A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma

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

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

[2] *University of Nottingham, Malaysia*

Keywords: Blockchain, Distributed Ledger, DLT, Blockchain Trilemma, Blockchain Platform Comparison, Review.

Abstract: As blockchains are more and more used to support information system architectures, the question of the suitability of a blockchain technology for a particular system arises. However, given the vast amount of existing blockchain platforms, this choice is difficult as each blockchain focuses on different aspects. The most critical ones are scalability, security, and decentralization, which make up the blockchain trilemma. We review a selection of the most popular blockchain platforms based on their blockchain trilemma properties and related aspects. Then, the platforms will be analyzed on the three aspects of the blockchain trilemma.

1 INTRODUCTION

Since peer-to-peer distributed systems emerged, blockchains have been used to supported decentralised and trusted storage needs of information systems many fields such as Banking and Finance, Healthcare, Government and Supply Chain Management. A blockchain is an immutable, decentralized ledger of transactions, where multiple transactions are grouped into a block which is appended to the chain of blocks. A particularity of the blockchain is that there is no need for a central authority. Instead, blockchains reach consensus thanks to their consensus protocol. Each node stores a (local) copy of the blockchain, which is considered immutable. Other benefits are better security and enhanced privacy.

We provide a systematic analysis of selected blockchain platforms and their consensus protocol based on the blockchain trilemma. For the review, we use information obtained from whitepapers, online documentation, articles, and blogs written by developers of different platforms. However, such sources tend to focus on the conceptual aspects of a platform and do not reflect the current state of a blockchain platform. Therefore, we will also look at specific analytic platforms for each blockchain which track different aspects such as transactions per second, block time, and the number of nodes in order to provide a reliable assessment.

2 BLOCKCHAIN, TRILEMMA, METRICS

Consensus protocols form the core of blockchains by defining the rules which dictate how a distributed system and its parts operate and interact. In terms of blockchain, the consensus protocol determines how the network can reach consensus on the future state of the blockchain. This means that most of a blockchain's participants have to agree on the same state to reach consensus. The protocol defines the rules and functionality of the blockchain and the blockchain platform realizes the consensus protocol. Different blockchains use different consensus protocols, which are essential for the blockchain trilemma.

An evolution are Smart Contracts which are programs on a blockchain that run when certain conditions are met. The outcome of the Smart Contract is known beforehand by both parties and is executed immediately without a third party.

2.1 The Trilemma and Metrics

The Blockchain Trilemma states that a blockchain can only fulfil two of three following aspects as they contradict each other: Scalability, Decentralization and Security. It is an amplification of the blockchain scalability issue - a problem arising from an increasing number of transactions but a limited throughput in major blockchain platforms.

Werth, J., Berenjestanaki, M., Barzegar, H., El Ioini, N. and Pahl, C.
A Review of Blockchain Platforms Based on the Scalability, Security and Decentralization Trilemma.
DOI: 10.5220/0011837200003467
In *Proceedings of the 25th International Conference on Enterprise Information Systems (ICEIS 2023) - Volume 1*, pages 146-155
ISBN: 978-989-758-648-4; ISSN: 2184-4992

Copyright © 2023 by SCITEPRESS – Science and Technology Publications, Lda. Under CC license (CC BY-NC-ND 4.0)

2.1.1 Scalability

Scalability is one of the most important aspects of blockchains and can be motivated by 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). 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 give up 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 network communication and increase scalability. However, Proof-of-Work (PoW) protocols do not differentiate between different types of nodes, and everyone has the same rights.

A low transaction rate leads to a problem where transactions can no longer be processed immediately. Therefore, scalability refers to the ability to support high transactional throughput while maintaining performance. Croman et al. (Croman et al., 2016) identified some key metrics to measure scalability of blockchain platforms, such as *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.

2.1.2 Decentralisation

Decentralisation is at the core of blockchain technology, but also a 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 decentralisation depends on the type of blockchain. Generally, 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 the node based on staked capital (Conway, 2022b). 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 (Conway, 2022a). 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 (Conway, 2022a). Another metric 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 Proof-of-Work and Proof-of-Stake, it is important to measure how many nodes or pools (a pool is a group of miners which join together to increase their chance of creating the next block) control the majority of the network. The NC 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 (BFT), it is only required to control one-third of the network's computing power or staked capital.

