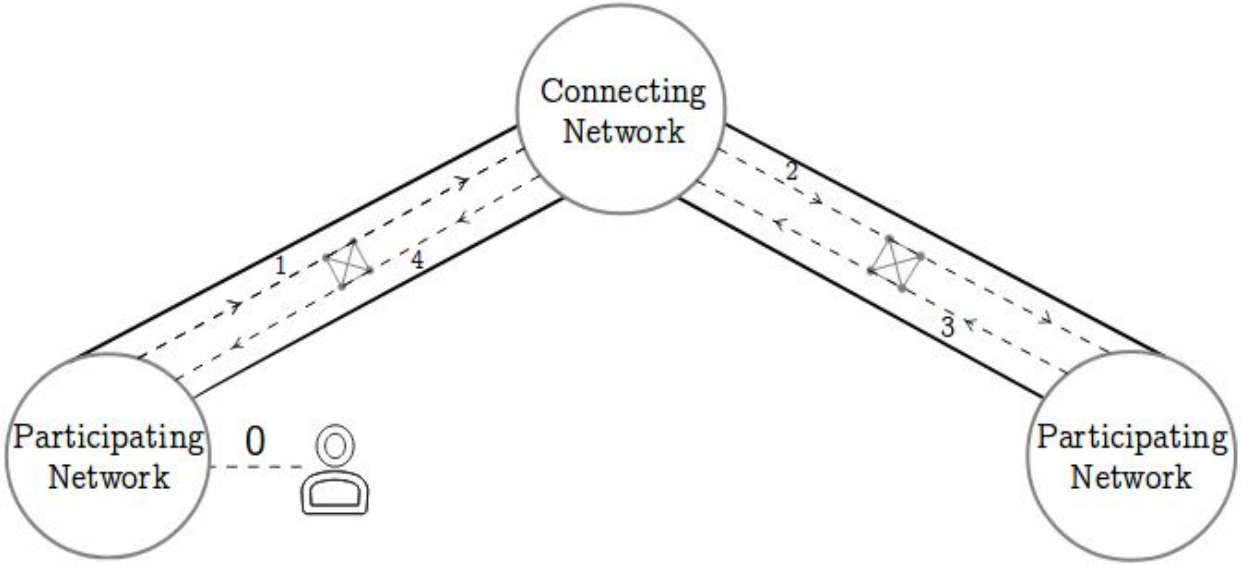
ICT

An interchain transaction is a trust-free message between blockchain networks.

Bridges

A bridge is a communication protocol that facilitates communication between the participating network and the connecting network.

ICT LIFECYCLE



CONNECTING NETWORKS

It provide a universal interface that enables blockchain developers and users to route messages from one network to another.

A connecting network uses bridges and a trust-free blockchain network to validate and ensure the correctness of flowing transactions. By introducing a third party that routes messages from point A to point B, the networks themselves do not have to manage difficult or unclear situations.

Functionality of Connecting Networks

- Route messages between different blockchain networks through a common bridging protocol.
- Provide decentralized accountability.
- Provide a bridging protocol.

INTER-CHAIN TRANSACTION

Interchain transactions are initially created on a source blockchain and then processed and forwarded by bridges and connecting networks before finally reaching the target blockchain.

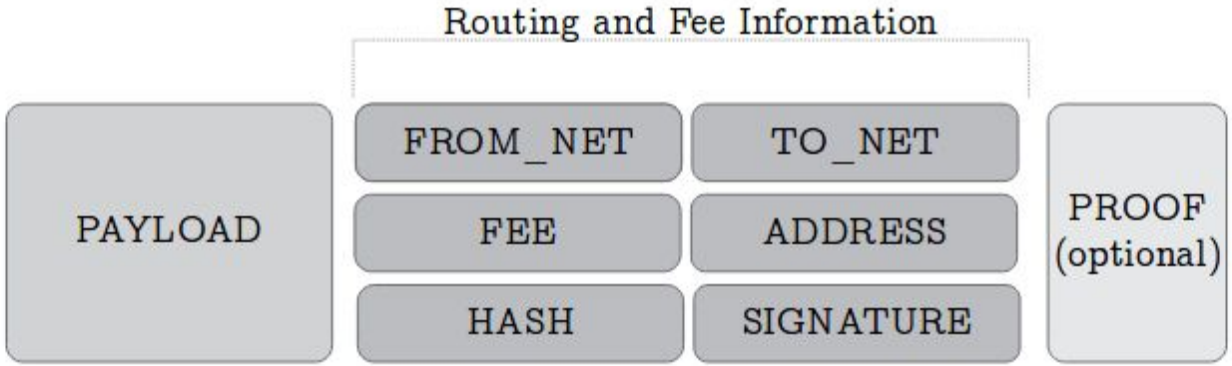
The creator of an interchain transaction must pay a transaction fee for the communication cost using AION tokens.

Format of an ICT

- Payload data: This data is specific to the creator and is typically regular transaction data.
- Metadata: This contains routing information and fee.
- Merkle proof that is only used when the sender wants to bypass the bridge.

The bridge and connecting network validators shall not interpret the data, but do check the integrity of the transaction as a whole.

Visual depiction of an inter-chain transaction



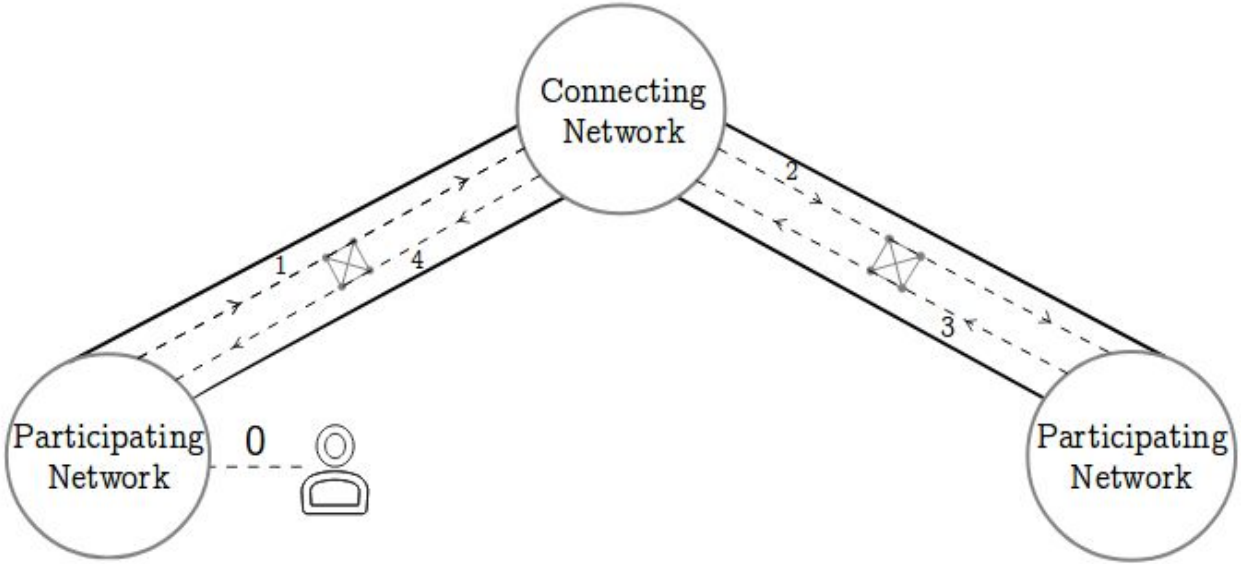
Routing

The routing of interchain transactions is a process in which the validators in each phase verify the transaction and reach consensus on whether the transaction should be forwarded or rejected.

The routing path can be divided into two subpaths: the forward path and backward path.

If a bridge refuses to broadcast an interchain transaction for any reason, the sender may choose to pass the interchain transaction, including proof,directly to the connecting network. The connecting network will validate the interchain transaction based on its knowledge of a merkle hash chain of the participating network and broadcast it if valid

ICT LIFECYCLE



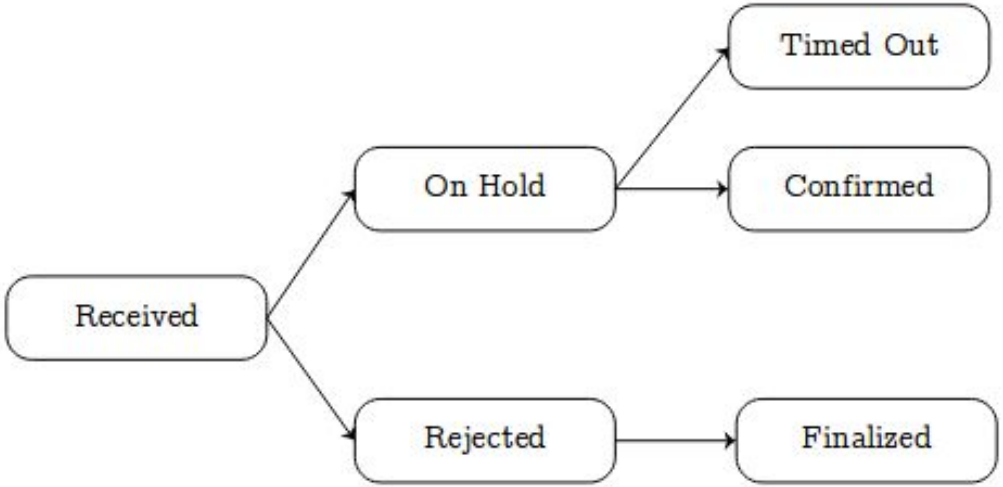
ICT State

Interchain transaction state is introduced to represent the different stages/status of a transaction from the perspective of the connecting network.

- ➔ When an interchain transaction is observed in the participating network by the bridge validators for the first time, the state changes to received.
- ➔ If over two thirds of the bridge validators vote yes for the interchain transaction, the connecting network will change the state of the interchain transaction to on hold.
- ➔ It will trigger an event where a corresponding connecting network token will be locked until the transaction is processed.

- If less than two thirds of the bridge validators vote yes for the interchain transaction, the state changes to **rejected**.
- Once a confirmation is received from the target blockchain, the state changes to **confirmed**.
- If no confirmation is received, the state changes to **timed out**.
- For confirmed interchain transactions, the state changes to **finalized** and all locked fees are distributed to the connecting network and bridge validators.

STATES OF ICT



Flow chart of the possible states that can occur within the lifetime of an ICT

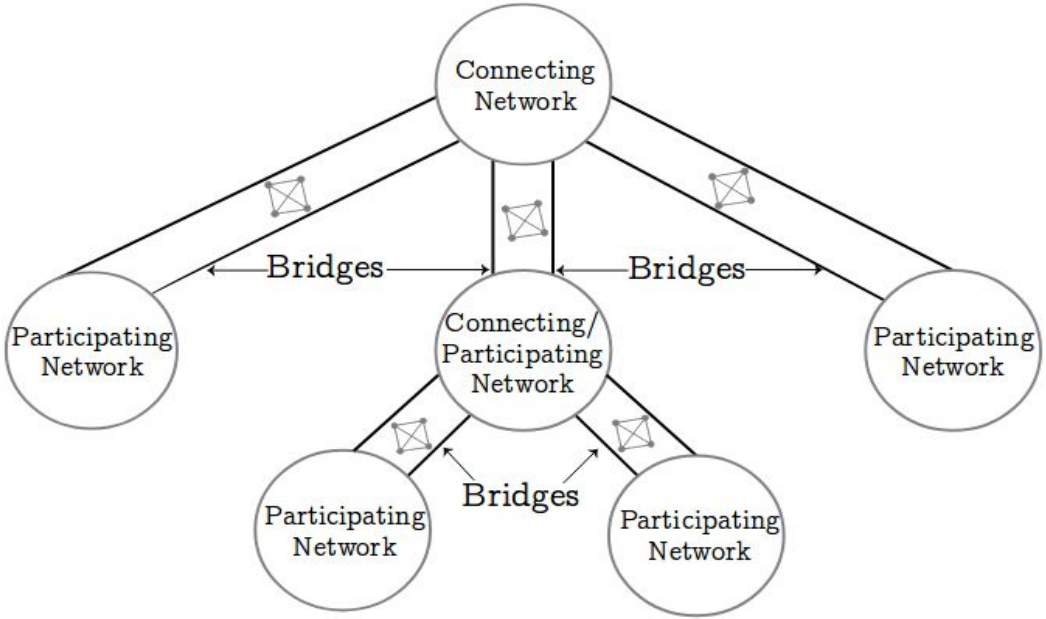
BRIDGES

- A bridge is composed of its own distinct network of validators.
- Bridges are directional.
- Transactions get approved only after receiving over two thirds of the total votes (weighted)

Responsibilities

- Signing and broadcasting an ICT only if they have been sealed in the source blockchain and an ICT forwarding fee has been paid.
- Informing the connecting network of the merkle hash updates of the participating network

Relationship between Bridge and Connecting Network



BRIDGES

Registration

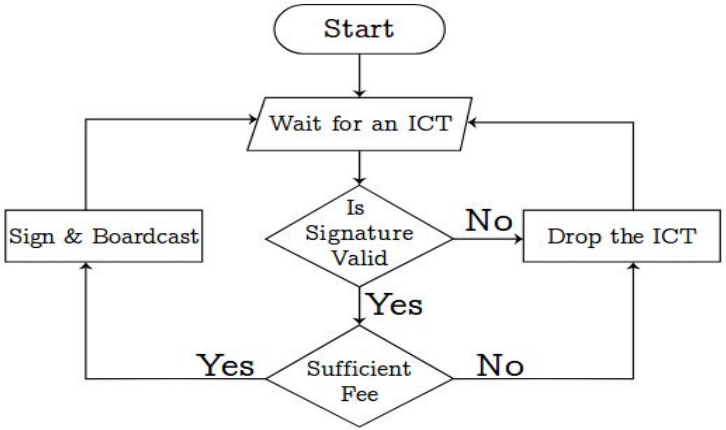
For each bridge, a dedicated table of validators will be maintained on the blockchain, sorted by stake.For a bridge to be considered valid, a minimum total stake is required.It maintains a global bridge registration, which is updated dynamically as nodes join or leave bridging networks.

Competition

Multiple bridges maybe generated when multiple groups of validators register for the same blockchain network using different identifiers. The intent is to drive an open market by incentivizing different bridging networks to compete in terms of stability, reputation, and pricing, with the goal of an optimal fee value driven by market demands

Bridge Consensus

An interchain transaction is deemed valid if two thirds or more of validators voted yes, at which point the next blockchain considers the transaction valid.



AION Compliant Blockchains

Aion-compliant blockchains refer to the participating blockchains that comply with the Aion protocol and on which bridges can be established easily to forward interchain transactions through Aion-1.

To be Aion-compliant, a blockchain must meet certain requirements including:

- Be decentralized in some fashion and support procedures commonly found in blockchains such as atomic broadcast and transactions. The exact implementation is left to the discretion of the bridging protocol and the network itself.
- Be able to recognize interchain transactions as distinct from regular transactions.
- Be aware of the consensus protocol used by the bridge and store a transaction deemed valid.
- Implement locktime or a similar feature that allows tokens to be held by the network for a period of time.

Integration with existing Blockchain

Unlike Aion-compliant blockchains, existing blockchains are not designed to be interoperable. To enable interchain transaction routing between the Aion network and existing blockchains , additional assumptions and/or compromises are required. In this section,we discuss the possibility of connecting the Ethereum blockchain to the Aion network.

Making Ethereum AION Compliant

The Ethereum blockchain does not have this built-in functionality, so it needs an interchain transaction contract.In this model, the interchain transaction contract will synchronize the public keys of bridge validators periodically, depending on the Aion network specification.The bridge validators sign a transaction with their private key and send the signature to the interchain transaction contract. The interchain transaction contract will collect all the votes (signatures) and provide a provable record of the event that contains the interchain transaction data and voting information.

Making Ethereum AION Compliant

Sending interchain transactions from the Ethereum blockchain to the Aion network is easier because of Ethereum's programmable transaction size. Transactions intended for other blockchains will need to incorporate routing information in the data field.

There are two possible scenarios that can occur from an Ethereum interchain transaction (interchain transaction from the Ethereum blockchain to the Aion network), depending on the receiving address. If the transaction is sent to an externally-owned account, the data field can be used without modification. If the transaction is sent to a contract account, a workaround will be needed as the data is also interpreted by the Ethereum VM.One approach for this would be appending the interchain transaction magic tag and routing information to original call data, as long as the contract logic does not rely on the CALLDATASIZE op code.

3

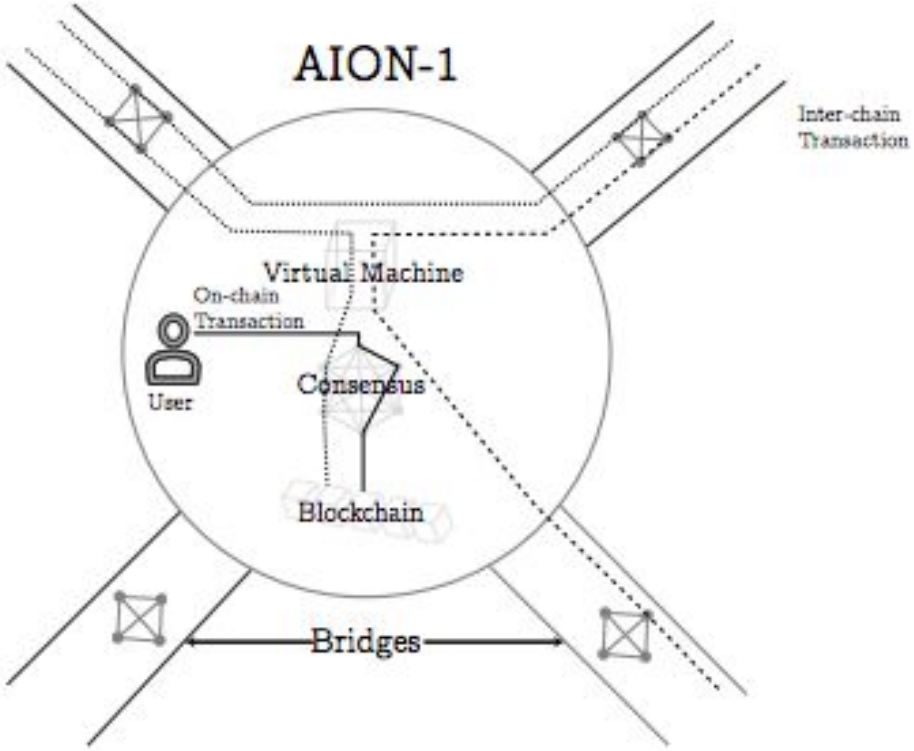
AION-1 BLOCKCHAIN

Overview

The Aion-1 block chain is the genesis implementation of the connecting network.

Aion-1 was designed with the following goals:

- ➔ Connecting blockchains and external services(e.g.,oracles and databases) together through the contiguous network and providing
- ➔ Accountable communication maintained through a decentralized network.
- ➔ Providing the necessary infrastructure to develop high-performance, decentralized, inter-blockchain applications.
- ➔ Creating a maintainable network through a robust and sustainable economic model.



AION-1 architecture

Key Components Of AION-1 Blockchain :-

Key components of the Aion-1 blockchain include:

- **Consensus** will be used to implement the proposed architecture of connecting two or more blockchains.
- **Aion virtual machine** (AVM) is a custom-built, lightweight, performant, and stable VM that leverages key characteristics of the Java Virtual Machine (JVM), providing concurrency and robustness within a blockchain-specific context

The Consensus Algorithm

Aion-1 uses a consensus algorithm based on a Byzantine Fault Tolerant (BFT) algorithm.

A **representative validation model** is used.The conceptual design behind a representative network validation scheme is similar to that of a representative democracy in which candidates register themselves and are elected based on the votes they receive from their constituents.

These elected candidates then become representatives and a consensus is reached based on 2/3rd majority of votes from these representatives.

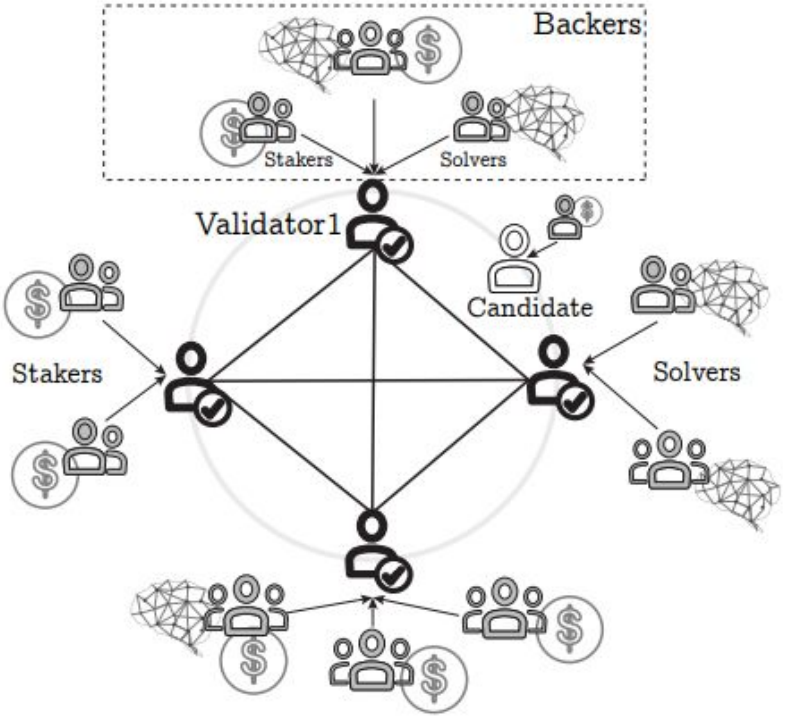
Process of the Representative Consensus Algorithm:-

1.Validator Nomination Process

Nomination is the process by which a node can register to become a validator to participate in representative consensus on Aion-1.Every node in the network can submit themselves as a candidate and pledge **backing** towards a candidate.**Backing** uses a hybrid model of proof of stake and proof of intelligence.

At the start of every term, the highest-backed set of candidates are selected to be the validators for this term.

Structural Representation:-



Process of the Representative Consensus Algorithm:-

2. Ranking

This is used to determine the nominated validators with the highest backing. This ranked list becomes the active set, which means that the validator node can contribute a vote towards the consensus process.

Process of the Representative Consensus Algorithm:-

3.Active Set

The members of the active set are always the highest backed candidates. To facilitate this continuous backing process, there are two copies of the nomination contract at any point in time.

The **live set** is updated as network users back or withdraw their backing from the candidates.

The **static set** exists only for the duration of the term.

The consensus protocol derives its active set from the static set. At the end of every term, the static set is overwritten with the live set for the duration of the next term.

Process of the Representative Consensus Algorithm:-

4.Term

Terms are a defined duration of time that a static set is used by the network for purposes of BFT-based consensus. In each term, a static set of validators validates new blocks. At the end of every term, the active set is frozen to generate a new static set based on changes in stake.

Process of the Representative Consensus Algorithm:-

5.Backup sets

The backup sets compose the candidate validators that are active, but are not on the active set. The backup set are the next highest backed validators. In the event of malicious behaviour or inactivity, the network looks towards this set for replacement validators.

Fee Distribution

Bridge validators are rewarded from interchain transaction fees and potentially a portion of block rewards.

Distribution models for external fees

- The sender of an interchain transaction specifies how the fees are distributed between bridges and the connecting network.

- The sender only specifies the total fee and the bridge and connecting network shares this fee based on agreements or hard-coded protocol.

Validator-backer rewards distribution

All users are required to present a certain amount of stake towards the network to be considered a candidate validator.

Tiered active set

Within the active set, the validators will be organized in a tiered structure. The tiered structure is ranked based on backing, in descending order, from the highest-backed validator to the lowest.

Tiered active set

Validators will compete to receive higher backing, and backers will benefit from backing validators, but only up until they are better compensated through diversifying their backing, including backing inactive validator.

Table depicting the reward amount (%) and voting power (%), per individual validator within that tier

Tier	Validators	Rewards/Validator	Voting Power/Validator
1	10	2.5%	1%
2	20	1.25%	1%
3	30	0.83%	1%
4	40	0.625%	1%

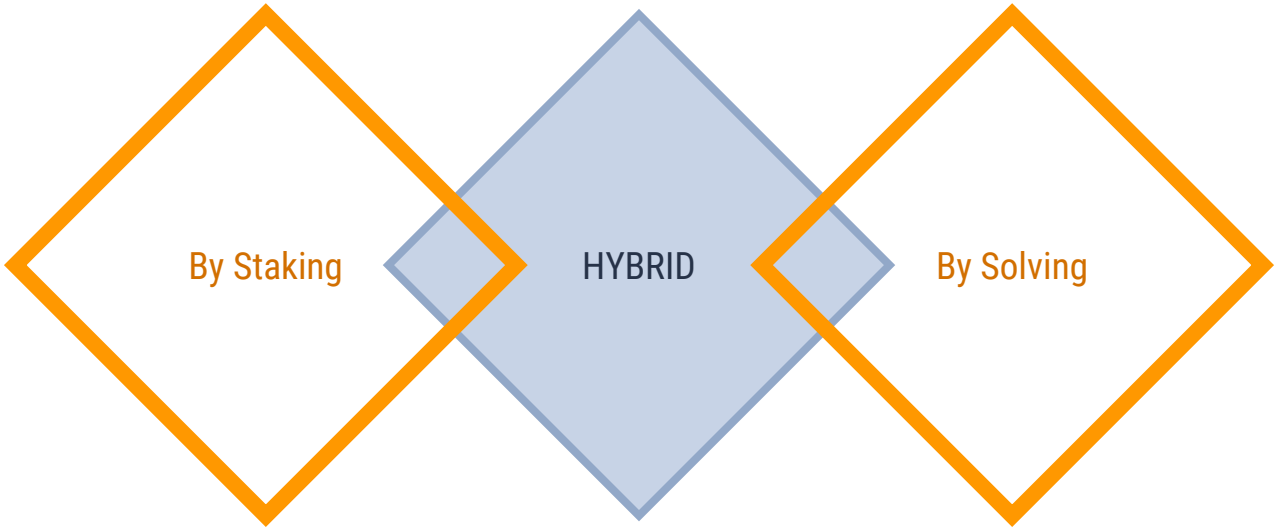
BACKING

The backing algorithm is broken into two distinct categories:

- ➔ Backing by staking
- ➔ Backing by solving

which are used to **determine the rank** of a validator, as well as the **proportion of rewards** given to a backer.

WAYS OF BACKING



BACKING BY STAKING

- ➔ Staking the tokens towards a particular validator.
- ➔ During a term, a user's staked tokens are **escrowed** by the network until the end of term,(provided no malicious actions have occurred) tokens are returned to the user.
- ➔ **Renewing the stake** refers to the backer keeping the stakes with the same validator. but these stakes have a **half life** to encourage liquidity and maintain competition between validators.
- ➔ For staking, backer receives a portion of the validators reward, reward is proportional to the amount staked.
- ➔ However, staking-based network creates a centralization of monetary value, thus backing by solving is needed.

BACKING BY SOLVING

- ➔ Solving a cryptographic puzzle.
- ➔ A unique puzzle is generated per request and the puzzle must be solved through the proof-of-intelligence algorithm.
- ➔ Proof is then submitted to the network as **proof of an amount** of backing for a particular validator.
- ➔ Solvers are rewarded proportionally to the amount backed.


Now?
PROOF OF INTELLIGENCE

Proof Of Intelligence

Solvers in AION-1 is to perform Artificial Intelligence(AI) computation which motivate the creation of AI-specific or specialised hardware that could be used for Machine Learning and Neural Network training in future.

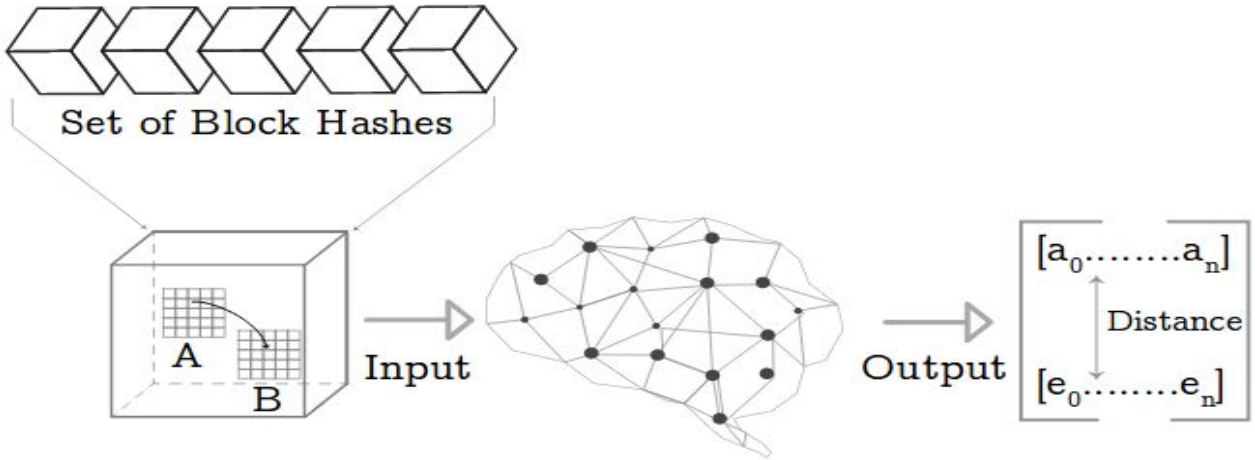
Mechanism

The proof of intelligence works by requiring participants to train a predefined neural network so that it will output similar results to the proposed ground truth (e.g., the hash of current block given the hashes of previous N blocks as input.)

Validation

- ➔ Load the neural network as defined by the provided parameter vector.
- ➔ Feed the neural network with the hashes of previous N blocks.
- ➔ Run and collect the outputs.

Proof Of Intelligence



Overview of the Proof-of-Intelligence

BACKING AS A FUNCTION OF STAKES AND SOLUTIONS

- ➔ Certain distribution of stakes and proof-of-intelligence is needed.
- ➔ Ratio is currently arbitrarily designed to be 60/40 for stakes and proof-of-computes.

INCENTIVES

- ➔ The proposed system is designed to **discourage** bad actors or actions. However, some events may occur.
- ➔ The validator will be **demoted tiers or removed** from the active set preventing participation in consensus
- ➔ **Preventing any rewards** for validators and their backers.
- ➔ Bad actors will be identified by the network, and through the validator's decrease in reputation and backing, they receive feedback immediately and **make corrective actions or are removed** from the active set.

INCENTIVES

Duplicitous Actions

- ➔ Punished by **locking all stakes** submitted by validators for a period of time and by removing him from consensus. Their backers are also punished.
- ➔ Stakers are punished by **locking their stakes** for an extended duration.
- ➔ Solvers are punished by the removal of the validator from consensus, thereby rendering their proof-of-intelligence solutions invalidated.

Inactivity

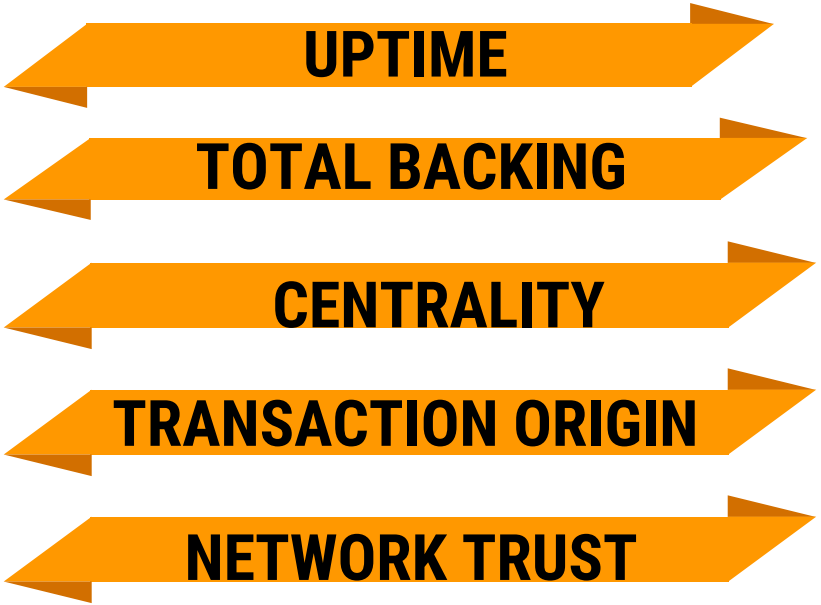
- ➔ **Demoting** validators in the tier system.
- ➔ If the inactive validator is at the lowest tier level, they are immediately dropped from consensus.

Incentive

	Previous Tier	New Tier
Member 1	1	Removed
Member 2	2	1
Member 3	3	2
Member 4	4	3
END ACTIVE SET		
Member 5	Candidate	4

REPUTATION

- The responsibility of selecting the **optimal validator** nodes is of network.
- It is achieved by observing past behaviour of candidates and active validators.
- Features that could be included in node reputation include:



AION Virtual Machine

The AVM provides the infrastructure for one of the primary functionalities of the connecting network, allowing the abstraction between the blockchain and application-specific logic and paving the way to powerful interchain applications.

Implementation

Implementation requires:

- **Performance**
- **Stability**
- **Determinism**
- **Compatibility**
- **Tooling**

References

- https://l.facebook.com/l.php?u=https%3A%2F%2Fdrive.google.com%2Ffile%2Fd%2F154ly0TKtBr36eSGdaQsT83NXLS5fIhb0%2Fview%3Fusp%3Dsharing&h=ATPFvGOe-De5iZAJG3UInBiYHJh-uarKWktOm_uKRDQrBPTk-WqLqm2Z_CSps4ocT7dV_0pOUP0StQcdYCbALWnyIj9l9sUFDCaQew_yjN1DPg

Presented by :-

- ICM 2015 003
- ICM 2015 501
- IIT 2015 504
- IIT 2015 119
- IIT 2015 105
- IIT 2015 059