# A Platform Selection Framework for Blockchain-Based Software Systems Based on the Blockchain Trilemma

Jan Werth[1], Nabil El Ioini[2], Mohammad Hajian Berenjestanaki[1], Hamid R. Barzegar[1] and Claus Pahl[1]

[1]*Free University of Bozen-Bolzano, Bolzano, Italy*

[2]*University of Nottingham, Malaysia*

Keywords: Blockchain, Distributed System, Distributed Ledger, Blockchain Trilemma, Scalability, Security, Decentralization.

Abstract: Blockchains are used in many software systems to deal with trusted storage. The selection of the appropriate software architecture stack in distributed systems is generally driven by scalability, security, and decentralization as central qualities. In the blockchain domain, these are known as the blockchain trilemma, as they oppose each other. We select the most popular blockchain platforms based on these trilemma properties and other indicators to provide a platform review. Specific metrics will be derived from the overall goals and applied to the platform options. This serves as a basis to create a Selection framework to facilitate the choice of the best possible platform for a given system architecture. The selection framework is evaluated through a use case.

## 1 INTRODUCTION

For many software systems, specifically in distributed architectures, blockchains can provide a trusted storage layer. A central trust authority is no longer required as the network participants manage the blockchain state. Here, each node stores a (local) copy of the blockchain, which is considered immutable. In addition, other benefits of blockchain technology are better security and enhanced privacy. Nevertheless, common qualities such as scalability, security, and decentralization often need to be considered. In the blockchain domain, these are known as the blockchain trilemma, as they oppose each other. Since blockchain platforms offer different performances regarding these properties, decision support for the right platform in an overall system architecture is needed.

We propose a selection framework that allows us to find the best possible blockchain for a given system with respective scalability, security, and decentralization requirements – for instance, as a decentralized exchange, for e-voting, or in the healthcare sector. The first goal is to provide a substantial analysis of a selected set of blockchain platforms and their consensus protocols based on the blockchain trilemma and subsequently draw out a selection framework for choosing the right platform. For this, we map the three goals scalability, security, and decentralization onto detailed, measurable metrics to allow a detailed assessment of the platforms. This in turn is used to define the selection framework for the selection.

## 2 BLOCKCHAIN TRILEMMA

The blockchain is an immutable, decentralized ledger of transactions, where multiple transactions are grouped into a block which is then appended to the chain of blocks. There is no need for a central authority. Instead, blockchains reach consensus thanks to their consensus protocol.

Consensus protocols form the pillar of blockchains by defining a set of rules which dictate how a distributed system and its parts operate and interact. The consensus protocol determines how the network can reach consensus on the future state of the blockchain, i.e., most of a blockchain's participants have to agree on the same state to reach consensus. Therefore it is essential to understand that the consensus protocol and the blockchain platform itself can be seen as two separate objects where the consensus protocol defines the rules and functionality of the blockchain and the blockchain platform realizes the consensus protocol. Different blockchains use different consensus protocols.

The Blockchain Trilemma states that a blockchain can only fulfil two out of the three following contradicting properties: Scalability, Decentralization and Security. It is an extension of the scalability problem -

Werth, J., El Ioini, N., Berenjestanaki, M., Barzegar, H. and Pahl, C.
A Platform Selection Framework for Blockchain-Based Software Systems Based on the Blockchain Trilemma.
DOI: 10.5220/0011837300003464
In *Proceedings of the 18th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2023)*, pages 362-371
ISBN: 978-989-758-647-7; ISSN: 2184-4895

a problem arising from an increasing number of transactions but a limited throughput in major blockchain platforms.

## 2.1 Scalability

Scalability is one of the most important aspects of many distributed systems such as blockchains. Here, it refers to the speed at which participants of a peer-to-peer network can reach consensus on the state of the blockchain (Hafid et al., 2020). Mathematically it can be represented as the maximum block size divided by the block interval (Croman et al., 2016). Following this, solving the scalability issue can be done by either increasing the block size or decreasing the block interval. However, external factors such as computing power, bandwidth, and storage space (Buterin, 2021) call for an internal solution to the problem. This is where the blockchain trilemma arises, existing solutions such as the Proof-of-Stake (PoS) consensus protocol trade in decentralization in favor of scalability. Using only a limited number of validators, a particular type of node allowed to create and confirm new blocks, PoS protocols can decrease required network communication and increase its scalability. Proof-of-work (PoW) protocols do not differentiate between different types of nodes, and everyone has the same rights.

Low blockchain transaction rates lead to a problem where transactions can no longer be processed immediately. Therefore, in the context of blockchain, scalability refers to the ability to support high transactional throughput while maintaining performance. Croman et al. (Croman et al., 2016) identified key metrics to measure scalability of blockchain platforms: *maximum throughput, latency, bootstrap time, and cost per confirmed transaction,* where the first two measurements are the most important for a user who intends to use a blockchain without being a *miner* or a *validator*.