2.1.3 Security

In cybersecurity, the CIA acronym stands for confidentiality, integrity, and availability. Confidentiality involves the tasks of keeping particular information secret. This is done in blockchain platforms in the form of encrypted addresses. Users can interact with the system using public key hashes without revealing their real identity. However, this only guarantees pseudonymity as the ledgers are public and transactions can be traced. Once a public address is compromised and the owner of an address is known, blockchain platforms no longer provide confidentiality. Integrity refers to data's consistency, authenticity, and accuracy. It also states that data must not be tampered with, which is achieved through the immutability of the blockchains. Availability means that the blockchain state is always available and readable.

Other security features come from the CAP theorem, i.e., consistency, availability, and partition tolerance , and states that none of these three can be achieved simultaneously. 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, the network 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., 2019) who state that consistency is not achieved simultaneously with availability and partition tolerance but only after a period of time (in Bitcoin's case the block has first to be confirmed before it can be considered consistent, which takes six confirmations where one confirmation takes 10 minutes). 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, under the denomination of availability such that we are left with: Confidentiality, which involves the privacy of a user, Integrity, which 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 can accept transactions at any time, Partition Tolerance means that the blockchain works even when part of the network fails.

A blockchain platform does not only have to fulfill the CIA properties, it also must be resistant against numerous different types of attacks, such as DDoS attacks, majority attacks (51% attack and single shard attack), double spending or transaction flooding (Zhang et al., 2019). Another measure of security is the Nakamoto Coefficient. Furthermore, 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.

3 SELECTION CRITERIA AND METRICS

Every platform takes a different approach to the trilemma properties. This poses a challenge for prospective blockchain developers and users as a particular blockchain platform may not fulfil their requirements, e.g., an application requires high, intermittent transactional throughput, which only a few platforms support.

3.1 Selection

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

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 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 is already applying a method called sharding to its blockchain, which Ethereum, the platform with the most protocols and highest TVL, apply in 2023. The selection is summarized in Table 1.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

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

3.2 Consensus Protocol Analysis

The different consensus protocols are summasrised in Table 2. It includes all the consensus protocols used by the selection of blockchain platforms and additional consensus protocols which may be necessary to understand more complex ones. Table 2 summarizes the analysis. However, given the lack of metrics, a comparison between consensus protocols in terms of throughput for scalability is not expedient. Therefore, the scalability of a consensus protocol can only be measured partially and transaction finality (latency of a new block) is used for it. Decentralization is measured in the number of nodes a network has and security in the network's Byzantine Fault Tolerance.

3.3 Platform Analysis

The metrics chosen to analyze the blockchains are generally available for all public blockchains, comparable and interesting for users. Table 3 includes the current transactions per second a platform can achieve. This shows that some platforms are not yet fully implemented but will reach higher tps in the future. These metrics (Croman et al., 2016) help to compare blockchains in terms of scalability.

Current TPS: measure the average throughput of a blockchain platform at the moment of writing, as some platforms are not fully implemented yet or are yet to gain more popularity.

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

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

Number of Nodes: is an important metric to measure the decentralization of a blockchain. The number will only include the nodes responsible for block creation.

Time to Finality: is the second measure 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 5 offers a detailed comparison of each platform's decentralisation and includes the Nakamoto Coefficient with the metrics (Conway, 2022a).

Number of Nodes: Reports the 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. 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.

Fixed number of Nodes: States whether the number of nodes participating in the block creation is fixed or can scale indefinitely.

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

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

Table 6 depicts the security aspect of the blockchain platforms, with the metrics:

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

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Table 2: Comparison of Consensus Protocols.

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

Availability: is important as transactions always occur.

Anonymity: illustrates whether the blockchain offers complete anonymity or pseudonymity where a transaction can still be tracked and linked to an address.

Note that the Nakamoto Coefficient is also a metric used to measure the security of a network as large entities which hold a lot of the networks computational power or staking capital could collude and take over the network..

The metrics are used in scientific articles and in the blockchain community to analyze the performance of different platforms (Hafid et al., 2020). The three trilemma aspects are:

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

The maximum throughput and latency of a network are the most decisive indicators for scalability for users who do not actively participate in the network. 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 will be assessed based on a network being deterministic or probabilistic. Block time will be rated by the sec it takes for a network to create a new block. Latter, however, will not be used in this decision framework as all the selected blockchain platforms present a similar block time. Thus, only the maximum transaction per second as some presented blockchains are not fully implemented yet and the time to finality (deterministic or probabilistic) will be used to measure the scalability of the blockchain platforms.

3.3.2 Decentralization

According to Conway (Conway, 2022a), 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. Following this, we will 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 than another.

3.3.3 Security

Security will be measured by means of the Byzantine Fault Tolerance of a network. It is stated by Bracha (Bracha, 1987) that 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. For networks with a Byzantine Fault Tolerance 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. In addition, to Ethereum, Avalanche, and Polygon, where >50% of the network needs to be malicious to bring it to a stop, also BSC is considered secure in this framework as all validators have to be

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Table 3: Scalability of Blockchain Platforms.

