Proof of Selection & Seligere: Going Around the Byzantine Generals

Kennie Jenkins
kennie.jenkins@cyberspec.net

July 7, 2018

Abstract:

A consensus algorithm in the most general form is a method in which decentralized nodes (e.g., computers, virtual machines, devices) come to an agreement on what data is added to a digital ledger. Consensus algorithms are often conceptually related to defeating the Byzantine Generals' problem: How can multiple generals agree on a plan of attack without being able to reliably communicate with each other while having possible traitors sending false messages?

This can be done with something less resource-intensive than Proof of Work, something more balanced than Proof of Stake, something without a centralized coordinating process (Tangle Coordinator), and something that is not proprietary (Swirlds). Proposed instead is Proof of Selection, which involves building a digital ledger with an agreed upon method of 'selecting' the next nodes to create a block. A consensus is pre-determined; it is akin to planning a time to attack or retreating and defining a method of detecting traitors before being separated and going to the battlefield.

Problem set 1: Define a new consensus algorithm called Proof of Selection that does not require mining, has equal block publishing rights that are not based on stake, and no centralized coordinating processes.

Problem set 2: Provide a new digital ledger infrastructure, called Seligere, based on Proof of Selection to achieve a more efficient method of decentralized currency, storage, data transactions, and research. Nodes must have the ability to customize processing and storage usage.

Problem set 3: Integrate Proof of Selection into existing digital ledger technologies needing better scaling or more decentralization.

Introduction

As of June 2018, it is estimated that cryptocurrency mining uses more power than 130 countries. The power consumption is justified by proponents, who reason that the power used for all the centralized banks and their infrastructure is also massive. While it is likely true that all the banks in the world and their infrastructure meet or exceed cryptocurrencies' power consumption, that fact does not justify the power usage. Mining proponents also reason that as a store of value performing work is a good way to ensure that the resulting coins always have value.

However, the digital age has taught us that some of the most valuable things: intellectual property, deeds, titles, personal records, and of course money; can be replicated in fractions of a second and shared to anyone or everyone in the world, at little to no cost. The digital age is all about efficiency. While there will always be a place for cryptocurrency mining, we are seeing the inevitable move from mining digital currencies into methods that can accomplish the same goals more efficiently.

The majority of these new methods utilize some form of Proof of Stake: staking resources to have the right to create a block or write to the ledger. While this can be used effectively, ensuring the stakes aren't applied unequally requires various methods such as 'delegation' to offset the threat of centralization. Seligere and Proof of Selection will provide a new method of consensus that at worst can compete with Proof of Stake and Delegated Proof of Stake models and at best will become the forefront of decentralized algorithms.

Competing Consensus Algorithms

It should be noted that the term 'consensus algorithm' is used to define any agreement between decentralized nodes. Due to the evolving complexity of digital ledger technologies, there are a number of areas decentralized nodes may need to come to consensus on. Even in Bitcoin, there is at least two different areas of consensus: Consensus on who has the next valid block and consensus on what transactions can be written in that block. In the case of this document, 'consensus algorithm' will be used in reference to the agreement required to write a block, event or other group of transactions to the ledger.

Proof of Work – There are a few fundamental problems that are created with digital ledgers using a Proof of Work consensus algorithm as the mechanism for building the ledger (e.g., blockchain). Computers must 'mine' to have the right to publish a block. Publishing a block then results in obtaining digital coins as a reward. This mining process takes a lot of processing power and as such, creates a few issues: Nodes with the most power or pooled power can control the blocks created, transactions logged, monetary reward, and ultimately the core of the program

(e.g., rules). Controlling each of these areas can skew the currency in a way that serves the purpose of the computers with the most power.