Maximum throughput refers to the above-explained concept of transactions per second. Latency is the time it takes for a blockchain to create a new block, append it to the blockchain, and regard it as confirmed. It can be divided into two parts which are the block time and the time to finality. The former refers to the time needed to create a block and add it to the blockchain. In contrast, time to finality can be once again subdivided into deterministic and probabilistic. Deterministic means that a block is considered final once it is appended to the blockchain. In other words, the block is no longer changeable once it has been published. Probabilistic refers to the blockchains in which a block is still subject to change once it has been added to the blockchain, i.e., due to the network not having reached consensus on the future state of the blockchain. Bootstrap time refers to the time it takes to download a blockchain and confirm all the blocks and transactions. Costs per transaction are external factors such as setup cost, hardware cost, storage cost, and power usage.

## 2.2 Decentralization

Decentralisation is the central ethos and given nature of the blockchain technology, but also a massive bottleneck regarding scalability and security. It describes the transfer of control and decision-making rights from a central authority to a distributed network. A characteristic of decentralisation in blockchains is the distrust between its participants, which is desired and required for it to work correctly.

Measuring a network's decentralisation depends on the type of blockchain. Two types of blockchains exist or rather two types on how decentralisation must be measured. One type uses the Proof-of-Work consensus protocol, while the other type uses Proof-of-Stake or a similar consensus protocol where the rights to create a new block are given to a node based on staked capital. The decentralisation (and security) of a Proof-of-Work blockchain depends on the network's hash rate and how distributed it is. A network's hash rate is the cumulative hash rate of all the (mining) nodes participating in the block creation competition. Therefore, the higher the network's hash rate, the harder it is to disrupt it.Decentralisation of a Proof-of-Stake or similar blockchain can be measured in the number of validators, the distribution of staked capital among the validators, and the percentage of token supply that has been staked. Another metric to measure decentralisation is the Initial Token Allocation. It can create unfair advantages for a group that receives many tokens and determine the next block and chain governance. For both Proof-of-Work and Proof-of-Stake (or similar blockchains), it is important to measure how many nodes or pools (a pool is a group of miners or validators which join together to increase their chance of creating the next block) control the majority of the network. his metric is also called Superminority or Nakamoto Coefficient. The Nakamoto Coefficient is defined as the minimum number of nodes required to get 51% of the total capacity (either in computing power or staked capital) (Srinivasan, 2017). However, for networks with a lower Byzantine Fault Tolerance, it is only required to control one-third of the network's computing power or staked capital.

## 2.3 Security

Security is the third aspect of the blockchain trilemma. A framework used in cybersecurity is the CIA triad which stands for *confidentiality, integrity, and availability.*

Some other security features come from the CAP theorem, which stands for *consistency, availability, and partition tolerance* and states that none of these three characteristics can be achieved simultaneously. This theorem is especially popular among blockchain developers and often mentioned in the whitepapers of different platforms, documentation, or online discussions. Zhang et al. (Zhang et al., 2019) applied the aforementioned CAP properties to a distributed ledger: *Consistency:* All nodes keep an identical ledger with most recent updates. *Availability:* Any transaction generated at any time will be accepted in the ledger. *Partition Tolerance:* Even if part of the network fails, it can still operate normally.

It seems that the blockchain implementation has violated the CAP theorem by achieving not only consistency but also availability and partition tolerance. However, this is not the case as a block's latency plays a role in consistency. This was also identified by Zhang et al. (Zhang et al., 2019) who state that consistency is not achieved simultaneously with availability and partition tolerance but only after a period of time. Given this weak characteristic and the existence of a higher-level term in the CIA triad, we can categorize consistency as part of integrity. We can also group availability and partition tolerance, where the latter is a sub-category of the former: Confidentiality concerns the privacy of a user. Integrity includes consistency, authenticity, accuracy and tamper-resistance of data. Consistency means that all nodes store the same state of the blockchain. Availability means that the blockchain is always available to be read and accepts transactions. Partition Tolerance means that it works even if part of the network fails.

According to Zhang et al. (Zhang et al., 2019) a blockchain platform does not only have to fulfill the above properties of the CIA triad, it also must be resistant against numerous different types of attacks, such as resistancd to DDoS Attacks, to majority attacks (51% attack and single shard attack), to double spending and to transaction flooding. These are some examples of attacks a blockchain platform, yet these properties represent the most crucial security properties a blockchain must satisfy (Zhang et al., 2019). Another measure of security is the Nakamoto Coefficient.

**Byzantine Fault Tolerance.** (BFT) refers to the ability of a distributed system to keep working correctly even when a fraction of its nodes fail or act maliciously. Blockchains reach BFT through their consensus protocols which dictate the rules. If a node is no longer following the consensus protocols' rules, it is a malicious node that does not act in the network's interest. Furthermore, most of the blockchains' attacks occur inside the network, implying the presence of byzantine nodes. A higher byzantine fault tolerance also means that a network is more secure. Other outside attacks (e.g., DDoS attacks) attack single nodes in the network and try to shut them down. Such an attack can not only be prevented by having a high byzantine fault tolerance so that fewer nodes are required to keep the network operating, but also high decentralization fends off DDoS attacks. Yet again, another example of how two aspects of the blockchain trilemma are connected.

# 3 SELECTION CRITERIA AND METRICS

We provide an analysis of different blockchain platforms, which will then be used to create a selection framework to facilitate the selection of which platform to use among the selection of platforms. The reason is that every platform takes a different approach to the blockchain trilemma with a different objective. This poses a challenge for prospective blockchain developers and users as a particular blockchain platform may not fulfil their requirements, i.e. the application requires high, intermittent transactional throughput, which only a few platforms support. Given the numerous existing blockchain platforms, an analysis of all platforms would go beyond the scope here and is not feasible. Therefore, only a selection of blockchain platforms will be included in the selection framework.

## 3.1 Platform Selection

The selection of which blockchain platforms to compare was made in April 2022 based on their blockchain trilemma properties, their type of blockchain, their initial token allocation, their Total Value Locked (TVL), and the number of miners/validators participating in the consensus.

The most important selection criteria to ensure diversity among the selected blockchain platforms were their blockchain trilemma aspects. In other words, it was essential to include blockchains that focus on the trilemma's different aspects. This was done by looking at different metrics which define the platform's scalability, decentralization, and security. The selected metrics for scalability are the platform's maximum transactions per second, their block time and their time to finality. For decentralization the number of nodes, their type and whether the number of nodes is fixed is essential. The number of nodes, their type, and the distribution of computing power and staked capital is also of interest for security, as well as the Byzantine Fault Tolerance of the network.

Another criterion which had to be considered is the type of blockchain. To ensure that the selected blockchains are programmable on only public permissionless blockchain platforms (Pahl et al., 2018), which also support Smart Contracts, were included.

The selection resulted in 9 blockchain platforms[1] with one Layer 0 solution (Cosmos), one Layer 2 solution (Polygon), and one platform which was included for its approach to the blockchain trilemma, Harmony. Harmony is already applying a method called sharding to its blockchain, which Ethereum, the platform with the most protocols and highest TVL, will apply in 2023. The selection is presented in Table 1.

We summarize the consensus protocols used by the selection of blockchain platforms and additional consensus protocols which may be necessary to understand more complex ones in Table 2.

### 3.2 Analysis of Platforms

The metrics chosen to analyze the blockchains are generally available for all public blockchains. Table 3 includes transactions per second. Some platforms are not yet fully implemented but will reach higher tps in the future. These metrics are identified in (Croman et al., 2016) to compare blockchain scalability.

**current TPS:** measure the average throughput of a blockchain platform.

**max TPS:** states the maximum transactions per second a blockchain can process.

**Block Time:** measures the time in seconds it takes for a blockchain to create a new block.

**Number of Nodes:** measures the decentralization of a blockchain. The number only includes nodes responsible for block creation.

**Time to Finality:** measures of block latency. In probabilistic networks, a block is not considered final even after it was created due to the risk of forks and other. However, some platforms in the selection offer deterministic finality, which means that a block is final the moment it was produced.

Table 4 shows a comparison of each platform's decentralisation and includes the Nakamoto Coefficient. The metrics to measure decentralization (Conway, 2022) (Srinivasan, 2017) are:

**Number of Nodes:** participating in the block creation process.

**Type of Nodes:** Different consensus protocols use different types of nodes for block creation. However, in this selection, most platforms use validators or some sort of validators[2].

**Fixed Number of Nodes:** states whether the number of nodes participating in the block creation is fixed or can scale.

**Hashrate / % of Supply Staked:** reports the network's total hash rate (for Ethereum) and percentage of how much of the token supply of a network's crypto-currency is staked.

**Nakamoto Coefficient:** measures how many entities are in control of 51% or 34% (depending on BFT) of the network's power (either in computing power or staked capital).

Table 6 depicts the security aspect of the blockchain platforms. The metrics are:

**Byzantine Fault Tolerance** measures the threshold of failed or adverse nodes a network can withstand.

**Availability** blockchains is imported as transactions always occur.

**Anonymity** shows if complete anonymity or pseudonymity where a transaction can be tracked and linked to an address is offered.

Note that the Nakamoto Coefficient is also a metric used to measure the security of a network as large entities.

### 3.3 Design of the Framework

To create a selection framework, we have to establish the metrics and rules which the selection framework will follow. The metrics are used in scientific articles and in the blockchain community to compare and analyze the performance of different platforms (Hafid

[1] Please note that we do not list all individual sources of information separately due to their large number. All information has been gathered from the documentation made available by the providers.

[2] For example, in BSC, validators have to be approved by Binance. Trons' Super Representatives are also validators. Only Ethereum does not use validators but uses competing nodes as participate in the Proof-of-Work consensus.

Table 1: Selected Blockchain Platforms.

| | Consensus | Structure | Architecture | Smart Contracts |
|---|---|---|---|---|
| **Ethereum** | PoW | Chain | Single Chain | YES |
| **Cosmos** | Tendermint PoS | Chain | Cosmos Parachain | YES |
| **BSC** | PoSA | Chain | Cosmos Parachain | YES |
| **Avalanche** | SoA | DAG | X-Chain, P-Chain, C-Chain | YES |
| **Solana** | PoH | Chain | Single Chain | YES |
| **Fantom** | LCA | DAG | Main Chain (Atropos) | YES |
| **Tron** | DPoS | Chain | Single Chain | YES |
| **Polygon** | PoS | Chain | Sidechains | YES |
| **Harmony** | FBFT | Chain | Sharding | YES |

Table 2: Comparison of Consensus Protocols.

| | Throughput | Transaction Finality | Decentralization | BFT | Energy Consumption |
|---|---|---|---|---|---|
| **Proof of Work** | Low | Probabilistic | High | $\leq$=50% | High |
| **Proof of Stake** | Low | Probabilistic | Medium | $\leq$=50% | Low/Medium |
| **Tendermint PoS** | Medium | Deterministic | Medium | $\leq$=33% | Low/Medium |
| **Delegated-Proof-of-Stake** | High | Probabilistic | Low | $\leq$=33% | Low/Medium |
| **Proof-of-Staked-Authority** | Medium | Probabilistic | Low | $\leq$=33% | Low/Medium |
| **Snowflake-to-Avalanche** | Medium/High | Probabilistic | Medium | $\leq$=50% | Low/Medium |
| **Proof-of-History** | High | Deterministic | Medium | $\leq$=33% | Low/Medium |
| **Fast Byzantine Fault Tolerance** | High | Deterministic | Medium | $\leq$=33% | Low/Medium |
| **Lachesis Consensus Protocol** | High | Deterministic | Medium | $\leq$=33% | Low/Medium |

et al., 2020) (Buterin, 2021). In the presentation of the blockchain trilemma (Buterin, 2017) Buterin described the three trilemma aspects as follows:

**Scalability:** Defined as being able to process $O(n) > O(c)$ transactions

**Decentralization:** Defined as the system being able to run in a scenario where each participant only has access to $O(c)$ resources

**Security:** Defined as being secure against attackers with up to $O(n)$ resources

### 3.3.1 Scalability

Maximum throughput and latency of a network are the most decisive indicators for scalability for users who do not actively participate in the network (Croman et al., 2016). Therefore, the maximum throughput (how many transactions per second a network can handle), the block time, and time to finality are selected to measure the scalability of a network. Time to finality is assessed based on a network being deterministic or probabilistic. Block time is rated by the seconds it takes for a network to create a new block, which, is not used in this selection framework as all selected blockchain platforms present a similar block time. Thus, only the maximum transaction per second as some blockchains are not fully implemented yet and the time to finality (deterministic or probabilistic) is used to measure the scalability of the blockchain platforms.

### 3.3.2 Decentralization

According to Conway (Conway, 2022), decentralization of Proof-of-Work networks is measured by its hash rate and its distribution among the participants of the network. A Proof-of-Stake network (and similar blockchains) is measured by the number of validators, the percentage of token supply staked, and the distribution of the token supply across its validators (Conway, 2022). Following this, we calculate a decentralization index for the selected Proof-of-Stake (or similar) blockchain platforms by their average ranking for the number of nodes, their percentage of supply staked, and their Nakamoto Coefficient. This decentralization index is used to determine how decentralized a network is as the number of nodes may be misleading due to the Nakamoto Coefficient. Ethereum's decentralization will be measured along with its peers (other Proof-of-Work blockchains). A lower decentralization index is favourable as it indicates that the network is more decentralized.

### 3.3.3 Security

Security can be measured by the Byzantine Fault Tolerance of a network. An asynchronous network can not provide safety (guarantee that all malicious nodes will eventually agree to the new state) and liveness (ability to process transactions) if the number of malicious nodes exceeds the BFT threshold (Bracha, 1987). For networks with a Byzantine Fault Toler-

Table 3: Scalability of Blockchain Platforms.

| | current TPS | max TPS | Block Time | Time to Finality |
|---|---|---|---|---|
| **Ethereum** | 10 | 12-15 | 12-14 seconds | 60 seconds |
| **Cosmos** | / | 10,000<br>per zone | ˜6 seconds | Instant |
| **BSC** | 40-60 | 160 | ˜3 seconds | 75 seconds |
| **Avalanche** | 5-10 | 5,000+<br>per subnet | ˜2 seconds | ˜1 second |
| **Solana** | 1,500-2,500 | 710,000 | ˜0.7 seconds | Instant |
| **Fantom** | 10-15 | 300,000 | ˜1 second | Instant |
| **Tron** | 50-200 | 2,000 | 3 seconds | 60 seconds |
| **Polygon** | 30-50 | 65,000<br>per sidechain | 2.3 seconds | ˜2 seconds |
| **Harmony** | ˜10 | 500<br>per shard | 2 seconds | Instant |

Table 4: Decentralization of Blockchain Platforms.

| | Number of Nodes | Type of Nodes | Fixed number of validators | Hashrate / % of supply staked | Nakamoto Coefficient |
|---|---|---|---|---|---|
| **Ethereum** | ˜6,000 | Competing | No | 913.74 TH/s [1] | 3* |
| **Cosmos** | 175 | Validators | Yes | 62.23% | 7 |
| **BSC** | 21 | Authorized validators | Yes | 81.47% | 8* |
| **Avalanche** | ˜1,250 | Validators | No | 60.82% | 52 |
| **Solana** | ˜2,000 | Validators | No | 73.79% | 27 |
| **Fantom** | 92 | Validators | No | 47.01% | 3* |
| **Tron** | 27 | Super Representatives | Yes | 45.81% | 8[2] |
| **Polygon** | 100 | Validators | Yes | 30.89% | 13* |
| **Harmony** | 250<br>per shard | Validators | Yes | 42.48% | 5* |

[1] Ethereum is the only PoW platform, thus hashrate is used to measure decentralization.
* Is estimated since no central source exists for the Nakamoto Coefficient for some.

Table 5: Decentralization Ranking of Blockchain Platforms, with Number of Nodes NoN, Hashrate / % of supply staked HR, Nakamoto Coefficient NC, Decentralization Index DI.

| | NoN | HR | NC | DI |
|---|---|---|---|---|
| **Ethereum** | 2 | 2 | 2 | 2 |
| **Cosmos** | 4 | 3 | 6 | 4.33 |
| **BSC** | 8 | 1 | 4 | 4.33 |
| **Avalanche** | 2 | 4 | 1 | 2.33 |
| **Solana** | 1 | 2 | 2 | 1.66 |
| **Fantom** | 6 | 5 | 8 | 6.33 |
| **Tron** | 7 | 6 | 4 | 5.66 |
| **Polygon** | 5 | 8 | 3 | 5.33 |
| **Harmony** | 3 | 7 | 7 | 5.66 |

ance of $\leq 33\%$ a number of malicious nodes between 33% and 50% can already halt the blockchain so that it can no longer produce new blocks (Bunin, 2022).

In addition, to Ethereum, Avalanche, and Polygon, where >50% of the network needs to be malicious to bring it to a stop, we also consider BSC secure all the validators have to be approved by a central authority and must publish their identity.

### 3.3.4 Resources and Repeatability

To analyse the different platforms we studied whitepapers and online documentation. As those sources mainly focus on the conceptual aspects, such as maximum throughput or the functions of their consensus protocol, block explorers are used to get real-time and historical information on a blockchain. Block explorers are mainly developed by the blockchain foundation, reputable community members, or former blockchain developers.

The process of analyzing and assessing the blockchain platforms is repeatable for most of the part. Scalability and Security of a network is measured with objective metrics. Only for decentralization, we compared the selected blockchain platforms to one another according to (Conway, 2022).

Table 6: Security of Blockchain Platforms.

| | BFT | Availability | Anonymity |
|---|---|---|---|
| **Ethereum** | $\leq 50\%$ | Transaction with low fees can become stuck (as miners receive the fee, a low fee does not offer any incentive to process the transaction over other transactions with higher fees)<br>Data availability is achieved by full nodes | Pseudonymity |
| **Cosmos** | $\leq 33\%$ | Validators are penalized for inavailability | Pseudonymity |
| **BSC** | $\leq 33\%$ | Validators are penalized for inavailability | Pseudonymity |
| **Avalanche** | $\leq 50\%$ | SoA can adaptably change byzantine fault tolerance for availability<br>Block and Transaction Data are simultaneously stored on Kyve | Pseudonymity |
| **Solana** | $\leq 33\%$ | Horizontal scaling gives up network availability for scalability | Pseudonymity |
| **Fantom** | $\leq 33\%$ | Validators and delegators are penalized for inavailability | Pseudonymity |
| **Tron** | $\leq 33\%$ | Fees to prevent transaction flooding | Pseudonymity |
| **Polygon** | $\leq 50\%$ | Validators and delegators are penalized for inavailability<br>Achieves data availability by the means of an additional data layer on the blockchain | Pseudonymity |
| **Harmony** | $\leq 33\%$ | Shards store only 1/n of the global state, new blocks from shards are crosslinked to the beacon chain. | Pseudonymity |

# 4 SELECTION FRAMEWORK

This selection framework aims to facilitate deciding which blockchain platform to use. It does not provide any method to decide whether the use of a blockchain (for a particular application) is reasonable or not. The user should have already made this decision. It is also assumed that the user knows their specifications regarding needed and desired scalability, decentralization and security.

## 4.1 Development Process

The development of the selection framework started with finding attributes which best split the selection of platforms into two homogeneous parts. However, finding a starting attribute that allowed all users to follow their wanted aspect of the blockchain trilemma was impossible.

Thus, the final selection framework starts with the question "What is most important" with all three aspects as answer possibilities. This split no longer produced pure nodes but mixed nodes where a blockchain platform could be part of two or all three pathways. Therefore, some platforms can be reached through different paths as they fulfil multiple criteria. The subsequent nodes in the selection framework were used to further down-sample the selection set.

Generally, at each decision node, the user can choose between one of the three trilemma aspects where scalability includes all platforms with a maximum tps rate greater than Visa's 1,700 tps. Decentralization is measured with the help of the Decentralization Index presented in Table 5, where all networks with an index <4 are considered to be more decentralized than others. This split was chosen due to the (large) gap in the decentralization index between Avalanche (index of 2.33) and the next best platforms, BSC and Cosmos (index of 4.33). Security embraces all platforms with a byzantine fault tolerance of $\leq 50\%$ and BSC where the validators are publicly known. Section 4.2 gives a detailed overview of all decision nodes.

Figure 1 shows our selection framework where multiple questions must be answered before the selection framework terminates with a suggestion. Furthermore, for some pathways, the selection framework terminates with two possible blockchain platforms. This is due to their similarity when measured in terms of the blockchain trilemma. In this case, further study of the differences between the two platforms is recommended.

## 4.2 The Selection Nodes

**a: What is most important?** The first question asked is what is most important for the user. The three choices offered are the three aspects of the blockchain trilemma.

**b: More scalability, or decentralization or security?** Following the scalability path from the first decision, the next question is what is the second most important to the platform. Yet again, the user is confronted with all three blockchain trilemma aspects.

**c: Scalability or Security?** The 2nd question for decentralization is whether the platform should focus more on scalability or security.

**d: Validators publicly known?** This question is to differentiate BSC from other secure platforms, as

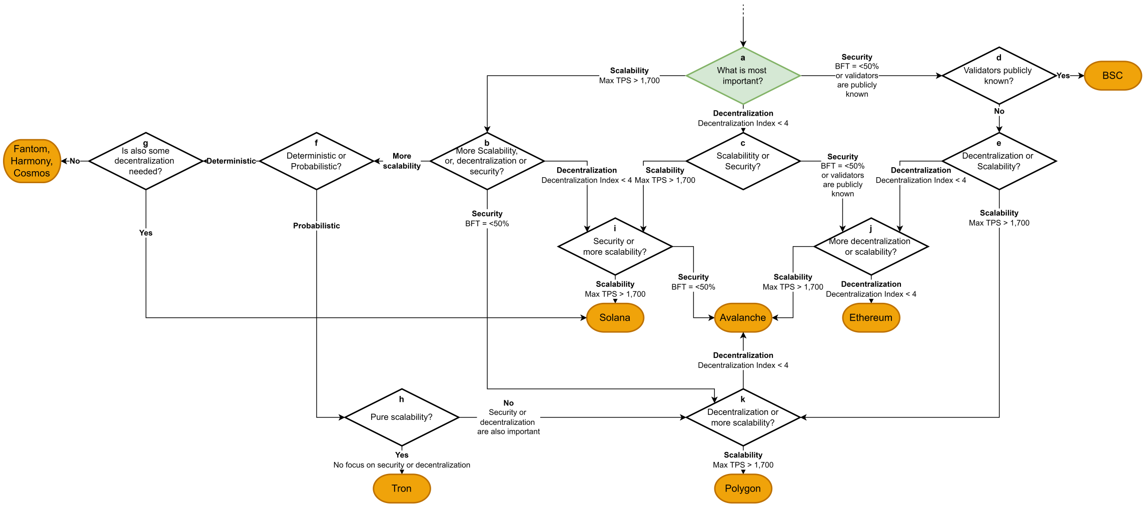
a
What is most important?
Scalability
Max TPS > 1,700
Security
BFT = <50%
or validators are publicly known
d
Validators publicly known?
Yes
BSC
No
Decentralization
Decentralization Index < 4
Fantom, Harmony, Cosmos
No
g
Is also some decentralization needed?
Deterministic
f
Deterministic or Probabilistic?
More scalability
b
More Scalability, or, decentralization or security?
Decentralization
Decentralization Index < 4
Scalability
Max TPS > 1,700
c
Scalabilitity or Security?
Security
BFT = <50%
or validators are publicly known
Decentralization
Decentralization Index < 4
e
Decentralization or Scalability?
Yes
Probabilistic
Security
BFT = <50%
Scalability
Max TPS > 1,700
i
Security or more scalability?
j
More decentralization or scalability?
Scalability
Max TPS > 1,700
Security
BFT = <50%
Scalability
Max TPS > 1,700
Decentralization
Decentralization Index < 4
Solana
Avalanche
Ethereum
Decentralization
Decentralization Index < 4
h
Pure scalability?
No
Security or decentralization are also important
k
Decentralization or more scalability?
Yes
No focus on security or decentralization
Scalability
Max TPS > 1,700
Tron
Polygon

Figure 1: Blockchain Platform Selection Framework.

BSC is the only platform in this selection where the validators have to publicize their identity. So if the validators should be known, we come to our first result. Else the selection framework continues.

**e: Decentralization or Scalability?** The third question for a secure platform also concerns the other two trilemma aspects.

**f: Finality?** This question follows the question of **b: More scalability, or decentralization or security?** and divides the subset of scalable platforms based on their block finality.

**g: Is also some decentralization needed?** If the platform should offer instant finality, the last question in the selection framework is the question of decentralization. Suppose less decentralization is required, the selection framework points to Fantom and Harmony. If, however, the platform should also be more decentralized, it terminates with Solana and Harmony as a result.

**h: Pure scalability?** If the answer to question **f: Finality?** is no and probabilistic finality is sufficient, the next question is whether the platform should offer some decentralization or security. If the answer is no and only scalability is required, the result of the selection framework is Tron. Else question **k: Decentralization or more scalability?** follows.

**i: Security or more scalability?** This question can be reached from decision **b: More scalability, or decentralization or security?** if chosen decentralization or from question **c: Scalability or Security?** if chosen Scalability and yields three different results. If the platform should be secure, it points to Avalanche. If it should be scalable, suggestions are Solana and Cosmos.

**j: More decentralization or scalability?** Just like the last decision, this question can also be reached from two former questions and confronts the user with the question of whether more decentralization or scalability is required. If the answer is decentralization, the selection framework points to Ethereum, the only platform in this selection where every node has the same rights. Else the selection framework results with Avalanche.

**k: Decentralization or scalability?** This question can be reached if both security and scalability have been chosen before and queries whether decentralization or scalability is more important. If the former is chosen, the selection framework terminates with Avalanche, otherwise, with Polygon.

## 4.3 Observations

The presented selection framework provides only a limited summary of a subset of selected blockchain platforms. Many platforms appear to be similar to others but utilize different underlying technology (i.e., consensus protocol, the structure of chain, data storage, etc.). Therefore, solely relying on this selection framework is not sufficient and all the technical details should be researched. This is particularly evident if we look at the result of ”Fantom, Harmony. Cosmos” when selecting ”no” at node **g: Is also some decentralization needed?**. While all three are results of the same pathway, Fantom is a DAG-based blockchain with a maximum of 300,000 transactions per second, Harmony is a sharded blockchain where each shard supports only up to 500 transactions per seconds but can reach higher transactions per seconds according to its whitepaper, whereas Cosmos is a platform to build blockchains on which can horizontally scale and reach thousands of transactions per second per zone. All three platforms are also similar in terms of block time, deterministic time to finality, decentralization (index of 6.33 for Fantom vs index of 5.66 for Harmony vs index of 4.33 for Cosmos) and security ($\leq 33\% BFT$).

## 5 EVALUATION OF THE FRAMEWORK

We apply the selection framework to a real-world application setting. A common field where blockchain technology is applied is public services and government. We apply our selection framework to a decentralized exchange platform and a conceptual example by means of e-voting.

Following this, the presented selection framework could have been of use for SushiSwap to decide which blockchain platform to build their application on. However, given the fact that SushiSwap is a fork of another decentralized exchange, UniSwap, which launched in November 2018. Back then, Ethereum was one of the only blockchain platforms to exist that offered Smart Contract support. Most of the platforms presented here only launched after UniSwap's initial launch.

In our local 2018 provincial elections a total of 284,361 voters cast their votes from 7am to 9pm on the 21$^{st}$ October 2018. This corresponds to a voter turnout of 73.87%. In the morning (until 11am) only 19.6% voted but this number increased in the afternoon as 50.5% of all eligible voters casted their vote until 5pm . At the closure of the election stands a total of 73.87% voted.

Table 7: 2018 Provincial Elections in numbers.

| Time | Voters | % | votes/h | votes/s |
|---|---|---|---|---|
| 7-11:00 | 75,241 | 19.6% | 18,810 | 5.23 |
| 11-17:00 | 118,200 | 30.9% | 19.700 | 5.47 |
| 17-21:00 | 89,479 | 23.4% | 22.370 | 6.21 |
| Total | 282,920 | 73.9% | 20.209 | 5.61 |

From Table 7 we can see that on average 5.61 votes were cast by second, alternating slightly depending on the time of the day. Therefore, an e-voting application for provincial elections must be able to process at least six votes per second. However, this number does not take into account that with e-voting, the distribution of votes cast may change and the number of votes increases, which is expected with e-voting (Anane et al., 2007).

Security is important in e-voting systems (Anane et al., 2007) (Abuidris et al., 2019). Both see anonymity as one of the most important points for an e-voting system, something that no platform in this selection offers as they all offer only pseudonymity (see table 6).

Disregarding this concern, we can move from node **a: What is most important?** to node **d: Validators publicly known?** following the security path. At this point, choosing BSC as the platform would also fulfil the provincial election transactions per seconds requirement. But also, the paths which lead to Ethereum, Avalanche, and Polygon are imaginable. Another aspect identified by Abuidris et al. is scalability (Abuidris et al., 2019) which leads us to node **k: Decentralization or more scalability?** from where one can choose between high scalability or decentralization. At this point, a precise suggestion of a blockchain platform for an e-voting application is difficult to make as we are faced with the blockchain trilemma. Is it more convenient to trade decentralization for scalability and choose Polygon, or is also decentralization required for an e-voting application and Avalanche is the better blockchain platform to choose?

In terms of scalability, both platforms are quite similar, whereas Avalanche is slightly faster in creating blocks and reaching consensus, but Polygon can handle more transactions per second. An assumption at this point is that the decentralization and adaptive changeable Byzantine Fault Tolerance from Avalanche are advantageous.

The objective of the selection framework is to facilitate the selection of the correct platform. In the case of the presented selection framework, it helps to decide which platform from the selected and analyzed platforms should be considered for usage. For this, the selection framework uses the blockchain trilemma. To answer the second question, the users must know their specifications and what they expect from the blockchain platform. If the users do not know if they prefer scalability over security or decentralization, the selection framework is not helpful. However, it is also not designed for that purpose. If the selection framework is helpful to the users in any way of narrowing down their final selection or eliminating some blockchain platform, it is considered to be helpful and adds value to the user.

The e-voting case presented above is a conceptual example of how the selection framework could be used to choose the best possible blockchain platform for a decentralized application. By knowing what is important to their application, the user can narrow down the selection of platforms.

## 6 CONCLUSIONS AND FUTURE WORK

In order to support a system architecture by trusted storage, the decision on the right blockchain platform depends on a range of required system qualities. Blockchain platforms offer more trust, security, and privacy as principal benefits, but system properties such as scalability or degree of decentralisation are equally important in distributed systems. We compared selected blockchain platforms in terms of scalability, decentralization, and security. The selection was made on multiple criteria, such as trilemma properties, their type of blockchain, and their initial token allocation. For the analysis of each platform, we studied their respective whitepaper and documentation and also interacted with the platform's community on social media platforms such as Twitter, Reddit, and Discord. However, as such sources cover only the platforms' conceptual aspects, we also utilized websites which track the analytics of each blockchain, so-called blockchain explorers. The results of the analysis indicated that the blockchain trilemma holds true.

We developed a selection framework based on the trilemma properties where each split asks for the most important aspect of the trilemma. Only later splits ask specific questions about the required scalability of the blockchain platform taking specific metrics into account.

## REFERENCES

Abuidris, Y., Kumar, R., and Wenyong, W. (2019). A survey of blockchain based on e-voting systems. In *Intl Conf on Blockchain Technology and Applications*.

Anane, R., Freeland, R., and Theodoropoulos, G. (2007). E-voting requirements and implementation. In *Proceedings CEC-EEE 2007*.

Bracha, G. (1987). Asynchronous byzantine agreement protocols. *Information and Computation*, 75(2):130–143.

Bunin, V. (2022). Proof of stake's security model is being dramatically misunderstood. *Medium*.

Buterin, V. (2017). Sharding faq. https://vitalik.ca/general/2017/12/31/sharding_faq.html.

Buterin, V. (2021). The limits to blockchain scalability. https://vitalik.ca/general/2021/05/23/scaling.html.

Conway, L. (2022). Measuring decentralization: Is your crypto decentralized? *Blockwors*.

Croman, K. A., Saxena, P., Shi, E., Gün Sirer, E., et al. (2016). On scaling decentralized blockchains. In *Intl conf on financial cryptography and data security*.

Hafid, A., Hafid, A. S., and Samih, M. (2020). Scaling blockchains: A comprehensive survey. *IEEE Access*, 8.

Pahl, C., El Ioini, N., and Helmer, S. (2018). A decision framework for blockchain platforms for iot and edge computing. In *IoTBDS*.

Srinivasan, B. S. (2017). Quantifying decentralization. *Medium*.

Zhang, R., Xue, R., and Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3):1–34.