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

Table 4: Decentralization Ranking, with NoN Number of Nodes, HR Hashrate / % of supply staked, NC Nakamoto Coefficient, DI Decentralization Index.

	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

approved by a central authority and must publish their identity.

3.3.4 Resources and Tools

To analyse the different blockchain networks we studied whitepapers and online documentation – we do not list all individual sources of information separately due to their large number. As those sources, mainly focus on selected properties, such as maximum throughput or the functions of their consensus protocol, block explorers were used to get real-time and historical information on a blockchain. These block explorers are mainly developed by the blockchain foundation, reputable community members, or former blockchain developers.

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

4 BLOCKCHAIN PLATFORM ANALYSIS

4.1 Ethereum

Ethereum was created to provide a blockchain with a built-in Turing-complete programming language that everyone can use to create Smart Contracts. Since then, Ethereum has become the most popular blockchain in building decentralized applications (DApps). This is also shown by its domination of the Total Value Locked and the number of protocols built across all blockchain platforms. For example, at the time of writing, the TVL on Ethereum makes up nearly two-thirds of the total TVL, and Ethereum boasts just about 500 protocols built on it.

Scalability. Similar to the most well-known blockchain - Bitcoin - Ethereum uses the **PoW** consensus protocol. However, by decreasing the **block interval** to **12 to 14 sec** Ethereum is able to achieve a higher throughput of **10 to 15 transactions per second** which, however, is not enough as daily 150,000-200,000 transactions are pending. Due to that, Ethereum plans to transition to a PoS consensus protocol which realizes higher throughput.After a transaction is processed in Ethereum, it is still not considered final as PoW is a **probabilistic** consensus protocol, but the time to finality is greatly lower than Bitcoins due to its lower block creation time.

Decentralization. Ethereum is the second-largest blockchain network with around **6,000 nodes** which are competing against each-other. However, three pools control over 50% of Ethereum's total hash rate.

Security. To fortify against attacks such as the Denial-of-Service-Attack, Ethereum uses the **gas system**. Gas fees compensate Ethereum miners for their work in processing transactions and securing the network.

4.2 Cosmos

Cosmos is a network of many independent blockchains which can communicate together thanks to the inter-blockchain communication (IBC) protocol. This allows for fast exchanges between the different blockchains built on Cosmos. Cosmos' objective is to create an environment that allows multiple parallel blockchains to inter-operate while retaining their security properties. Cosmos uses its in-house developed **Tendermint BFT consensus**

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Table 5: 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 Represent.	Yes	45.81%	8[2]
Polygon	100	Validators	Yes	30.89%	13[*]
Harmony	250 per shard	Validators	Yes	42.48%	5[*]

[1] Ethereum is the only PoW platform, i.e, hashrate is used to measure decentralization.

[*] No central source exists for the Nakamoto Coefficient for some, i.e., is estimated.

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) 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 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 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

protocol. Therefore, it is also called a **Layer 0 solution** as it allows for multiple Layer 1 blockchains to be built on. Following this, building a new blockchain on Cosmos allows for future compatibility between all blockchains on Cosmos and new blockchain innovations.

Scalability. This also means that in general Cosmos applies horizontal sharding to further increase its **10,000 transactions per second** per built-on blockchain which are also called **zones**. However, this number drops wrt. the number of validators a blockchain chooses to utilize.

Decentralization. Currently, the platform is secured by **175 validators** where 7 of them possess over 33% of the staked capital.

Security. Any $\geq 1/3$ coalition of voting power (staked capital) can halt the blockchain by no longer participating in the consensus. This may result in the blockchain forking. Cosmos employs slashing to prevent such an attack where malicious nodes are penalized for not casting their vote. Additionally, to prevent transaction flooding, Cosmos uses fees to discourage possible attackers due to the financial cost of such an attack.

4.3 Binance Smart Chain

The Binance Smart Chain (BSC) is the second blockchain developed by Binance after the Binance Chain (BC). The critical difference between these two chains is that the BC did not support Ethereum-based applications, while the BSC is equipped with the Ethereum Virtual Machine (EVM). Furthermore, both BC and BSC are built upon Cosmos, allowing for fast communication between the two Binance Chains.

The reasoning behind the creation of a new parallel blockchain to the Binance Chain is the support of Smart Contracts. As BC focused on its na-

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

tive DeFi application Binance DEX (Decentralized Exchange), BSC aims to be more flexible and usable. Even though BSC is built on Cosmos SDK, it does not use the Tendermint PoS consensus protocol. However, it uses the **Proof-of-Staked-Authority (PoSA) consensus protocol**, which is a combination of the Delegated-Proof-of-Stake (DPoS) and Proof-of-Authority (PoA).

