Tọ̀rọ̀Net Decentralized Consensus System

A Community-Oriented Consensus Scheme Formulated to Deliver Low Cost, Fast, and Highly Scalable Transactions

V1: July 2021
V2 Revision July 2023

Ver 2.0

Table of Contents

1.0 Introduction 3

2.0 Review of Existing Consensus Systems 3

2.1 Proof of Work 3

2.2 Proof of Stake 4

2.3 Voting Based Consensus 6

2.4 Proof of Authority 7

2.0 Security of a Core Blockchain 9

2.1 Blockchain Core Foundation is in its Cryptographic Primitives 9

3.0 Toronet Consensus System 11

3.1 Details of the TọrọNet Consensus System 11

3.1.1 Types of Nodes on the Network 12

3.1.2 PoS Rules of the Network 13

3.1.3 PoA Rules of the Network 14

3.2 Comparative Review of Validator Incentives 15

3.2.1 Some Potential Exploits of the System and Their Mitigation 17

4.0 Recent Slight Modification to the Toronet Consensus System 18

4.1 Utility Validator Rules 18

4.2 Effect of Adding Utility Validators to the Network 19

4.3 Conclusions 19

References 20

1.0 Introduction

The consensus scheme is at the heart of every platform built on delivering decentralized transactions. The scheme determines how the platform as one selects, transmits, evaluates and agrees on the validity of such transactions. In order to describe the consensus algorithm that Toronet is based on, a review of prevalent consensus algorithm is presented in the first section. These schemes are then analyzed based on their merits and challenges. A detailed description of the Toronet algorithm is then presented, including how it maintains the security of the network while delivering low cost transactions at high speed, instant transaction finality, and at a large enough scale to potentially power micro-transactions in our communities.

2.0 Review of Existing Consensus Systems

Most of the prevailing consensus system for public blockchains fall into four broad categories:

- Proof of Work
- Proof of Stake
- Voting Based and Byzantine Formulations
- Proof of Authority

2.1 Proof of Work

Proof of Work (PoW) is a consensus mechanism used in blockchain networks to achieve distributed consensus and validate transactions. In a PoW system, participants, often called miners, compete against each other to solve complex mathematical puzzles. The first miner to solve the puzzle earns the right to add the next block to the blockchain and is rewarded with newly minted cryptocurrencies.

Here is a breakdown of how a typical PoW system works:

1. Puzzle Generation: The network generates a cryptographic puzzle that miners must solve. The puzzle is designed to be computationally expensive and requires significant computational power to find a solution.

2. Mining Process: Miners utilize their computational resources, typically in the form of specialized hardware called mining rigs, to attempt to solve the puzzle. They repeatedly hash the data in the block they want to add to the blockchain, combined with a random number known as a nonce, until they find a solution that meets certain predefined criteria.

3. Difficulty Adjustment: The difficulty of the puzzle is adjusted periodically to maintain a consistent block generation rate. As more miners join the network, the difficulty increases to ensure that blocks are not added too quickly, and vice versa.

4. Proof of Solution: Once a miner finds a solution that satisfies the puzzle's criteria, they broadcast it to the network. Other miners can quickly verify the solution by applying the same hashing algorithm and confirming that the solution is valid.

5. Block Addition: The miner who successfully solves the puzzle adds the new block to the blockchain, including the verified transactions. This block becomes part of the blockchain's permanent record.

6. Incentives: Miners are incentivized to participate in the PoW system through block rewards, typically in the form of newly minted cryptocurrencies, and transaction fees paid by users who want their transactions prioritized.

7. Longest Chain Rule: In the event of multiple miners finding valid solutions simultaneously, temporary forks may occur, resulting in multiple competing blockchain branches. The network follows the "longest chain rule," where the chain with the most accumulated computational work (the longest chain) is considered the valid one. Miners then choose to continue mining on the longest chain, further securing the network.

The PoW system provides security to the blockchain network by making it computationally expensive to reverse transactions. However, it has drawbacks including high energy consumption due to the intensive computational requirements and the centralization of mining power in the hands of those with significant resources. It also makes transactions expensive on networks predicated on POW since the incentives that must be provided to validators to compensate for the electrical and computational resources expended. **In short, the mining rewards must exceed the cost of running a node or sufficient numbers of nodes may not participate if they do so at a loss.**

Examples of chains that utilize PoW schemes include Bitcoin, LiteCoin, Bitcoin Cash, and Monero. However, the trend appears to be towards more recent blockchains moving away from PoW systems due to it’s power requirement.

2.2 Proof of Stake

Proof of Stake (PoS) is a consensus mechanism used in blockchain networks to achieve agreement on the state of the blockchain. Unlike Proof of Work (PoW), where participants solve complex mathematical puzzles to validate transactions and create new blocks, PoS relies on the concept of "staking" or "bonding" tokens to participate in the consensus process.

In PoS, participants (also known as validators or stakeholders) are chosen to validate transactions and create new blocks based on the number of tokens they hold and are willing to "stake." The likelihood of being selected as a validator is proportional to the number of tokens staked. The more tokens a participant stakes, the higher their chances of being selected.

To understand how PoS works technically, we can use the following equations:

1. Validator Selection Probability (P):

$P = (S / T) * 100$

where:

- P is the probability of being selected as a validator.
- S is the number of tokens staked by a participant.
- T is the total number of tokens staked by all participants.

This equation calculates the probability of a participant being chosen as a validator based on the ratio of their staked tokens to the total staked tokens in the network. It is represented as a percentage.

2. Block Creation Reward (R):

$$R = (S / T) * B$$

where:

- R is the reward for creating a new block.
- S is the number of tokens staked by a validator.
- T is the total number of tokens staked by all validators.
- B is the total block reward available for distribution.

This equation determines the reward a validator receives for creating a new block. The reward is proportional to the number of tokens staked by the validator, relative to the total staked tokens in the network.

3. Validator's Staked Tokens (S'):

$$S' = S + R - E$$

where:

- S' is the updated number of tokens staked by a validator.
- S is the initial number of tokens staked by a validator.

- *R* is the reward received for creating a new block.

- *E* is the amount of tokens voluntarily "unstaked" or "unbonded" by the validator.

This equation calculates the new stake of a validator after receiving the block creation reward and possibly unstaking some tokens. Validators can choose to unstake their tokens voluntarily or due to penalties for malicious behavior.

These equations illustrate the technical aspects of PoS, where validators stake their tokens, are rewarded for creating blocks, and can adjust their stake by adding or removing tokens. The probability of being selected as a validator and the block creation rewards are determined based on the staked tokens of each participant relative to the total staked tokens in the network.

Although PoS systems have been around for some time, the schemes have not been as widely tested on large networks compared to PoW systems. Where the PoS chain includes smart contract functionality, and the existence of multiple independent tokens, many of them with significant value, one questionable aspect of PoS systems is that the selected stake for these systems has not considered the value of the tokens also embedded in the blocks. It is conceivable that a node could create a block whose value in auxiliary tokens could exceed 10x or even 100x the value of the native tokens within the block. **Essentially, nodes could create blocks whose value exceeds their stake several fold putting into question how the stake secures such activity, or how the slashing penalty provides enough deterrence, even where the only malicious route is via a double spend.** Even when the nodes are randomly selected, it does not seem that the staking arrangement might present sufficient deterrence from the actions of a malicious node.

Examples of chains that utilize PoS schemes include Ethereum, which switched to PoS in 2022, less than a year ago from the date of this writing. Other chains utilizing PoS systems include Polkadot, Cardano, Tezos, and Cosmos.

2.3 Voting Based Consensus

Voting based consensus systems achieves consensus by requiring a certain proportion of nodes vote to agree on a block proposed by one of the nodes participating in the network. The Byzantine General's algorithm is the most popular of voting consensus systems, and is described here.

Byzantine consensus algorithms are a class of algorithms designed to achieve consensus in distributed systems, where some nodes may act maliciously or fail. The most well-known Byzantine consensus algorithm is the Byzantine Fault Tolerance (BFT) algorithm.

In a Byzantine consensus algorithm, a certain threshold of correct nodes is required to agree on a value before it is considered as the consensus value. This threshold is determined by the number of faulty or malicious nodes in the system. The Byzantine consensus algorithms aim to achieve safety and liveness properties, ensuring that the agreed-upon value is correct and that the algorithm terminates.

One popular Byzantine consensus algorithm is the Practical Byzantine Fault Tolerance (PBFT) algorithm. PBFT works by having a designated leader (or primary) who proposes a value to the other nodes in the

system. The other nodes, called replicas, receive the proposal and perform a three-phase protocol to agree on the proposed value. The three phases are the pre-prepare, prepare, and commit phases.

The equations and probability foundation of Byzantine consensus algorithms can be understood through the analysis of their fault tolerance capabilities. Let's consider the PBFT algorithm as an example.

Assuming there are N total nodes in the system and f is the maximum number of faulty nodes, the equation to determine the threshold of correct nodes required for consensus in PBFT is given by:

$$2f + 1 \leq N$$

This equation ensures that the number of correct nodes is greater than or equal to the number of faulty nodes, ensuring that consensus can be reached.