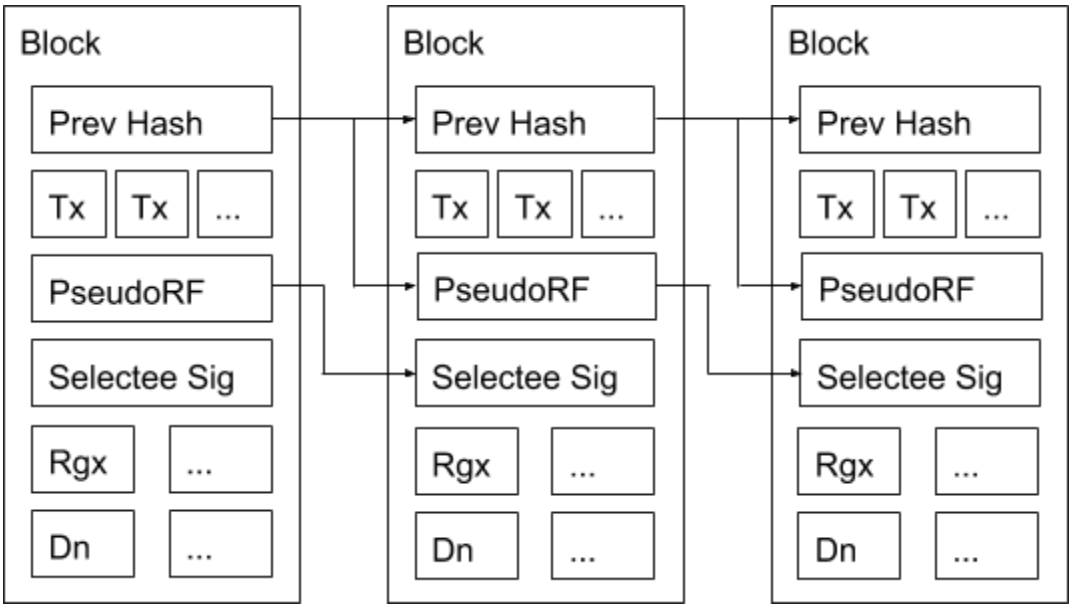
Proof of Stake – This method can capture many different techniques; in general, it requires using a 'value system' or tokens to bet or invest on the valid blocks (e.g., events). Some implementations remove mining. However in some cases, the weighted dynamic creates a volatile environment that is sometimes not ideal for an equally distributed system.

Tangle Coordinator (IOTA) – This method removes mining and integrates with a digital ledger technology called the Directed Acyclic Graph (DAG). However, there is a central coordinator who provides rudimentary functions to validate the new blocks at regular intervals. This coordinator is not provided by the decentralized nodes and is controlled by the IOTA Foundation. Tangle also requires some Proof of Work prior to accepting a new block. It is not considered mining, so currently the possible disadvantages are not well documented.

Swirlds (Hashgraph) – This method also removes mining and is used in conjunction with DAGs. It uses complex algorithms that basically have nodes that 'vote' on the next valid event (similar to a block) based on what events they see. This, in itself, is a novel way to obtain consensus. The primary negative issues with this protocol are that it is proprietary software and not open source, making it more difficult for innovation and limiting in its full technological review. Second, there is a proxy staking component that is very important and can create interesting investing dynamics and competition. The downside however, is participants not running nodes can influence consensus with their stake; essentially Swirlds uses a modified proof of stake methodology.

Proof of Selection

Proof of Selection involves an agreement of who is eligible to be selected and who is selected to build the next block. An eligible node is a node that has registered their public key into the chain by a digital signature and is still considered 'active.' Only a node that has registered (Rgx) can be selected by the pseudo-random function, PseudoRF. The PseudoRF is baked into the blockchain and scripted to automatically choose a number of node(s) to create the next block(s). This pick is determined by the previous block hash and block creation timestamp. Transactions are timestamped and monitored by the rest of the network; a block is valid only if the rest of the network agrees that it is valid.



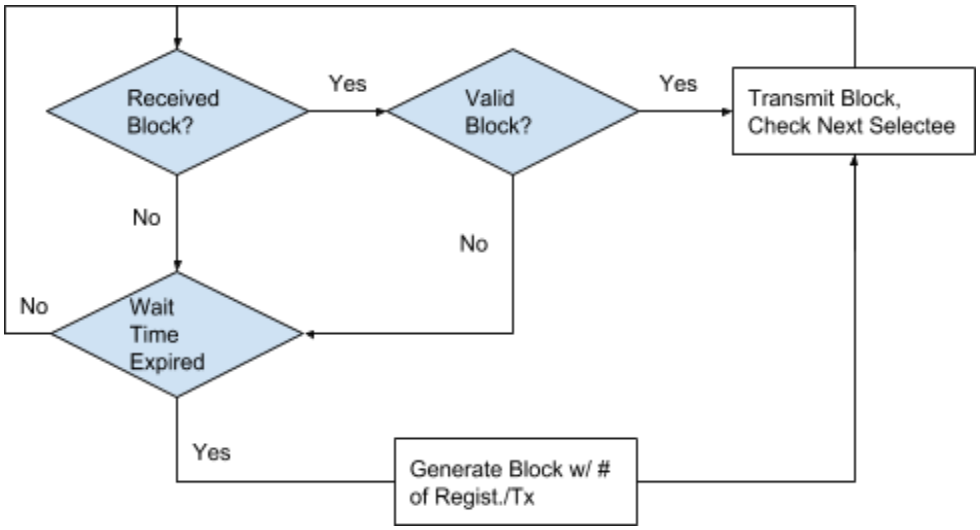
Various implementations of Proof of Selection can be used for different effects and scaling. For example:

1. Select a single node to publish a single block
2. Select multiple nodes to publish a single block
3. Select multiple nodes to publish multiple blocks

As mentioned, eligible nodes must be registered, active nodes and along with registering nodes, dead nodes (Dn) must be similarly identified. To register a node, a simple function logging a node's public key into the blockchain is used. To register a dead node, an invalid block or no response upon selection must occur. After an adjustable number of dead registrations occur, the node is considered dead and is removed from the selection process.

The actual selection is simply based on the number of valid registrants and the resulting random number in the appropriate range. Essentially if we have 10 registrants, a number from 1 to 10 is generated, if number 4 is selected, it will refer to the 4th valid registrant in the chain.

The rate of block creation will be very fast, and there will need to be checks and balances in place. For example, a single node will have to know when to give up waiting for a valid block from a selectee. After an automatically adjusted timeframe, which is based on network size and responsiveness, the node would generate the block without the selectee and include a predetermined number of newly registered nodes as well as a dead node entry. Because all the nodes need to be in sync, they must agree on registration requests, as well as the fact that the selectee never created a block.



A New Digital Ledger – Seligere

Many great digital ledger infrastructures already exist, Ethereum, EOS and Cardano; as such, only the core requirements that Seligere will adhere to will be addressed here. Key to this new digital ledger is simply three concepts:

1. Use the Proof of Selection algorithm.
2. Do not require an internal currency for applications (e.g., ether/gas).
3. Ensure registration and tagging of transactions to allow nodes to ignore blocks or data not slated for their needs.

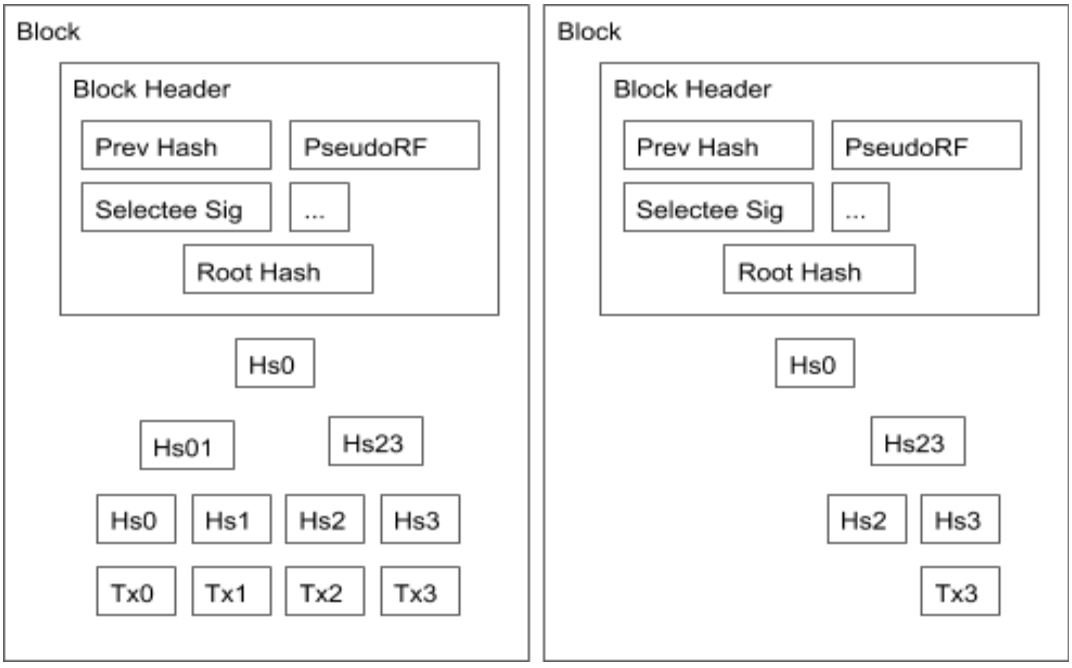
Ethereum, for example, uses gas/ether to incentivize miners to prioritize the applications paying the most gas. This creates a dynamic that allows miners to ignore applications paying the least, meaning new applications may struggle to gain adoption. In an infrastructure, this creates a natural bias for high-paying apps. If there is no natural bias, all transaction rewards would be equal; some of the resulting incentives include:

1. The issuance of currency at block creation (similar to bitcoin)
2. The value of the currency based on the cryptocurrency exchanges
3. The use an application has would act as an incentive
4. Any application owner could pay nodes to host their application if desired
5. Application owner retains the ability to have anyone else host the same decentralized application and data

For example, if we were to hypothetically decentralize a large mail provider, then that provider would be able to essentially install the new digital ledger, associate their nodes with the new mail application, collect digital currency for processing transactions, and at the same time, continue their previous marketing and revenue strategies. The end user would have a decentralized mail system that is not controlled by a single provider, even if that provider happens to have more nodes hosting the application than other providers. In this paradigm, if the provider chooses not to host anyone else's application, they can do so. The resulting digital ledger they retain would simply have Merkle trees (described below) for the transactions not relating to their application.

Merkle Trees & Cleaning Up Space

An immutable linked digital ledger containing all transactions throughout the life of the ledger will be very large in time. If a linked digital ledger processed the same amount of transactions as Visa (over 2,000 per second) and had a mere 1024 bits per transaction, the ledger would grow by roughly 1MB every 4 seconds, which would end up being just under 8TB per year. This amount of data would not be feasible to maintain and is the reason technologies, like Bitcoin and Ethereum, make use of Merkle trees. Essentially, Merkle trees use hashes of transactions to maintain integrity without having to keep all the actual data.



The above figure is adapted from the Bitcoin white paper. The root hash shown is the Merkle root of the Merkle tree. If only Tx3 is needed (e.g., approved applications' transactions), then all the other transactions could be hashed and ignored. Every node can choose to prune the tree in

their own way as long as the transactions and the categories of the transactions are hashed in the same order.

Transaction Rewards (Digital Coin Issuance)

The principle purpose of rewards is to promote nodes to stay online, send transactions and process blocks. There is no competition mechanics built into Seligere, if a node is selected, a reward is issued, one 'Sel' will represent the reward for the creation of a block. The actual value of a Sel will be sorted by the market. Along with block creation however, the ratio between created blocks to active nodes could create an environment where nodes have limited natural incentive to be a part of the network.

If a block were created every second, roughly 31.5 million Sels would be issued in a year. At that rate it would take 100 years before circulation rivaled that of the current estimated global currency in circulation; an estimated 4 trillion. Yet, even still, if the number of nodes increases dramatically there could be a point where obtaining a Sel will become more and more scarce. If for example the US population of 250 million owned a node,a node could go 8 years without creating a block and earning a Sel. In that case, there would be less built-in incentive for nodes to stay online.

In an attempt to ensure a built-in incentive for all network users, a configuration will be available to reward active nodes at configurable intervals for nodes that haven't been selected within a configurable timeframe. The opposite configuration will also be available, not issue rewards if the number of blocks created vastly outnumbers the active nodes. The effects of rewarding or not rewarding those not selected is still under research, and the methodology may change as further testing is performed.

Attacks

In all consensus algorithms, there is an aspect of 'agreement' that must occur when establishing a valid block (e.g., event or transaction groups). For example, Proof of Work requires that the network agree that the fastest mined block is the correct block, and if two miners create a block at the same time, the one who gets 51% of the network wins. A malicious actor would have to do more work, assuming they were not the winning block, to recreate a valid block. Transactions are only validated to the extent that a double spend does not exist. There are a large number of cryptocurrency attacks, and in many cases, lessons from more mature technologies such as Bitcoin or Ethereum can be used. However, a few should be addressed with regard to any new consensus algorithms: Double spending, forks, 51% attacks, Sybil attacks (fake nodes),selection fixing (specific to Proof of Selection).

The biggest double spending threat to Proof of Selection is that a single node that is selected can attempt to publish multiple valid blocks very fast. However, because the rest of the network must also be aware of the transactions that are registered to the block, any attempt at double spend would be detected quickly. If a fork based on a valid block were to occur, the network would know to discard the block due to a single selectee submitting multiple valid blocks, possibly due to a hack, and therefore would treat the block as invalid.

In Proof of Selection, while an attacker is not limited by massive work, they are limited by the fact that they would need to compromise a selectee's key. 51% attacks and Sybil attacks, which control a large number of nodes, cannot be reasonably done with regard to creating new blocks, but it can still be done in relation to manipulating transactions. If the network agrees that an invalid transaction is the 'right' transaction, then it will eventually be added to a block. This assumes that a malicious attacker was able to steal private keys and gain control of a large portion of the network.

The coin issuance paradigm Seligere uses creates an indirect incentive for someone to create as many nodes as possible (fake nodes) to obtain more selections, thereby earning more Sels. This paradigm gets around the Byzantine Generals, but creates an environment where creating multiple virtual nodes would allow them to have more possible rewards. There are a few methods to address this: 1. Selection & reward nodes based on routable IP 2. Charge a fee to create a node, based on network size, issued Sels and possibly market value 3. Restrict registration based on human factors or other selection criteria. When comparing the fake nodes issue to a cryptocurrency that uses mining; there is a similar dynamic, instead of increasing the number of nodes owned, they increase the processing power of their nodes. This is markedly harder to implement and is one of the most significant benefits of a mining algorithm. Yet, because of the ability to de-incentivize fake node creation, the end result leans in favor of the Seligere methodology with regards to the ability to stay as decentralized as possible.

Selection fixing refers to an attempt to re-generate the next selectee's number by trying different combinations of transactions. Due to the fact that transactions must be verified by the network, a single node does not control the transactions that are approved to be in the block. A complicated Sybil attack could possibly perform selection fixing, but again it would require a significant portion of the network to execute. It is fair to say that in *any* publicly decentralized system a large-scale Sybil attack could succeed. In the case of Seligere, that large scale attack would have to be sustained to earn any significant amount of Sels, and as such is unlikely.

Privacy

Another issue to address is the idea of privacy, publicly decentralized systems are inherently not completely private. In fact, the state of government regulations across the globe are pushing for various laws to be enforced on cryptocurrencies to combat money laundering. Yet if we compare this to the inherent level of privacy in ‘fiat’ currency, privacy cannot be completely taken suggesting that governments are treating digital currencies much more stringently.

To that end, Seligere as an infrastructure will be open, yet it should be emphasized that privacy does not necessarily have to occur at the infrastructure. In digital ledger technologies, the infrastructure can be described as the Layer 1 technology. It provides the network of nodes connected by the same code, sharing a set of rules to abide by. Layer 2 applications, often referred to as smart contracts, on the other hand, ride on top of the Layer 1 technology. They do so by uploading code to the digital ledger and run based on scripts made available by the Layer 1 technology.

There are two primary reasons many Layer 2 privacy applications are having a hard time with existing technologies:

1. Mixers, which is a method of combining transactions to obfuscate the origin and destination, cost too much in transaction fees.
2. Zero knowledge proofs, which is a complex algorithm for privacy, are resource-intensive.

Seligere addresses these problems by eliminating transaction fees, eliminating mining, and adding the ability to selectively process applications.

Conclusion

Proof of Selection is only a consensus algorithm, but it is one that takes the problems of existing consensus algorithms and improves on them. It removes mining requirements and promotes equal block publishing and transaction rights without any centralized coordinating processes or authority. Proof of Selection is fast with no time restrictions on block creation and is also scalable due to the ability to increase the number of selected nodes. Seligere, with the Proof of Selection consensus algorithm will provide another much needed method to decentralized services.

The state of digital ledger technologies and cryptocurrencies today are in a constant flux, many critics have identified real problems that need to be addressed. In successful societies however, the need for decentralization of services is not apparent; large providers are legally binded to not take advantage of their customers, and the legal system adequately enforces the laws. Yet in economically distressed societies, or societies where governments are in turmoil, where corruption is extensive, or censorship is high, decentralization gives people the ability to bypass the corruption, the economic stressors and turmoil and ultimately change their society for the better. Unequivocally, decentralization of many commonly centralized services will occur through a continuous evolution of digital ledger technologies.