Scalability. BSC supports a rate of **40 to 60 transactions per second**. Given the usage of the PoSA consensus protocol and not Cosmos' Tendermint PoS the **maximum throughput** BSC can achieve is **160**. To reach **block finality** BSC requires two thirds of all validators to sign a block, which takes about **75 second** with a **block time** of around **3 sec**.

Decentralization. In a PoSA network, there exist only **21 validators**, which take turns creating a new block just like in a PoA network. However, the validators are selected every 24 hours based on their stakes, where the highest-staking nodes win. The decentralization of BSC due to the lower number of validating nodes leads to improved scalability, which is visible when looking at the TPS. Out of the 21 total validators 8 control more than ⅓ of the staked capital.

Security. As PoSA also implements Slashing to penalize Byzantine validators for most transactions ½N+1 signatures are enough as confirmation. Therefore, a validator is not promptly punished for being unavailable but must remain over a certain threshold. However, they receive less or no reward when they are offline.

4.4 Avalanche

Contrary to other blockchains, Avalanche is not built using the typical blockchain data structure (linked list), but instead uses a **Directed acyclic graph (DAG)** data structure to improve its scalability. To ensure security Avalanche uses the **Snowflake-to-Avalanche (SoA) consensus protocol**. The objective of Avalanche is to cover three blockchain-related areas:

1. Building application specific blockchains
2. Building scalable decentralized apps (DApps)
3. Building digital assets with custom rules (smart assets)

To realize points 2 and 3 above, Avalanche supports Solidity-based smart contracts through the Ethereum Virtual Machine (EVM). To further increase scalability Avalanche offers three built-in blockchains for different use cases.

X-Chain. The Exchange Chain is the main chain for trading and creating digital smart assets.

C-Chain. The Contract Chain allows for the creation and execution of Smart Contracts.

P-Chain. The Platform Chain is the chain which coordinates validators, tracks subnets and allows the creation of new subnets.

Scalability. Avalanche can reach **thousands of transactions (5,000+)** while retaining full decentralization thanks to its DAG structure. This number scales even higher with an increase in different subnets (X-Chain, C-Chain, and P-Chain). Currently, Avalanche processes 5-10 transactions per second and a **block time** of just under **2 sec**. The **time to finality** in Avalanche is nearly instant (up to **1 second**).

Decentralization. Avalanche is secured by around **1,250 validators** where 52 establish a superminority. This high NC is reached due to a staking limit imposed on validators to create more diversity among the network.

Security. Avalanche can uphold safety even when the attacker exceeds 51% of the network's staked capital. However, the platform gives up liveness in exchange for security.

4.5 Solana

Solana is a blockchain platform based on its own consensus protocol Proof-of-Stake (PoS) realized by **Proof-of-History (PoH)**. Solana aims to solve the blockchain trilemma, which they state to resolve by achieving a **maximal throughput of 710,000 transactions per sec** while having thousands of validators and being byzantine fault tolerant. This performance is achieved by combining PoS with the horizontal scaling of PoH.

Scalability. The block creation time is also under one second, which holds true with a current **block time of 0.7** sec. In contrast, finality is **achieved instantly** as Solana is deterministic.

Decentralization. Presently, Solana reaches **between 1,500 and 2,500 transactions per second** while being secured by nearly **2,000 validators**. Out of this 2,000 validators 27 control over one third of the staked capital.

4.6 Fantom

Fantom's primary goal is to solve the scalability issue of existing blockchains by introducing a new ”DAG-based Smart Contract platform”, which is secured by the **Lachesis Consensus Algorithm (LCA)**. Fantom does not only see throughput as the major problem of the scalability issue but also time to finality - how long it takes for a transaction to be processed and confirmed.

Scalability. The main focus of the Opera Chain (Fantom's main chain) was to provide **deterministic (absolute) finality** with **block time of 1 to 2 sec**. Given the structure of the network, Fantom is also able to support up to **300,000 transactions per second**.
Decentralization. The drawback comes with decentralization as currently (14-June-2022), only **92 validators** are securing the network. This is due to the vast limits Fantom imposes for a node to be a validator, as they have to hold at least 500,000 (or around $115,000). Fantom achieves a Nakamoto Coefficient of 3.
Security. To prevent Sybil attacks (one entity tries to create multiple nodes), a single computer can only create a single node. Other attacks include Parasite Chain, double spending, and transaction flooding. The verification of blocks through Clotho and Atropos event blocks prevents the former. If a block is not connected to the main chain, it is deemed invalid and is ignored. Transaction flooding is averted by imposing fees.