The probability foundation of Byzantine consensus algorithms lies in the assumption that the faulty or malicious nodes behave arbitrarily and independently. This assumption allows for the analysis of the probability of successful consensus. By modeling the behavior of faulty nodes probabilistically, one can determine the probability of a successful consensus based on the number of faulty nodes and the total number of nodes in the system.

Overall, Byzantine consensus algorithms like PBFT provide a robust and secure approach to achieving consensus in distributed systems, even in the presence of faulty or malicious nodes.

Byzantive consensus systems tend to have fewer number of nodes compared to PoW and PoS systems. As a result, they can also potentially operate at faster speed since information and new blocks can be transmitted through the network comparably faster. They can also operate at lower cost, since they do not need to secure the network by simply expending computational resources. Critics of Byzantive systems contend that the fewer number of nodes could lead to nodes banding together or exhibiting cartel behavior that could include censorship of some participants of the network or to further the interests of a few.

Examples of chains that utilize Byzantine schemes include Libra, Ripple, Hyperledger Fabric, Hedera Hashgraph, Tendermint, Tron, EOS, Solana, and Avalanche.

2.4 Proof of Authority

The Proof of Authority (PoA) consensus algorithm is a type of consensus algorithm that relies on the identity and reputation of certain nodes, known as authorities, to validate transactions and achieve consensus. In PoA, the consensus is reached based on the identities of the authorized nodes, rather than through complex computations or mining.

In a PoA consensus algorithm, a set of pre-approved authorities is chosen to validate and add new blocks to the blockchain. These authorities are typically known and trusted entities, such as reputable organizations or individuals. The consensus is achieved when a majority of the authorities agree on the validity of a block.

The equations and probability foundation of the PoA consensus algorithm can be understood in terms of the voting power and majority threshold. Let's consider a simplified example with *N* total authorities and *m* malicious authorities. In order to achieve consensus, the equation for the majority threshold is:

$$N - m > N/2$$

This equation ensures that the number of non-malicious authorities is greater than half of the total authorities, ensuring a majority. The probability foundation of the PoA consensus algorithm lies in the assumption that the malicious authorities cannot collude or coordinate their actions. This assumption allows for the analysis of the probability of successful consensus based on the number of malicious authorities and the total number of authorities.

In reality, the authorities are usually selected by the users of the network via a voting or delegation system, or more recently a decentralized autonomous organization (DAO) tasked with ensuring the sustainance of the network. Game theory would indicate that users of the network will collectively select authorities that would not act in compromising the network. In short, trust and reputation of the authorities play a crucial role in the security and reliability of the PoA consensus algorithm.

PoA systems are usually fast since the number of nodes are typically smaller than PoW and PoS systems. The smaller number of nodes ensure that nodes are transmitted very quickly across the network allowing for faster transaction times. Due to the fact that nodes are not usually in competition, the need for huge computational resources to secure the network does not exist. As a result, PoA systems potentially can operate networks with relatively lower transaction costs than systems that engage huge number of nodes.

Critics of PoA systems contend that it is more centralized because of the relatively fewer nodes, or that nodes could band together and exhibit cartel-like manifestations including potential censorship of participants on the network. The antidote to this would like in the manner in which the network and its community selects such nodes. With sufficient independence, and selection of nodes with high reputational stakes, creation of well developed constitutional processes that are also enforced by code, proponents of PoA systems believe an autonomous set of nodes can be selected to operate a network with sufficient fairness and independence sufficient to protect the network and the communal interest of all it’s participants.

Examples of chains that utilize PoA algotithms include Vechain, Xinfin, and several private Ethereum-based chains.

2.0 Security of a Core Blockchain

Prior to detailing the TọrọNet consensus system (TSC), it would be instructive to review the potential attack vectors to a blockchain. This is so that subsequent discussion on how the TSC mitigates any such vector becomes clear, as well as the roles of the nodes in securing the network.

2.1 Blockchain Core Foundation is in its Cryptographic Primitives

Blockchains are intrinsically very secure formulations due to their cryptographic primitives. They are defined in such a way that every actor is represented by an address, which utilizes a private-public key pair. In this formulation, the owner or holder of a private or secret key is able to reveal a public key (or it's hash) to anyone on the network. The owner is then able to use the private key to sign any message to the network, where such message could be an instruction to transfer some amount belonging to that public address on a public ledger. (Note that the message does not need to correspond to a ledger, it could also be instructions to move or transfer ownership of some data associated with that address. Transferring ownership of data would be activity involving secured data such as a non-fungible token that could represent an offchain digital artwork, or a physical land or property, for instance.)

Anyone on the network presented with the message can use that public key to decode the message and recognize that it is a legitimate message which only a holder of a private key corresponding to that address could have generated. This is a powerful concept because even custodians and owners of such a network, be it a single party or a decentralized entity, can not create that message without having that secret key. (Note that this property is also shared by non-public chains, including private chains and even central bank digital currencies CBDCs). As a result, not many exploits are actually available in compromising the core workings of a blockchain developed based on this formulation. However, a few tangential exploits remain available to an actor with intent to subvert the network. These are detailed below:

1. Doublespend Attack: Since blockchain transactions and modification of data tied to any address can only be initiated by the owners of the address, the main direct transaction related attack is a doublespend. This can be deployed by a malicious node creating a transaction using their own address to another, for instance. After the transaction has been honored by a recipient, if somehow the node could reverse the blocks to prior to that transaction, then the node could create another transaction spending the same account. Note that the attack would not be possible without somehow reversing the blocks back because the computational rules or the network would normally not allow a double spend since the balance would no longer exist following the first spend. As a result, a doublespent attack requires one of the other two attack vectors below – where the node has sufficient computational resources or controls or colludes with other nodes to permit the reversal of blocks – and effectively their desired transaction.

2. 51% Attack: In a PoW blockchain, if a single entity or a group of colluding miners controls more than 50% of the network's mining power, they can potentially manipulate the blockchain. They could reverse transactions, double-spend coins, or halt the network's operations. For several BFT algorithms such as the PBFT, the threshold is 1/3 of nodes banding together that could allow a double spend.

3. Collusion of a Plurality of Nodes: Similar to the 51% attack, if a sufficient number of nodes collude, or one or several nodes gains overwhelming computational resources or staking resources in the case of PoS systems, they could control the network sufficient to initiate a double spend attack.

4. Future Quantum Computer Decryption Attack: In future, it is believed that quantum computers would be developed that can decrypt current encryption algorithms. This is not an exploit that exists today. Cryptographers believe that new algorithms will also evolve that advanced computers of that time will not be able to decrypt.

5. Phishing of Keys and Other Offchain Key Compromise Attacks: There are entities that have developed whose entire activities consists of seeking ways to obtain the secret key of users. This includes phishing attempts such creating clone or fake websites and applications to induce users into sending their keys to them. Private keys are not intended to ever be stored in or sent to a blockchain, so these types of attacks are offchain, can not be influenced much by the consensus system, and are included here for completeness.

6. Smart Contract Exploits: These are separate additional exploits opened up by smart contracts. They are not core blockchain attack vectors and are not usually influenced by the consensus scheme.

Based on the foregoing, the overwhelming focus in assuring security of a blockchain is ensuring that there is a plurality of nodes that are independent, will maintain the integrity and expected functioning of the network, and that computational resources are not concentrated with few nodes, or in the case of PoS systems that a few nodes do not have majority of the stakes to ensure that they get to write majority of the blocks. This objective needs to be balanced against a need for the network to operate at a high capacity and at a high speed. (The blockchain trilemma refers to a balance between scalability, security, and decentralization whereby an enhancement in one would usually result in a tradeoff in the one or the other.) In the next sections, the design of the TSC towards achieving this balance is described.

3.0 Toronet Consensus System

The consensus system devised for Tórónet is a hybrid and modified Proof of Stake, and Proof of Authority system. The rationale behind our design principle are similar to the that of the entire platform – which is one devised to actually be usable in communities not well served by the traditional financial system. The focus is on having a chain with low transaction costs that will allow projects in our communities to develop and thrive, fast transactions, high capacity, and related to low cost is the ability to sustain microtransactions. For this reason, blockchains utilizing proof of work, or other schemes that imposes computational penalties, or deliberately slows down the network to secure it, or needs to provide a huge reward to validators as compensation will not be sustainable. The cost per transaction would exceed the average cost of transactions in underbanked communities, or will exceed the average value of microtransactions.

Similarly, PoS, PoA, and other public consensus systems that rely on significant miner rewards will also not be viable in the long run. The Tórónet consensus system combines the merits of PoS and PoA systems, while reformulating them to address some of the identified short-comings listed in the prior section.

The details of the modifications devised in our consensus system, and the overall formulation is described in detail here.

3.1 Details of the TọrọNet Consensus System

In the TọrọNet consensus process only trusted validators are accepted in the network to write blocks. Transaction processing nodes are approved nodes with deposits or contribution into the reserves. All blocks have instant finality based on this algorithm and are irreversible once accepted by all nodes.

To ensure that the stake is predicated on the value of transactions in the blocks, the algorithm limits the total transaction value that can be mined by any node within a span of time to be no greater than the value the node operator has invested in reserve (staked value.) Using this model, node operators can be trusted to produce blocks without requiring them to run expensive calculations.

Nodes may only create a block whose total transaction value is less than the stake of the miner's account in the reserves:

$$\sum_T |\Delta V_m| < \sigma_m \tag{1}$$

where ΔV represents the total value of transactions written by a miner, m, within T time period, and σ represents the stake the miner has in the network. The settings for the network are as follows:

- Transaction time is set at 2 seconds.
- The time, T is taken as 24 hours. This allows the community, and other observer nodes sufficient time to flag any transactions generated by a node and invoke proof of stake penalties, if needed.

Besides the fact that nodes are all vetted, this ensures that nodes will not create rogue transactions since they will simply cover any such transactions with their own stake and possibly also lose validator status.

The Association via the DAO is able to review the network risks and set the staking (membership) to reflect the risk. Such changes will apply to future nodes.

The following sub sections describes the rules for the nodes of the network, the details the rules and modification made to traditional PoS systems, PoA systems, and then the DAO which is necessary for essentially overseeing the parameters of the system.

3.1.1 Types of Nodes on the Network

There are two types of nodes in the network:

1. Validator Nodes – these nodes can create new blocks consisting of transactions submitted to the global memory pool. Validator nodes have the authority to create such blocks, and are selected by the community via the DAO. Validator nodes will typically be organizations whose reputation are such that there is greater risk to their standing than any potential rewards from intentionally compromising the network. Validator nodes are subject to the following rules:
    a. The network is limited to 25 validators – this ensures the network can operate at high speed and capacity.
    b. They are selected by majority votes of the DAO. There is no delegation or means to reward members who vote to select a node – removing the prospect of vote buying. The game theory expectation is that the community will eventually select majority of nodes that will serve and secure the interests of the community.
    c. Validators do not get to mint tokens or receive rewards related to the core blockchain tokens. In other blockchains where validators get to mint new tokens, the inflation represents a cost to the network that gets passed on to the community.
    d. Validator nodes need to be affirmed annually by DAO votes in case there are changes to their standing within the community over time.
    e. Validator nodes receive a portion of the transaction fees from the network. Whereas there is no minting of core blockchain tokens, where project tokens charge fees on the network, a portion of the fees is provided to nodes and equally shared by all nodes regardless of computational power, or stake. This ensures that a node or few nodes will never be able to gain control of the network or disrupt the instant block and transaction finality designed with the TSC.
    f. Validators are expected to be independent, disparate, and unconnected, to ensure decentralization and reduce the chances of collusion among nodes. Examples of potential validators include a mix of major reputable projects on the platform, non-governmental organizations, governmental institutions, traditional financial institutions, possibly Corporations that provide valuable services within the community, and utility providers. The selection of validators is completely left to the DAO and ultimately to the community based on its votes.

2. Observer Nodes – anyone can set up and join the network as an observer. Observer nodes do not create any blocks but can check the validity of blocks. There are no rewards for setting up an observer node, and there are no limits to how many observer nodes can join the network. Observer nodes extend the number of participating nodes in the network without necessarily slowing down the network, or increasing the cost of transactions. Indeed, there are organizations, businesses, and

members of the community that are willing to provide computing resources to the platform just like there are community contributors on community-oriented projects. Such community contributions can be found in projects that predate blockchains, for instance the Wikipedia project.

3.1.2 PoS Rules of the Network

The following are the rules of the PoS system on the network, with emphasis on some of the modifications compared to traditional PoS systems:

1. The value of transactions in a block includes the values of project tokens within the network. While any project can technically build on the platform, the community via the DAO does vote on projects that are listed in the community App repository. This allows the community to weed out or refuse to platform projects of little to no value. This also allows a block's value to be computed more accurately based on the value of community vetted projects on the network.

   Compared to other PoS systems, the true value of blocks in comparison to the stake within the network is thus reflected closer to reality.

2. All validators are required to provide the same amount of stake on the network.

3. The current staking requirement for validators is 30,000 governance tokens.

4. The DAO is responsible for maintaining the parameters of the network based on ongoing operations. For instance, the duration for *T* may be reduced, or the required stake may be increased if the value of transactions begin to exceed the stake behind the network.

5. All validators share equally from the same portion of the transaction fees provided to validators, regardless of how many blocks each creates – there is no competition between nodes. Besides, the probability that any node will submit a block of transactions is roughly equal so the count of blocks per validator does not vary by much.

6. Validator nodes also receive governance tokens that enable them to participate in the governance of the network. Each validator node receives 70 governance tokens daily, for a potential total of 25,550 governance tokens each year. The daily governance token allocation is halved following the second and fourth year, after which it remains constant until allocation for transaction processing is completed. This is programmed into the governing tokens contract code ensuring confidence in the system for participating nodes. The consensus smart contracts allocates the governance nodes to each participating node daily, and nodes must have generated at least 80% of the number of expected blocks for the contract to initiate the allocation.

   The potential annual governance tokens accruing to nodes is shown below:

Year	Daily Allocation	Yearly Maximum
1	70	25550
2	70	25550
3	35	12775
4	35	12775
5	17.5	6387.5
6	17.5	6387.5
7	17.5	6387.5
8	17.5	6387.5
	Total	**102200**

7. The amount of governance tokens allocated to validator nodes is 3.5m governance tokens, ensuring governance tokens will continue to provide incentives to validators least the first seven to ten years of the network, if all 25 validator slots are engaged throughout the period. Following this early period, it is expected that transaction fees would be sufficient to provide incentives to have validators join, besides the community service interest of some of our validators.
8. Validators can exit the system at any time, or are also programmed within the system to lose status if they do not maintain sufficient uptime in generating at least 50% of the expected share of blocks on the platform. Validation stakes remain in the system once committed to the platform.

3.1.3 PoA Rules of the Network

The following are the rules of the PoA system on the network, with emphasis on some of the modifications compared to traditional PoA systems:

1. The DAO selects the validators of the network by community votes.

2. Validators are rule prohibited from contacting members of the community or to engage with or encourage anyone to support their selection beyond submitting a publicly available summary of their profile and potential merits in serving the community as validators.

3. There is no delegation of governing tokens used for voting or admitting validators.

4. Validators must be reputable organizations of significant size and reputations that make the chances of any malicious conduct on the network highly unlikely in comparison to their own existing reputations within the community and without.

5. Validators that do not maintain sufficient uptime to produce at least 50% of their expected block contribution to the network, over a three-month span will have their slot put up for replacement by the DAO.

6. Validators must be independent and drawn from different sectors of the community. The DAO, through the Toronet Association is tasked with flagging any dependency between potential validator applications and existing nodes, and can raise a DAO vote to disqualify such applications.

7. The DAO is not able to censor any fully completed validator application but reposes the decision to the community via votes based on the governance tokens of the network.

3.2 Comparative Review of Validator Incentives

In this section, we compare the incentive and reward systems for the TSC to that of several prominent blockchains, and to traditional financial institutions. The main incentive for committing resources to the network to run it and create blocks, is the transaction fees that accrues to validators. Both traditional financial system and blockchains have transaction fees to cover the cost of transactions. However, at the start, there are little to no transaction fees, and in a decentralized system, there needs to be an incentive to ensure that sufficient number of validators join the network.

The means by which categories of blockchains incentivize this decentralized participation is included in the table below, as well, as compared to the TSC method.

Platform or Organization	Incentives and Coverage of Transaction Costs During the Startup Phase
Traditional Financial system	Traditional financial institutions typically have investors and venture capitalist, or broadly shareholders, who fund the organization until the volume of transactions become sufficient and the transaction and service fees exceed the cost of transactions. The end goal eventually is for the network to be operated successfully based on its fees and service charges.
Bitcoin and Blockchains with Time Limited Token Issuance or Transitional Minting	Transaction costs are also covered by fees. However, in the initial stages, the blockchain also mints new Bitcoins or tokens to reward transaction processors or validators. The value of those tokens compensates validators or miners beyond the transaction fees. This is almost akin to programmatically issuing ownership of the network, like shares to miners working on running the network. However, the cost of transactions is significant due to the chain's consensus system. The rewards to miners must exceed this cost or the system could lose its decentralized number of miners. In fact, there are instances, during which the value of those tokens threatens to drop below the cost of creating blocks. (Example here: https://beincrypto.com/bitcoin-miners-will-go-broke-if-btc-price-falls-below-this-level/) And there is the question of what would incentivize miners when all Bitcoins are issued. With each reduction in the incentives, the design and its similarity to a break-even mechanism becomes more poignant, especially when considering its effect on the cost of transactions. (Example: https://www.coindesk.com/business/2023/06/07/bitcoin-halving-is-coming-and-only-the-most-efficient-miners-will-survive/) In addition, the halving every few years has similar effect to the reducing upside of series participant in a startup.

	Rewards or minting of new Bitcoins are designed to end. So essentially, similar to traditional systems, the end goal is for the network to operate based solely on its transaction fees. What is notable is that Satoshi designed this incentive to end in 2140. Usually, design features have a purpose. The question is if it was expected that the network would need 130 years to transition to one operating and breaking even on transaction fees alone. (https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/.) Curiously, it would be unlikely given this long transition period, that the designers would be around to resolve and assure the viability of this arrangement. Given the powers of ingenuity and technology, it is not implausible that the network can one day truly operate based on fees alone, without the fees been too prohibitive to make its transactions viable – but it might take a century to find out.
Blockchains with Perpetual Minting Mechanisms	Similar to transitional minting, some blockchains such as Ethereum mint new tokens as rewards to transaction processors. Unlike the above category of blockchains, this arrangement is not designed to end. The design does not anticipate that the chain would ever run on fees alone. Similar also to transitional mining rewards, the issued tokens have demand in their use for transaction fees. As such, mining rewards gain value ostensibly from the demand for those tokens, or use of the network, long term. However, in the short term, the relationship has a potentially perverse effect on the affordability of transaction fees. The gas or transaction fees are based on the same tokens issued by the network, so when ETH gains in demand, and value, transaction fees go up and vice versa. The more successful the network becomes, the more expensive its fees, which potentially leads to a success penalty. For instance, as recently as September 2021, the average fee on the network was USD 9. It is currently about USD 1-2. The variance within the transition period might not augur well for real world projects with true economic activity and businesses operating on such a platform. Also, issuance rate of ETH affects transaction fees. As the chains have operated and reviewed the trends, adjustments and improvements have been proposed to improve the issuance. EIP1559 is one such adjustment. https://eips.ethereum.org/EIPS/eip-1559. Long term, it appears that an end steady state or equilibrium would be reached where the rate of issuance and burning is steady, the value of ETH reaches some stable value, and the rewards earned by miners added to the transaction fees always presents sufficient incentives to keep miners on the network, and transaction fees affordable for users. The time it would take to reach such a steady state is not that determinable but is already nearly a decade in the making.
TSC Transaction Processor Rewards	TSC like with transitional financial systems and also the Bitcoin network has an end goal of services operating based on transaction and service fees. To reach the end state, governance tokens are provided as rewards to transaction processors, as described in Section 3.1. However, the network is also designed to achieve this end state within 5 years. As such the incentives will end after the fifth years in the extreme scenario. By

	that point, any new validators are expected to join a network that generates sufficient fees to reward its operators. To enable such an arrangement, the network had to be designed with very low transaction costs, as described in 3.1. In addition, TSC decoupled the transaction fee medium from the rewards medium, similar to traditional financial system. The core chain's tokens is a stablecoin – the Toro. Fees are paid in Toros, which ensures they remain stable and predictable for participants on the network. Rewards, on the other hand, are provided as a governance token – ToroG. The governance token derives its demand from its utility: • in deploying smart contracts • determining governance of the network, and • is required in providing the stake by validator nodes. This arrangement removes the huge fluctuation in transaction fees witnessed on platforms which uses deflationary tokens as the fee medium of the platform.

3.2.1 Some Potential Exploits of the System and Their Mitigation

The following vectors can be identified whereby participants on the network could attempt to game the system. The manner in which the current design mitigates such risk is also identified:

1. The DoubleSpend Attack: In the current design, the usual blockchain double spend would be difficult to execute because all blocks have instant finality and are immediately irreversible. Ostensibly, the only reversion that could occur would be if over half of the nodes collude and decide to restart the chain from a past block. This is virtually unfeasible given the reputation of the validators, their independence, as well as their stake in the network. The protection from the doublespend attack is both from a PoA and a PoS mechanism. In addition, the PoS mechanism is based on a computation closer to the true value of the blocks being generated.

2. Validators could join the network, stay long enough to receive the maximum governance tokens allowed validators, then leave and reconstitute a new vehicle to potentially rejoin and collect a fresh allocation of governance tokens. This will be very difficult to engineer as much of the reputation of entities elected as validators would have been one built over years and represent entities known and trusted within the community.

4.0 Recent Slight Modification to the Toronet Consensus System

The TọrọNet platform has been operating its mainnet for over six months, and some of the parameters of the TSC are now analyzable in practical and operational terms. An observation based on operations is the communal thrust and strength of the network that has seen request by reputable organizations who wish to serve as validators at their own cost, and without requiring any rewards, simply to contribute positively to the community (This is similar to the Wikipedia model where participants donate their resources to the platform which they believe in, and serves their interest or community.)

This weighs more in the PoA side of the TSC, and prompted the definition of a third type of validator, in addition to those listed in 3.1.1. This type of validator are reputable nodes that serve as a validator but without providing the stake, nor receiving transaction fees or rewards accruing to staking nodes. This node type will be referred to as utility validators. Utility validators will tend to be entities that possess computational resources as a core service or a byproduct, and wish to provide it in service to the communities served by TọrọNet through the platform.

4.1 Utility Validator Rules

The detailed list of rules applied to utility validator are presented in this section.

1. Utility validators are purely PoA nodes – they are not required to deposit a stake in the platform.

2. Similar to other validators, utility validators are selected by the community via the DAO voting mechanism.

3. The number of utility validators in the platform will be roughly limited to no greater than a third of all validators, when adding a new validator.

4. Similar to other validators, utility validators may choose to cease validation of blocks at any time.

5. Utility validators receive seven governance tokens daily for participating on the network. For validators that do not wish to receive the rewards, the Association will create the address to which such allocations would accrue, and utilize this as part of its charter; for developmental initiatives in participating communities.

6. Utility validators are expected to provide sufficient computational resources to generate new blocks on the platform, using the shared communal node validation programs, but are not required. Where the resources provided by a node is insufficient, the node simply cease producing new blocks.

7. Any validator that does not provide sufficient resources or up time to reach 50% of their expected block contribution to the platform, over a three month time span, will be removed from the network by the validator program, and will have their validation slot replaced by the DAO.

8. Utility validators do not have any additional obligations to the platform beyond following the computational rules encoded in the TǫrǫNet node validation program, which programmatically accesses the transaction request pool, and creates new blocks from it.

4.2 Effect of Adding Utility Validators to the Network

Addition of utility validators allows the platform to broaden its base of validators to include highly reputable organizations that can provide decentralization, security, and reputation to the platform, but by policy might not have the mandate to participate in a rewards-based enterprise besides their own central charter. Besides the service they bring to the network, utility validator contributions to processing also extends the validator incentive years described in 3.1.2, potentially by a third. Thus, their addition is expected to benefit the platform and the community it serves significantly.

4.3 Conclusions

A detailed description of the TǫrǫNet consensus scheme is presented. The TSC combines the security of provided by decentralized reputable members of the community via the Proof of Authority System, with the security ensured by having validators also providing a collateral or stake in the system via the Proof of Stake system to develop a consensus system that is highly secure and decentralized, while delivering data and transactions at fast, low cost, and at a high capacity. The decentralization inherent in the scheme is further extended, similar to earlier public blockchains, by enabling a limitless number of observer nodes from the community to join the chain to review blocks.

In addition, modifications to the traditional PoS to more accurately reflect the true value of blocks being underwritten by validators in relation to their stake in the network is described. Finally, following mainnet operations for over a year, and receiving interest from highly reputable members of the global community in providing validator resources, the consensus system was expanded on the PoA side to include utility validators that bring their resources freely onto the platform to provide a service to the community.

References

1. Nakamoto, Satoshi (24 May 2009). "Bitcoin: A Peer-to-Peer Electronic Cash System" (PDF). http://bitcoin.org/bitcoin.pdf, Accessed May 20, 2017.
2. Vitalik Buterin, Sep 1 2014, “Ethereum Whitepaper: A Next-Generation Smart Contract and Decentralized Application Platform”, https://github.com/ethereum/wiki/wiki/White-Paper, Accessed May 30, 2017.
3. Ken Alabs, July 2020, “A 2020 perspective on “Digital blockchain networks appear to be following Metcalfe’s Law””, Electronic Commerce Research and Applications, Special 20 year issue, Volume 40 Issue C, March 2020, https://dl.acm.org/doi/abs/10.1016/j.elerap.2020.100939.
4. Ken Alabs, July 2017, “Digital blockchain networks appear to be following Metcalfe’s Law”, Electronic Commerce Research and Applications, Volume 24, July–August 2017, Pages 23–29 https://doi.org/10.1016/j.elerap.2017.06.003
5. The World Bank, March 4 2013, “Africa’s Agriculture and Agribusiness Markets Set to Top US$ One Trillion in 2030”, http://www.worldbank.org/en/news/feature/2013/03/04/africa-agribusiness-report. Accessed October 6, 2017.
6. Bitcoin Energy Consumption Index. Accessed May 20, 2017. http://digiconomist.net/bitcoin-energy-consumption
7. The Ideal Digital Currency Needs Scaling Solutions http://www.trustnodes.com/2017/11/05/ideal-digital-currency-needs-scaling-solutions
8. Jacob Dziadkoviec, October 2022, “Bitcoin Miners Will Go Broke If BTC Price Falls Below This Level,” https://beincrypto.com/bitcoin-miners-will-go-broke-if-btc-price-falls-below-this-level/
9. Eliza Gkritsi, June 2023, “Bitcoin Halving Is Coming and Only the Most Efficient Miners Will Survive,” Coindesk Publication. https://www.coindesk.com/business/2023/06/07/bitcoin-halving-is-coming-and-only-the-most-efficient-miners-will-survive/
10. Adam Hayes & Jeffery Brown, April 2023, “What Happens to Bitcoin After All 21 Million Are Mined?”, Investopedia Publication. https://www.investopedia.com/tech/what-happens-bitcoin-after-21-million-mined/
11. Buterin et. Al, Feb 2019, “EIP-1559: Fee market change for ETH 1.0 chain.” https://eips.ethereum.org/EIPS/eip-1559