4.7 Tron

Tron is a network built on a fork of EthereumJ and seeks to offer a public blockchain with high throughput, scalability, and availability. It uses the **DPoS consensus protocol**.
Scalability. Thanks to the limited number of SRs, the need for communication and approval is reduced, and the Tron network can achieve a high throughput of a **maximum of 2,000 transactions per second**. It also supports Smart Contracts thanks to the Tron Virtual Machine (TVM), which is fully compatible with the Ethereum Virtual Machine (EVM). Currently, it processes an average of 50 to 200 transactions every second, sometimes spiking up to nearly 600 transactions per second. After a new **block** is produced **every 3 sec** it takes another **60 sec** (19 blocks) for a new **block** to be **finalized**.
Decentralization. The network is secured by 27 Super Representatives (SR), who are elected every 6 hours from the over 6,000 nodes connected to the Tron blockchain. Eight of them control more than one-third of the staked capital. The intention behind the election is to support diversity of the SRs in a way to avoid that not always the same nodes are creating new blocks.
Security. Transactions on Tron are not paid with their tokens but are paid by ”bandwidth points”. Each day, an account receives a certain amount of free bandwidth points, whereas accounts with staked capital receive more points. If an account runs out of bandwidth points, tokens must be burned (destroyed) to pay for additional points. This system is implemented to prevent transaction flooding attacks.

4.8 Polygon

Polygon, formerly called Matic, is a **Layer 2 solution** that works atop the Ethereum blockchain and tries to solve its scalability issue. ”Matic Network strives to solve the scalability and usability issues, while not compromising on decentralization and leveraging the existing developer community and ecosystem. It is an off/side chain scaling solution for existing platforms to provide scalability and [...] user experience” according to their whitepaper. Polygon achieves high throughput by implementing **PoS**. Instead of sending single transactions to the Ethereum main chain, it groups up clusters of transactions which are then committed to Ethereum so that Ethereum can still process what is happening. **Scalability** A single sidechain can handle up to **65,000 transactions per sec** and can horizontally scale by adding more sidechains. Presently, Polygon achieves a throughput of 30-50 transactions per second, creating a new block every 2.3 sec while maintaining a block confirmation time of 2 sec.
Decentralization. Polygon has **100 validators** where 13 create a superminority.
Security. Since Polygon is built on Ethereum, it also implements the Gas system to prevent transaction flooding and to help secure the network. Polygon also provides Fraud Proofs where any individual can state a transaction as fraudulent and challenge its veracity. If the challenge is successful, the parties involved in the fraud are penalized (slashed) and the challenger is rewarded the slashed fund. This constitutes an incentive for parties to investigate the veracity of transactions and to detect frauds in the network.

4.9 Harmony

Harmony aims at high and secure throughput by dividing the blockchain into different shards. This is realized by implementing a beacon chain to which all shard chains report (beacon chain is also a shard) and using the **Fast Byzantine Fault Tolerance consensus protocol**.
Scalability and Decentralization Currently, Harmony deploys four shards where each shard can process up to 500 transactions per second and is secured by **250 validators each**. Five of them currently hold over 33% of the staked capital. In the long run, Harmony can scale up to 2,000 shards, allowing for a theoretical **throughput of 1 million transactions per second**. However, at the moment, the network only

processes around ten transactions per second. Furthermore, thanks to Harmony's FBFT consensus algorithm, the block creation time is reduced to 2 sec, and a **new block is considered to be final instantly**.
Security. All validators who participated in signing a new block are rewarded a protocol-defined number of new tokens and the transaction fees. Later exists to protect the network from the transaction flooding attack just like in other consensus protocols. The security of the different shards and to prevent Single Shard attacks is achieved through a combination of Verifiable Random Function (VRF) and Verifiable Delay Function (VRD), where validators are randomly assigned and mixed among shards.

Similar to others, Harmony uses slashing to penalized dishonest validators. It is also possible for a validator to challenge a transaction and to prove the misbehaviour of another validator.

5 CONCLUSIONS AND FUTURE WORK

The decision on the right blockchain platform to support storage and trust management in information sytems is difficult. We compared a selection of blockchain platforms in terms of important qualities for information systems such as scalability, decentralization, and security. The selection was made on multiple criteria, summarized as the platforms' 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' theoretical 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.

REFERENCES

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

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

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

Conway, L. (2022b). Proof-of-work vs. proof-of-stake: which is better? *Blockworks*.

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.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS