Network Security and implications of PoS. Is PoS the future of Distributed Ledger Technology?

On the example of the Cosmos ecosystem.

Author:
Zafercan Cakir
Stake&Relax Validator

Lucerne, 12.09.2022

Abstract

The Crypto-industry is one of the fastest growing industries in the world. Within only 12 years of its existence, the total market capitalization shot from zero to $1.2 trillion and reached an all-time-high of more than $3 trillion back in November 2021. With the rapid growth of the industry, fundamental technological assumptions are being innovated in order to accommodate the needs and demand of the market.

One of the major transitions is the vast adoption to so called proof-of-stake based consensus algorithms. In short: proof-of-stake networks replace „mining“ with „validating“- or „physical hardware" with „virtual servers“. Even the second largest cryptocurrency in the world, Ethereum, is making the switch and replaces the resource-heavy proof-of-work algorithm with a newly designed PoS algorithm as early as Q3 of 2022. The rise of PoS networks also opens up new revenue-models for network *Validators* (node operators), as physical mining hardware is being replaced by less energy intense servers and cloud operators. Those network *Validators* can be anything between individuals to large software companies. All it requires is a running node and enough capital (native tokens) to validate blocks and verify network transactions.

To better understand how PoS works, this paper also contains a case study to analyze the cosmos ecosystem which pioneered the PoS concept with „Tendermint“ back in 2014. In addition, a survey will be conducted to get insights form the active network *Delegators* and *Validators*. For a representative survey, outreach to delegates was randomly committed.

Keywords: Distributed Ledger Technology, Proof of Stake, Validator, Delegator, Staking

Table of Content

Table of Figures

List of Appendices

List of Abbreviations

Abbreviation	Definition
AAA	Authentication Authorization Accounting
ABCI	Application Blockchain Interface
AuD	Assets under Delegation
BFT	Byzantine Fault Tolerance
BGP	Border Gateway Protocol
BGP	Byzantine General Problem
BSC	Binance Smart Chain
BTC	Bitcoin
CEX	Centralized Exchange
CIA triad	Confidentially, Integrity and Availability
DAP	Decentralized Autonomous Organization
DOT	Polkadot
DLT	Distributed Ledger Technology
DeFi	Decentralized Finance
DPoS	Delegated Proof of Stake
ETH	Ethereum
HBAR	Hedera Hashgraph
NIST	National Institute of Standards and Technology
NFT	Non fungible Token
pBFT	practical Byzantine Fault Tolerance
PoA	Proof of Authority
PoH	Proof of History
PoS	Proof of Stake
PoW	Proof of Work
PPC	Peercoin
PPoS	Pure Proof of Stake
SDK	Software Development Kit
SOL	Solana
TPS	Transactions per second
OTC	Over the Counter
IBC	Inter-Blockchain Communication Protocol
ICO	Initial coin offering
ICF	Interchain Foundation
ISP	Internet Service Provider

1. Introduction

The topic of cryptocurrencies is omnipresent and repeatedly in the news headlines of various media outlets. Experts agree that cryptocurrencies have evolved from a niche to an established sector of alternative investments. But what is the underlying technology behind it, and what does the future look like? Is the Consensus Mechanism PoS, which is gaining widespread acceptance, safe? Does it have vulnerabilities? If yes, what are these?

This study aims at answering these questions. The paper is structured as follows. Chapter 2 presents the related literature and introduces network security and the implications of Proof-of-Stake. Chapter 3 will guide the reader through the chosen methodology and data aggregations used to conduct the survey. The case study and survey, as well as the results, are presented in Chapter 4. Before Chapter 5 concludes the study with a critical discussion of the empirical findings.

1.1 Relevancy

Validating becomes a Business, therefore the operations getting more proficient, and several companies specialize on this sector. Smaller Validators which are present since the early days growing rapidly and have already established themselves as a brand. This brings the interest of private equity company firms to the table. Small entities becoming companies with several employees providing infrastructure to the largest Layer 2 blockchain solutions. Powerful partnerships and strategic private equity investments across blockchain foundations and Web 3.0 companies throughout the world is becoming normal.

More and more companies evolving during this stage of professionalization. As the industry is still young and Proof of Stake (PoS) becomes further adopted. Especially venture capital funds focus on positioning themselves quite early in young but fast-growing industries. Accordingly, it is important for the company to analyze the current environment and implementation of POS. In this context, the future viability of operating *Validators*, network security, and potential weaknesses and criticisms is to be addressed.

1.2 Problem

As cryptocurrencies and the underlying public blockchains acquire popularity on the mass market, and progressively institutions show increasing interest in this sector, it is more vital than ever to conduct research on the security aspects of various consensus mechanisms.

The change of the consensus mechanism of Ethereum from Proof-of-Work (PoW) to Proof of Stake (PoS) triggered many projects to launch directly with PoS. Furthermore, the long-standing and harsh criticism that the PoW process is not environmentally friendly and consumes too much energy was one of the driving forces behind the current largest Layer 0 and Layer 1 operating on PoS. With the transition of Ethereum from PoW to Ethereum 2.0 PoS, which is presently underway, the second largest cryptocurrency, with a market value of ~377b $ as of February 8th, 2022, will rely on the security and consensus method of PoS.

Accordingly, it is of great relevance to examine the functionality and the infrastructure as well as the advantages and disadvantages. This includes among other *Validator sets* and tokenomics as PoS cannot be implemented on a fixed max cap on the supply side, since both the network *Validators* and the token holder needs to be incentivized to run a node and stake their tokens. Therefore, the supply issuance must be inflationary. For instance, the token "ATOM" has an inflation of 9.38% per year as of March 31st, 2022 and the staking reward is at 14.86%. The spread between the inflation and the staking rewards comes from the fact that not all tokens are staked. If every token of $ATOM would be staked, the staking reward would be equal with the inflation rate. So, all token holders would maintain their share of the network and it would not be diluted. In the case of $ATOM, 63.24% of the circulating market supply is bonded *or staked*. The less token holders decide to stake their funds, the higher the staking rewards.

In addition, the economic incentive structure needs to be designed in a very mindful way in order to align the sustainability of the security model with the token circulating demand. Node operators can be considered as company-like individuals. If it is not profitable for the validator to run a node, they will move to other networks which are more profitable. Subsequently, the network would be less secure and more vulnerable to malicious attacks. However, if it becomes too profitable, it is possible that large institutions would run very large nodes, resulting in network centralization. This would result in a higher risk for the whole network as few players could control the chain and perform consensus attacks.

As a result, it is critical to examine the *Validator sets* and drivers for businesses (or individuals) to secure the network and run a node.

1.3 Research Objective

This study aims to provide insights about the current PoS environment and the implementation of PoS. In particular, the paper addresses a specific ecosystem and examines the future viability of *Validators* in the context of network security and potential vulnerabilities and also points out some criticisms. It also mentions the challenges and opportunities that occur with this consensus mechanism and if PoS is suitable and contributes enough security for the network.

Although nodes can be controlled by anyone with appropriate technical knowledge, it is more viable for businesses because they have the necessary infrastructure and resources. In the end it is an investment to set up a node. Besides the costs to bootstrap a node, it also needs enough delegations to get in the active *Validator set*. As a result, developing a brand for the node is critical. In some situations, it also aids in the creation of a community around a node, which can be difficult. This paper will deal with the specific roles of individuum's, companies, nodes, and the projects itself.

To elaborate the topics of PoS, certain questions need to be clarified. As Distributed Ledger Technology (DLT) has different elements to achieve decentralization, the specific roles that the consensus mechanisms play must be elaborated. By taking a closer look into PoS, various kinds of characters needed to be addressed. It must, among other things, explain what nodes are, what kinds of nodes exist, why they are important, and how they are dispersed. It should also specify which roles are played within the PoS system by whom and what motives they have. Ultimately the aspect of network stability and security must be researched.

<u>The research question is therefore:</u>

What does the current environment of PoS resemble to and what implication does it have? The following four sub-questions are derived from this:

- - How does the existing PoS environment appear, and what vulnerabilities do they have in terms of network security?
- Does PoS provide an additional value for node operators and the projects compared to PoW nodes besides validation transactions?
- Which aspects must be considered in the PoS regarding network stability?
- Is PoS the future of DLT, or can certain improvements be made?

2. Theoretical Knowledge / Literature Review

Before diving into the case study and further analysis the current literature and theoretical concept will be explained. This chapter provides sufficient knowledge to understand the new rising technology of DLT and the underlying concept. It is organized by concept importance to help the reader gradually grasp the concepts of blockchain and network security.

First, it is of importance to differentiate DLT from Blockchain. Blockchain technology is only a type of distributed ledger technology. Distributed ledger means that the databases are spread across different nodes, whereas a blockchain needs a consensus mechanism. There are also other approaches like Tangle which is implemented by IOTA or the Gossip-over-Gossip protocol which is used by the cryptocurrency Hedera Hashgraph (HBAR).

Many people think that the blockchain has only existed since the invention of Bitcoin (BTC) in 2009, but this is a common misconception. The prototype of the blockchain was created in 1991, when two cryptographers, Stuart Haber, and Scott Stornetta, drafted a paper about their idea of providing electronic documents with a timestamp and a hash value. They wanted to ensure that documents could be stored in a tamper-proof manner. In 1995, they printed a weekly ad in the New York Times for their company 'Surety', founded in 1994. The ad included the hash value that could verify that documents had not been altered or forged. Thus, the first blockchain was available for public viewing as early as 1995.

After the pseudonym “Satoshi Nakamoto” solved the double-spending problem, the concept of blockchain became widely public. "Bitcoin" has the consensus mechanism PoW, which is under fire due to its massive energy consumption, among other things, and a kind of revolution has begun in which more projects are moving to the consensus mechanism PoS.

2.1 Consensus Mechanisms

As already mentioned in the introduction above, the first consensus mechanism was the PoW mechanism, which was adopted by Bitcoin. However, the problem of consensus existed long before Bitcoin, the first and most widely known cryptocurrency. The so-called Byzantine Generals Problem (BGP), which Adnan Shkoor described in a medium article[1] and showcased

[1] Shkoor, 2019

the connection between a problem from the Byzantine empire (330 AD – 1454 AD) and the blockchain today. Even back then there was the problem of validating information for its correctness and approving transactions.

This problem was later summarized[2] and explained in 1982 as follows:

Several divisions of the Byzantine army surround an enemy city and each division has its own lieutenants. They can only converse through communications, and a commander sends orders to the lieutenants to attack or retreat. The commander or some of the lieutenants can be dishonest and try to manipulate the orders. When a lieutenant receives a communication from the commander and the lieutenants, he must assess whether the order can be carried out and is not influenced. Therefore, the Byzantine Fault Tolerance (BFT) states that a consensus is reached if 2 out of 3 actors are honest and provide the same information.

Over the years, new concepts and consensus mechanisms have developed. However, it is first necessary to clarify what consensus mechanisms are and what purpose they serve before going into detail about individual mechanisms. Traditional information is centralized, and it is controlled by few authorized centralized nodes. Trust is generated since the participants are known and it is easy to control since its centralized. The central party has the authority to maintain and update the database, thus allowing data to alter quickly. This, however, has a disadvantage, and that would be if a mistake was made or if bad intentions were pursued. The distributed system works without any single authority rather by many nodes. Therefore, it needs to achieve trust among participants. With adopting consensus mechanism, the blockchain can ensure a trustless point-to-point information transfer of the different nodes. This ensures that each node validates information and will only execute if all decentralized nodes agree on the validity of the information transaction. Through this the reliability of the whole network is possible. The blockchain ensures that the transaction cannot be maliciously tampered. Without any consensus mechanisms, the information could suffer from a malicious attack and the information could easily be manipulated. So, the consensus mechanisms are the backbone of a working blockchain and have been experienced immense development in the past years. It plays a significant role in ensuring the integrity, performance, and the networks security.

[2] Lamport, Shostak, & Pease, 1982

Bitcoin is solving the Byzantine General Problem by a consensus algorithm based on an economical incentive where computer power must be deployed in exchange for distribution of block rewards and transaction fees. However, the PoW consensus mechanism is established by an arduous mining process that consumes a lot of energy, which is criticized as inefficient. In addition to the problem of energy consumption, there are other limitations such as inefficiency, delay, and its vulnerability to security threats. This mechanism is still in place and run on various blockchains. As already mentioned, new consensus mechanisms have been developed over the years, namely PoS and DPoS. In both PoW, as well as PoS the tokenomics and the game theory of the distribution of the regards plays a vital role. However, this will be addressed later in the chapter. Aside from occasional code problems, the consensus process is the core architecture that binds a blockchain together and plays an important role in network security.

The article „Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack" elaborated on the weaknesses of consensus mechanisms in the context of attacks, which can be seen below in Table 1[3].

Consensus mechanisms	51% attack	Sybil attack	Routing attack	Phishing attack
PoW	✓	✓	✓	✓
PoS	✓	✓	✗	✓
DPoS	✓	✓	✗	✓

Table 1: Vulnerable attacks for different consensus mechanisms

This demonstrates which attacks are applicable for certain consensus mechanisms. Some of the attacks will be described in more detail in the following section "network security".

2.2 Network Security

Blockchain technology has a structure of data that has inherent security. It is based on fundamentals and has different facets like cryptography, decentralization, and consensus, which ensure trust in a transaction as described in the section before. Implementing the right design,

[3] Sayeed & Marco-Gisbert, 2019

game theory and flawless code are also significant aspects. The blockchain is designed to have no single point of failure; also, the entire architecture is designed for a specific purpose that must function and be maintained. Blockchain security goes beyond its inherent security characteristics and differs from network security[4].

For understanding reasons, the definition of network security is needed. It is a broad term and includes a variety of technologies and processes. In general, it deals with rules and configurations to protect the integrity, confidentiality, and accessibility of networks and data with help of software and hardware[5]. Every company irrespective of the branch, size, or infrastructure needs some kind of network security to protect its data from malicious attacks. The networks of today are becoming increasingly complex and are constantly changing. In order to protect the reputation of the company and avoid balance sheet damages, it is necessary to eradicate weak points in the system so that the management of the network becomes indispensable. Network security is a subcategory of cyber security that safeguards the network and its data from DOS attacks, trojans, viruses, and worms. So, the data can be transferred safely within the network without being changed and the confidentiality must be ensured

After defining Network security, it is necessary to explain why it is crucial for blockchains and what it has to do with it. Because DLTs and blockchains are networks, network security applies as well, albeit with additional ramifications. So blockchain security is a subset of network security. The distinction is that various procedures, such as consensus or game theory, must be considered when the network's stability is to be guaranteed. Blockchain security is a complete risk management system for networks including best practices to mitigate the risk of fraud and cyberattacks. In principle, it includes everything that could jeopardize the network and provides precautions to prevent malicious participants. As a result, blockchain security differs from cyber security in that both systems inherit various traits, functions, and serve different purposes. Therefore, also the security prerequisites diverge from each other. It is also important to distinguish between different blockchains as each of them come with different challenges[6].

Private permissioned blockchains are networks that are run by trusted and legitimized participants, whereas new participants must be approved. This is done by a central party, which also establishes the network's rules and can change them at any time. The permissioned

[4] IBM, 2022
[5] Patel, 2020
[6] Thames & Schaefer, 2017

blockchains usually have a Proof-of Authority consensus mechanisms. Within this system, confidential data can be transferred or recorded among the participants, and it is ensured that the data is not tempered[7]. To secure this kind of network certain control and security features have to be implemented. As only authorized people or devices have access, it is critical to ensure that access control regulations are in place and that the person in the network is identified. The central party can choose whether a member has full access and control, allowing them to upload data, or if they can only read particular data. Furthermore, it is significant to avoid harmful programs that gain access to the network through trojans or similar. Additionally, education of the members is important since social engineering can enable access to the potential assailant. This sophisticated attack may result in a verified network member disclosing the log-in credentials. According to the Data Breach Investigations Report 2021, 61% of breaches are attributed to compromised credentials, with social engineering accounting to 85% in the way this information was obtained[8]. The hackers can gain privileged access to organizational networks and obtain information or even financial benefits.

Next to the mismanaged and compromised credentials, there are more potential vulnerabilities for the network and its security. Beyond the malware, the administrative level has great influence as a result of the centralized structure and can carry out hostile acts. It should be noted, however, that the structure of the private blockchain means that the participants are known and can be identified and penalized in the event of incorrect behavior. This leads to the fact that under ordinary circumstances, the participants adhere to the set rules and there is no substantial danger for the network due to internal activities. Private permissioned blockchains are also known as corporate blockchains, however the centralized party does not have to be a single person; instead, it might be a consortium in which a group or parties collaboratively set the network regulations.

These have four main characteristics [9], which can be summarized as:

- Accountability: Participants are known and can be penalized for their behavior.
- Permissioned: Only authorized entity can participate within the network.
- Mutable: The data can be changed if agreed to do so.
- Scalability: Fast transaction are possible based on the centralized structure.

[7] Simplilearn, 2021
[8] Verizon, 2021
[9] Hertig, 2021

The public permissionless blockchain differs from the private & enterprise blockchain. To elucidate, it can be compared to the internet and the intranet in the early 2000s. Whereas the public blockchain is open to everyone, the private/ corporate blockchain functions similarly to an intranet within a firm to transfer data that is not open to the public.

Figure 1 illustrates the four dimensions of blockchains public/private and permissionless/permissioned[10]. Each of the quadrants has a specific use case and distinctive characteristics[11]. This paper will focus on the most common and wildly spread blockchain; the permissionless public blockchain.

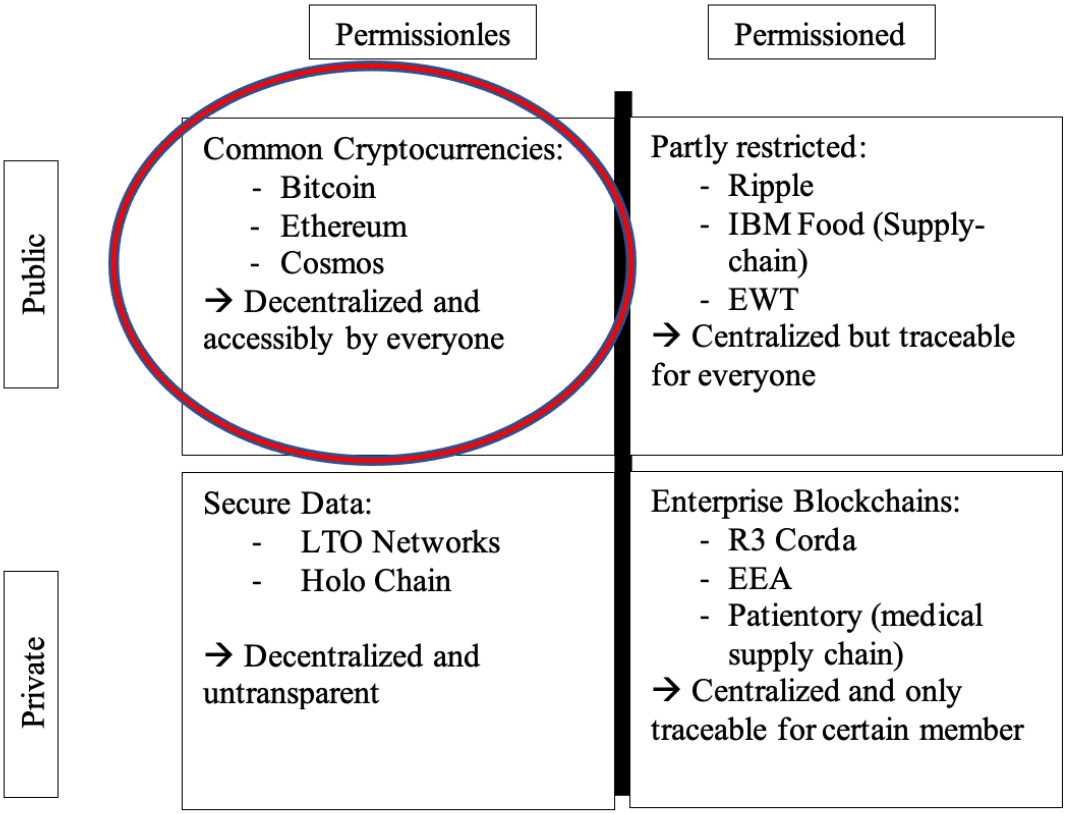


Figure 1: Types of Blockchains

Permissionless public blockchains have their strengths in decentralization and network security but are lack scalability[12]. This leads directly to the "Blockchain Trilemma" which emphasizes the different advantages and challenges of the four different blockchains seen in Figure 1. The blockchain trilemma, illustrated in Figure 2, describes the goals of scalability, security, and decentralization. But only two out of three points can be achieved simultaneously. Whereas scalability and security are secured in permissioned blockchains, it is however, controlled by a

[10] Daniels, 2018
[11] Vardai, 2021
[12] Wachal, 2021

few participants, and the point of decentralization is not given, therefore the risk of point of failure is high. Decentralization and security are given in permissionless blockchains like Bitcoin, but it lacks scalability as the transaction throughput is around 3 – 10 transactions per second (TPS)[13]. As described above public blockchains are accessible by everyone without any certain permission and the data can be tracked by any individuum. The code is open source and everyone with enough technical knowledge can launch a node which contributes to the network security. This also further leads to more decentralization. As the strength of public permissioned blockchains is network security it should be emphasized more specifically.

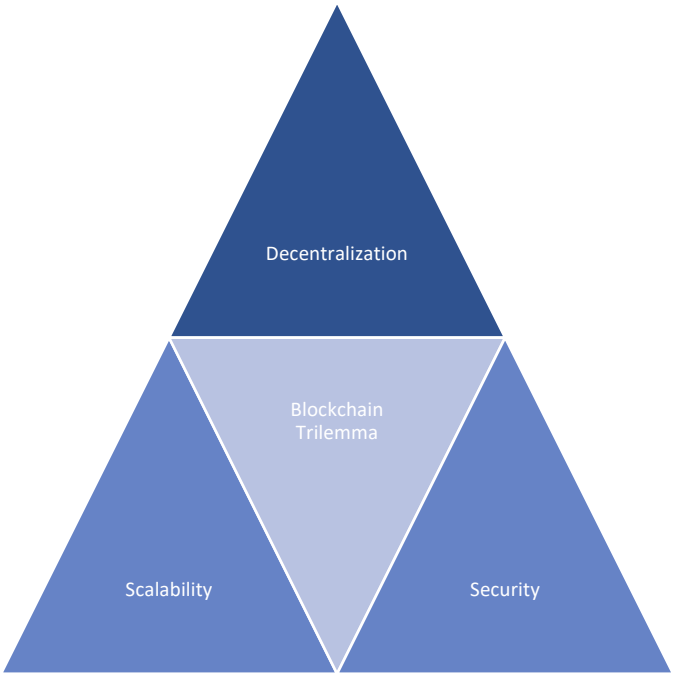


Figure 2: Blockchain Trilemma

To identify problem areas and develop security policies the current state of literature uses the CIA triad model. The three main components: confidentiality, integrity, and availability (CIA) represent a fundamental objective of information security. This model can be used to assess the current maturity level of blockchain technology according to an article from Deloite[14] as it is comparable to the rising adoption of the internet in the 2000s.

[13] Mehammed & Lemma, 2021
[14] Piscini, Dalton , & Kehoe, 2017

Confidentiality mean that the data is only accessible by authorized and interested parties. Public blockchains are generally designed without any authentication and authorization controls. Hence, it is accessible to everyone and has an open-source nature. This is especially essential for private blockchains since attackers could gain sensitive data. The implementation of box full of block data encryption and Authentication Authorization Accounting (AAA) will provide confidential access and ensure controls such that only authorized participants gain access to the data. As blockchain alone cannot solve this problem, other technologies, such as security measures, must be incorporated directly at the application level. Confidentially of Data could also be ensured if end to end encryption is implemented where only authorized recipients can decrypt the data through the private key. The risk is that the attacker compromises the private keys, which serve various purposes, including user information protection, data secrecy, and network authentication and authorization.

Integrity is already ensured by nature of blockchains, as the architecture provides immutability and traceability. Therefore, it difficult to tamper the with data within the network. There are several types of attacks that can pose a potential threat for the blockchain, which will be explained in the latter section of this chapter. Another key element of integrity is the right to be forgotten. As all data is housed on blockchains, visible data privacy laws may be difficult to enforce. A solution for this would be that the personal data is encrypted and the private key, which gives access to that information will be forgotten so it can be ensured that the data is no longer accessible. Another option would be that the real data is stored outside of the blockchain and only the access key is saved within it.

Availability is significant and complements the CIA triad. According to the National Institute of Standards and Technology (NIST), it is defined as "ensuring timely and reliable access to and use of information"[15]. Many attacks aim to put services and networks offline, which causes not only financial or reputation damages but also leads to data losses. To halt, a blockchain is unusual and is more costly for the attacker since the network must be overpowered. As there is no single point of failure and every node has a copy of the ledger, so data losses are unlikely. Once a node is down another node takes over and provides service for the network. This also makes the blockchain operational resilient[16]. To conclude it is important to note that it does not consider the aspect of hardware resources which can be manipulated and used without

[15] Paulsen & Byers, 2019
[16] Piscini, Dalton , & Kehoe, 2017

authorization[17]. Network security is nothing new and blockchain does not solve all the issues as there are still some vulnerabilities and challenges the technology must face against malicious hackers. Likewise, the types of attacks remain similar. In the following, different attack possibilities are shown, which could endanger the network.

51% attack: A 51% attack is likely the most dreaded problem in the blockchain industry, and it poses a particular threat to the PoW consensus mechanism. It aims to control most of the mining power, so the bad actor(s) can seize control over the ledger and falsify the transactions to their favor. However, it is less likely that the control can be maintained for an extended period. Commonly, it is financially motivated, and a double-spending occurs so the currencies get spent several times. Nonetheless, these attacks are expensive, as it requires significant amounts of resources. The Bitcoin network has yet to be subjected to a successful 51% attack. To achieve this, it would cost several billions and the value of the network would immediately lose significant value. It should be noted that this attempt to manipulate the network is not possible for private blockchains and less likely for PoS consensus operated blockchains[18].

Sybil attacks: A Sybil attack is an attempt to manipulate the network in a Peer-to-Peer Network through pretending to be various fake identities. This identity appears to be true for other network members, and the attacker can take control, allowing him to block transactions or validate illicit transactions for his own gain, as the attacker can outvote honest nodes in the network. In the worst case, this would cause an 51% attack as the attacker have so many fake identities that he controls the majority of it[19].

Routing attacks: A routing attack also known as border gateway protocol (BGP) is an efficient way to manipulate the network as the blockchain users can not notice the suspicious procedure. Hereby, the communication between nodes gets influenced. The attackers use the internet service provider (ISP) to redirect the data flow. This is a serious threat for the network and one of the attacks which can be dangerous for many blockchains including BTC. The potential danger is that a double-spending attack could be executed. However, this attack is not applicable to the PoS nor DPoS consensus network, which will be explained in the following section[20].

[17] Nasiri, Sadoughi, Tadayon, & Dehnad, 2019
[18] Sayeed & Marco-Gisbert, 2019
[19] Hooda, geeksforgeeks.org, 2019
[20] Apostolaki, Zohar, & Vanbever, 2017

Phishing attack: A phishing attack is used to get the credentials of a network participant. In the case of the blockchain, this would be the private key, giving the attacker complete access to sensitive data and the member's assets. The fraudster can contact the potential victim via emails, which includes fake hyperlinks. As far as the user is concerned, it appears to be a reputable source; hence, they insert their key and risk losing control. However, this is not a blockchain specific attack and is applicable for every consensus mechanism[21].

Further potential risks and vulnerabilities are described in the chapter twenty "Attacks on blockchain" of the book Advances in Computers[22]. The DDoS and DAO attack affected the Ethereum (ETH) chain in 2016, where 3,600,000 ETH tokens were stolen and forced the community to do a fork[23]. The study "Blockchain Technology Security Concerns" included a literature analysis describes many attacks and vulnerabilities of the various layers that make up the blockchain architecture. The article divides the vulnerability in four different layers: the *application layer*, meaning that the vulnerability is the user interface and the risk that the user gives permission to access unauthorized parties due a changed and limited visibility. The *data layer*, where the database is vulnerable as information's get restricted and false transactions could flow. The *consensus layer*, which is the backbone of the blockchain, and the majority of the participants have to agree whether the transaction is correct or not. An example for this issue is the 51% attack. The *network layer*, have vulnerabilities rooted from the internet infrastructure, where insufficient authentication, improper configuration or an insecure API design could cause a threat to the security of the blockchain[24].

Depending on the consensus mechanism the network security relies on distinctive characteristics. In general, the chain's and thus the network's security is determined by the consensus mechanism, which is related to the mining process, and thus the incentive for network participants, particularly the nodes that validate transactions. To solve the question if there are interdependencies between the incentives and the security of the blockchain the paper "Interdependencies between Mining Costs, Mining Rewards and Blockchain Security" analyzed the correlation of network security and mining incentives in a PoW blockchain like Bitcoin. As other parameters play a role, the results of the article cannot be applied one-to-one to the PoS consensus mechanism, but it may provide an indication of which direction it could

[21] IBM, 2022
[22] Aggarwal & Kumar, 2021
[23] Nicolle, 2022
[24] Tuyisenge, 2021

go as it is essentially the antithesis to this current paper. The findings revealed that there is empirical evidence that there is a correlation and that the blockchain security of a PoW blockchain is intrinsically linked with mining rewards and the price of that cryptocurrency when using an autoregressive distributed lag approach that makes every moment of the blockchain endogenous. This means that the elasticity of block rewards is higher than the cost of mining regarding the stability of the network[25].

2.3 Proof of Stake

The PoS consensus mechanism is not a new concept but has gained more and more attraction in recent years. The slow transition and switch of the consensus mechanism of the second biggest cryptocurrency namely Ethereum from PoW to PoS triggered many projects to launch directly with PoS. Especially the long-lasting and hard critic, that the PoW mechanism is not environmentally friendly and consumes too much energy was one of the drivers that currently the biggest Layer 0 and Layer 1 running on PoS. But the concept of this consensus mechanism was already covered in a paper by Scott Nadal and Sunny King in 2012. Where it the authors already acknowledged that energy consumption is critical as well as the issue of the slow transaction time which reflects the scalability aspect in the blockchain trilemma explained previously in Section 2.2 Network Security. The concept of the first cryptocurrencies with the new PoS consensus mechanism was born in 2013 and Peercoin (PPC) was established with a hybrid approach. The currency is still up until now and has a market capitalization of around $17 million[26] as of April 09th, 2022. In the beginning, the cryptocurrency PPC still had the PoW consensus mechanism to address the issue of the distribution of the coin. To prevent that in the initial distribution phase, a decreasing PoW-based distribution was used. Subsequently, it does not come to a centralization from early on.[27]

[25] Ciaian, Kancs, & Rajcaniova, 2021
[26] Coingecko, 2022
[27] King & Nadal, 2012

The evolution of PoS cryptocurrencies can be divided into 3 waves[28]:

In the *beginning*, where the first idea of a new consensus mechanism developed as PoW was too slow in transaction time, expensive in transaction cost, and the high energy consumption. Peercoin with the first real implementation of the PoS consensus mechanism although it was a hybrid model. Whereas NXT followed in the same year as a pure PoS cryptocurrency. In 2014, three years after the first public mention of PoS in the BitcoinTalk forum the first blockchain with the "Delegated Proof of Stake" (DPoS) consensus mechanism was launched, namely BitShares. In the following years, other projects like Steemit and Lisk also launched with a DPoS mechanism.

The *First Wave*, where new projects based on the development of the past appeared. As the fundraising rounds began in 2017, many of today's most important and well-known PoS initiatives were seeded. The Cardano Foundation finished its initial coin offering round (ICO) at the beginning of 2018 but already launched its coin in September 2017[29]. To be notated is that Cardano did not use the same PoS algorithm as other protocols they invented their own unique PoS algorithm called "Ouroboros", and the whitepaper used the term "πSPoS"[30]. In the same year which Cardano launched their coin called $ADA, the ICO of Cosmos ended, and two years later the software was complete so that the corresponding coin "ATOM" could be distributed, and the chain could launch its mainnet[31]. Whereas $ATOM uses the consensus mechanism "Tendermint BFT", which will be further elaborated in the upcoming chapter 3.2 Consensus mechanism of ATOM[32]. Polkadot (DOT), which is the direct competitor of Cosmos, as both projects focus on interoperability had their fundraising also in 2017[33]. $DOT launched their token and mainnet in May 2020 with the PoA mechanism and afterward transitioned to a Nominated Proof of Stake algorithm (NPoS).

The *new wave* accrued in recent years as new scalability-focused projects like Solana (SOL) and NEAR protocol entered the market and caused attention as the price of Solana spiked, resulting in recognition and attraction of many new investors. These new blockchain protocols are touted as potential ETH-killers. $SOL was launched in March 2020 and uses the PoS

[28] stakefish, 2020
[29] Cardano Foundation, 2022
[30] Kiayias, Russell, David, & Oliynykov, 2019
[31] (nterchain Foundation, 2019
[32] Kwon & Buchman, cosmos.network, 2022
[33] Coinspeaker, 2017

algorithm but additionally also include the Proof of history (PoH) mechanism which improves the scalability[34]. As the development of PoS algorithms proceeds, various new types of improvements are implemented as the next generation of PoS blockchains tries to achieve more efficient mechanisms. The Near protocol, therefore, uses their variant of PoS called "Doomslug" to become more scalable[35]. Whereas Algorand (Algo) tried to solve the blockchain trilemma with the Pure proof of stake mechanism (PPoS), whereby random *Validators* get elected which then validate the next block[36].

The whole evolution of the PoS landscape, which was described above can be seen in Figure 3. It is expected that every 5 years a new blockchain appears since Bitcoin was invented in 2009. 5 years later Ethereum was changing the paradigm of blockchains. 2019 the cosmos hub introduced with the IBC protocol the interoperable blockchain and facilitated new opportunities. Variations happened more quickly in PoS Networks, whereas large changes occur generally every three years.

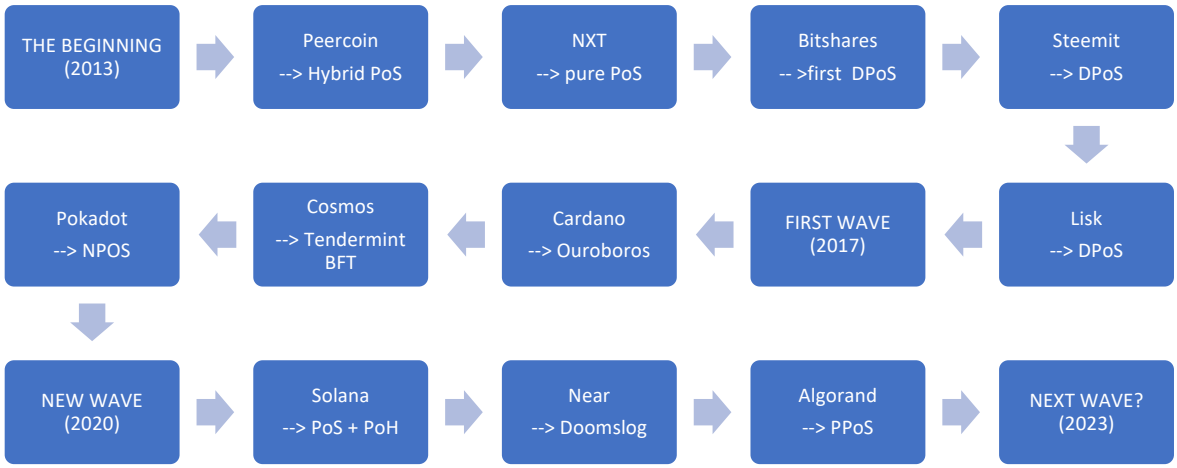


Figure 3: Evolution of the PoS Cryptocurrencies

In general, there are a couple of improvements and advantages compared to the PoW consensus mechanism, but it also brings some challenges. As highlighted among others by the whitepaper of Peercoin the advantages of PoS are clear. A more efficient, faster, and scalable blockchain that does not require too much energy. Figure 3 stresses that many protocols have adapted PoS consensus processes to promote scalability; each protocol has its own strengths and weaknesses, but there are some common issues that will be discussed in the following section.

[34] Locke, 2021
[35] Philips, 2021
[36] Algorand Foundation, 2022

When looking at the beginning of cryptocurrencies the ideology was always to eliminate the middleman and distribute wealth in a fair way where every participant has the same chance to contribute and improve the network. As a result, the code was open source. The point of decentralization in PoS seemed in danger as critics claimed that staking mechanism only allowed the rich to get richer, which could undermine the decentralization aspect as block rewards are distributed proportionally to the number of coins staked. Thus, the already richer participants of the network, who have a bigger share of the network continue to gain more and more percentage of the total coin supply. The writers Rosu and Saleh examined the argument that affluent people get richer through the PoS mechanism in an article published in the Management Science journal. According to the article "Evolution of Shares in a Proof-of-Stake Cryptocurrency," the PoS method does not make the affluent richer, but rather allows for a steady share percentage[37].

Specifically, to avoid this aspect of centralization where maybe early participants or rich individuals could get high proportions of the network the challenge of the initial distribution peaks out. For instance, Satoshi Nakamoto could mine full blocks at the beginning of the bitcoin chain and accumulated between 750,000 and 1,100,000 Bitcoin, however, these are not moved since 2011[38]. But it also caused uncertainty in the crypto community as the pseudonym could technically sell off this substantial number of coins at any given time. Therefore, it is of vital importance that the initial distribution goes to a variety of people and in the best-case, they also become active participants of the network. This aspect of how the distribution could look will be accessed later more closely in Section 3.1 Cosmos.

When looking at the consensus layer, it is clear why the distribution is so crucial since the challenge of a 51% attack occurs and must be solved. The 51% hack has already been described detail earlier, but in a PoS setting, it means that the aggressor can buy up the majority of the coins and therefore control the entire chain. Similar to the 51% hack is the “Long range hack”, where the aggressor starts a new chain from the genesis but assigns a significant share to himself and runs it by making it indistinguishable from the original chain, and then tries to deceive the nodes so that they adopt the fake chain. Although this kind of attack never happened there are mechanisms to prevent this. Implementing checkpoints or assigning a list of nodes that bootstrapped the chain for example would be sufficient to avoid this risk[39].

[37] Rosu & Saleh, 2021
[38] BTC-ECHO GmbH, 2022
[39] Choy, 2020

On the contrary, the “Nothing at Stake” (NOS) problem is a security issue that can occur if a block in the chain gets proposed simultaneously. This would lead to a fork in the blockchain.

As both chains would be running, miners would have the risk that if they chose one chain and it turned out that it was invalid, they would be left without any rewards while on the other hand they would not be impacted as they continue to run both chains at the same cost. The risk here is, however, that a double-spending could happen as the attacker could create a fork before he spent the coins and only mines his fork. So it could be that his chain becomes the longest chain as miners act in their best interest and continue to mine both chains because they do not risk their own stake if they simply validate both chains until one gets dropped[40]. This issue is not present in PoW networks as validating the chain costs computing power.

In the next section the PoS itself will be described without going into specific PoS consensus mechanisms. As the history, evolution, and potential threats are already covered.

Contrarily to the PoW consensus mechanism where the miners must invest in hardware (disregarded cloud mining) to validate transactions in the PoS networks where miners are referred to as *Validators* are required to commit to a stake. Hereby, the native coin of the network must be locked up. The lock-up period depends on the network and is usually between 14-28 days. The number of deposited and locked tokens plays a role in the selection of the next *Validator*, who is then allowed to validate the upcoming block. Although it is more likely that *Validators* with more coins and a longer holding time will be selected with greater probability, a random principle is usually integrated into the selection process, although it is nevertheless deterministic in the end. When determining the *Validators*, there are various approaches and algorithms that determine who is allowed to create the next block. Either the size of the take stake, the age of the token, or a random selection could be the method to select the next block *Validator*. The selected *Validator* is called a ”leader”. These mechanisms ultimately influence the characteristics of the network, such as scalability and security. Since most networks use their own protocols, the various PoS networks differ from each other. The paper “Proof-of-Stake Consensus mechanisms for Future Blockchain Networks: Fundamentals, Applications, and opportunities” summarized the different protocols and implications, which are illustrated in the Table in Appendix 1[41].

[40] Li, Andreina, Bohli, & Karame, 2017
[41] Nguyen, et al., 2019

The reason for the committed stake is a security aspect where *Validators* with malicious behavior get slashed. A slashing penalty occurs under two circumstances. Either when an extended downtime or fraudulent signing also referred to as double-signing of blocks occurs. Extended downtime can lead to a slashing. To avoid this, the *Validator* can for instance run multiple nodes alongside its primary node as a backup in case the primary node goes down. It should be noted that a short downtime is accepted and do not lead inevitably to slashing. The bigger punishment for the *Validator* takes place if he signs invalid blocks. The slashed tokens either get burned or redistributed to other stakeholders of the network. In the worst case, a *Validator* also could get jailed respectively "tombstoned", which means that the *Validator* gets excluded for further validation of the network. It should be emphasized that not all PoS networks have the same penalties or even use the idea of slashing at all.

Providing infrastructure as a *Validator* and running a node necessitates having sufficient technical knowledge and running servers (bare metal or cloud) in addition to the minimal number of coins. *Validators* do not normally do this out of altruism; instead, there is a monetary incentive for running a node on a chain. This could either be the transaction fees and/or the block rewards. The amount of the rewards depends on the tokenomics of the network. In the following chapter 2.5 Tokenomics, this topic will be discussed in more detail, and it will be shown why these is of significant importance in connection with the game theory. As far as incentives go, they should be aligned with the overall goal of having a long-lasting and secure network.

To reach a more efficient and more democratic consensus the PoS mechanisms undergo several modifications to achieve the best result. One of the developments in recent years was that several networks implemented a specific type of PoS the delegated proof of stake consensus mechanism (DPoS). This evolution allowed integrating of features like voting and delegation mechanisms. In addition to the *Validators,* another stakeholder, the *Delegators* also emerged. Whereas the *Validators* still run the node and secure the chain, the *Delegators* can help to secure the chain by delegating their coins to one or more *Validators*. The Validator might charge a commission for the service it provides to run the node, which can range from 0% to 100%. Obviously, this are extreme commissions as the *Validator* does not make any profit with the node if the commission rate is at 0% and with 100% barely any *Delegator* would delegate to this *Validator,* as all the rewards would directly go to the *Validator* and the *Delegator* would take the risk without any profit. In an efficient market, this would never be the case.

Nevertheless, there are cases where *Validators set* up these commissions and it still makes sense. The reason for the 0% commission rate could be like a marketing action to get as many delegations as possible. This, as well as other actions from *Delegators* will be elaborated in greater depth later in Chapter 2.6 *Validator set*. There will be also explained why this plays a significant role. The reason for a 100% commission node from a *Validator* is for instance to avoid any other delegation and to self-delegate a significant number of coins. This makes sense when analyzing the risk aspects of staking.

Next to the price fluctuation risk of the asset which is given as collateral there is the risk of slashing as also described earlier.

This is now also important for the *Delegator*, as delegating the coins to the *Validator(s)* introduces a third-party risk. As a result, larger stakeholders, particularly central exchanges (CEX) and venture funds, set up and maintain their own node to avoid these risks and comply with their compliance departments. Using a service provider to pool your tokens with a remark that the selected *Validator(s)* are liable, even though the coins are not physically moved to the wallet of the *Validator* rater.

The *Validator* also gets the right to vote on governance proposals. However, the *Delegator* always has the right to override the vote. The voting power depends on the number of coins staked. Submitting proposals have different procedures depending on the architecture of the network. Nevertheless, these proposals can have an incremental influence on the future of the chain wherewith the point of voting becomes relevant. *Validators* can propose a decision and if the *Delegator* does not vote by themselves, the proposed vote of the selected *Validator* becomes valid.

The paper „Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks" compared the different consensus mechanisms, which gave a good overview of the speed and energy consumption illustrated in Table 2, where the DPoS mechanism is added manually[42].

	PoW	PoS	Hybrid	DPoS
Leader selection	Based on hash rate	Based on stake	Depends on variant	Depends on stake
Energy consumption	Significant	Negligible	Medium to negligible	Negligible
Hardware requirement	High	Low	Medium to none	None
Block generation speed	Slow	Fast	Medium to high	Depends on *Validator set*
Transaction confirmation speed	Slow	Fast	Medium to high	Depends on *Validator set*
Applications	BTC, ETH, etc.	ADA, Algo, etc.	Casper, PPS, etc.	Cosmos, EOS, etc.

Table 2: Comparison Consensus Mechanism

2.4 Decentralized Economics

Decentralized economics better known as DeFi gained a lot of attraction back in summer 2020. Staking and therefore enabling passive income went viral. Furthermore, lending and borrowing became possible and widely distributed. However, there is more than simply earning interest. It includes different types of game theory and incentive mechanisms. More cryptocurrencies arose as a result of Satoshi Nakamoto's notion to cut out the middleman, but there was no need for decentralized economics beyond simple tokenomics (hard cap of 21 million BTC) and a release schedule that included havening. It will not be explored further what ramifications this has or what it is. However, the tokenomics in general will be explained in more detail in the following chapter 2.5 Tokenomics.

Bitcoin for instance has a relatively simple game theory built into the code, which is also open source and therefore does not need any kind of governance. With the forthcoming DeFi buzz

[42] Nguyen, et al., 2019

and the decentralized autonomous organization (DAO) flood, this requirement has grown. After the massive ETH DAO hack, this has subsided[43]. Bitcoins consensus mechanism rewards the miners. The game theory of Bitcoin therefore can be condensed down into “If Miners put Mining power (Hash Power) in the potentially get rewarded with the block reward, where the rule is that the more computing power is inserted the higher the chance is to get the rewards. Additionally, the mechanism of the code adjusts the difficulty of the “riddle” which must be solved with the computing power. This leads to fair competition and avoids the blocks that are mined too fast. As a result, the reward and, eventually, the supply would rise too quickly. The miners usually must sell their rewards to cover the costs of the mining facilities and the energy consumption.

The supply of Bitcoin and other PoW consensus mechanisms is limited, which is referred to as a Hardcap. As a result, the inflation model is based on the notion that there can never be more than 21 million coins, whereas in PoS networks, inflation occurs without a Hardcap. The inflation or deflation of the coin has direct implications for the game theory of the network as a user must be incentivized without inflating the networks and correspondingly damage the network as demand and supply must be at least in balance. If not the price of the coin would crash (under normal market conditions). This would, in turn, lead to economic damage to the participant whereby there would not be a logical reason to continue the actions.

The game theory is an old theory, which is a branch of math. It describes a decision-making process where different participants interact and influence the outcome of the individuals. It was first brought up in the 1940s[44]. Neumann and Morgenstern discussed the concept in relation to economics, stating that it was formally utilized for decision-making in games such as chess or checkers. It is a method to analyze the rational behavior of actors in a market to come to a better decision where complex actions are described in a simple way.

With the publication of John Forbes Nash's Nash-equilibrium in 1950, game theory became well-established and widely accepted in economics and the social sciences. 20 years later, the theory was further developed, from which, among other concepts, the evolutionary game theory was derived. Within game theory, there are two types: cooperative and non-cooperative. The cooperative game theory states that players can make binding contracts whereas in non-

[43] Cryptopedia Staff, 2022
[44] Neumann & Morgenstern, 2007

cooperative game theory players make decisions via self-enforcing reasons as the act out of self-interests. Cooperative game theory is payout based and non-cooperative game theory is action and strategy based. So, game theory is a fundamental mechanism that allows cryptocurrencies to manage and model human paths of behaviors within a dynamic and interactive environment to map out a strategy for a desired outcome.

The most common example to understand the game theory is the prisoner's dilemma. It describes a situation where two individuals are accused of a crime. Both get queried separately and neither of them has the possibility to communicate with each other. If both confess both of them get a six-year sentence. If prisoner 1 confesses and prisoner 2 does not confess, prisoner 1 gets a one-year sentence, and prisoner 2 gets a nine-year sentence, and vice versa. If both do not confess both of them will get a three-year sentence. So, the most logical and favorable strategy would be not to confess where the punishment is the smallest (biggest incentive). But the problem is that both are unaware of the counterparty's choice and therefore act out of self-interest, so they confess. This leads to a much worse result as they both do confess, and they end up with a six-year sentence[45]. Illustrated is this example in Table 3.

Prisoners' dilemma		Prisoner 2	
		Confess	Not confess
Prisoner 1	Confess	Both 6 years	Prisoners 1 1 year Prisoners 2 9 years
	Not confess	Prisoner 1 9 years Prisoner 2 1 year	Both 3 years

Table 3: Prisoner's Dilemma represented in a Bimatrix

That is exactly what the Nash equilibrium states. It is the balance where no player gets a better reward by changing their action. In a non-cooperative game theory players tend to select the option/strategy which is not the best option for anyone. But every player would select the same choice again as it seems the best for the player itself and they would not deviate from their choice as the only one. This is what John F. Nash called the dominate strategy[46].

The game theory also applies in cryptocurrency networks as described earlier with the PoW network Bitcoin. However, with PoS networks, the ramifications are completely different

[45] Hayes, investopedia.com, 2022
[46] Nash, 1950

because the players now have more parameters to deal with. Including which *Validator* should be delegated to, how much should be delegated, does it make sense to run your own node, what are the dangers, and so on. As a result of this, the so-called "crypto-economics" arose, as network participants' behavior is dependent on possible incentives, which are influenced by the tokenomics (supply, inflation, etc.). This will be explained in more detail in the next chapter. A working game theory for a PoS network should be designed so that the security and decentralization aspect is protected but also the scalability, and the transaction speed are secured. The Polkadot (DOT) PoS, for example, employed game theory to reward smaller nodes more than larger nodes. So, a decentralized *Validator set* is ensured[47].

Further enhanced through more parameters namely the governance mechanism it gets clear why it is important that a decentralization is significant. Within open public blockchains, diverse players from all over the world compete for the greatest reward. Through the governance, the participants generally the stakeholders (coin holders) have the opportunity to influence the future of the chain. Different changes and improvements can be implemented through governance proposals where different networks have different structures.

The Uniswap network (biggest DEX), for instance, has the requirement to set up a governance proposal that the issuer must has at least 1% of the total supply to submit a governance proposal. This should ensure that no spam governance proposals are submitted. Different networks also have different quorums, which must be reached so that the proposals pass. Uniswap has a required quorum of 4% and a fixed 7-day voting period. When a proposal is submitted every coin holder has 7-days to vote on this proposal, where it is also possible to abstain. However, as the community of Uniswap recognized that this barrier is too high and enforced the power of so-called "Whales" (holders with a substantial number of coins), a governance proposal went through, which lowered the requirement to 0.25% of the total supply. It is also possible if there are not enough funds for a network participant to submit the proposal via "Fish.vote". This enables participants to participate on submission and exceed the required amount[48].

[47] Bitcoin Suisse, 2020
[48] Fish.vote, 2022

2.5 Tokenomics

As mentioned in the previous chapter, the term tokenomics and the mechanisms involved are going to be explained in this chapter. The term "tokenomics" is derived from economics and token, which describes the interaction between the tokens of a network and the effects of it.

This pertains to token-based networks and cannot be extended to networks that rely solely on permissions, as is frequently the case in centralized networks[49]. In this context, the term token is used synonymously to coins although they are fundamentally differentiated. A coin is a unit that runs on its native network whereas a token is rather a unit that is built on top of another network. Tokenomics was firstly mentioned by Skinner, who said: "that behavior is shaped by its consequences. If you receive rewards for certain behavior, you will continue these behaviors". That is also how he described token economics[50]. This again demonstrates aspects of game theory, such as how the asset operates and participant behavior.

The tokenomics of Bitcoin can be explained relatively easily. It has a Hardcap of 21 million tokens, which means the supply is limited and ensures scarcity. Currently, over 19 million BTC are mined[51]. The spend of issuance is controlled by the havening where roughly every four years (every 210,000 blocks) the block rewards get halved also referred to as "halving"[52].
Demand is generated by the utility of the token. It is utilized to execute transactions and is regarded as a store of value. With the rising demand for BTC and the fixed supply (Hard Cap), the price tend to rise[53].

Tokenomics can be described as the interplay of supply and demand. This is reflected by the token's inflation, number of circulation tokens, and locked tokens. This is significant since it affects the price of the token, i.e., the valuation, also known as market capitalization. As it suggests the rewards for the behavior of staking vanishes whereas the real profit can be deviated. For instance, if a network has no inflation and the token holder remains with his 100 tokens at 1$ each, he will have holdings worth 100$ after one year.

[49] Eliason, 2021
[50] Longchamp, 2021
[51] blockchain.com, 2022
[52] Meynkhard, 2019
[53] Longchamp, 2021

However, if the inflation would be 100% and the token holder gets a 110% staking reward, (Assuming the additional 10% is coming from a community treasury, that incentivizes staking) they would have 210 tokens after one year. Assuming the Market Cap would remain the same, the token price would drop to 0.5$ at each as the circulating supply doubled with 100% inflation. This would lead to the appearance that the token holder lost some value, even though their holdings are now worth 105$. It should be noted that the stated reward was 110%, which relates to the quantity of tokens but does not represent the value of the token in percentage calculation. Nevertheless, this structure incentivizes to hold the token as otherwise the share of the holder gets inflated and ends up with a loss. Projects with a poor design of tokenomics are most likely to fail as people tend to sell. Commonly there is a misconception between the price of the token and the value of the network, as people tend to think that when the price of the token is low that it is undervalued even if in reality the value of the network is reflected by its market cap which is the number of circulating tokens multiplied by its price.

The supply side of a token determines if the value of that token will increase or decrease. The fewer token is in circulation the value of that token will increase which is called also deflation and in turn if there are more tokens the value will decrease which is called inflation. Supply is made up of the total number of tokens in existence right now, how many will ever exist, and how quickly they are released. Creating a low supply token without any demand generally does not imply any value to the token. This shows that the demand side is also a significant factor to gather value for the token. There are some mechanisms to control the supply side of a token like the emission plan which will avoid a supply shock as seen in the example of BTC previously. Additionally, the burning mechanism can be used to reduce the supply and eventually increase the price. Either regularly scheduled burns can take place as seen with the BNB token on the Binance network, or a part of the fees get burned as seen in the newly implemented EIP-1559 protocol within the Ethereum network[54].

The demand can be derived from the faith of the people that believe that the token will have a higher value in the future. This can be driven by the community and the culture a project, as evidence with the Meme coin “Doge” and fueled by memes. Secondly, the demand can be derived from the cash flow a token can produce from simply holding and staking it. The greater the potential income without a hefty price, the greater the demand as more individuals engage in that incentive. The cash flow can be either generated by the staking rewards, participation of

[54] Scheuerman, 2021

transaction fees, or rebasing. Lastly, the game theory comes to play when analyzing the demand side. This includes mechanisms like lock-up periods, the longer the lock-up the higher rewards[55]. Since price is determined by supply and demand, if demand stays the same but supply decreases then the price will naturally increase. On the contrary, if these locked up tokens get released and the demand remains the same it will lead to a plummeting price. In general, demand should be derived from the utility of the token, such that network participants utilize these tokens to either pay for network fees or as a Governance token to participate in votes and determine the network's future.

The ETH network for example is contrary to the Bitcoin tokenomics as it is implemented as a burning mechanism with the last update (London hard fork EIP-1559) which led to a restructuring of the networks fee structure and decreasing inflation and in the future even deflationary[56]. Additionally, with the merge of ETH 2.0 it will be possible that users earn up staking rewards up from 2% to 20% pa[57]. Also, the demand for ETH is rising as investors want to buy it as an investment and also network participants are required to spent ETH in order to operate the applications on the ETH network.

The distribution of tokens in the beginning especially for PoS networks is crucial as it is determining from one side the de-/centralization aspect and from the other side the supply side. Herby, it can be distinguished between a pre-mine where the supply of the token is partially or fully created and a fair launch where everyone interested has the opportunity to acquire the tokens from the beginning. Bitcoin with the PoW mechanism had a fair launch where everyone could mine bitcoins and get a share of the network, which is nowadays not that simple anymore.

Many PoS networks have pre-mined tokens. As many networks get settled by a team, they first devise a distribution while determining the supply schedule. Commonly tokens for incentives are locked up in a community pool which then can be used for certain campaigns. These either are set by the developer team or can be ruled via governance proposals. Marketing campaigns or ambassador programs can be bootstrapped with this supply. Further, the supply schedule states how many tokens will be unlocked after which time. The team allocation is usually locked up for a longer period of time and has vesting period, which may include a cliff. A token allocation is illustrated via the pie chart as also can be seen in Figure 4.

[55] Eliason, 2021
[56] Kelly, 2022
[57] ethereum foundation , 2022

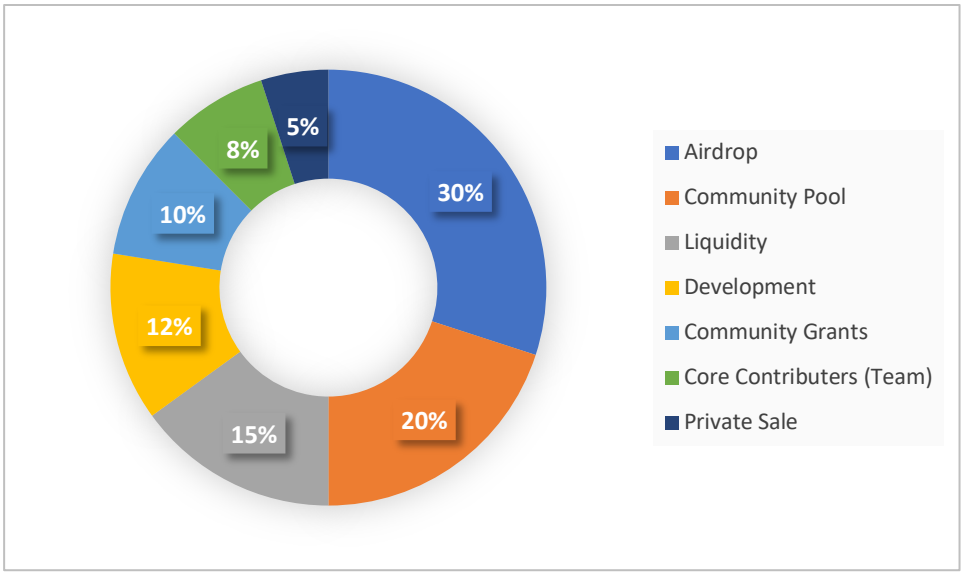


Figure 4: Example of a Token Allocation

To bootstrap, a decentralized community from early on many PoS networks decided to do Airdrops where a part of the supply goes to a targeted group. This allocation should result in the adoption of market participation since people acquire free money and then engage with it and become part of the community. A part of the tokens can go to early investors where so-called "Private Sale" happen so that the developer team has enough funding to cover the expenses for implementation of the ideas and deliver a product. A big allocation to the team and early investors is perceived as it is not decentral and large token holders exert a certain price pressure. Moreover, the fear of a fire sale of early investors after the lock-up period is observed[58]. In general, if there have been seed rounds for early investors, the token is locked and cannot be moved, even if this token occasionally sold via over-the-counter (OTC) deals, where the lock-up period remains and is sometimes extended. However, OTC deals do not influence the market price.

2.6 Validator Sets

When the decentralization and security aspects are considered, the *Validator set* becomes crucial. A *Validator set* consists of a group of participants who support the consensus mechanism and confirm the transactions. Either they produce or witness the upcoming block of the network and sign messages about them to verify. The set can vary from network to network and ultimately also determine the speed and the security aspect of the network. The more *Validators* run a node the more decentralized it is and can be seen as more secure, particularly against 51% hacks. On the contrary the more *Validators* there are the longer it takes until the

[58] Beckett, 2021

next block is assigned and therefore interferes with the transaction speed. As mentioned in the earlier chapter generally everyone can become a *Validator*. It requires some technical knowledge to set up the node. A server can be either rented via services like AWS, Microsoft Azure, GCP, or IBM Cloud whereon the nodes run, or a physical server can be used but this requires, on the other hand suitable facilities and particular investment upfront. If a *Validator* runs their node on their own server, it is referred to as "BareMetal". This becomes a crucial factor as the *Validators* are the most important instrument to maintain the network and should be decentralized to eliminate the "single-point of failure". If all *Validators* ran their nodes, for example, on the AWS service provider, the entire network would be dependent on Amazon's availability, which is centralized and therefore technically can control the entire network.

Additionally, some networks have restricted *Validators sets,* which means that the total number of *Validators* is limited to a certain amount so that it is ensured that the transaction speed does not get affected.

3. Research Design

In this chapter, the PoS mechanism of the Cosmos ecosystem will be analyzed with an empiric approach of a case study. Herby, two surveys are concluded, and the methodology is outlined subsequently.

3.1 Methodology

In order to gather information directly from the network participants two surveys were conducted. Therefore, a draft was made and further developed. This was a continuous process until the surveys were sent out. One survey was for the "*Delegators*" as they represent one side of the network, and a separate survey was for the "*Validators*" to cover the other half.

The distribution of the survey to potential participants was executed through several social media channels. First personal contacts and friends were contacted to get an initial impression and double-check the relevance. After the survey was set up, the broader mass was targeted via Twitter posts. At this time, the Twitter account had roughly 700 followers, most of whom followed the account since it mostly covered content from the Cosmos ecosystem. In order to get a large sample size and as many participants as possible for a representative survey, a raffle was announced among the participants. Three winners were chosen among the participants, each receiving 10 $OSMO Tokens each worth 7,86€ (3x 78,60€) at that time, for a total of 235.80€[59].

The effect of retweeting was also exploited to increase the randomization of the participants and to ensure more participants. Users who retweeted that post, which contributed to the distribution and outreach of the post by sharing the tweet with their followers had the chance to win 2x 3 $JUNO. This leads to another 174.35 €[60] prize money, resulting in a total of 410.15 €. The amount was self-funded and randomly distributed via a web-based randomizer. The winners were announced publicly[61]. There was no affiliation at any given time to the cryptocurrency projects $JUNO and $OSMO. These currencies were selected as they were the most vibrant ones in the Cosmos ecosystem at that time. So, the prize money would generate more outreach. In addition, the Tweet was posted within a Telegram Channel[62] with almost

[59] Appendix 2
[60] Appendix 3
[61] Appendix 4
[62] Appendix 5

2,000 members, mainly focus of the Cosmos ecosystem. The reason for the selection of the channel was the co-foundation and the admin position of the group.

The *Validators* were contacted personally after it was discovered that the post within the give-away was not as promising as expected. Section 3.2 Data preparation describes the selection of the *Validators* that were contacted, as it became evident that not all *Validators* could be contacted. This would not be possible within the time frame of the study. In addition, new *Validators* are constantly joining, and some have ceased to be *Validators* for a variety of reasons.

3.2 Data Preparation

This section will deal with the selection of the *Validators* for the survey, the data whereas the result from the survey will be described and analyzed in more detail in Chapter 4.Survey.

In order to target the *Validators* with the survey, first, an overview was gathered. These are in the minority compared to the *Delegators* and therefore it is more difficult to achieve the critical number of 100 survey participants to determine a representative survey. Therefore, the goal was set to get at least 51% of the voting power from as many chains as possible.

The following projects were prioritized: $OSMO $ATOM $JUNO, as they are currently the leading networks in terms of IBC volume in $-nominations during a 30-day period [63] according to the website “mapofzones.com”. If 51% of the voting power was not obtained, the strategy was to obtain at least five of the Top10 *Validators* as well as five of the lowest ten to assure the opinions and views from many different perspectives. To achieve the overview of the *Validators* and accordingly the voting power the block explorer “mintscan.io” was used, as it was the most reliable source for the Cosmos ecosystem and provided a list for the most projects.

After analyzing how many *Validators* are on each project the approach was followed to write down the biggest *Validators* of each available chain from top to down manually. After realizing that this task was inefficient and too time consuming, another approach was used to gather the relevant data for conducting the data compilation. This was done with the help of data scraping, therefore the programming language Phyton was used to scrape data from the website

[63] Appendix 6

"Mintscan.io". Web scraping is a method of compiling data from a website where the company did not provide any kind of public API for assorted reasons. All *Validators* lists from the respective projects were saved in a separate excel sheet following called "Mastersheet". The snapshot was taken on the 16th of March 2022. It should be noted that the data is updating every few minutes, which is why total aggregation of 100% was not achievable in some chains. All information was then compiled together in one main Mastersheet. To figure out the importance of each *Validator* in an economical sense the assets under delegation (AuD) were calculated.

This study examines the interdependency between network security and economic implications. For this purpose, the voting power which also was aligned with the number of coins delegated to each *Validator* was multiplied by the current price of the native coin. This was done for every chain where data was available on Mintscan.io. In this way, the percentage power of each *Validator* and in addition the economical dimension could be seen at one glance. It should be noted that chains such as "Evmos" and "Axelar," which were previously mentioned but had a price of zero, were removed from this table since the economic impact could not be determined. It is also worth noting that not all of the 43 IBC compatible chains indicated in Mintscan were listed; 34 of them were included in the table, while some were eliminated as previously stated. According to "coingecko.com," a renowned cryptocurrency ranking website, there are 72 coins running within the Cosmos ecosystem, as shown in Figure 5. They also have a market capitalization of 62.272.801.489 $ on the day of the snapshot.

#	Category	Top Coins	1h	24h	7d	Market Capitalization	24h Volume	# of coins	Last 7 Days
14	Cosmos Ecosystem		-0.6%	-6.6%	3.6%	$62,271,801,489	$4,428,285,719	72	

Figure 5: Cosmos ecosystem according to "Coingecko.com"

The difference results from the fact that Coingecko shows chains that run on the Cosmos hub, where the Cosmos SDK was used, whereas Mintscan displays only projects that incorporate the IBC protocol, which permits interchain transactions. The Cosmos SDK and the IBC protocol will be described in Chapter 4.

The following chains were included in the data gathering process to select the *Validators* and therefore represented in this study:

COSMOS // OSMOSIS // JUNO // UMEE // STARNAME // STARGAZE // SIFCHAIN // SENTINEL // SECRET // RIZON // REGEN // PERSISTENCE // MEDIBLOC // LUM // KONSTELLATION // KI-CHAIN // KAVA // IRIS // INJECTIVE // FETCHAI // EMONEY // DESMOS // CRYPTO.COM // COMDEX // CHIHUAHUA // CERTIK // BITSONG // BITCANNA // BAND // AKASH

Several *Validators* included in the chains may validate on different chains as well, but *Validators* that only operate on chains which are not included in the data cannot be represented. Chains like TERRA or BNB were not included since the data was not available on Mintscan, which are relatively big and important chains, but also smaller chains were not included. However, the majority and the most important chains were included.

After clearing the data for chains that have no price yet, the Mastersheet was created where all *Validator* names were listed. So, it was possible to begin by listing all of the different chains side by side, with the name of the chain, the percentage of voting power, the voting power in number of coins, and the AuD. This can be seen in Table 4. All the names of the *Validators* were copied out of the single sheets and pasted below each other.

Name of Chain	cosmos		
	Voting Power %	Voting Power	AuD ($)
Current Price	$28,27		
Sum of Tokens	100,0800%	184.605.155	$ 5.218.787.732

Table 4: Example of the Data header for each chain

To double-check the numbers the sum of tokens was added to the header. Subsequently, the data from each chain was imported from every single sheet which only contained the data for one chain. This was done by the combination of the two commands IFERROR and VLOOKUP: “=IFERROR(VLOOKUP($C6;cosmos!$B$2:$H$250;3;WRONG);"")”

If the *Validator* runs a node on the chain, that command ensures that the name of the *Validator* is looked up in the associated sheet for the chain. To calculate the AuD in Dollar nomination the command “IFERROR” was used where the voting power in number of coins was multiplied by the current price. With two-dollar signs before and after the cell number of the current price of the coin” in the command, the column and row were fixed. This was then done for every chain. Additionally, an extra column was added to count the number of chains where each *Validator* ran a node. To sum up the total number of nodes for each *Validator* the formula

“COUNTIF” was used where the condition was to only count it if the number was above one and then divided that by 2. So, it was ensured that the percentage of Voting Power was not counted and as both the Voting Power and subsequently the AuD in $ must be bigger than one if the *Validator* runs a node the number was not double-counted.

As it is still an early sector the Names of several *Validators* slightly differed from chain to chain. For instance, due to unprofessionalism and mistakes, or the annex “.com” was absent. Further, some *Validators* had used the field of the name to make active marketing where they added that *Delegators* could win NFTs, or the fees are lowered until a certain time to attract more delegations. This is further elaborated in the following chapters. Furthermore, some *Validators* had different emojis for different chains, for their internal recordings, or just for fun. This can be seen in the example of the *Validator* NosNode (Figure 6) which is an established and recognized *Validator* as they also operate as a Developer and further develop projects. The Dog stands for the Chihuahua chain whereas the test tube stands for the OSMOSIS chain.

Figure 6: Example of different Names across different chains

At the beginning of the data compiling 3,222 *Validators* were listed, after eliminating certain chains and assembling the duplicate nodes, 1,174 different *Validators* across 33 chains were identified. For each *Validator*, the “Total % Voting Power” was compiled and the “Total AuD in $” terms were summarized. The “Sort and filter” function was used to arrange the *Validators* from top to down according to the voting power and thus also the AuD. As the goal was to reach the highest possible coverage of voting power a Top-down approach was used to contact the *Validators.* Some *Validators* stayed anonymous because being a *Validator* in the Cosmos ecosystem does not necessitate any KYC process. These *Validators* could not be contacted. Some *Validators* did not respond at all, while others stated that they do not wish to participate in the survey due to “security threats”. From the roughly 200 contacted persons, 25 participated in the survey, which equals a turnout rate of 12.5%. A good turnout rate is between 5% and 30%; however, it varies from channel to channel. According to the platform “delighted.com” a good response rate for the channel e-mail is around 6% on average. Therefore, the survey can be counted as valid[64].

[64] Chung, 2022

3.3 Theory

This study follows an inductive research approach. Literature research was conducted in Chapter 2. Theoretical Knowledge to provide sufficient basic theoretical knowledge to grasp the implications, but no further research was conducted on the topic of PoS and the implications of network security, only for the PoW network as described in the paper "Interdependencies between Mining Costs, Mining Rewards, and Blockchain Security"[65]. As not enough literature was available, no hypotheses could be set and assessed. Therefore, a theory will be devised.

The inductive approach consists of three steps, which are outlined below and applied to the paper:

Observation: In this explicit paper the PoS mechanism is discussed, and the Cosmos ecosystem is observed. The PoS mechanism requires nodes to validate transactions.

Observe a pattern: More infrastructure providers appear on the market and fight for delegations. Node operators are small companies, although some of them are run by individuals. Patterns can be observed. Especially in recent times, it has become apparent that nodes are increasingly taking targeted marketing measures to generate delegations. Among other things, token holders are lured to delegate to specific nodes through airdrops of tokens or NFTs.

Develop a theory: It is obvious that the market is becoming increasingly mature. It can be assumed that there is a similarity to the operation of miners for Bitcoin at the beginning of 2013. Also, it can be expected that a whole market will develop around the operation of nodes and that it will become increasingly difficult and capital intensive to enter as a node operator. In the future, nodes will also need to offer more than just transaction validation to get delegations.

As the niche is getting more professional and capital intensive, fewer individuals can join the circle of *Validators* and only companies or high network individuals are feasible to run nodes in a PoS network. Besides non-profit organizations or foundations, companies run with the purpose of profit at least in a capitalistic economy. This would imply that the network security and the profitability would correlate. The node operators are responsible for the network security where they verify transactions and protect the network from malicious actors. They have an extrinsic motivation as downtime is punished and a higher volume of AuD gets

[65] Ciaian, Kancs, & Rajcaniova, 2021

rewarded. Additionally, they have their own stake within the network. Besides that, node operators get rewarded higher if the price of the underlying coin of the network increases rises in $ nomination. Conversely, if the price of the coin drops the reward in $ nomination is vanishing. This has an impact on node operators because their profit is calculated in $ nominations, as the initial investment was in $ nomination when they bought or rented the servers and purchased the underlying coin. Furthermore, if there are employees, they also would have to be paid in $ nomination even if not the *Validator* would have to cash out their cryptos to make a living. Dollar determination in this context was used as a synonym for any FIAT currency.

4. Case Study „Cosmos ecosystem“

The Cosmos ecosystem is more vibrant than ever before and sees massive growth. Tendermint, the Cosmos ecosystem's consensus mechanism, was devised in 2014 by Jae Known and was also a milestone in the development of the PoS consensus. Many other projects derived their own variant of the PoS from the Tendermint mechanism and it is now the leading technology. The Cosmos ecosystem was selected as its promises to be the “internet of blockchains” and its goal is to connect many independent blockchains with each other. Also, the Tendermint BFT consensus mechanism is widely used across the industry and considered the standard consensus for building PoS networks[66]. Currently, over 260 applications and services are built on Cosmos using the Cosmos software development kit (SDK)[67]. As mentioned in an earlier Chapter 2.3 Proof of Stake, Polkadot aims to reach the same goal as Cosmos, but the reason why Polkadot was not used for this case study is that the chain architecture and mechanism are built differently The Ethereum network was not employed because the switch from the PoW to the PoS consensus mechanism has not yet been completed, and thus the final implementation could still change, rendering the study meaningless. After analyzing the implications of the PoS regarding network security, the insights could be applied to the ETH network. Even the purpose of these projects is different. This case study should provide insights into the consensus mechanism and network security so it can be partially applicable to other networks. It should be noted, however, that different networks have different methods and implications. As a result, it cannot be used one to one; moreover, it should provide a direction with distinct impacts and interactions between the consensus process and network security.

4.1 Native Token $Atom

To analyze the Cosmos ecosystem first it should be clarified what the Cosmos Hub is. It is an open decentralized network that aims to scale and connect blockchains with each other. Interoperability or in other words becoming the “Internet of Blockchains” is the core goal of the Cosmos Hub. To achieve this the Cosmos SDK and IBC were implemented. This will be elaborated more briefly in this chapter. $ATOM is the underlaying native currency to be used to pay network/transaction fees as well as used as the staking token to secure the network and incentivize *Validators* and *Delegators*. The token $ATOM and its tokenomics will be discussed before elaborating the core technology and consensus mechanism.

[66] Tendermint Inc , 2022
[67] Tendermint, 2022

In early 2017, the Initial coin offering (ICO) was conducted by the Interchain Foundation (ICF) to kick off the network and develop the project further. Thus, the token was sold at a price of 0.075$ in the first round, also known as the private Pre-Sale, and at a price of 0.1$ in the public ICO, which finished on April 6th, 2017. The Interchain Foundation could rise with the most successful ICO, 17.6 million $ within 28 minutes. Whereas 10% of the Token supply was allocated to “ALL IN BITS INC” better known as Tendermint and another 10% was allocated for the ICF itself[68]. Despite the fact that, the funding was more like a fundraiser than an ICO because there was no certainty of token distribution, the target amount was raised in record time[69]. This highlighted the immense trust towards the project and the team consisting of Ethen Buchman and Jae Kwon. The Swiss based non-profit organization sold the raised Bitcoins and Ethereum to pay the expenses. The Treasury's holdings are valued at 168 million, according to the "Asset and Grant Overview Q3." Whereas 76% is held in cryptocurrencies, 14% in fiat currency, and 10% in public investments[70].

The holder can use the native Token to pay network and transaction fees, or to secure the network by using it as a staking token. In that case, the tokens are then delegated to one or more *Validators* and the token gilder then becomes a *Delegator*. Here the *Delegator* gets staking rewards which consist of new-minted tokens and parts of the transaction fees. Thus, the network is secured, and the *Delegator* gets rewarded, which is all part of the game theory. However, it should be noted that with the staking also comes a lockup period. This means that the tokens are locked in for a certain time, in the case of $Atom it is locked up for 14 days via smart contract. The tokens cannot be transferred or sold for 14 days if an unbonding was requested. This means that the asset is no longer liquid for the duration of the stake. Currently, 183 million Tokens are bonded which is about 62.25% of the total supply. In comparison the bonded ratios of the biggest PoS Networks are the following: Polkadot 55.5%[71]; Solana 75.8%[72]; Avalanche 67.1%[73]; Cardano 72.5%[74].

[68] CoinCodex, 2022
[69] Cuen, 2021
[70] Interchain Foundation, 2022
[71] Polkadot, 2022
[72] TRITON, 2022
[73] Avascan, 2022
[74] Adapools.org, 2022

This might be a measure of how many people trust the network and support or secure it through staking, among other things. Besides the risk of illiquidity, which can be detrimental to the "investor" in the event of a price drop, there is also the risk of slashing as mentioned in the previous chapters. Hereby, the *Delegator* can lose parts of his deposited capital in case of bad due diligence and misbehavior of the *Validator(s)*. However, the interesting mechanism is that if more *Delegators* decide to undelegate, the reward for the remaining *Delegators* increases, as the staking rewards and the inflation is a built-in mechanism. That means that a certain amount of token will be created after a certain time no matter what and a part of it gets distributed to the *Delegators*. Next to the staking rewards, the *Delegator* receives rights to participate in the governance process, whereby one token staked equals one voting right. This governance decides om further improvements and incremental changes of the network.

This leads not only to decentralization as everyone with a staked token can vote Aside from the fact that it is often criticized that more money equals more power, but it can also lead to little benefits. As the Cosmos hub serves as the foundation for additional networks that are built on top of it, it becomes relevant for new token allocations for new networks. Projects must reach out to a community and onboard them in order to have an active community. So, they allocate the freshly minted tokens to $ATOM holder or staker also referred to as “Stakedrop” or “Airdrop”. The most famous example was the Osmosis Stakedrop where 50 million tokens were distributed among $ATOM staker, which was 16,67% of the total supply. The eligible user had to fulfill small tasks to receive 80% of their Stakedrop the other 20% was claimable immediately[75]. Through Air-/Stakedrops, new participants for the network can be gathered, as the newly distributed tokens are free money. Osmosis developed into a significant part of the Cosmos ecosystem and early user and loyal Stakedrop participants get rewarded plentiful. Because this method was so effective, many other projects adopted it and utilized it to onboard users and distribute tokens. The distribution of the tokens is quite significant as described in Chapter 2.5 Tokenomics; it enforces the decentralization which is more important in PoS networks.

So, to wrap it up, $ATOM is an inflationary token currently about 10.66 % with a staking reward of 16.77 % (also fluctuating) and the current price of 21.55 $[76]. The circulating supply is 292,586,163 tokens, which leads to a market cap of 6,289,865,352 $ as of April 26th, 2022[77].

[75] Osmosis, 2022
[76] Cosmostation, 2022
[77] Cosmostation, 2022

According to CoinGecko.com this makes $Atom to the 25th biggest Token regarding market cap[78]. It should be emphasized that 62.25% of the circulation supply is locked for at least 21 days, with ongoing unbondings and locked tokens in liquidity pools on DEXes not being taken into consideration. This leads to a significantly smaller amount of $ATOMs on the market (110.451.277 $ATOM), which means less supply, affecting the price of the token considerably faster.

4.2 Cosmos Hub and Interoperability

Blockchains were independent and segregated prior to the development of the Cosmos Hub. There was no way for the chains to communicate with one another, and assets could only be transferred between chains via so-called "Bridges." Kicking off and building a blockchain was time-consuming and hard. The Cosmos Hub with its pioneering solutions is solving the problem of scalability, usability, and interoperability[79]. But before going into detail with the Cosmos SDK and the IBC Protocol the history of the Cosmos Hub and their development will be outlined.

It all started in 2014 with the paper from Jae Known itself, where he applied the Byzantine Fault Tolerance (BFT) to a PoS consensus mechanism[80]. The result was the consensus mechanism Tendermint which is the most advanced implementation of the BFT algorithm and the cryptoeconomics to date. The Tendermint BFT will be described in the following chapter more briefly. Jae founded “All in Bits Inc” which is nowadays known as Tendermint Inc. The company was formed to imporve the work on this project because it addressed the challenges of the PoW mechanism and he understood that in terms of speed, scalability, and environment the new consensus mechanism could provide a solution to it. In 2015 Ethan Buchman who is a co-founder of the Cosmos hub joined Jae Kwon with his work after a Crypto Conference. In the same year “All in Bits Inc” collaborated with the Start-up Monax which worked on a contract management platform, and they launched Ethermint 1.0, which was the first implementation of an Ethereum Virtual Machine (EVM) on the Tendermint. An EVM is a state machine, that allows in addition to sending and receiving a digital currency as seen in the BTC network, to apply specific rules of changing state from block to block[81]. This was the first step

[78] CoinGecko, 2022
[79] Tendermint Inc., 2022
[80] Kwon, Tendermint: Consensus without Mining, 2014
[81] devtooligan, 2022

towards the “Application Blockchain Interface (ABCI), which allows applications written in any language to simply plug and apply on the Tendermint BFT.

In 2016 the finalized Whitepaper of Cosmos “Cosmos: A Network of Distributed Ledgers” was published. Thereupon, Cosmos created a buzz and won the prize of the “Most Innovative Project”. The ICF was founded to enhance the development of the Cosmos ecosystem and contracted Tendermint Inc (All in Bits Inc) to kick off Cosmos.

In 2017 the successful ICO of the $ATOM token funded the ICF. It continued to fund the building process of the Cosmos Network architecture via Tendermint Inc. The early prototype of the Cosmos SDK begins as developers staring to build the applications on top of Cosmos.

Tendermint made a breakthrough in 2018 with the concept of Inter-Blockchain Communication (IBC). Various testnets were launched and many nodes joined the network. In the following years, Cosmos continued to gain traction and various projects build on top of the Cosmos SDK among others also the world’s largest cryptocurrency exchange “Binance”, which launched later their own chain, the “Binance Smart Chain” (BSC) utilizing the Tendermint BFT mechanism, deployed on the Cosmos hub. On March 13th, 2019, the Cosmos Hub was launched officially, and since then it is running without any interruption.

The ICF is still active and awards numerous grants each year to aid in the development of Cosmos and the ecology. It is based in Switzerland more precisely in Zug and is non-profit organization[82]. The Tendermint Inc is a for-profit company and still actively managed from Ethen Buchman and Jae Kwon which focus on maintaining the Cosmos Network. It is headquartered in Berkeley, California, and contracted from the ICF[83]. Since February 23rd, 2022, Tendermint Inc reformed to “Ignite”. The rebranding was also prompted by the company’s quick expansion and the introduction of two new products, the All-in-One solution “Starport” and the Cross-Chain-DEX-Aggregator “Emeris”, according to CEO Peng Zhong[84].

[82] Tendermint Inc, 2022
[83] Crunchbase, 2022
[84] Business Wire, 2022

The Cosmos Hub can be divided up into 3 sections:

- Cosmos SDK (Blockchain Framework)
- IBC Protocol (Interchain Standard)
- Tendermint BFT (BFT Consensus)

The Cosmos Software Development Kit in short SDK is the Blockchain framework that enables projects to deploy a custom blockchain with the help of prebuilt modules and allows adding custom modules for the project-specific requirements. This makes it easy for new projects to launch their own chain by using the same Tendermint BFT consensus mechanism and secure the network. Modules are open source and the variety of modules in the Cosmos SDK is increasing. Another built-in benefit is that they can natively interoperate with other blockchains[85]. Currently, there are assets worth over 6 billion $ built on the Cosmos SDK[86]. Every chain is secure and scalable as well as sovereign as changes can be proposed via governance module. To fully understand what the Cosmos SDK means as a whole, the architecture standpoint of blockchains should be comprehended.
A blockchain can be divided into three conceptual layers:

- **Application:** Responsible for updating the state given a set of transactions, i.e., transaction processing.
- **Networking:** Responsible for the propagation of transactions and consensus-related messages.
- **Consensus:** Enables nodes to agree on the current state of the system.

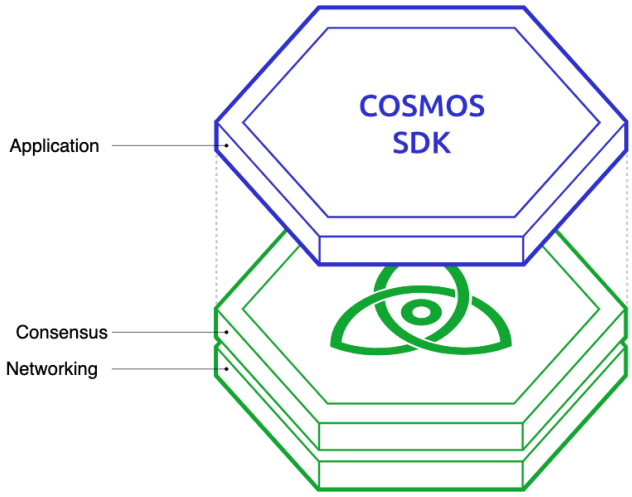


Figure 7: Architecture of Blockchain[87]

[85] Tendermint Inc , 2022
[86] Tendermint Inc, 2022
[87] Tendermint Inc, 2022

As seen in Figure 7, the Application layer can be built and modified according to need through the modules, which are offered in an open-source library. The Tendermint BFT consensus mechanism handles the Consensus- and Networking layers (shown in green) of the blockchain. The academics have identified six layers of technology making up a blockchain whereas the Modeling, Contracts and Data layers, are included in the Tendermint BFT.

The Cosmos SDK is a framework that is based on two major principles.
To begin, as previously mentioned, the *Modularity* allows developers to design application-specific blockchains using modules rather than starting from scratch. The second principle is the *Capabilities-based security* which means that the security boundaries between modules exist, and modules can be assessed according to the security aspect. This limits the interaction of malicious or unexpected functions. Currently, the Cosmos SDK builds on top of the Tendermint BFT, but it is expected that in the future other consensus mechanisms which implementing the Application Blockchain Interface (ABCI) can utilize the Cosmos SDK and build different architecture models. The majority of projects are being developed on top of Virtual Machine blockchains like as Ethereum since it was easier to implement smart contracts rather than build an entire blockchain from scratch. With the Cosmos SDK, it is now possible and becomes easier and easier to build application-specific blockchains which are sovereign, flexible, secure, and perform well. Ethermint is a great example of the modularity of the Cosmos SDK. As it is a program that converts the Ethereum Virtual Machine into an SDK module, so all Tools and Smart Contracts that are existing on Ethereum can be ported to Cosmos and still benefit from the Tendermint BFT.

The Cosmos SDK inherits a key element of the Cosmos ecosystem which is the Interblockchain Communication (IBC) the backbone of the Cosmos Hub. It allows to build blockchains to talk to each other and trade assets. The reason for this is that without the ability to communicate and move assets between independent chains, data silos would emerge and liquidity between distinct assets would be insufficient, resulting in higher slippage. Cross-chain bridges were developed to address the issue of transferring assets between multiple chains; nevertheless, they pose significant risks because they are established independently by third parties and security is not guaranteed. In recent times some bridges get exploited which led to large losses of users. This external risk factor is a danger for some projects since the stolen assets lead either to a concentration of assets and therefore to centralization or usually get dumped immediately which cause a rapid price plunge. Both cases harm the projects and could even lead to the end of a network.

IBC solves this problem as it enables reliable, ordered, and authenticated communication between heterogeneous blockchains. As Aristotle already said: “the whole is greater than the sum of the parts “. This also applies to networks as the value of a system is greater than the sum of its chains. This makes the Cosmos Hub with IBC worth more than the chains stand alone. To achieve this and establish synergies, the chains must be heterogeneous, which implies that the blockchain that wants to enable IBC must meet certain standards, one of which is the consensus layer’s fast finality. PoW consensus mechanism does not fulfill this as they have probabilistic finality. Finality refers to the moment when the transactions are completed and cannot be canceled, reversed, or altered. Fast finality is commonly referred to as deterministic because the transaction is regarded finality immediately as it is added to the chain. Probabilistic finality is condition in which it is added to the chain and becomes progressively difficult to manipulate; as a result, it is frequently advised to wait until other blocks are added and completed[88].

But there is a solution for Probabilistic-finality chains. It is known as “Peg-Zone”, which is a blockchain itself, that tracks the state of the chain, that does not fulfill the requirements and has a fast-finality consensus mechanism. So, it is interposed between both the chains.

Summarized IBC is constructing channels that will allow parties to communicate and transfer assets between different chains. Where single projects/networks can be seen as islands and the IBC connection as a shipping route. The problem with that approach is, that as the network increases, the number of connections grows quadratically if every “island” would be connected to each other. This issue was solved with the introduction of Zones and Hubs. Whereas Zones are regular heterogeneous blockchains also referred to as “islands” earlier. Every blockchain that has enabled IBC. Hubs are specially designed blockchains, whose purpose is to connect different Zones. The advantage is that every Zones which is connected per IBC with a Hub can automatically access all other Zones that are also connected with the Hub. The Zones, therefore, do not have to be directly connected individually to send and receive from other zones, as also illustrated in Figure 8. This reduces the requirement for connections because the Hub prohibits double-spending and requires only trust in the Hub[89].

[88] Anceaume, Pozzo, Rieutord, & Piergiovanni, 2020
[89] Tendermint Inc., 2022

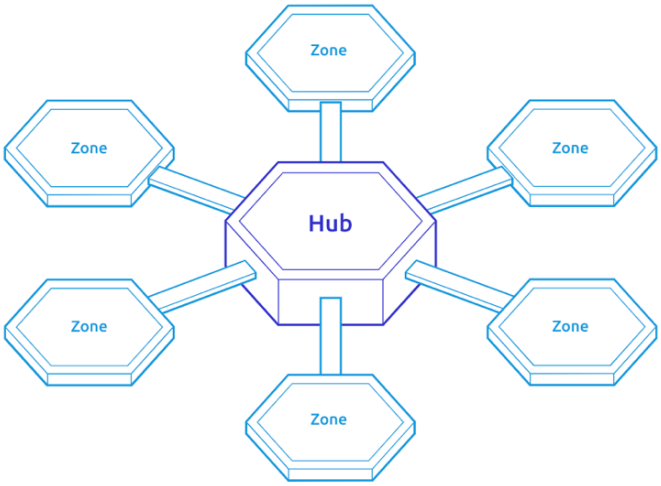


Figure 8: IBC Connection via Hub[90]

Every connection between Zones and Hubs has its own channel ID. To perform a transfer, it is necessary to know the ID. The Cosmos ecosystem can have multiple hubs but the most trusted and well-known one is the Cosmos Hub. Osmosis is the best example for IBC as it has the most transactions accruing. It enables users to swap the assets seamlessly from different chains. The network and the connections of the Cosmos ecosystem are growing significantly and getting increasingly complex.

The current connections between various zones can be seen in Figure 9. This illustration is a snapshot of the current state of IBC-enabled chains presented by MapofZones. Connections can be activated or be taken inactive. This network grows from time to time and shows that the vision of Cosmos to be the "internet of blockchain" becomes reality. IBC launched in March 2021 and within just over a year it connected already 43 souverain blockchains. As of April 29th, 2022, the 30-day IBC volume was around 5 billion $ with over 4 million IBC transfers[91]. The most active Zone regarding volume and transfers is Osmosis. As DEX allows users a seamless transfer/swap of their tokens, it is currently the leading AMM with the deepest liquidity and has over 3 million transfers as of the last 30-days.

[90] Tendermint Inc, 2022
[91] Mapofzones, 2022

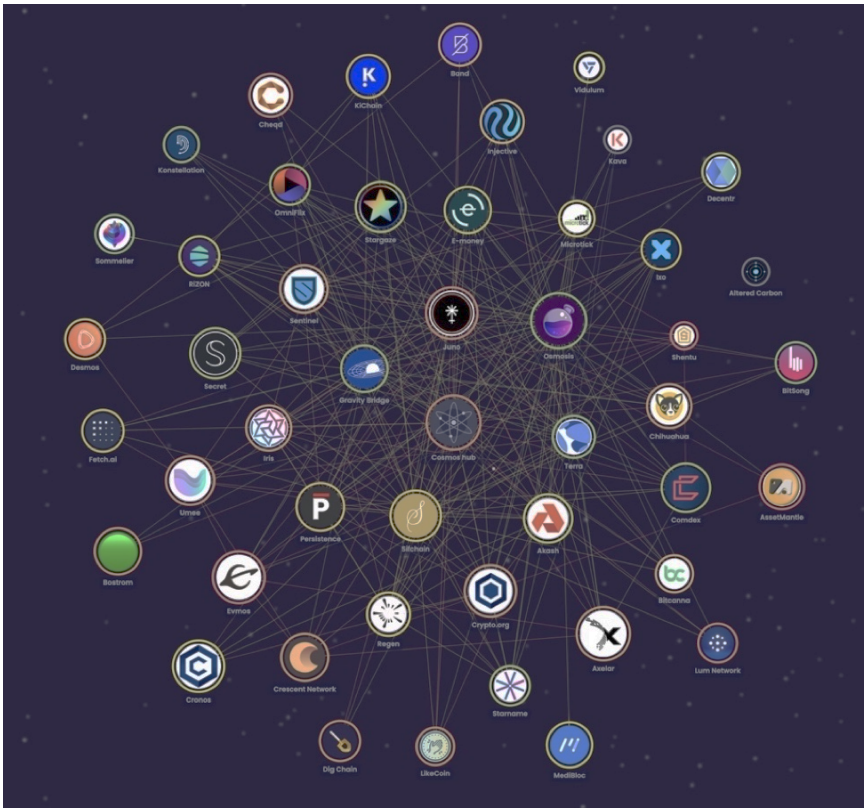


Figure 9: IBC Connections by MapofZones[92]

4.3 Consensus Mechanisms of the Cosmos Hub

This chapter will describe the most important part of the Cosmos Ecosystem, its consensus mechanism called Tendermint. It was invented by Jae Kwon and published in 2014 and is the foundation of the whole Cosmos ecosystem. Often referred to as Tendermint BFT the application manages the network and consensus layer of a blockchain. The application layer can be defined individually where the *Validator set* is determined[93]. It is possible to launch a public or a private blockchain on top of Tendermint BFT. If the *Validator set* is restricted and only pre-authorized *Validators* are able to confirm transactions a private blockchain is built but if the *Validators* are selected independently and the number of tokens determines the power of the *Validator*, the network is public and can be classified as a PoS[94]. This is currently the case as no private network was built with the Tendermint BFT so far. The Cosmos SDK is connected to the Tendermint BFT mechanism through the protocol called Application Blockchain Interface (ABCI). The protocol can be wrapped in any programming language like Java, C++, or Go. Hence, developers can build all three layers (Networking, Consensus, and Application)

[92] Mapofzones, 2022
[93] Tendermint Inc., 2022
[94] Tendermint Inc., 2022

in their favorite language so they can design it as desired. With these three layers, the Blockchain node can be built as illustrated in Figure 10.

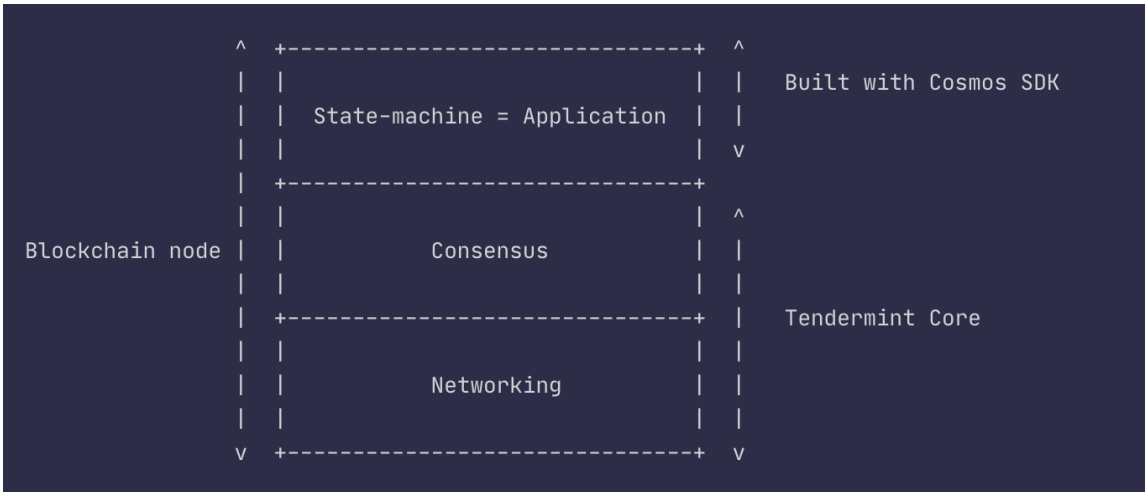


Figure 10: Tendermint and Cosmos SDK architecture[95]

The primary distinction between Tendermint and other consensus algorithms is that the Tendermint consensus has a build-in BFT fault tolerance, which implies that even if 1/3 of the *Validators* would fail, the transactions may still be validated, and the chain is secure because a consensus is still reached. This also leads to an instant finality, as blocks that are created are final and forks cannot be created. Furthermore, it solves the issue with legal and operational finality. As Transaction on PoW systems may never achieve the status of finality or even can be undone[96]. The PoW of Bitcoin for instance follows the longest chain rule, where if a fork happens both chains are valid until one of them is the longer chain whereas the other one gets dropped, leading to orphan blocks. Tendermint, therefore, is secure, has an instant finality, and can have a block time of 1 second where it can manage thousands of transactions per second, which leads to high performance. The instant finality is also possible through the round-robin protocol which is used by the Tendermint consensus. It allows nodes of the *Validator* nodes to communicate intermittently[97]. Through the practical Byzantine fault-tolerant algorithm pBFT, which, in addition to DPoS, is implemented in the Tendermint consensus mechanism. The pBFT is used to secure the system in case of malicious participants. In case one node is a bad actor at least four *Validator* nodes are required in total, whereas the other three must be trustworthy.

[95] Tendermint Inc, 2022
[96] Nabilou, 2022
[97] Fridman & Ugrinovskii, 2014

Another example would be the following:

If the system should tolerate up to three faulty participants → 3 x (3 malicious actors) + 1 = 10. Therefore 10 nodes would be needed. The formula is seen in Figure 11, whereby "f" stands for the number of malicious actors in the network. The pBFT is commonly used in various consensus algorithms and is not only used in DLT systems. It was outlined in the late 90s by Barbara Liskov and Miguel Castro[98].

$$|\mathcal{R}| = 3f + 1$$

Figure 11: pBFT Algorithm

This mechanism is implemented to ensure that even if the selected *Validator* fails, the system remains operational. The Nodes in a pBFT distributed ledger are ordered sequentially. Whereas one node is the primary (leader) node and the following act as backups in case the leader fails. Using the majority rule, the consensus should be reached with the help of all honest nodes. To understand the functionality of the pBFT, Figure 12 can be used. It describes the four phases of the pBFT consensus mechanism. The client sends a request to the leader node. In the case of a blockchain, the transaction should be signed. This information then gets shared with the backup nodes. Each node, the primary as well as the secondary node then processes the transaction and sends it back to the client. If the client receives "m+1" similar replies from the nodes the request is served successfully, where "m" is the maximum number of allowed faulty nodes. The sequence of the nodes is changing every time when the leader node gets replaced.

This can be adjusted with another protocol. However, also this mechanism has its vulnerabilities as the needed communication between the nodes is increasing exponentially with every additional node. The network becomes increasingly secure the more nodes are operating. Hence, it will be most successful if the number of nodes is not too large, but also not too tiny, so that it does not become insecure due to malevolent actors. In addition, the scale issue is subsequently dealt with by the implemented DPoS technique. The Sybil attack is an issue as it was described in Chapter 2.2 Network Security.

[98] Castro & Liskov, 1999

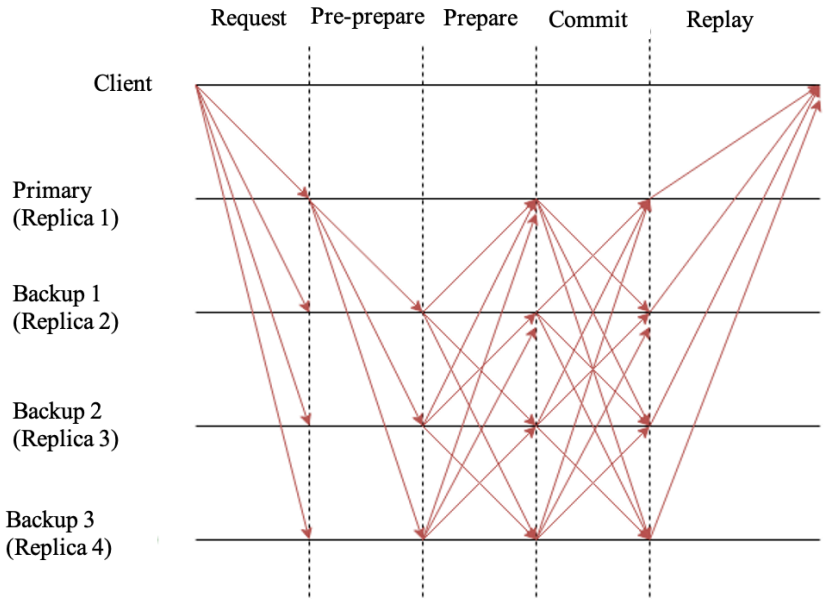


Figure 12: Functionality of pBFT[99]

The pBFT was introduced into Tendermint because it provides various benefits such as energy efficiency due to low computer power required and instant finality of the transaction[100].

Next to the pBFT implementation, the DPoS plays a major role within the Tendermint consensus mechanism. The nodes are run from *Validators*, which create new blocks and confirm transactions. The proposer, respectively the *Validator*, who finally adds the block to the chain, is chosen deterministically. More precisely the next proposer gets determined in proportion to the voting power which is resulting from the bonded native Token $ATOM. *Validators* are required to post a bond transaction that will lock a set amount of their coins (stakes) for a set duration. If the *Validator* is found to be involved in any malicious activity within this duration, it can be punished by slashing away his deposited stake. After this duration, stakes are unlocked and returned to the *Validator*[101].

4.4 Validator Sets

Validators are the backbone of the consensus mechanism, whereas in a DPoS consensus mechanism *Delegators* delegate their assets to selected *Validators*. To run a *Validator* some technical requirements must be met. First, there are hardware requirements for servers that run the Tendermint consensus mechanism algorithm and validate transactions. Hardware can also

[99] Hooda, geeksforgeeks.org, 2019
[100] Hooda, geeksforgeeks.org, 2019
[101] Thin, Dong, Bai, & Dong, 2018

be replaced with cloud servers as they provide sufficient computing power to run the operations. This, however, accommodates the risk of a single point of failure and undermines the entire concept of distributed ledgers because the *Validators* rely on the central services. This was also mentioned earlier. *Validators* who run their own servers on physical devices are also called a part of the "BareMetal-alliance". Nevertheless, *Validators* should not only run a single node as the potential danger is too significant of getting slashed. This will be also described later on.

Running various nodes to avoid downtime is recommended and also set up "sentry nodes" to protect the node from DDoS attacks. In order to set up the node, in addition to the hardware requirements, software requirements must be met. This includes in addition running the node, monitoring, and managing the node. This can be done with several solutions which can alert the *Validator* in any case. These software solutions are also used by non-blockchain specific applications. The open-source toolkit "Prometheus" which runs a multi-dimensional data model with time-series data can be used to identify several metrics. To set up a sufficient monitoring infrastructure instruments must be used to visualize data from various sources for this purpose "Grafana" can be used. To check the capabilities of your hardware the "node exporter" or "blackbox exporter" is suitable. These are only some examples of tools that can be applied to maintain the node.

An internet connection is a basic requirement, but it is important to have sufficient bandwidth since larger networks such as $ATOM require a correspondingly large amount of data. Multiple gigabytes per day are very realistic. After setting up the node and meeting all requirements it is expected that the *Validator* stays active as regular software updates and bug fixes are common. As a result, configuring a node is not something that should be done once and then forgotten about. It needs continuous service. As the Cosmos ecosystem is a DPoS network, delegations are necessary, and self-bonding is also required to launch a node where the *Validator* delegated authority to himself. This is almost neglectable due to the small amount required, which can be as low as 1 $ATOM.

In comparison to a Masternode in the $DASH Network, which is a hybrid of a PoS and a PoW, setting up a node requires at least 1.000 $DASH Token[102]. With the current price of 85.57$ as of May 06th, 2022, this would be around 85.570$ and would be a significantly higher barrier. Although this kind of barrier is also seen in the Cosmos ecosystem with the *Validator set*, which

[102] Bybit Learn, 2021

will be described later in this chapter. These needs, particularly setting up the node and monitoring it, necessitate certain knowledge and skills that not everyone possesses or is willing to acquire. Therefore, token holders are able to delegate their assets to certain *Validators*. When token get staked into a *Validator* staking pool two distinct types of revenue can be expected.

Firstly, there are Block rewards which interplay with the inflation of the network as inflation usually is diminishing. For every newly added block, new tokens get issued and distributed among the stakers. The higher the bonded rate the lower the block reward/staking reward per staked token. For instance, suppose 100,000 new tokens are released each year, with 100 million tokens being the current circulating supply and 50 million being staked/bonded. The 100,000 new tokens get divided among these 50 million staked tokens, which would lead to a block reward of 20% (100,000/50,000,000). The inflation in turn gets calculated through supply divided by newly issued tokens, which would be in this case 100 million divided by 100,000 and therefore 10%. Token holder who does not stake their token and do not contribute to the security of the chain get indirectly punished with inflation as their share of the network gets diluted by 10% per year.

The second revenue for the staked assets is the transaction fees that are paid by users of the network. However, without the *Validators*, this would not be possible therefore the *Validators* receive certain incentives for taking care of these tasks and securing the network. The incentives come from so-called commissions. The two revenue streams which are accrued in the pool of the *Validator* get paid out after deducting the percentage commissions of the revenue which the *Validator* demands for the service. The commissions can be set freely by the *Validator* and vary from 0% - 100%. The 100% commission is only used by *Validators* who delegate all their funds to themselves. The commissions can be changed daily up to a maximum daily change rate, the maximum commission rate cannot be changed after once being set. If a pool earns for instance 100 $ATOM on revenue and the *Validator* has a commission rate of 5% and 10 users with equal stake bonded and delegated to this pool, then the *Validator* would get 5 $ATOM as a commission from this pool. The remaining 95 $ATOM would be divided proportionately in this case equal to the *Delegators*. Where every *Delegator* could claim 9.5 $ATOM. As more assets are delegated to the pool the more the *Validators* earn on commission. This is a scalable business, and some *Validators* try to reach the highest AuD. To achieve this in some cases for a brief period of time, *Validators* set a 0% commission to attract as many *Delegators* as possible. As mentioned in Chapter 2.3 PoS, logically many *Delegators* are attracted as it optimizes their return.

Nevertheless, *Delegators* do a proper Due Diligence (DD) before they delegate to the *Validators*. They trust them not only with their coins, but also with the overall security of the network.

A proper DD could include the following aspects:

- Amount of self-delegated $ATOM

  The higher the number of self-delegations, the higher the trust of the *Validator* in his own operations as he would also face consequences for his actions. Also referred to "stake in the game".

- Commission rate

  A solid commission rate is required as too low a commission is not sustainable to run the operations and a too-high commission rate would harm the return.

- Track record

  Analyzing the *Validator's* track record in other networks may further demonstrate its dependability.

- Uptime

  The Uptime is shown in percentage and should usually be around 100% as low uptime is an indicator of bad management of their operations and can lead to penalties and a risk for the *Delegator*.

- Participation in governance proposals

  Active participation in governance proposals shows the genuine interest in the network and is an indicator of activity in the network. Further, the votes are viewable, which points out the opinion of the *Validator* about certain topics. The *Delegator* could then check if their views are matching.

- Community contributions

  Some *Validators* are also developers and use the nodes as an income source to fund their operations. Other *Validators* simply try to deliver any value with certain applications such as monitoring interfaces, displaying charts, or providing other kinds of services.

- Amount of delegated $ATOM

  This indicates trust from other *Validators*. However, it should be considered that a concentration of delegations is harmful to the network.

It should be noted should be that the coins are not directly transferred to the *Validators* and are held in the custody. Practically, the coins get locked/bonded for a certain amount of time. In the case of $ATOM, it is an unbonding period of 21 days. After the *Delegator* requests to unbond his tokens, he can transfer them after 21 days. This unbonding period can change from network to network. It is a mechanism to secure the chain. Two major risks are inherited if coins are staked next to the fact that the price volatility and the illiquidity play a part as mentioned in Chapter 2.3 PoS. Namely, it is the risk of getting slashed if the *Validators* have any downtime or a double signing occurs. Different networks handle the penalty differently. As can see in Table 5[103], in the Cosmos network *Validators* and *Delegators* get penalized simultaneously whereas in the CELO or Tezos network only the *Validator* get penalized. This means that the *Delegators* are protected more, and users of other networks are taken in responsibility to do proper DD regarding the selection of the *Validator*.

Furthermore, the differences in the amount of the penalty vary from network to network. In the Cosmos network, the assets get slashed at 0.01% if the node of the *Validator* is not able to connect for around 16 hours and therefore is not online. This influences the Uptime, which is evident to the *Delegator* and other potential *Delegators* when the *Validators* once go offline. The Uptime is shown in percentage. So, if a *Validator* was online for 100 hours and then went down for 30 hours, the Uptime would be 70%. If a *Validator* node performs a double-sign, which implies they confirm within the same block twice, this can occur if the backup nodes is running concurrently with the primary one. The staked assets get slashed by 5%. As a result, they not only lose potential rewards but also lose existing funds. Furthermore, they get jailed and even worst they could get tombstoned.

[103] Novum Insight, 2021

Network	Validator slashed?	Delegator slashed?	Downtime slashing of staked assets	Double-sign slashing of staked assets
Cosmos	Yes	Yes	Yes, after 16 hours at 0.01%	Yes, at 5%
Tezos	Yes	No	No.	Yes, at 8,000 XTZ
Solana	Yes	Yes	No	Yes, at 100%
CELO	Yes	No	Yes, at 100 CELO	Yes, at 9,000 CELO
Polkadot	Yes	Yes	Yes, if more than 10%, at 7%	Yes, at 1 – 100%
Terra	Yes	Yes	Yes, after 16 hours at 0.01%	Yes, at 5%

Table 5: Slashing penalties

Table 5 shows that some networks impose sanctions on a fixed basis, while others use percentage-based sanctions. Polkadot also have an extra variable where the double-signing can be penalized heavily. Double-signing can occur accidentally or could also be a malicious behavior. At the Polkadot network, developers can generally detect this and alter the penalty.

It seems like selecting the *Validator* with the lowest commission and the highest uptime is only logical. But the low commission is contradictory to the economical setup. *Validators'* only incentive is commissions, whereas maintaining a node costs money and time. It becomes obvious that running a node at 0% commissions is not economically reasonable. Moreover, supporters of the network who do not run a node for monetary reasons have to pay their bills somehow and only a few can afford to pay this out of their pocket. The reason 0% commission are offered by *Validators* is that it is often seen as a marketing measurement. Running a *Validator* node is scalable since the cost of setting up and maintaining a node does not increase as the delegations respectively the voting power increases. Hence, with a higher AuD the lower the commission could be to cover the cost. Nevertheless, there is another reason getting a certain amount of delegation is of significant. The reason is the so-called *Validator set*.

The *Validator set* is a group of *Validators* actively participating in finding a consensus. On the Cosmos Hub, only the Top 175 *Validators* candidates with the most voting power form a *Validator set*. The *Validator set* in the Cosmos hub is enlarged from 125 to 150 by governance proposal #54 and to 175 via governance proposal #66 to decentralize and expand the network. Every network built on top of the Cosmos Hub has a *Validator set.* The reason why a set was selected and not everyone was allowed to be a part of the consensus is that the pBFT is integrated into the Tendermint BFT consensus mechanism. It is an interplay between the Block Time and the security of the network. As previously said, the more *Validators* in the set, the higher the security since it is better protected against malicious players. However, it also leads

to a higher block time, which means that the scalability suffers as it takes more time until transactions get verified. If a *Validator* no longer belongs under the Top 175 (depending on the network) *Validators* the node no longer gets any staking reward and their votes in governance proposals are not valid anymore. As a network grows and the price of the related native chain rises, so does the barrier to entering the active set.

This brings advantages and disadvantages. As it becomes more difficult for new *Validators* to enter the active *Validator set* (e.g., Top175), active nodes have a vested interest in remaining in the active set because the revenue would vanish and the reputation would suffer if the *Validators* and therefore the delegations were to fall into the inactive set, missing out on rewards and losing power. Therefore, it makes sense that *Validators* run their commissions for a certain time at 0% and try to achieve higher delegations. This is also a part of the game theory as active *Validators* get rewarded with higher delegations and *Validators* that care less and are not active drop into the inactive set where their rights for rewards and voting rights get revoked.
There are various strategies to recruit new delegations, but not of them add any value. Same *Validators* provide tools to monitor statistics or present charts of new tokens on the Cosmos ecosystem, as well as create instructive content and further develop the technology. As the fight for the active set especially in bigger networks get heated, *Validator*s try to lure *Delegators* with giveaways, NFT drops or Stakedrops.

In smaller chains, staying in the active set may be easier because it may just require some self-delegations to exceed the minimal delegations and get respectively stay in the active set. Following that, several networks will be examined to determine their economic value. Table 6 shows the *Validator set* of the Cosmos network. This network has already indicated that it has 175 *Validators* in the active set, which indicates that 175 separate entities can monitor and confirm the network's transactions and so receive rewards and vote. It should be noted that if a *Validator* votes with its voting power in a governance proposal, the *Delegator* retains the power to overwrite the vote and give his opinion based on his proportional voting power. If the *Delegator* does not vote and the *Validator* votes, the vote counts for the *Validator's* view as well. Usually, the *Validator* coordinates the vote with the community and communicates it clearly.

Rank	Validator Name	Voting Power	Commission	AuD in $
1	stake.fish	10,955,369	4%	186,241,273
2	Binance Staking	10,553,758	2.5%	179,413,886
3	Kraken	9,689,468	100%	164,720,956
…..	…..	…..	…..	…..
173	Nodeasy.com	27,196	10 %	462,332
174	Stake Frites	19,536	5 %	332,112
175	Numenor.one	15,719	5 %	267,223
176	Valnodes	15,336	1%	260,712

Table 6: Snapshot of the current Validators set of $ATOM

Based on the price of 17$ as of May 7th, 2022, for the native token $ATOM, the AuD is calculated in Table 6, where the voting power, which is the amount of delegated $Atom to the *Validator* gets multiplied by the price.

This excerpt shows that the biggest *Validator* currently has over 10 million $ATOM under delegations, which makes up to over 186 million US $. The smallest *Validator* as of May 7th, 2022, had about 15,719 $ATOM under their delegation, making up to over 267,000 US $. This indicates that in order for the new entity to reach the active set, it must have delegated at least 15,720 $ATOM. If they do not know how to attract *Delegators*, they will have to delegate $ATOM valued roughly 267,000 $ to themselves. Not everyone is capable to do this.

Being on the lower edge of the set also carries the risk of being kicked out because another *Validator* in the set could obtain some delegates and overtake you the $ATOM network currently has 402 *Validators,* out of which only 175 are contributing to the consensus. The remaining 227 are either jailed, which means that they are out of the set due to inactivity or must have fewer delegations. However, these *Validators* still have the chance to get into the active set again. The *Validator* at Rank 176 has only 383 $ATOM less than the *Validator* above him. That means he could surpass him at any point and resume his active role in the set. For this, he must get either these delegations or delegate around 6.000$ worth of $ATOM to his node.

Another example shown in Table 7 is an excerpt of a network, that is significantly smaller than the Cosmos Network. The Chihuahua Network, which is the first Meme-Token in the Cosmos ecosystem, where the native token is called “HUAHUA” and has a price of 0.00022$ as May 7th, 2022.

Rank	Validator Name	Voting Power	Commission	AuD in $
1	Provalidator	2,224,613,838	5%	489,415
2	Cosmosstation	2,197,843,099	5%	483,525
3	kingnodes	1,488,982,778	5%	327,576
….	….	….	….	….
123	Dabu Dabu	16,579,768	5%	3,647
124	20MB Restake	15,566,100	5%	3,424
125	Chainmasters	12,409,036	10%	2,729
126	Redwood	4,867,749	5%	1,070

Table 7: Snapshot of the current Validators set of $HUAHUA

The AuD shown in Table 7 is rounded off. The current set is changing continuously and therefore a snapshot was taken from the block explorer “Mintscan”. The AuD of the lowest active *Validator* is roughly 2.700 $, indicating that it is less capital costly to enter the active set than the $ATOM network. The gap between the *Validator* in Rank 125 and 126 seems big but as the coin value is so low the difference is 1.700$ and could be beaten anytime. If the technical requirements are met and a potential *Validator* has the financial means to fund his *Validator* with around $3.000 worth of $HUAHUA token as of May 7, 2022, the *Validator* would immediately enter the active set and make ceteris paribus the *Validator* “Chainmaster”, an inactive *Validator*. This shows that with a growing network and an increasing price of the native coin the chain becomes more secure as it requires a more capital intense barrier to cross. This, however, also depends on the size of the *Validators set*. As a larger set within a new network with a higher market capitalization could nevertheless result in a low entrance barrier. The older chains with a relatively smaller *Validator set* requires a bigger $-nominal amount to enter the active set. This can only be accomplished through professionalization, as recruiting this number of delegations, or deploying enormous sums of finance is not straightforward

Network	Market Cap	Price	Top Validator	Minimum delegation	Δ to inactive Validator	Validator Set
$CRO *$-Nomination*	$6,635,683,734	0.26 $	366,082,643 *$ 95.181.487*	1,294,827 *$ 336.655*	Δ 761.532 *$ 197.998*	100
$ATOM *$-Nomination*	$4,724,527,830	16.10 $	10,960,665 *$176.466.707*	15,720 *$253.092*	Δ 353 *$ 5.683*	175
$OSMO *$-Nomination*	$1,263,589,462	3.46 $	15,572,897 *$53.882.224*	75,105 *$ 259.863*	Δ 1.007 *$ 3.484*	135
$EVMOS *$-Nomination*	$710,482,832	3.51 $	716,056 *$2.513.357*	2,623 *$ 9.207*	Δ 135 *$ 474*	150
$KAVA *$-Nomination*	$670,948,491	3.57 $	26,637,935 *$95.097.428*	6,396 *$ 22.834*	Δ 4.177 *$ 14.912*	100
$SCRT *$-Nomination*	$559,114,374	3.30 $	12,995,929 *$42.886.566*	15,737 *$ 51.932*	Δ 8.734 *$ 28.822*	80
$JUNO *$-Nomination*	$501,653,012	10.17 $	2,649,141 *$26.941.764*	32,374 *$ 329.244*	Δ 2.215 *$ 22.527*	125
$XPRT *$-Nomination*	$207,008,534	2.07 $	9,777,439 *$20.239.299*	31,255 *$ 64.698*	Δ 17.457 *$ 36.136*	75
$INJ *$-Nomination*	$203,588,782	3.58 $	2,869,779 *$10.273.809*	2,535 *$ 9.075*	Δ 1.341 *$ 4.801*	30
$MED *$-Nomination*	$197,298,854	0.03 $	188,208,913 *$5.646.267*	123,128 *$ 3.694*	Δ 8.149 *$ 244*	50
$FET *$-Nomination*	$174,994,023	0.25 $	27,343,619 *$6.835.905*	9,355 *$ 2.339*	Δ 9.151 *$ 2.288*	60
$SIF *$-Nomination*	$170,371,022	0.13 $	51,361,310 *$6.676.970*	4,550 *$ 59*	Δ 2.743 *$ 357*	115
$AKT *$-Nomination*	$129,092,020	0.81 $	15,519,108 *$12.570.477*	13,765 *$ 11.150*	Δ 4.916 *$ 3.982*	100
$BAND *$-Nomination*	$116,723,737	2.80 $	9,748,058 *$27.294.562*	1 *$ 3*	Δ 1 *$ 3*	78
$NGM *$-Nomination*	$80,406,269	1.47 $	2,108,008 *$3.098.772*	159,381 *$ 234.290*	Δ 147.613 *$ 216.991*	100
$CTK *$-Nomination*	$70,165,716	0.96 $	6,010,608 *$5.770.184*	1 *$ 1*	Δ 1 *$ 1*	120
$REGEN *$-Nomination*	$65,764,028	0.51 $	5,741,467 *$2.928.148*	99,282 *$ 50.634*	Δ 18.508 *$ 9.439*	75
$STARS *$-Nomination*	$57,256,791	0.06 $	45,165,771 *$2.709.946*	1,123,516 *$ 67.411*	Δ 12.976 *$ 779*	100
$IRIS *$-Nomination*	$48,834,717	0.03 $	96,682,691 *$ 2.900.481*	24,869 *$ 746*	Δ 1.015 *$ 30*	115
$MNTL *$-Nomination*	$31,965,852	0.28 $	17,413,735 *$ 4.875.846*	93,716 *$ 26.240*	Δ 60.517 *$ 16.945*	50
$XKI *$-Nomination*	$29,995,702	0.13 $	62,633,733 *$ 8.142.385*	32 *$ 4*	Δ 20 *$ 3*	100
$DVPN *$-Nomination*	$21,418,467	0.0025 $	777,844,993 *$ 1.944.612*	24,239,085 *$ 60.598*	Δ14.142.752 *$ 35.357*	80
$CMDX *$-Nomination*	$20,197,317	0.74 $	3,055,232 *$ 2.260.872*	58,249 *$ 43.104*	Δ 52.792 *$ 39.066*	75

Table 8: Overview of required delegations for networks

The Cosmos SDK and its modular structure make it possible that the standards and requirements are almost similar. Only the network size determines the required server capacity and the minimum delegation, which varies. Table 8 shows an overview of the minimum required delegations for each network. The Networks were ranked from top to down according to the market capitalization. When compared to other chains, $EVMOS, which has comparatively large market capitalizations, still has noticeably low entry barrier in relation to its minimum delegation to get into the active set. The reason for this could be that the chain was launched recently and there is a higher centralization of delegations. Analyzing the table reveals that some chains are more contentious than others. $DVPN and $COMDEX have admittedly tiny market capitalizations even after being in operation for some time, but they have a high entry hurdle.

The table with the overview does not represent the whole Cosmos ecosystem. Coins with a lower market cap than 10 million were left out to keep the list short. Other networks are not listed because either there is no reliable price for them or they are not listed and tracked via Mintscan yet, which lists the delegations for each chain. Some of the Tokens with a stated price on Coingecko do not have any information on the circulating supply, hence the market cap cannot be determined and is therefore not listed in this table. To keep it reliable only the source "Mintscan.com" was selected as it is the commonly used and most trusted block explorer for the Cosmos ecosystem. The Binance Chain was excluded even though it is listed on Mintscan and has a price since Mintscan updated and the specific *Validators* for that chain are no longer observable. In comparison to the Table created to monitor the *Validators* for the survey, some additional chains were included as they were freshly constructed, such as $EVMOS. It should also be noted that the minimum delegation and price were taken at 3 p.m. UTC+2 on May 8th, 2022, and are subject to change at any time.

4.5 Survey

The conducted survey was used to collect data about the viewpoints of *Delegators* and *Validators*. This should help to identify the strengths and potential weaknesses of the network security of PoS Networks. As the paper specifically addresses the Cosmos ecosystem and examines the future viability of *Validators* in the context of network security and other potential vulnerabilities only *Validators* which also validates within the Cosmos ecosystem were surveyed. The aim was to conduct a representative survey with a broad and randomized

participants amount. As two diverse groups were consulted, two different requirements were fulfilled. The *Delegators* survey [104], as well as the *Validator* survey[105] can be found in the Appendix.

To get qualitative survey results the goal of the survey "*Validators*" was to get at least 51% of the voting power from as many chains as possible. The minimum was to cover 51% of the following projects: $ATOM $OSMO $JUNO. If 51% of the voting power was not reached, the approach was to get at least 5 of the Top10 *Validators* and in addition 5 of the lowest 10 to ensure the opinions and views from different perspectives. It soon it became evident that reaching out to *Validators* and meeting this predetermined objective would be impossible. Therefore, a new approach was pursued. The 200 biggest *Validators* of the Cosmos ecosystem according to the AuD were contacted. For this purpose, the table was created which was already explained in Chapter 3.2 Data preparation. Furthermore, smaller *Validators* were randomly selected to include the views of less professional *Validators*. It is possible to distinguish between single *Validators* that execute their nodes independently and possibly only on one chain. This group of *Validators* are referred as "Shark Validators" as they are custom *Validators* and run all application by their own. The bigger *Validators* which also have bigger amounts of AuD are referred as "Killer Whare Validators". This kind of *Validators* have a team behind the *Validator* node and operate as a company. The third group of *Validators* is so called "Whale Validators". These are nodes from centralized exchanges (CEX) and investment funds. In this survey, all three groups of *Validators* were contacted; however, as expected the "Whale Validators" form CEXes did not replied as it had implications with their compliance, and they could not give out information also for security reasons. Other *Validators* from the Shark or "Killer whale" section replied but informed that they are not confident with sharing certain information.

Of the contacted *Validators*, 25 filled out the form and completed the survey. The total AUD of the participated *Validators* was over 2 billion US-Dollar on the day of the snapshot. This amount is changing constantly as delegations in and outflow. Constant redelegations, unbondings, and new delegations happen. The biggest *Validator* had 29 Nodes running, and the smallest ones only have one running node on one chain. Given the fact that a significant amount of AUD and all kinds of varieties of *Validators* were covered within the survey, it can be

[104] Appendix 37
[105] Appendix 38

considered representative. Small (Shark) and Big (Killer Whale) *Validators* were included and shared their viewpoint in the survey. All of the participating *Validators* validated at least one Cosmos ecosystem chain, although it is possible that they validated other chains outside of the Cosmos ecosystem, indicating that the survey results can be partially generalized to the PoS consensus mechanism. It can be assumed that the participants of *Validators* have significantly more knowledge about network security and the PoS system than *Delegators*. However, the viewpoint of *Delegators* is also of immense importance.

For this paper, also various *Delegators* were addressed to show the viewpoint of the other stakeholder group. Also, in Chapter 3.2 Data preparation it was explained how *Delegators* were reached out and how *Delegators* were incentivized to participate in the survey. It should be noted that the retweeting factor, which was implemented in the giveaway, resulted in randomness, and increased coverage. The survey for the *Delegators* was divided into 5 different parts. Within the first part, the participants provided basic information such as age, working field, origin, portfolio size, and allocation. The second part covered the staking behavior and the staking strategy. The third chapter dealt with the *Validator's* knowledge and preferences. The fourth chapter was covering the knowledge about tokenomics. The final fifth chapter managed the network security aspect.

The survey for *Delegators* had in total of 416 participants from all age classes as can be seen in Figure 13. The distribution of the ages is a bit skewed as younger people use Twitter and are involved with cryptocurrencies. Still, it is evident that the participants are between their early 20s to late 30s. This can also be corroborated by a Forbes magazine survey from the end of 2021, which shows that the majority of crypto users are between the ages of 18 and 39[106].

[106] Dellatto, 2021

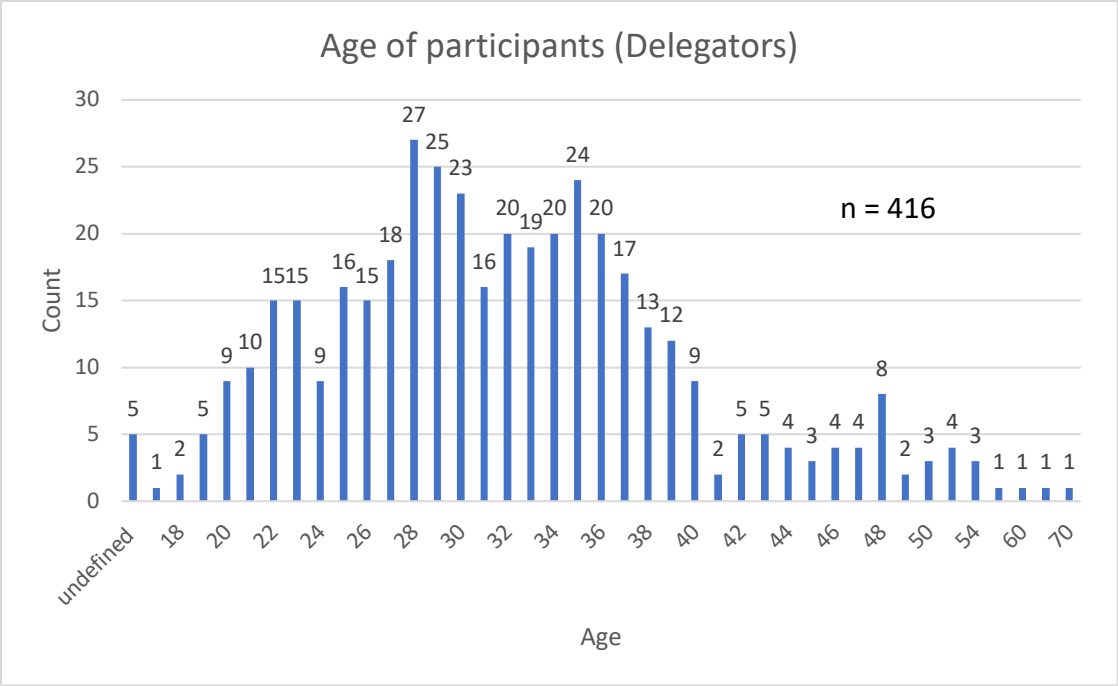


Figure 13: Age of participants

As Figure 14 illustrates participants of the survey coming from all over the word. It becomes also evident that the survey was completed by *Delegators* from 62 different countries, the most of them were from Russia and the United States. All continents are covered except of Australia. The fact that the United States is also prominently represented indicates the reality that many Americans use cryptocurrencies.

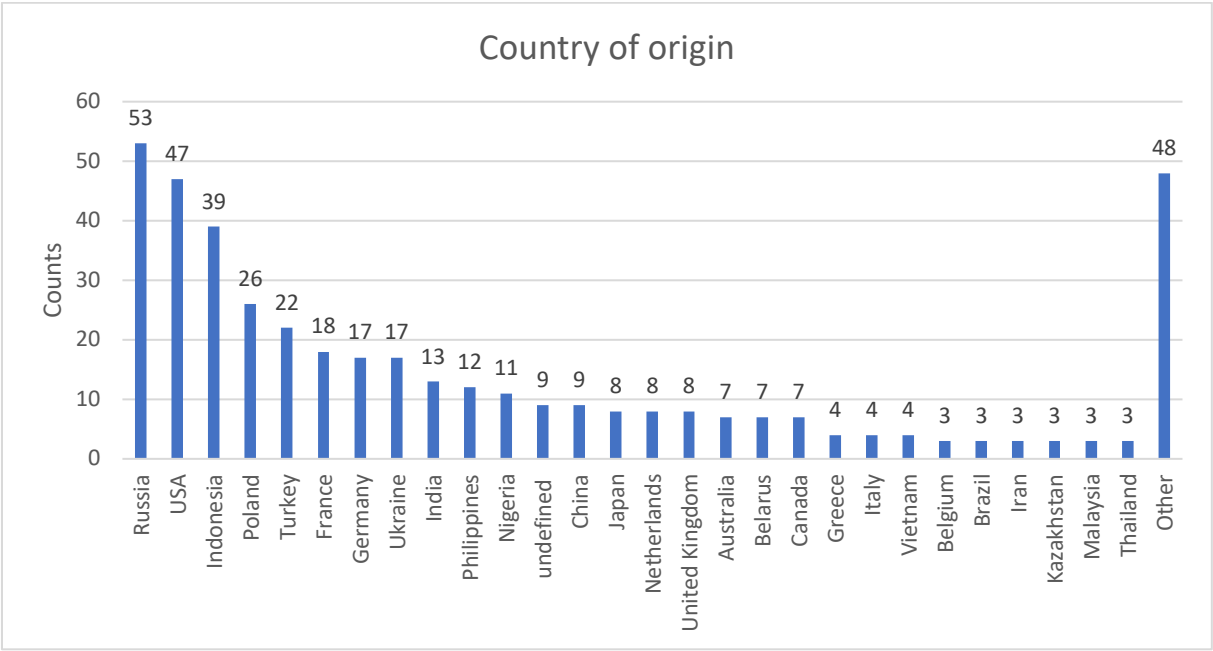


Figure 14: Origin of survey participants

It might be argued that the survey was falsified because it was distributed via Twitter, which has a large number of crypto users. The participants come from a variety of industries and fields of work. Despite the fact that 32 of the 416 participants work full-time on cryptocurrency. Table 9 demonstrates that, in addition to investors and IT professionals, other fields, including the unemployed, are represented. Smaller sets of working fields are included together as "Other," as they appeared separately.

Field of Work	Number of people	%	Cumm.
Collage student	42	10.1%	10.1%
Engineering	40	9.6%	19.7%
Crypto	32	7.7%	27.4%
IT	29	7.0%	34.4%
Undefined	26	6.3%	40.6%
Healthcare	26	6.3%	46.9%
Manager	18	4.3%	51.2%
Office worker	17	4.1%	55.3%
Unemployed	14	3.4%	58.7%
Construction	12	2.9%	61.5%
Finance	11	2.6%	64.2%
Freelancer	9	2.2%	66.3%
Sales	9	2.2%	68.5%
Education	8	1.9%	70.4%
Entrepreneur	8	1.9%	72.4%
Academia	7	1.7%	74.0%
Computer Science	7	1.7%	75.7%
Investor	7	1.7%	77.4%
Cook	6	1.4%	78.8%
Artist	5	1.2%	80.0%
Other	83	20.0%	100.0%

Table 9: Field of Work of participants

To analyze if the survey was biased with only Cosmos ecosystem crypto users the first part of the survey asked if the participants also invested outside of the Cosmos ecosystem and if so in which another projects. This should show which other projects the participants are invested in, so that the survey results may be compared to a broader filed

Figure 15 shows the allocation of the portfolios. It should be noted that the 416 participants could submit different projects, therefore the total number of projects does not equal 416 moreover, it sums up to 971. As some networks were mentioned only once or twice, they were grouped under "Other." The section “Other” was not included in the Pie chart as it would only dilute the more often mentioned projects. When analyzing the chart, it becomes evident that 130 out of 416, so roughly 30% were only invested into the Cosmos ecosystem. Two-thirds were invested in other projects thus becoming apparent that here also many projects with the

PoS are covered. Ethereum was mentioned 67 times, which in the future will also switch to the PoS mechanism as mentioned earlier in this paper.

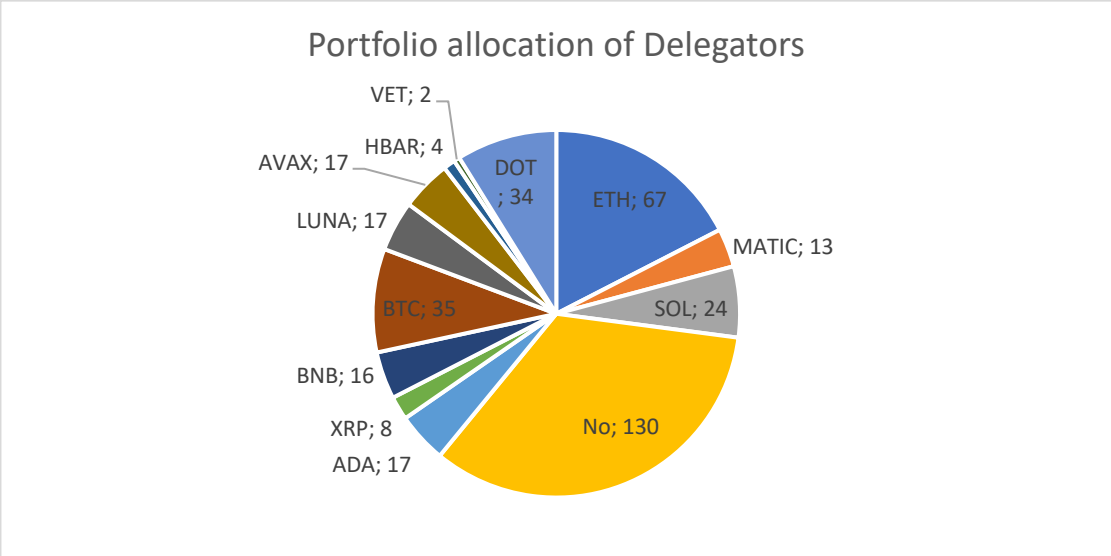


Figure 15: Portfolio allocation of participants

The portfolio size was covered in the survey, in addition to the holdings of Cosmos ecosystem users. This should be used to determine how professional the participants are, as it can be deduced that more professional users have larger portfolios, whereas individuals with lower portfolios are most likely to retail as less proficient investors/users. With 46%, the main participants of the survey had a portfolio size smaller then 5,000$. Only 3% of the participants had a portfolio size of more than 250,000 $. The rest were between 5,000 and 100,000 $, which is also illustrated with in the Figure 16.

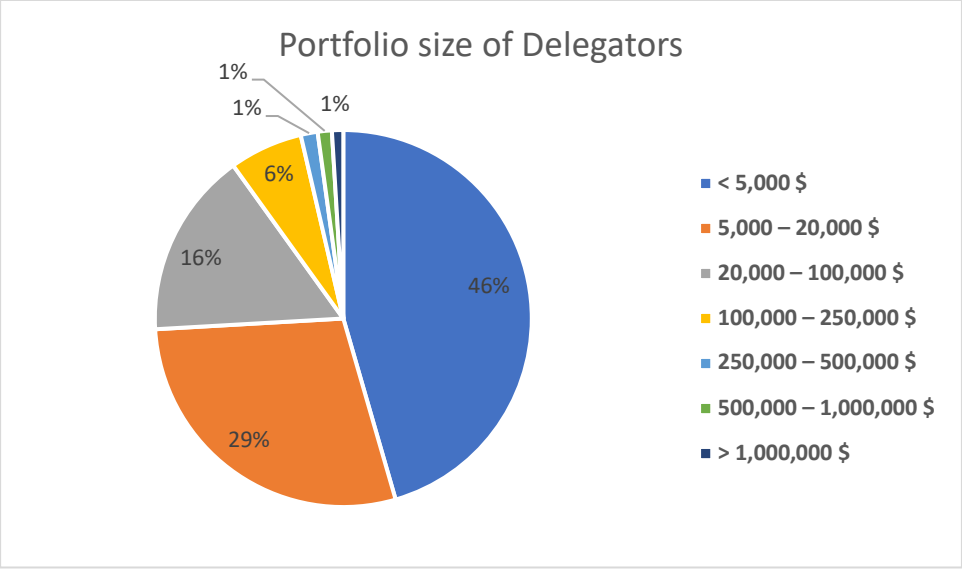


Figure 16: Portfolio size of participants

4.6 Survey Results

The two surveys are analyzed separately. The *Delegator* survey came first, followed by the *Validator* survey. This chapter just compiles the survey data and helps to highlight the results. However, the results and the interpretation will be done in Chapter 5. Discussion. The survey should help to understand the different viewing points of the two different interest groups.
As *Validators* are supposed to have at least a higher technical understanding but are also ultimately remunerated, it is considered that they have a better comprehension of the PoS network than *Delegators*. The survey results should point in the proper direction and aid in answering the question: What obstacles and opportunities exist with the PoS consensus mechanism? Is PoS a long-term answer for a secure network? This chapter is divided into two sections, the *Delegator* survey, and the Validator survey.

4.6.1 Delegator Survey

When assessing the survey findings, the structure provided in Chapter 4.5 was used. The survey comes in handy as it is separated into sections. After the Basic information, the staking behavior and strategy were surveyed. This should provide data on the level of knowledge. The association between first investing in cryptocurrencies in general and then into the Cosmos ecosystem was investigated, as well as whether it is indicative of other PoS networks. Two unique questions were utilized to determine when survey participants first became involved in the crypto world in general, and specifically the Cosmos ecosystem. Appendices 10 and 11 have unique schematics of entrance. Figure 17 depicts the exaggerated image. As a result, it is clear that entry into cryptocurrency peaked at all-time highs (ATH). In contrast, the most dynamic year for entries into Cosmos ecosystem was 2021, where $ATOM peaked at 44$.

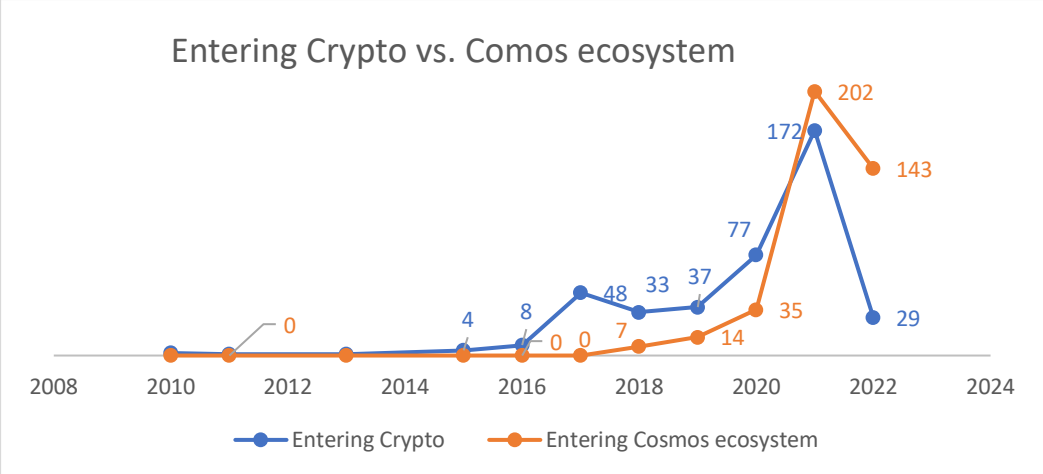


Figure 17: Entering Crypto vs. Cosmos ecosystem

As seen in the chapter before participants of the survey were also invested in other projects. But do the participants only stake and therefore trust the Cosmos ecosystem? As the token gets locked for a certain amount of time when it is staked. Figure 18 shows that the answer is "YES"[107]. 60% of participants have a staked only in the Cosmos ecosystem, while roughly 40% have a stake outside of the Cosmos ecosystem. This means that people tend trust the Cosmos ecosystem more than other networks when it comes to staking.

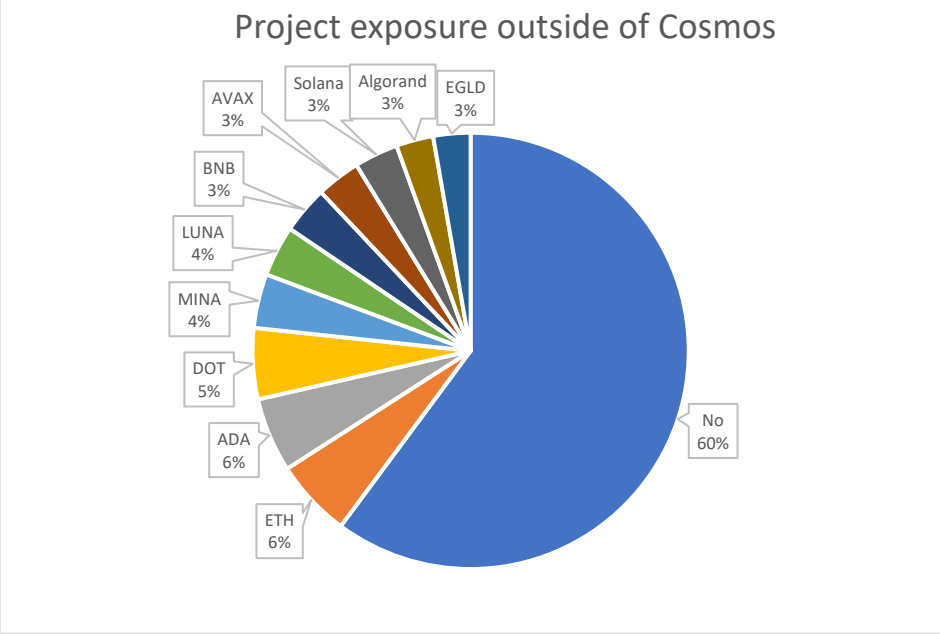


Figure 18: Staked Token outside of Cosmos

Of the 416 participants around 97% had their tokens staked[108]. This underlines the aspect that people trust the Cosmos ecosystem more than other networks. Question 2.6 inquired how many hours participants spent interacting with the consensus mechanism as part of further education/ claiming rewards or engaging with the governance. Herby, Figure 19[109] showed that more than 50% of the participants spent less than 3 hours per day and a quarter of the participants an hour or less. However, around 10% spent more than 8 hours per day which is equal to a full-time job. Therefore, it can be concluded that these users are quite sophisticated with the PoS consensus mechanism.

[107] Appendix 9
[108] Appendix 7
[109] Appendix 12

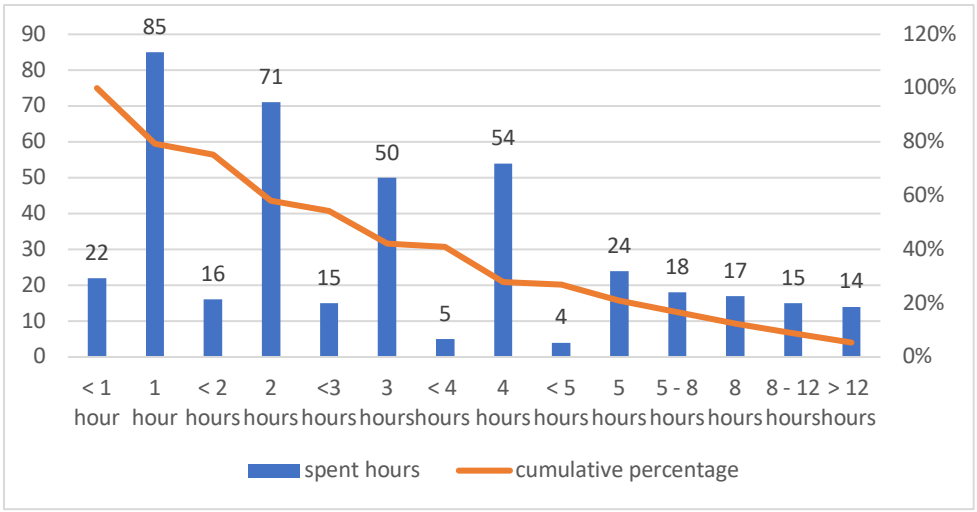


Figure 19: Daily spent hours

The reason the participants deal with the PoS network for a significant amount of time becomes clear when analyzing the results from Question 2.2. A large share of the participants roughly 28%, staked almost 100% of their portfolio. Around 53% of the participants had at least 70% of their portfolio staked[110]. This could be also an indicator that users of the PoS network either want to support the network and therefore want to contribute to the security of the network or simply want to skim the high staking APRs. However, the latter is not the case as the Question 4.4[111] states that 70% of the Cosmos users also referred to as "Cosmonauts" would stay within the Cosmos ecosystem if there would be no staking rewards anymore. As stated in the literature, especially PoS networks are dependent on game theory and good tokenomics. To conclude if an investment decision is dependent on the staking rewards, Question 4.3[112] elaborated on this field. The participants answered that in 71% of the cases the investment decision is based on the staking reward APR. The tokenomics with high inflation and high staking APR were preferred by 35% as stated. Another third of the answers would prefer low inflation and low staking APR[113].

As it is well known that PoS is tokenomics driven, which is influenced by the chain's APR, and as the survey reveals, it is also primarily a driver for investments, but a staking incentive is not required within the Cosmos ecosystem. This outcome may have been influenced by the recent "Airdrop session." Where network participants of particular chains, like as $ATOM, $JUNO, and $OSMO, received Airdrops of new chains in addition to the original token owing to staking. Some Airdrops had significant economic value. However, Question 4.2 was used to back test

[110] Appendix 8
[111] Appendix 22
[112] Appendix 21
[113] Appendix 19

if the survey participants' responses were appropriate. As a result, the recommended inflation and staking APR was requested. To compute the net profit, the staking reward must be lowered by inflation. The participants were given three options. The majority selected the correct answer: 40% inflation, staking APR 105%, which resulted in a net profit of 65% which was the biggest of the three options[114]. Therefore, it can be concluded that the participants mainly understand the bigger picture of tokenomics. However, it might be argued that the answer is biased because investors may be drawn to high staking APRS rather than price increases. This different strategy can also be seen in the stock market. So, the Question 4.3 elaborated exactly this point. The result highlighted that the investors had balanced strategies. However, high inflation and high APR were selected more often than other options[115]. For 24% of the participants, it did not matter as other factors played a bigger role such as team, quality of the project and product market fit.

Following clarification that there are various strategies and the general survey participant comprehended at least broadly the concepts of tokenomics. It became clear that higher APR is a part of game theory and attract users, but the survey tried also to understand the reason behind it. Is it pure greed or do users only try to maximize their share of the network as early participants? As PoS networks, in particular, must issue their tokens at the outset, high APRs are frequently associated with significant inflation. This was also already described in chapter 2.5 Tokenomics. Question 4.5 provided clarity to this question. The participants were asked how they used their staking APRs. Figure 20[116] shows that ¾ of the participants restake their tokens and therefore tried to gain a higher share of the network.

[114] Appendix 20
[115] Appendix 21
[116] Appendix 23

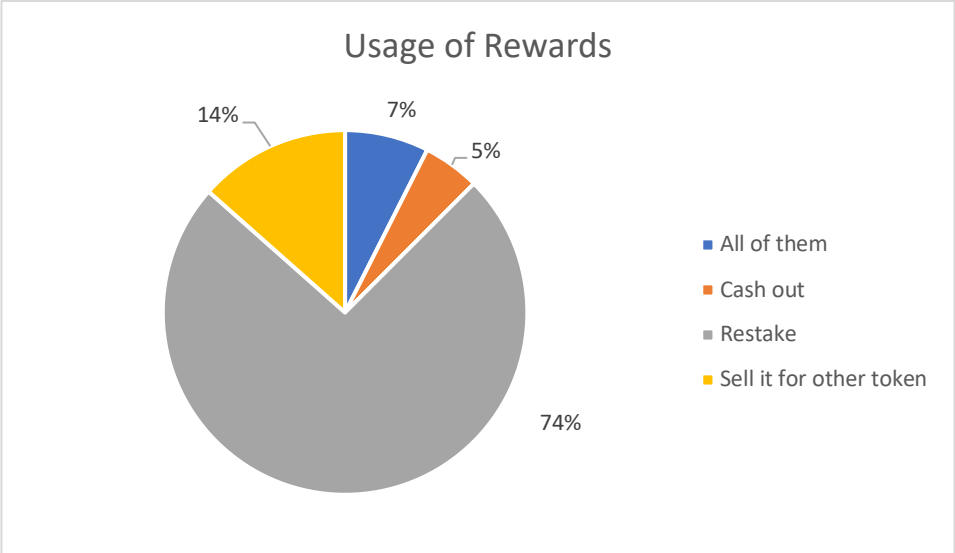


Figure 20: Usage of staking rewards

This reflects the fact, that the design of PoS works. The distribution of the tokens to early participants empowers the community and strengthens the loyalty to the associate project. Only 5% sell their rewards and 14% try to diversify their portfolio as they trade to other tokens. Most important is the fact that through restaking the newly issued tokens get locked in for a certain time, these strengthening the network security aspect.

To further investigate network security, Delegators' perspectives on PoS were developed, as well as their opinion about potential flaws and further critics. The participants stated that overall (79%)[117] PoS is sustainable in respect of network security. But when analyzed in more detail it indeed becomes evident that the participants think that there are some vulnerabilities. It was stated that it is currently the best solution (12%) by means that it is a good consensus mechanism, but it must be developed further. In comparison to the PoW consensus mechanism, the PoS mechanism performs better (9%) due to energy efficiency, etc. However, 17% of participants believe that PoS has flaws, and 5% believe that PoS is not suited because it has too many vulnerabilities[118].

The biggest criticisms can be seen in Figure 21. Several arguments were pointed out. Low frequent critic points were summarized under “Other” which roughly made up 14% of the participants. Around ¼ did not see any vulnerabilities and therefore had no criticisms on PoS. 132 participants (31%) could not answered the question and were also not included in the Figure.

[117] Appendix 25
[118] Appendix 24

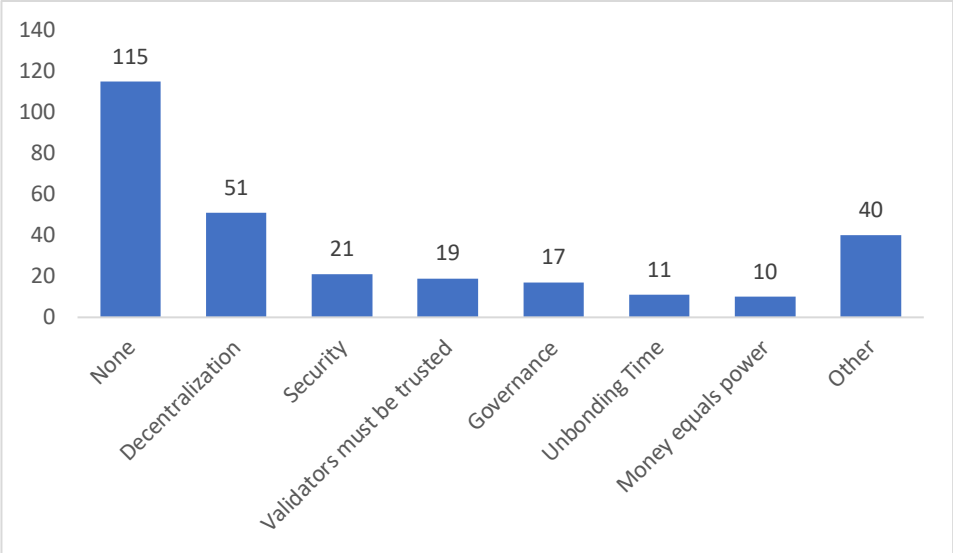


Figure 21: Critics on PoS

In comparison to other critic points Decentralization were pointed out the most which were also reflected in Question 5.6[119]. The participants had to choose between Decentralization, Network Security, and profitability. These three aspects are the most important pillars as decentralization is the main ideology of Cryptocurrencies and DLTs. Network security is significant to verify and trust the network as an unstable and manipulable network is worthless. Profitability is the fuel to hold the network together as participants only act for incentives.

Nevertheless, the general opinion about PoS is positive as 88% of survey participants have indicated that PoS will be there in the next 10 years[120]. Furthermore, the fact that certain *Validators* run nodes across multiple networks has not been viewed as a vulnerability, despite the fact that decentralization has been identified as the most important factor in a PoS network. Only ¼ submitted concerns about this[121]. When it comes to the most crucial aspects of network security, the survey network participants opinion was widely spread. Even though 38% were unable to respond, 1/5 of those who could respond stated that decentralization is the most important aspect as mentioned previously. The Figure in Appendix 28 shows an aggregated overview where again only few frequently given answers were summarized under "Other". Nonetheless, the presented results provide a summary of more than 80% of the answers. The most critical factors are a reliable network and the trust of *Validators*.

[119] Appendix 29
[120] Appendix 26
[121] Appendix 27

This leads directly to the topic of *Validators*. As in Question 5.2, the second most prevalent criticism was that *Validators* must be trusted, and in Question 5.5 trustworthy *Validators* were the third most common answer when asked which aspect of network security is the most important one. It is obvious that in a DPoS network like the Cosmos ecosystem *Validators* play a significant role. Therefore, the survey elaborated on the question of which criteria do *Delegators* select their *Validators*. Surprisingly, it was NOT a doxed and well-known team; rather, it was the contribution to the network that received the most votes (35%) followed by the commission rate (18%). Only 8% of the participants stated that a known team is important in the selection process.[122] In Question 3.3 it was asked who the favorite *Validator* is and why. As a result, none of the previously indicated reasons were used to justify the preferred *Validator*. The top three reasons, which accounted for 30% of the responses, were "active on social media," "sympathy (name or logo)," and "additional incentives" such as free NFTs or prospective Airdrops[123]. It should be noticed that 187 people (45%) did not provide a reason the chosen *Validator* is their favorite. Furthermore, around 10% of *Delegators* do not have a favorite *Validator*. When analyzing the favorite *Validators* few frequent answers are aggregated together to the section “Other”[124].

The Top 5 Validators are the following[125]:

- POSTHUMAN (84)
- STAKECITO (38)
- FRENS Validator (35)
- Cosmosstation (25)
- Smartnodes (21)

Furthermore, when asked what *Validators* should do in addition to running the node and validating transactions, which results to 100% uptime, 5% of the participants answered that this is sufficient, while over 30% could not answer the question. Whereas the most frequently submitted response was that the *Validator* should be active in the community and should communicate their governance decisions. After all, *Validators* can be seen as political parties because their votes count for the voting power assigned to them if not replaced by the *Delegator* itself.

[122] Appendix 13
[123] Appendix 16
[124] Appendix 14
[125] Appendix 15

Figure 22 shows an overview of wishes from *Delegators* that *Validators* should do in addition to the uptime. Once again, a known team is the last frequent given answer[126].

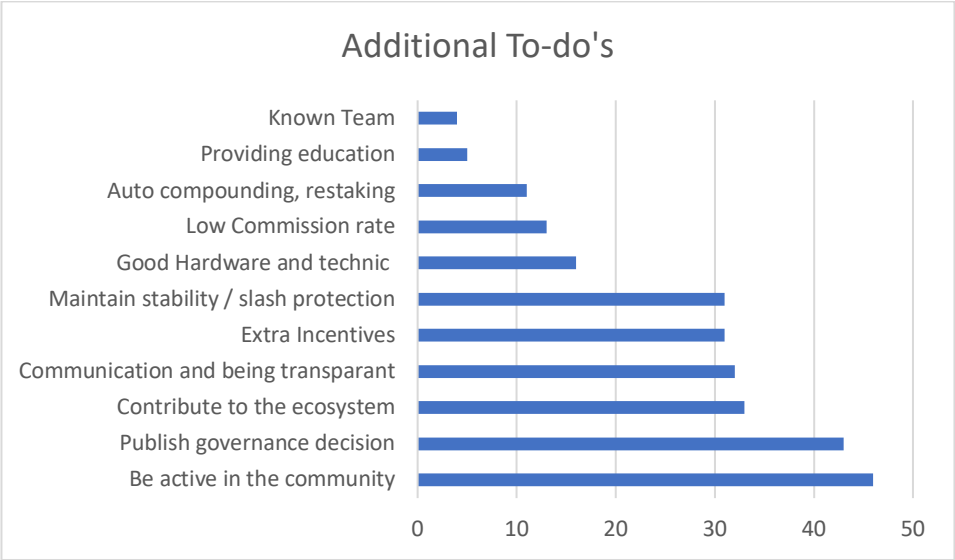


Figure 22: Additional To-do's of Validators

As previously mentioned, *Validators* have a vital role and responsibility within the PoS network, but they do not do it for free. Before analyzing the profitability of *Validators*, *Delegators* were asked to determine how much *Validators* earn and how profitable it is to host a node. A large group (38%) assessed the profit to run a node between 5 and 20%. Approximately 25% of the participants estimated the profitability to be between 0 and 5%[127].

4.6.2 Validator Survey

The survey for the *Validators* was built similarly to the survey of the *Delegators*. Firstly, general information was collected to get an overview of the current landscape of *Validators*. Following that, additional question such as commission rate and server type were asked to better elucidate on the current state. Sections 3 and 4 of the survey cover motivation and other benefits.

To gather an overview of the current state of the *Validator* landscape the founding year was asked. It becomes apparent that in the year 2021, that the number of *Validators* quadruplet and reached its peak[128]. As the survey was conducted quite early in the year 2022 and is still ongoing the number of *Validators* found within this year could still increase. Although many *Validators* are founded recently are organizations. The survey shows that the ratio between organizations

[126] Appendix 17
[127] Appendix 18
[128] Appendix 31

and private *Validators* is 50/50[129]. This kind of professionalization becomes evident when the result of the team size is examined. The average Team size of organizational *Validators* is around eight, whereas the biggest *Validator* "Citadel.one" has a team of 45 Members. Private *Validators* are also no longer geeky lone wolfs but have a team size from 1 to 5 members with an average or around two members. Overall, it appears that there is an interest in validating, which is heightened by the survey question about when the first and last node was established, as seen in Figure 23. Almost every *Validator* is still validating in new networks. When looking at the first year of new node setups, one *Validator* sticks out: the one who had already set up a node in 2016.

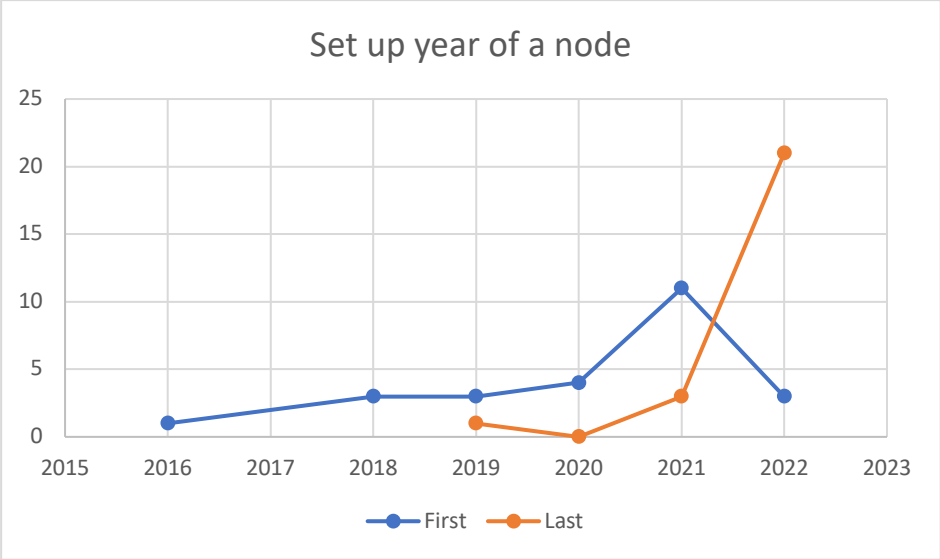


Figure 23: Set up year of a Node

The mix of *Validators* which are newcomers, and the veterans help to display the entire range of *Validators*. To check if the survey results help to also understand the general *Validator* spectrum it was asked if they also validate outside of the Cosmos ecosystem. 11 out of 25 *Validators* only run nodes within the Cosmos ecosystem and 13 also have nodes on other networks. One *Validator* could not give an answer to this question. As it was anticipated that the *Validators* have more understanding because they work in this industry, they were directly asked if they believe the Cosmos PoS ecosystem represented the general PoS environment. Whereas 80% (20 out of 25) responded that it is comparable and likewise represents the broader PoS environment. The other five *Validators* mostly agreed but emphasized that each PoS is unique as Ethereum 2.0 employs the PoS mechanism "Casper," and therefore differ even each

[129] Appendix 32

chain in the Cosmos ecosystem can also add their own parameters and regulations (e.g., smaller *Validator sets*). To round up the current environment of *Validators*, the survey polls the commission rate of each *Validator*. The result was that the average commission rate is around 5%. Some of them have lowered it to 1% and some outliers have it at 10%, however, 5% is seen as a default commission rate even when some *Validators* sometimes lower their fees to 0% to lure new *Delegators*. This was not observed in this survey. A further point of the survey was to analyze the often-criticized subject of how *Validators* run their nodes. Therefore, it was surveyed if they run their nodes on Cloud Servers or Bare Metal.

The assumed picture was confirmed, and the most *Validators* run on a cloud server and only 5 run Bare Metal whereby three of them are dedicated servers in a data center[130]. Some *Validators* also use a mixed approach. The reason becomes obvious when the cost structure of the services was analyzed. The participants stated that the costs to set up a node are significantly higher than a cloud server whereas the maintenance is lower. It should be emphasized that these are average values, and the costs of servers vary greatly from chain to chain due to the wide range of requirements. Table 10 shows the stated figures, which include the costs of putting up a node as well as the costs of maintain a node.

COST OF NODE	Set Up	Maintance
BareMetal	1.425 €	269 €
Cloud Server	278 €	339 €
Mix approach	175 €	344 €
Ø total	552 €	312 €

Table 10: Cost of a Node

To backtest these figures, different providers for servers were browsed. Since the cost of servers can vary substantially depending on the requirements of the network, the Binance Smart Chain (BSC) was selected to determine the requirements and therefore a suitable server. The BnB chain has some of the highest requirements among the networks in the Cosmos ecosystem. The requirements are listed in Table 11. Table 12 shows where the costs for could servers and dedicated server (BareMetal) are.

[130] Appendix 33

Requirements	BNB Network
RAM	48 GB
CPU	12 Core
Storage	2 TB
Broadband	10mb/s

Table 11: Requirements BNB Validator node

Provider	Dedicated	Cloud Server
Hetzner	~ 100 €	N/A
Webtropia	~ 200 €	N/A
AWS	~ 500 €	~ 450 €
OVH	~ 165 €	N/A
VULTR	~ 675 €	~ 930 €

Table 12: Comparison of different Provider for the BNB Network

These costs are the prices to rent the servers per month. The cost for human work was not encountered. The servers were selected so that the requirements for the BNB network could be fulfilled. Compared to the results of the survey it can be seen that the results match the selection of providers. As the requirements vary widely the question could come up why all *Validators* do not run or at least start with the chain of lowest requirements. Therefore the *Validators* was asked how they select the projects and networks which they validate.

The results showed that *Validators* mainly check if the project and the team are solid and have upside potential. As a result, belief in the project is a major motivator in the selecting process. Also, whether it is relevant to the broader marketing strategy, as *Validators* symbolize trust. As a result, the project's community must be large/strong enough, and/or the *Validator* community must support running on this chaim. Personal preferences or contacts can sometimes be used to validate a chain.In some circumstances, a Delegation program and related to that, if it is possible to get into the active set from the start as a genesis *Validator* or a foundation delegation, is crucial. It is most important to certain *Validators* that it be profitable. The tokennomics are crucial not simply because the staking incentive determines how much profit the *Validator* makes. A *Validator* mentioned that they exclusively validate with networks with which they have personal contacts this however was an outliner.

After seeing the results of the selection process, it will be evident what is necessary for validators when running a node. Multiple answers were given. Figure 24 illustrates which factors were the most important ones.

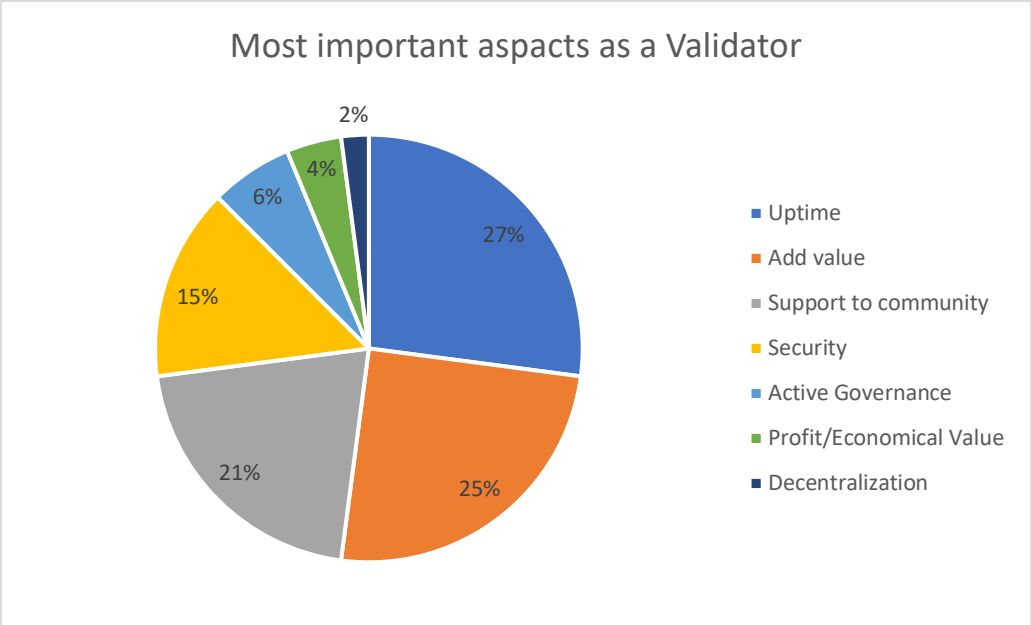


Figure 24: Importance when running a node

It can be seen that Uptime makes up a quarter of the results followed by adding value to the project. By adding value, it is meant that the network gets secured, and the *Validator* not only helps to decentralize the chain but also builds tools to monitor key numbers. Another significant factor is supporting the community by providing educational content, being active on social media, and being the link between the developers and the *Delegators*. The point security which was made up 15% of the answers, *Validators* argue they are also liable against any attacks. The Only 4% of the time was the economic value acknowledged.

So, would 96% of the *Validators* also run without profit?

The answer that it depends. Despite the fact that 60% of the participants claimed that they would continue to run the operations if it became unprofitable[131], but only under certain conditions. Even while many *Validators* support decentralization, they would want to run at least break even with the node operations and would concentrate it on a few significant chains, or they would run the unprofitable node only if they received any other benefit from it. As a result, they would contribute to the chain's security and limit the operation to networks in which they have faith in. However, receiving appropriately waiver revenue is one side, while pouring their own money into the projects is the other. As a result, the *Validators* are asked if they also invest in the projects that they validate, and the answer is unequivocal: practically everyone stated that they do so[132].

[131] Appendix 34
[132] Appendix 35

On the other side which additional benefits do *Validators* bring to stakers and the network besides confirming transactions and securing the chain?

Validators can offer different benefits to the *Delegators* and mostly mentioned was developing new features like Dashboards for the *Delegators*. Figure 25 provides an overview of the responses given by the *Validators*, with the responses grouped together to provide a comprehensive overview immediately. Enabling Auto-compounding so that the *Delegator* may maximize their profit from delegating is also considered as a service that a *Validator* can give. It becomes clear that the *Validator* can provide two kinds of services: one is the technical side where they secure the chain, develop new tools, and build relayers between different chains the other kind of service is to directly benefit the *Delegator* with additional benefits e.g., NFTs eligibility for new Airdrops or educating the Community. It becomes clear that indeed *Validators* can bring additional value to a project besides only validating the chain.

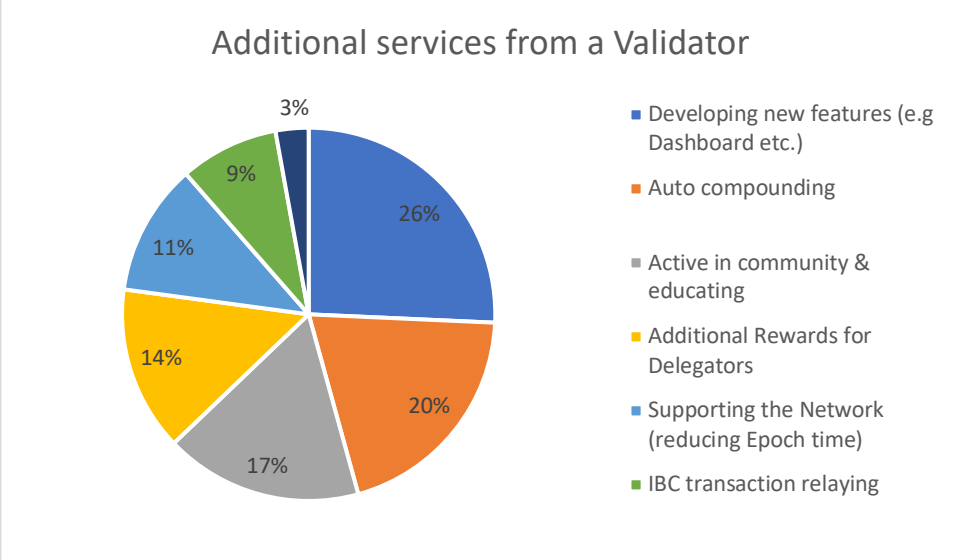


Figure 25: Additional Benefits form Validators to Delegators

These additional benefits, which the *Validators* can provide could attract more *Delegators* but to be certain about this the *Validators* were also asked in the survey how they would try to attract more *Delegators*. They stated that marketing would bring awareness to the *Validator*, thus building a community around the *Validator* and educating them is of great significance. Clear communication and transparency are crucial since the word of mouth attracts even more *Delegators*. This can be enhanced through contributing to the network with building tools.
According to the responses, doing Airdrops or other types of benefits like NFTs to *Delegators* are other approaches to attract more delegations. Also, tools like Auto-compounding for increasing *Delegator* profits or for monitoring purposes are a good approach to gain more delegations.

To further elaborate about, whether there is unreasonable competition among *Validators*, the survey sought to know if *Validators* also *Delegate* to other *Validators*, and if so, to how many different *Validators*. As a result of the survey, 16 out of 24 *Validators* (approximately 67%) delegate on average to three other *Validators* to assist them. Four *Validators* did not submit a number to how many they delegate.

After clarifying the behavior of *Validators*, the survey wanted to know further what the general opinion is about PoS. 80% were the opinion that PoS is a suitable consensus mechanism. The core statement was that everything has vulnerabilities but overall, it is a good mechanism. It is critical that the networks sufficiently distributed and have several nodes, to ensure decentralization. Another question, asked about the biggest critics of PoS. The main issue was mentioned precisely the point of decentralization. Enough *Validators* are necessary, and it should not be overly concentrated within the *Validator set*, as observed in some networks. The Top 5 *Validators* already control a sizable portion of the voting power in certain networks. This interacts with delegations from the foundations because they fundamentally control who gets into the active set, at least on larger chains like $ATOM.

Validators are also criticized for relying too heavily on centralized services (Server provider), which may jeopardize the network's integrity. Another criticism is that voting on proposals is critical, and *Validators* with too much voting power might affect the entire network or, on the other hand, block the entire voting mechanism because the quorum would not be met without their voting in a less engaged community. All in all, the *Validators* still think PoS is a great consensus mechanism and will remain in the next 10 years. The reason for this is that the PoS consensus is simply better than the yet available mechanisms. However, the *Validators* also agree that PoS will improve and change over time so that other variants of PoS will appear within the next 10 years. The majority of the *Validators* also do not see any vulnerabilities if a *Validator* validate across several chains[133].

Ultimately, it all comes down to network security, where the *Validators* believe that sufficient expertise and monitoring of processes are the most important aspects to be secure against attacks. To contribute to a secure chain the network should be Decentralization so it can be ensured against any security risks or at least are minimalized. Also, instead of relying on cloud service providers, having bare metal servers, distributed around the world could boost network security.

[133] Appendix 36

5. Conclusion

The chapter conclusion critically reflects the survey results and states the study's outcome. After the introductions and evince the relevance of the study topic, the literature and the fundamental knowledge were provided. Where different aspects of Network Security were pointed out such as certain vulnerabilities be it different kinds of attack vectors or poorly designed Tokenomics. Afterward the research design showcased chosen methodology and data aggregation/preparation. Followed by the Case Study of the "Cosmos Ecosystem", herby the survey and the results were presented. This chapter will summarize the study and present the study's findings. It will also address the important research questions/hypotheses.

5.1 Discussion

The discussion is divided into three subchapters. Firstly, the results of the survey will be critically reflected. Afterward, the critics of the study will be elaborated on. Lastly, the key results and the hypotheses will be analyzed.

5.1.1. Reflection of the Survey Results

This section will compare the answerers of *Validators* and *Delegators* in a PoS network. Both the view of the *Delegators* and the *Validators*. The first comparison which should be emphasized is the question for *Delegators* 3.1 "Selection criteria of Validators" and the question for *Validators* "How to attract Delegators"

Delegators	%	Validators	%
Contribution to the Network	35%	Marketing	25%
Commission Rate	18%	Build Community though social media	22%
Participation in Governance	10%	Contribution to the Network	19%
Sympathy	10%	Education	17%
Voting Power	9%	Transparency	6%
Doxed Team	8%	Build Tools	6%
All of the above	5%	Low Commission Rate	3%
Slash Protection	4%	Addition Benefits (NFTs and Airdrops)	3%
Uptime	1%		
Airdrops	1%		

Table 13: Comparison of Validator selection and Delegator attraction

Table 13 illustrates the different needs and offers, where it becomes obvious that *Validators* mainly focus on marketing and attracting new *Delegators*. *Delegators,* on the other hand, are concerned with a variety of factors, including the creation of additional value for the network at the lowest possible commission rate. This resembles the chicken and egg problem. When profit is ignored in favor of break-even, *Validators* can only lower the fee if they have enough delegates, because contribution in the form of Tools or upgrading code costs time and resources, both of which are costly. The focus of *Validators*, therefore, is to raise a loyal community and build a personal brand so, that they can use the scales effects and bring even better value to the community assuming that pure profit is not the main focus.

When the results of Question 3.3. Favorite *Validator,* which was asked to the *Delegators,* are analyzed, it becomes clear, which *Validator* are preferred and why. Social media activity, which is ultimately a type of marketing, is one of the key reasons why the specific *Validator* is their favorite since it increases sympathy. The literature calls this the "Mere-Exposure-Effect". In 1968, Robert Zajonc proposed the hypothesis that the more frequently an object or logo is exposed to an individual who senses the stimulus, the greater the sympathy for it[134]. **It can be stated that social media appearance is crucial to enhance the delegations.** Of the Top 10 favorite *Validators*, six are covered in the *Validator* survey. This is shown in Table 14. This confirms that the survey is matching with the *Validators* and covers significant players within the *Validator* industry of the Cosmos ecosystem.

Rank	Validator	Covered	Rank	Validator	Covered
1	Posthuman	Yes	6	SG-1	No
2	Stakecito	Yes	7	Stake.Fish	No
3	Frens	Yes	8	Citadel.One	Yes
4	Cosmosstation	No	9	Golden Ratio Staking	Yes
5	SmartNodes	No	10	Omniflix	Yes

Table 14: Top10 Favorite Validators

When studying Question 4.2, which was given to the *Delegators* to evaluate their grasp of basic tokenomics, particularly the independency of staking rewards and inflation. Although the majority of *Delegators* could choose the correct answer, 31% did not, raising the possibility that some *Delegators* are unfamiliar with staking procedures. This could also be attributed to the market's youth and the early stages of stake acceptance.

[134] Zajonc, 1968

Table 15 shows that *Delegators* likely to stay longer than *Validators* when analyzing the association between profitability and continuous staking versus validating. This could be attributed to the additional cost a *Validator* have to cover whereas the *Delegator* may even get appreciation of their investment as the token price would increase with constant demand but no inflation.

Ongoing operations	**Delegator**	**Validator**
Yes	70%	60%
No	30%	40%

Table 15: Comparison of profitability and ongoing staking/validating

As this study aims to research Network security and the implications of PoS the critics from the *Delegators* and *Validators* were aggregated. Different points are noticeable.

Validators underline the importance of faith in *Validators*, and decentralization is important. In the sense that the *Validator* set should be large enough, the delegation should be balanced, and the Top 5 *Validators* should not have too much impact. This is all legitimate criticism; the exception is the statement of unbonding time by 4% of the respondents. The unbonding is a security mechanism to protect the network from fire sales and should ensure that malicious actors can get rid of their financial stake before they could get penalized. Security is important for the *Delegators* and they see this as a critical point, it does not make sense to see the unbonding period as a weak point. Also, slashing was named as a critic point in a PoS network whereby this also ensures the security aspect of the network. This highlights that not all *Delegators* grasped the mechanisms that appear within the PoS network and greed was predominant. As many as 3% of respondents condemned the inflation and incentivization of the notion that not every *Delegator* understood tokenomics and the PoS network. As previously stated in Chapter 2.5 Tokenomics, one of the most difficult aspects in avoiding centralization is the distribution of PoS coins. As a result, it can be seen that the APRs are notably high in the early years of the token.

That kind of greed and the will to maximize profit is normal in early markets. This was already seen in the development of Web 1.0 and Web 2.0. Early market participants enter big risks but therefore the returns are also big. A great critic point was the mentioning of immature legislation. But this is already an ongoing critical point not only in the PoS environment but also in the whole crypto space.

When the answers from the *Delegators* are compared with the answerers from the *Validators,* it can be seen that they mainly converge. Obviously, their viewpoint is more focused to get into the active set and which also correlates with the decentralization aspect. They also have more insights in regard to foundation delegations. Foundations, therefore, can contribute/incentivize *Validators* who provide a value of any kind to the network, be it through educational content, bringing awareness to the project, helping to secure the chain, or building tools. Two responses of *Validators* are remarkable; one is the long unbonding time which was explained why this critique does not make sense, and secondly the point that capital is required to get into the active set. This is only half true. A large quantity of money is only required if a *Validator* want to participate directly with their own capital. But as mentioned with contribution *Validators* can get foundation delegations and become a part of the active set. The reason why there is a minimum required set for *Validators* is that it ensures enough extrinsic motivation. If everyone could join the set it would be exposed to network security risks as malicious actors could join.

Comparing *Delegators'* and *Validators'* responses to the question of whether they believe PoS continue to exist in the next ten years. It is evident that *Validators,* with 96% are more confident that it will remain then *Delegators,* with "only" 64% of the responses indicating that it will remain. Despite the fact that the PoS consensus process will be improved. Nonetheless, it demonstrates that both parties feel PoS is viable in the future and will continue to exist. This can also be observed in the growing interest in *Validators*, who are constantly establishing new nodes.

When coming to the vulnerabilities of the PoS networks both *Delegators* and *Validators* were of same opinion that decentralization is the most important aspect. This means that it should be ensured that there are enough *Validators* and within the *Validator set* the delegations should be balanced. The point of governance has been mentioned by 6% of *Delegators* and 12% of *Validators* but not emphasized enough. Since Governance can decide about everything around and within the network, as seen recently with the Proposal 16 in the $JUNO community where funds of the "JUNO WHALE" was seized. As this is of tremendous relevance and has an impact on network security, several aspects will be discussed in greater detail.

The first issue occurs when a *Validator* runs nodes across different networks. *Validators* and *Delegators* stated that this should not be an issue. But indeed, it could affect the network security as the *Validator* gets into a conflict of interest. This would happen when a proposal in one network (A) arises that would benefit the network (A) but could have an adverse effect on the network (B). The *Validators* run into political issues. Moreover, they could get pressure from the foundation of network (A) when the *Validator* gets foundation delegations. However, if the *Validator* now also gets foundation delegations from both sides, both foundations have threatened to withhold those delegations if he votes against the interests of a certain network. This leads to the following issue: if governance becomes more political, social engineering may become a problem if it is exploited. Because it might be used to either infiltrate any vulnerabilities in an upcoming governance plan or simply divide the community. This would weaken the network and it would be more vulnerable to certain attacks. Another issue is that tangent governance and decentralization simultaneously; Since larger *Validators* especially, centralized exchanges do not vote in governance proposals the risk of not reaching the quorum ($ATOM 40%) is threatening the network. If these non-voting nodes continue to grow and stop voting on governance proposals, a point could be reached where no proposal could pass anymore. As a result, one feasible remedy would be for *Validators* who do not vote in multiple proposals in a row to have their voting rights withdrawn and redistributed to active *Validators*.

A possible solution could be also to lower the quorum. This again would probably lead to less participation as fewer votes are required. A decentralized network lives from an active and engaged community and especially *Validators* build an important backbone which should have an economic and social interest to participate. Another possible solution would be to divide economic power and voting power in governance proposals.

5.1.2 Critics of the Study

1. Was the methodology used the right approach?

This study has taken the approach to research the current state of technology and speaking with experts in the industry within the Cosmos ecosystem. Additionally, two surveys were conducted to get insights from the *Delegator's* and *Validator's* perspectives. Interviews with other industry experts were not conducted since enough data could be collected. The used methodology, therefore, was sufficient.

2. Can the results be generalized?

The generalization of data is limited through it focused on the Cosmos ecosystem. Also, with more *Validators* within the survey, it would give a more general overview but still, the data shows an overview of the perspective of the *Validators* within the Cosmos ecosystem and also important players in the industry were captured. Therefore, the data can be generalized for the particular ecosystem. In addition, *Validators* who validate also outside of the ecosystem participated in the survey.

3. Reliability of the Data?

In general, the data can be trusted however subjectivity and limited know-how from the *Delegators* affected the data. The newness and rapidly changing environment of the sector also affected the data collection process.

5.1.3 Key Results

The key results of the study will answer the questions, which were asked at the beginning of the study. Herby following questions are to be answered:

- How does the current PoS environment look like, and what are the vulnerabilities in terms of network security?

The current PoS environment is a fast-growing and vibrant industry that is on the way to get more professional. Current players are getting bigger and validate more chains, almost no *Validator* stops at only one Network. In terms of network security and weaknesses, the results state that decentralization respectively centralization, is the biggest vulnerability. Governance is also significant aspect, at least in a DPoS network.

- Does PoS provide an additional value for node operators and the projects compared to PoW nodes besides validation transactions?

Yes! For the node operators, the benefit compared to PoW is that they have less costs (No miner, who has to be renewed every few years) and additionally there are in constant exchange with the community. *Validators* can build their own brand and profit supplementary from that. Projects and the network get additional value from *Validator* since they have to provide benefits to receive delegations. Tools, outreach for projects, and additional improvements for the networks are extra benefits compared to the PoW. Also, the suitability aspect is a big surplus as less energy is consumed.

- Which aspects must be considered in the PoS regarding network stability?

Prior to the voting, clear communication with *Validators* and governance plans without centralized instances must be ensured.

- Is PoS the future of DLT or could there be certain improvements to be done?

PoS is the future of DLT and more PoS networks will launch. Possible improvements could be done on the voting power and governance aspect. Furthermore, a mechanism has to be found to ensure decentralization without having a negative effect on block time as more *Validators* equals longer block time.

5.2 Conclusion

The crypto industry is a fast-changing but also a growing market. Since Bitcoin launched in January of 2009, the whole crypto industry developed on the peaked to a roughly $3 billion market cap industry, whereas many players positioned well and participated in this sector. Many well-established banks and financial intuitions such as JP Morgan, UBS, Barclays, BNY Mellon, Goldman Sachs and many more saw this huge opportunity and hopped in as well[135]. Also, various financial instruments developed and even got approved such as the Bitcoin ETF, which enables more investors the opportunity to participate within the crypto market without any crypto-specific knowledge. The adoption and the growth were also be seen in traditional monitoring and news outlets like Bloomberg and Yahoo finance. For instance, the Bloomberg Crypto outlook is a monthly report where general news, technical analysis, market data, and insights are given. The adoption and the user count also grow exponentially. A report from the worldwide known crypto exchange crypto.com which partners with the UFC, Formula 1, and recently also the FIFA[136] stated that there are 295 million crypto users as of December 2021[137]. Expected is that the number of global crypto owners will reach one billion by the end of 2022.

When observing the development of the consensus mechanism, it becomes evident that this also evolves consequently. As demonstrated by this study, incremental improvements were made, not least because PoW consumes a lot of electricity and has a slow transaction speed. Ethereum encountered the same issue. In 2017, a single application, “CryptoKitties”, caused network

[135] Sanyal, 2022
[136] Crypto.com, 2022
[137] Crypto.com, 2022

congestion because unprocessed transactions could not be processed quickly enough. However, even the PoS consensus process, which is not a novel invention, has evolved steadily and currently reigns supreme. The Cosmos ecosystem therefore is positioned well with the Tendermint BFT, which has instant block finality and even provided additional features, like interoperability.

What can be expected in the future?

The evolution of the crypto market and the consensus mechanism is not done yet. The scalability and the interoperability between blockchains become increasingly important to reach more effectiveness. After resolving this with the Tendermint BFT and the Cosmos ecosystem, the only aspect left to address is regulation, which is expected to be settled in the upcoming years. Further research can be made when keeping an eye on this industry and continuing this research which should serve as a basis. To enhance this study further case studies of other PoS networks should be conducted. Also, the future environment with liquid staking should be explored.

To conclude it can be said that:

PoS is the future of Distributed Ledger Technology and *Validators* are going to play a key role to ensure the network security. This industry, particularly *Validators*, is becoming more industrialized, with larger team sizes and a more professional appearance. As the number of PoS networks and users of cryptocurrencies is growing it can be expected that the niche is growing at least with the same speed. The number of users is predicted to triple, while the market capitalization has increased by a factor of 4.6x in the last three years. It can be concluded that the PoS niche will develop at a factor of at least 3-5x until 2025.

Bibliography

Adapools.org. (2022, April 26). *adapools.org*. Retrieved from https://adapools.org/

Aggarwal, S., & Kumar, N. (2021). Chapter Twenty - Attacks on blockchain. In S. Aggarwal, N. Kumar, & P. Raj, *Advances in Computers* (Vol. 121). USA: Academic Press.

Algorand Foundation. (2022, April 11). *algorand.foundation*. Retrieved from https://algorand.foundation/algorand-protocol/about-algorand-protocol/pure-proof-of-stake

Anceaume, E., Pozzo, A. D., Rieutord, T., & Piergiovanni, S. T. (2020). *On Finality in Blockchains.* Renes, France: IRISA.

Apostolaki, M., Zohar, A., & Vanbever, L. (2017). Hijacking Bitcoin: Routing Attacks on Cryptocurrencies . *2017 IEEE Symposium on Security and Privacy (SP)* (pp. 375 - 392). San Jose, CA USA: IEEE.

Avascan. (2022, April 26). *avascan.info*. Retrieved from https://avascan.info/stats/staking

Beckett, A. (2021, June 25). *medium.com*. Retrieved from https://alexbeckett.medium.com/an-introduction-to-token-economics-tokenomics-c6eb9211778f

Bentov, I., Pass, R., & Shi, E. (2016). *https://allquantor.at/.* Retrieved from https://allquantor.at/: https://allquantor.at/blockchainbib/pdf/bentov2016snow.pdf

Bitcoin Suisse. (2020, May 21). *bitcoinsuisse.com*. Retrieved from https://www.bitcoinsuisse.com/de/research/specials/game-at-stake-game-theory-analyze-staking-2

blockchain.com. (2022, April 19). *blockchain.com*. Retrieved from https://www.blockchain.com/charts/total-bitcoins

BTC-ECHO GmbH. (2022, May 20). *btc-echo.de*. Retrieved from https://www.btc-echo.de/academy/bibliothek/wer-ist-satoshi-nakamoto/

Buchman, E. (2016, June). Tendermint: Byzantine Fault Tolerance in the Age of Blockchains. *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains*. Guelph, Ontario, Canada.

Business Wire. (2022, February 23). *finance.yahoo.com*. Retrieved from https://de.finance.yahoo.com/nachrichten/tendermint-gr%C3%BCnder-cosmos-%C3%B6kosystems-ignite-152300066.html

Bybit Learn. (2021, May 13). *learn.bybit.com*. Retrieved from https://learn.bybit.com/altcoins/what-is-dash-crypto/

Cardano Foundation. (2022, April 11). *cardano.org*. Retrieved from https://roadmap.cardano.org/en/byron/

Castro, M., & Liskov, B. (1999). *Practical Byzantine Fault Tolerance* . Massachuetts, USA: MIT Laboratory for Computer Science.

Choy, E. (2020, June 15). *messari.io*. Retrieved from https://messari.io/article/long-range-attack

Chung, L. (2022, May 20). *delighted.com*. Retrieved from https://delighted.com/blog/average-survey-response-rate

Ciaian, P., Kancs, d., & Rajcaniova, M. (2021, February 16). *arxiv.org.* Retrieved from arxiv.org: https://arxiv.org/pdf/2102.08107.pdf

CoinCodex . (2022, April 25). *coincodex.com*. Retrieved from https://coincodex.com/ico/cosmos/

Coingecko. (2022, February 08). *Coingecko*. Retrieved from Coingecko.com: https://www.coingecko.com/en/coins/ethereum

Coingecko. (2022, April 09). *coingecko.com*. Retrieved from coingecko.com: https://www.coingecko.com/en/coins/peercoin

CoinGecko. (2022, April 26). *coingecko.com*. Retrieved from https://www.coingecko.com/en/coins/cosmos-hub
Coinspeaker. (2017, November 01). *coinspeaker.com*. Retrieved from https://web.archive.org/web/20180712085709/https://www.coinspeaker.com/2017/11/01/weekly-cryptocurrency-ico-market-analysis-october-23-29-2017/
Cong, L., Li, Y., & Wang, N. (2019, August 26). *clevelandfed.org.* Retrieved from clevelandfed.org: https://www.clevelandfed.org/~/media/content/events/2019/fsc/yli%20token2.pdf?la=en
Cosmostation. (2022, April 26). *mintscan.io*. Retrieved from mintscan.io/cosmos
Crunchbase. (2022, April 27). *crunchbase.com*. Retrieved from https://www.crunchbase.com/organization/tendermint-2
Crypto.com. (2022). *Crypto Market Sizinh.* Crypto.com.
Crypto.com. (2022, May 29). *Crypto.com*. Retrieved from https://crypto.com/eea/partners
Cryptopedia Staff. (2022, March 17). *gemini.com*. Retrieved from https://www.gemini.com/cryptopedia/the-dao-hack-makerdao
Cuen, L. (2021, September 13). *CoinDesk.com*. Retrieved from https://www.coindesk.com/markets/2019/11/11/how-to-turn-a-17-million-ico-into-104-million-the-cosmos-story/
Daniels, A. (2018, October 18). *medium.com*. Retrieved from https://medium.com/ltonetwork/the-rise-of-private-permissionless-blockchains-part-1-4c39bea2e2be
Dellatto, M. (2021, November 11). *forbes.com*. Retrieved from https://www.forbes.com/sites/marisadellatto/2021/11/11/cryptos-super-user-young-men-43-of-us-males-aged-18-to-29-have-bought-the-currency/?sh=7b13ba72349a
devtooligan. (2022, April 11). *ethereum.org*. Retrieved from https://ethereum.org/en/developers/docs/evm/
Eliason, N. (2021, December 17). *every.to*. Retrieved from https://every.to/almanack/tokenomics-101
ethereum foundation . (2022, April 19). *ethereum.org*. Retrieved from https://launchpad.ethereum.org/en/faq
Ethereum Foundation. (2022, February 10). *ethereum.org*. Retrieved from ethereum.org: https://ethereum.org/en/staking/
Fish.vote. (2022, April 18). *fish.vote*. Retrieved from fish.vote
Fridman, E., & Ugrinovskii, V. (2014). A Round-Robin type protocol for distributed estimation with H∞ consensus. In E. Fridman, & V. Ugrinovskii, *Systems & Control Letters* (Vol. 69, pp. 103 - 110).
George, J. T. (2022). *Introducing Blockchain Application.* Rome,Italy: Apress.
Gupta , A. (2021, January 15). *hackernoon.com*. Retrieved from hackernoon.com: https://hackernoon.com/what-is-liquid-staking-and-how-can-it-improve-the-defi-ecosystem-232331i3
Hayes, A. (2022, January 20). *Investopedia*. Retrieved from Investopedia.com: https://www.investopedia.com/terms/b/blockchain.asp
Hayes, A. (2022, February 02). *investopedia.com*. Retrieved from https://www.investopedia.com/terms/g/gametheory.asp#:~:text=Game%20theory%20is%20largely%20attributed,applied%20science%20to%20this%20day.
Hertig, A. (2021, February 19). *coindesk.com*. Retrieved from https://www.coindesk.com/tech/2021/02/19/what-is-an-enterprise-blockchain/
Hooda, P. (2019, January 10). *geeksforgeeks.org*. Retrieved from https://www.geeksforgeeks.org/sybil-attack/

Hooda, P. (2019, December 12). *geeksforgeeks.org*. Retrieved from https://www.geeksforgeeks.org/practical-byzantine-fault-tolerancepbft/

IBM. (2022, April 06). *ibm.com*. Retrieved from https://www.ibm.com/topics/blockchain-security#:~:text=Blockchain%20security%20is%20a%20comprehensive,risks%20against%20attacks%20and%20fraud

Interchain Foundation. (2019, February 09). *blog.cosmos.network*. Retrieved from https://blog.cosmos.network/cosmos-hub-to-launch-mainnet-a453d2247a34

Interchain Foundation. (2022, February 22). *cosmos.network*. Retrieved from cosmos.network: https://cosmos.network/learn/staking/

Interchain Foundation. (2022, April 25). *interchain.io*. Retrieved from https://interchain.io/static/Asset-and-Grant-Overview-Interchain-Q3-2020.pdf

Kelly, L. J. (2022, March 21). *decrypt.co*. Retrieved from https://decrypt.co/95574/nearly-6-billion-eth-burned-ethereum-2-0-edges-closer

Kennedy, T. (2020, August 1). *medium*. Retrieved from medium.com: https://medium.datadriveninvestor.com/itcoin-unhackable-it-happened-twice-not-blowing-smoke-9e16bcddd5ab

Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2019, July 20). *iacr.org*. Retrieved from https://eprint.iacr.org/2016/889.pdf

King, S., & Nadal, S. (2012, August 19). *PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake.* Georgetown University. Washington, USA: Georgetown University. Retrieved from https://people.cs.georgetown.edu/~clay/classes/fall2017/835/papers/peercoin-paper.pdf

Kwon, J. (2014). *Tendermint: Consensus without Mining.* New York, USA: Cornell University .

Kwon, J., & Buchman, E. (2022, April 11). *cosmos.network*. Retrieved from https://v1.cosmos.network/resources/whitepaper

Lamport, L., Shostak, R., & Pease, M. (1982, July). *lamprot.azurewebsites.net.* Retrieved from https://lamport.azurewebsites.net/pubs/byz.pdf

Li, W., Andreina, S., Bohli, J.-M., & Karame, G. (2017). Securing Proof-of-Stake Blockchain Protocols. In J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, & J. Herrera-Joancomartí, *Data Privacy Management, Cryptocurrencies and Blockchain Technology* (pp. 297 - 315). Oslo, Norway: Springer Verlag.

Locke, T. (2021, November 05). *cnbc.com*. Retrieved from https://www.cnbc.com/2021/11/05/what-to-know-before-investing-in-ethereum-competitor-solana-sol.html

Longchamp, Y. (2021, October 21). *cvj.ch*. Retrieved from https://cvj.ch/wissen/basiswissen/die-bedeutung-von-tokenomics/

Mapofzones. (2022, April 29). *mapofzones.com*. Retrieved from https://mapofzones.com/?testnet=false&period=720&tableOrderBy=ibcVolume&tableOrderSort=desc

Mehammed, S., & Lemma, D. (2021, December 01). *ijisrt.com.* Retrieved from https://ijisrt.com/assets/upload/files/IJISRT21DEC657_(1).pdf

Meynkhard, A. (2019, November 15). Fair market value of bitcoin: halving effect. *Investment Management and Financial Innovations, 16*(4), pp. 72 - 85.

Nabilou, H. (2022). *Probabilistic Settlement Finality in Proof-of-Work Blockchains: Legal Considerations.* Amsterdam, Netherlands: Amsterdam Law School.

Nash, J. F. (1950). *Non-cooperative Games.* Princeton, USA: Princeton University.

Nasiri, S., Sadoughi, F., Tadayon, M. H., & Dehnad, A. (2019, December 12). Security Requirements of Internet of Things-Based Healthcare System: a Survey Study. *Acta Informatica Medica*, p. 6.

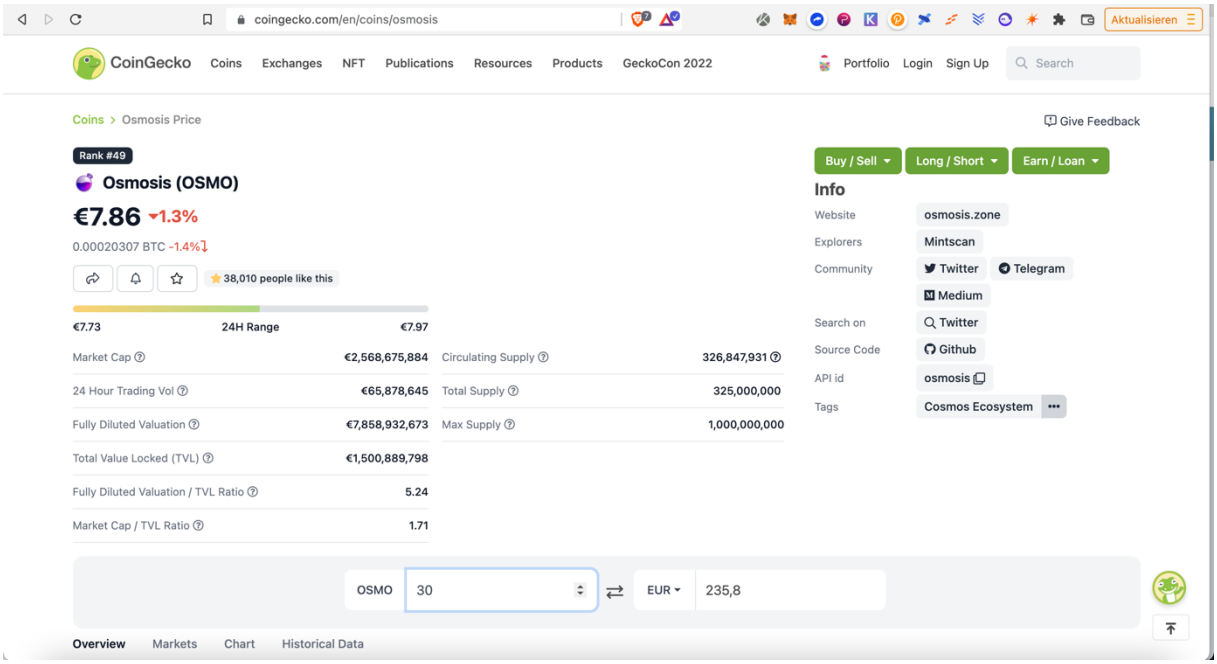
Neumann, J. v., & Morgenstern, O. (2007). *Theory of Games and Economic Behavior.* Princeton, USA: Princeton University.
Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019, June 26). *Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities.* IEEE.
NGUYEN, C., HOANG, D., NGUYEN, D., NIYATO, D., NGUYEN, H., & DUTKIEWICZ, E. (2019, June 26). *https://ieeexplore.ieee.org/.* Retrieved from https://ieeexplore.ieee.org/: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8746079
Nicolle, E. (2022, Febraury 22). *bloomberg.com*. Retrieved from https://www.bloomberg.com/news/articles/2022-02-22/attacker-behind-record-2016-crypto-hack-might-have-been-found
Novum Insight. (2021, March 12). *novuminsights.com*. Retrieved from https://novuminsights.com/post/slashing-penalties-the-long-term-evolution-of-proof-of-stake-pos/
Osmosis. (2022, April 26). *osmosis.zone*. Retrieved from https://app.osmosis.zone/airdrop
Pan, J., Song, Z., & Hao, W. (2021, July 30). *ieeexplore.ieee.org*. Retrieved from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9565684
Patel, P. (2020, March 30). *geeksforgeeks.org*. Retrieved from https://www.geeksforgeeks.org/difference-between-network-security-and-cyber-security/
Paulsen, C., & Byers, R. (2019, July 01). *nvlpubs.nist.gov.* Retrieved from nvlpubs.nist.gov: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf
Philips, D. (20212, April 16). *decrypt.co*. Retrieved from https://decrypt.co/resources/what-is-near-protocol
Piscini, E., Dalton , D., & Kehoe, L. (2017, Januar 1). *https://www2.deloitte.com/.* Retrieved from https://www2.deloitte.com/: https://www2.deloitte.com/tr/en/pages/technology-media-and-telecommunications/articles/blockchain-and-cyber.html#
Polkadot. (2022, April 26). *polkadot.io*. Retrieved from https://polkadot.subscan.io/
Rosu, I., & Saleh, F. (2021, February 01). Evolution of Shares in a Proof-of-Stake Cryptocurrency. *Management Science*, pp. 661 - 672.
Sankeu, J. (2018, October 05). *medium.com*. Retrieved from medium.com: https://medium.com/@yourcryptoguide/a-deeper-look-at-proof-of-stake-masternodes-5137ad8dd0cb
Sankeu, J. (n.d.). *medium.com*. Retrieved from medium.com.
Sanyal, S. (2022, February 17). *analyticsinsight.net*. Retrieved from https://www.analyticsinsight.net/10-banks-that-have-invested-in-cryptocurrencies-and-blockchain/
Sayeed, S., & Marco-Gisbert, H. (2019, April 29). Assessing Blockchain Consensus and Security Mechanisms against the 51% Attack. *Applied Sciences*, p. 9.
Scheuerman, D. (2021, August 05). *cvj.ch*. Retrieved from https://cvj.ch/fokus/hintergrund/was-ist-eip-1559-und-kann-die-implementierung-ethereum-helfen-deflationaer-zu-werden/
Shkoor, A. M. (2019, August). *medium.com*. Retrieved from https://medium.com/swlh/what-is-byzantine-generals-problem-and-how-technology-solves-it-5087888ca821
Simplilearn. (2021, July 19). *simplilearn.com*. Retrieved from https://www.simplilearn.com/what-is-blockchain-security-and-its-examples-article
stakefish. (2020, September 14). Retrieved from medium.com: https://medium.com/stakefish/proof-of-stake-a-brief-history-4baa3effc917
Tendermint. (2022, April 23). *cosmos.network*. Retrieved from https://cosmos.network/ecosystem/apps

Tendermint Inc . (2022, April 28). *cosmos.network*. Retrieved from https://docs.cosmos.network/main/intro/overview.html
Tendermint Inc. (2022, April 28). *tendermint.com*. Retrieved from https://tendermint.com/sdk/
Tendermint Inc. (2022, April 25). *v1.cosmos.network*. Retrieved from https://v1.cosmos.network/about
Tendermint Inc. (2022, April 27). *cosmos.network*. Retrieved from https://v1.cosmos.network/about
Tendermint Inc. (2022, May 03). *docs.cosmos.network*. Retrieved from https://docs.cosmos.network/main/intro/sdk-app-architecture.html#abci
Tendermint Inc. (2022, May 03). *v1.cosmos.network*. Retrieved from https://v1.cosmos.network/intro
Thames, L., & Schaefer, D. (2017). *Cybersecurity for Industry 4.0: Analysis for Design and Manufacturing* . USA, Atlanta: Springer.
Thin, W. Y., Dong, N., Bai, G., & Dong, J. (2018). *Formal Analysis of a Proof-of-Stake Blockchain.* Melbourne,Australia: IEEE.
TRITON. (2022, April 26). *solanabeach.io*. Retrieved from https://solanabeach.io/
Tuyisenge, M. J. (2021). *BLOCKCHAIN TECHNOLOGY SECURITY CONCERNS: Literature Review.* Upsala University , Information Systems. Uppsala, Sweden: Uppsala Universitet: DEPARTMENT OF INFORMATIC AND MEDIA.
Vardai, Z. (2021, September 8). *forkast.news*. Retrieved from https://forkast.news/what-are-public-private-permissioned-blockchains/#:~:text=Some%20examples%20of%20permissioned%20networks,marketplace%20secured%20by%20blockchain%20technology.
Verizon. (2021). *2021 Data Breach Investigations Report.* https://www.verizon.com/business/resources/reports/2021/2021-data-breach-investigations-report.pdf.
Wachal, M. (2021, June 14). *softwaremill.com*. Retrieved from https://softwaremill.com/what-is-private-blockchain-why-do-you-need-it/#when-would-you-need-private-blockhain
Web3 Foundation. (2022, December 21). *polkadot.network*. Retrieved from polkadot.network: https://support.polkadot.network/support/solutions/articles/65000150130-how-do-i-know-%20which-validators-to-choose-
Worner, M. (2021, March 09). *medium.com*. Retrieved from medium.com: https://medium.com/tgradefinance/delegators-or-no-delegators-which-path-does-tgrade-follow-63a0a3543d18
Zajonc, R. B. (1968). Attitudinal effects of mere exposure. *Journal of Personality and Social Psychology*(2), pp. 1 - 27.

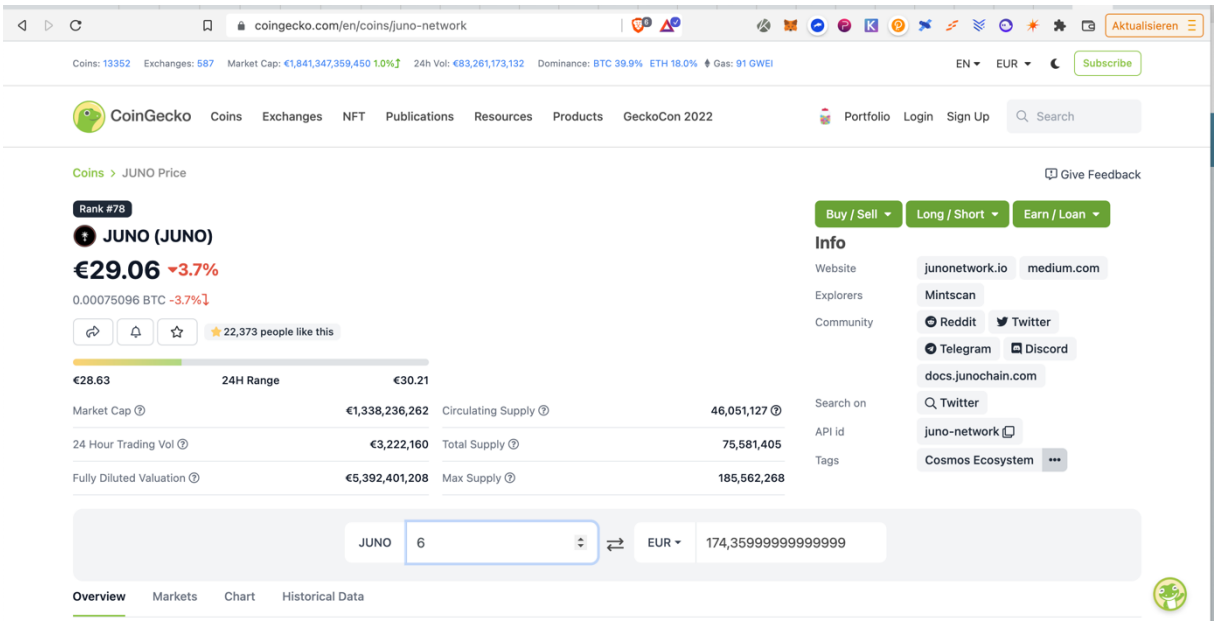
Appendix

Protocol	Ouroboros	Casper	Algorand	Tendermint
Type	PoS	PoS-PoW hybrid	PoS	PoS
Consensus process	-Dynamic committee -Leader selection by 3-phased coin-tossing protocol -Utilize FTS algorithm	-Leader selection by PoS -Validators vote via BFT protocol to justify the checkpoint blocks	-Dynamic committee -Leader selection based on stake -Utilize VRF	-Leader selection by round-robin selection -Validators vote to confirm blocks
Transaction adding	Input endorsers	Block creator	Block creator	Block creator
Incentive Mechanism	Rewards are divided between the slot leaders and the input endorsers	Deposit is confiscated for malicious behaviors	Undefined	-Rewards divided between Validators. -Deposit is confiscated for behaviors
Network Synchrony	Partial Synchrony	Partial Synchrony	Asynchronous period in between synchronous periods	Partial Synchrony
Adversary Toleration	1/2	1/3	1/2	1/3
Security issues	51% attack, bribe attack	Depends on underlying chain	Ignore incentive compatibility	-Ignore dynamic stake distribution -Leader selection is not clearly defined
Finality	Delayed	Delayed	Immediate	Immediate
Transaction confirmation	2 minutes	Depends on underlying chain	20 seconds	1 second
Transaction throughput	257 Tx/s	Depends on underlying chain	875 Tx/s	800 Tx/s
Applications	Cardano	Ethereum 2.0	Algorand, Arcblock	Ethermint

Appendix 1: Different PoS variations

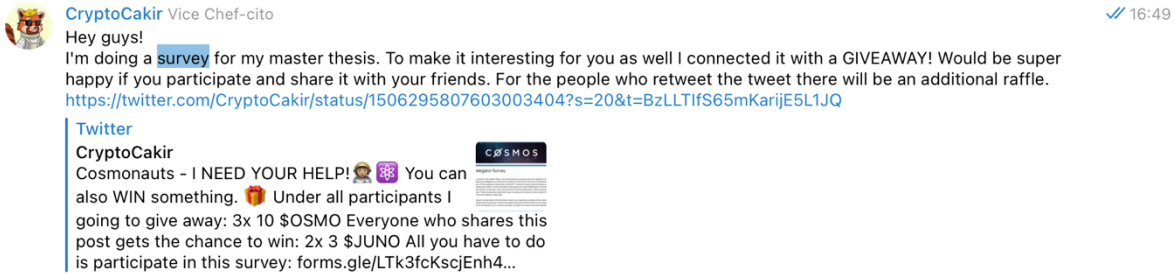


Appendix 2: Amount of prize money $OSMO

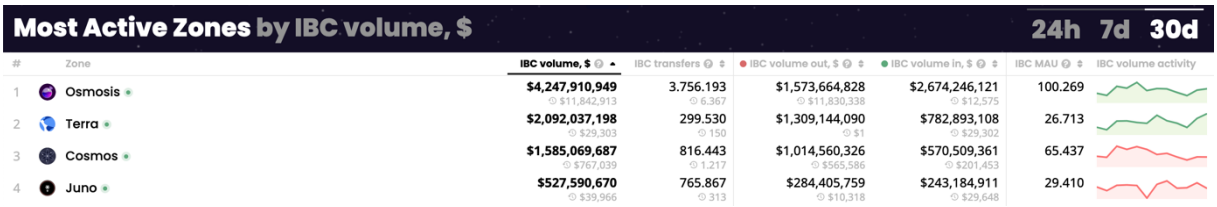


Appendix 3: Amount of prize money $JUNO

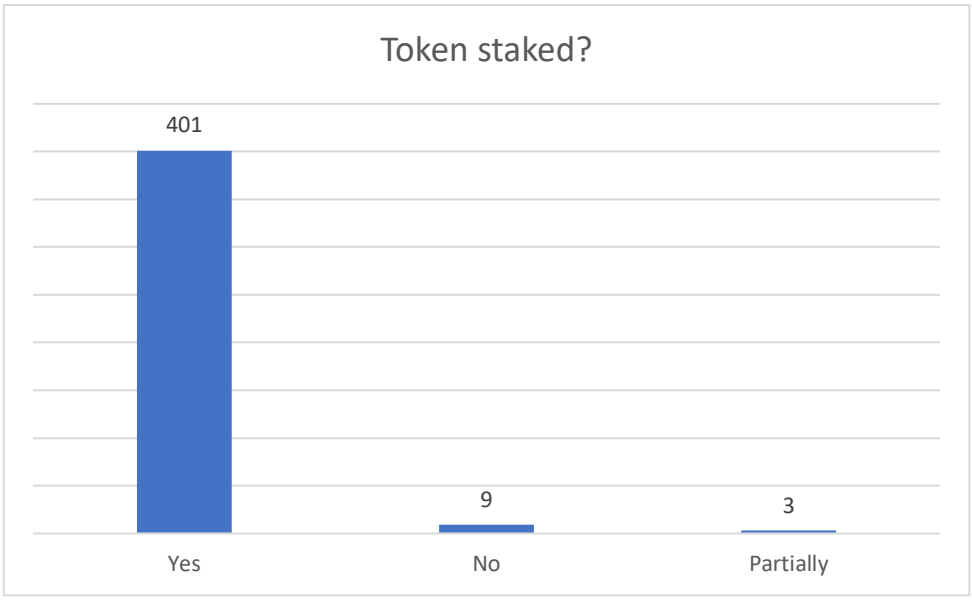
Appendix 4: Winner announcement on Twitter



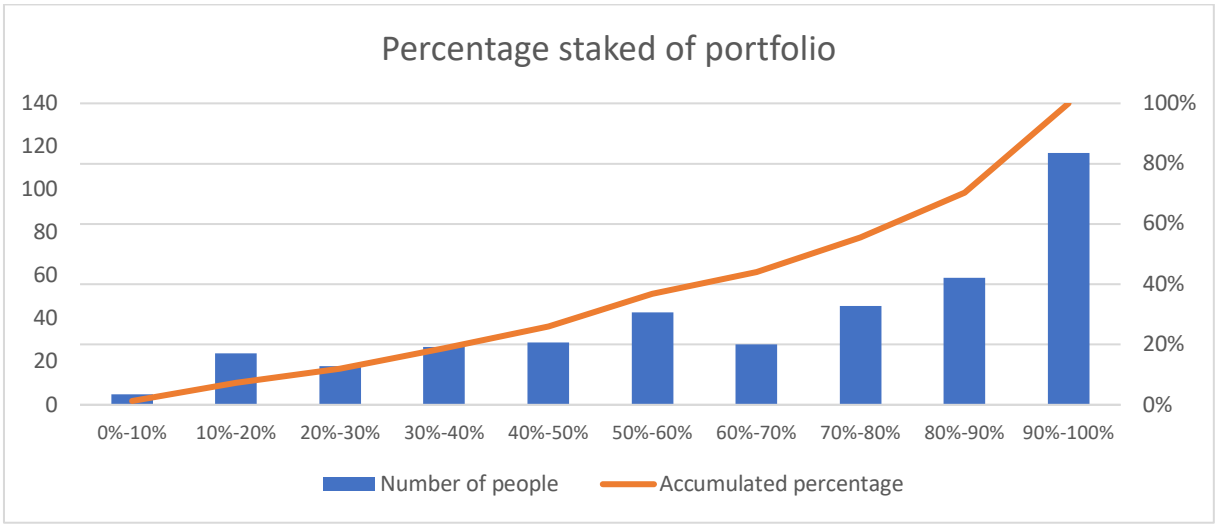
Appendix 5: Giveaway announcement on Telegram



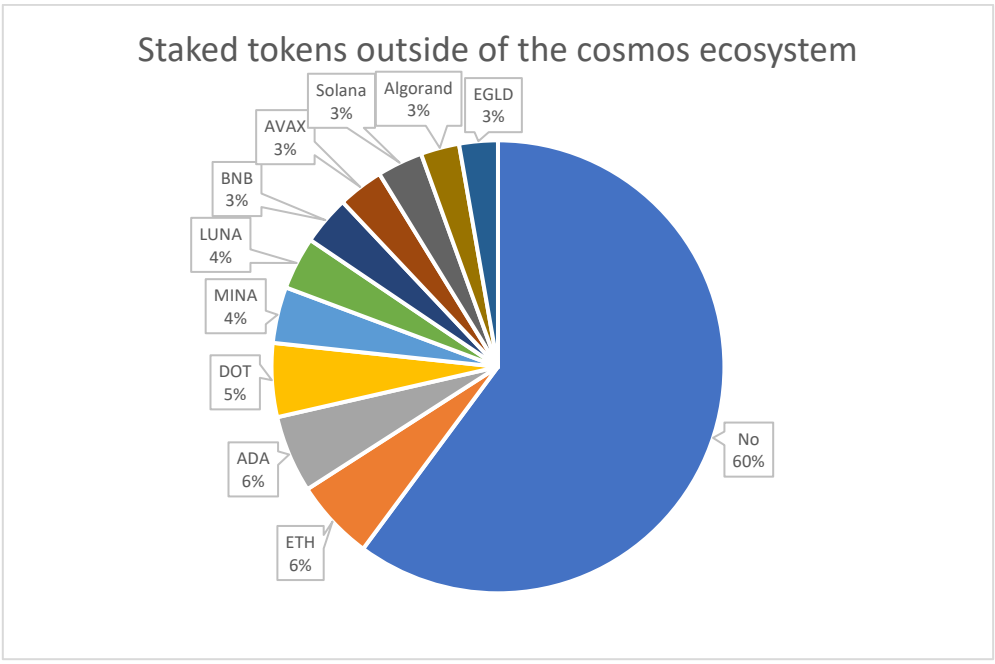
Appendix 6: IBC volume



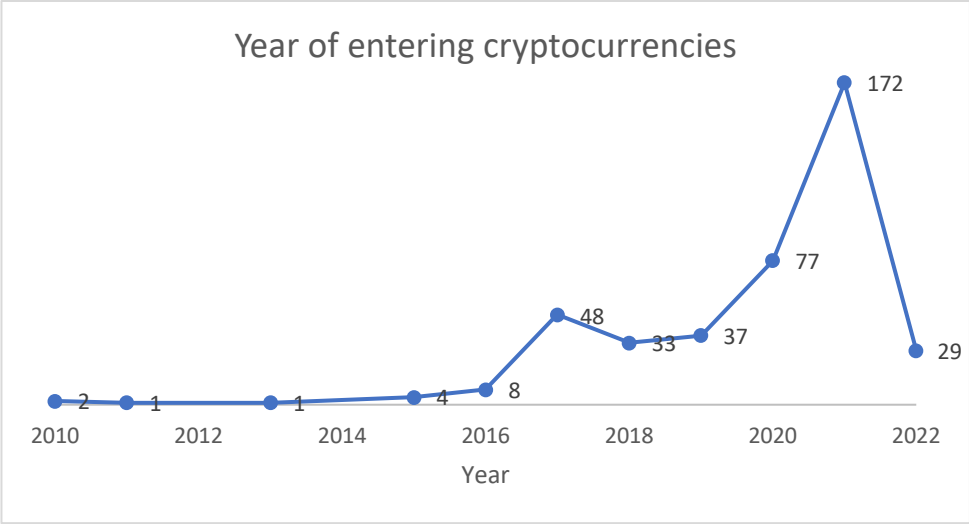
Appendix 7: Question 2.1 Amount token staked



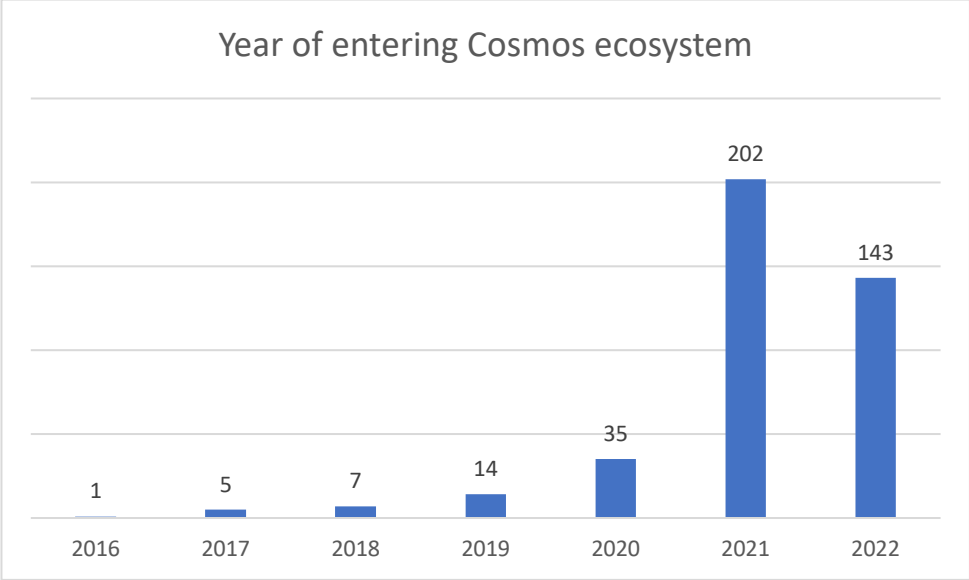
Appendix 8: Question 2.2 Percentage staked of portfolio



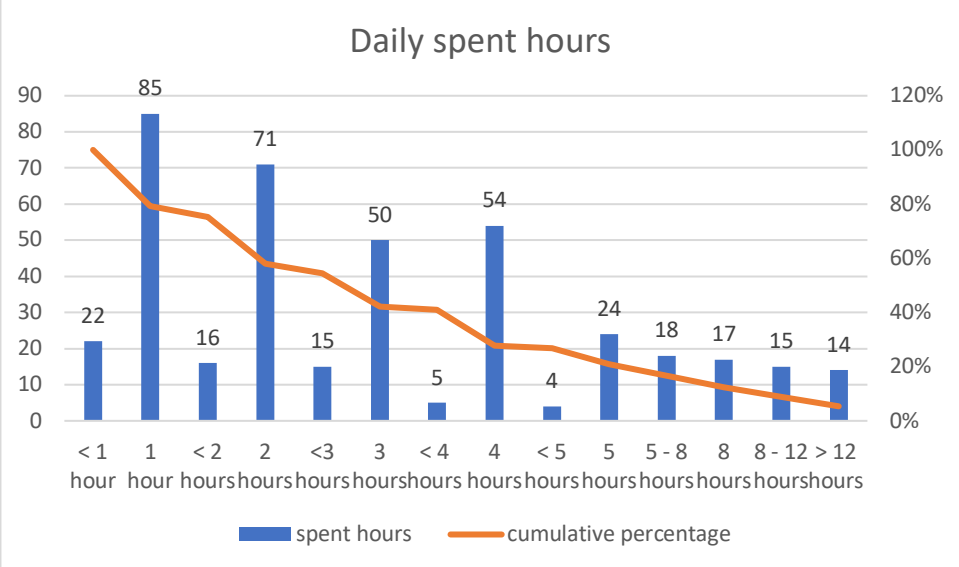
Appendix 9 Question 2.3 Staked token outside of Cosmos



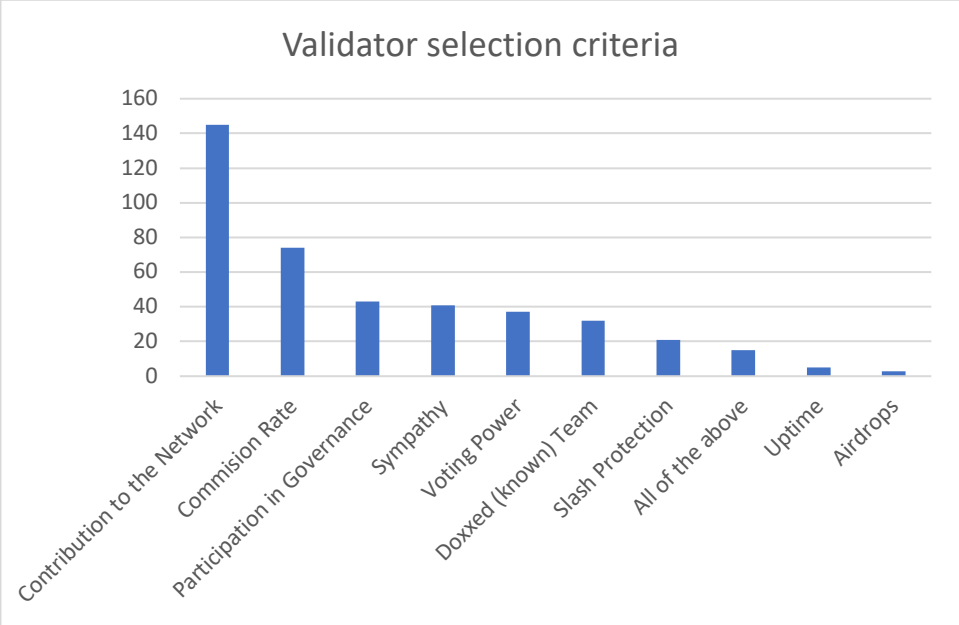
Appendix 10: Question 2.4 Year of first investment into cryptocurrencies



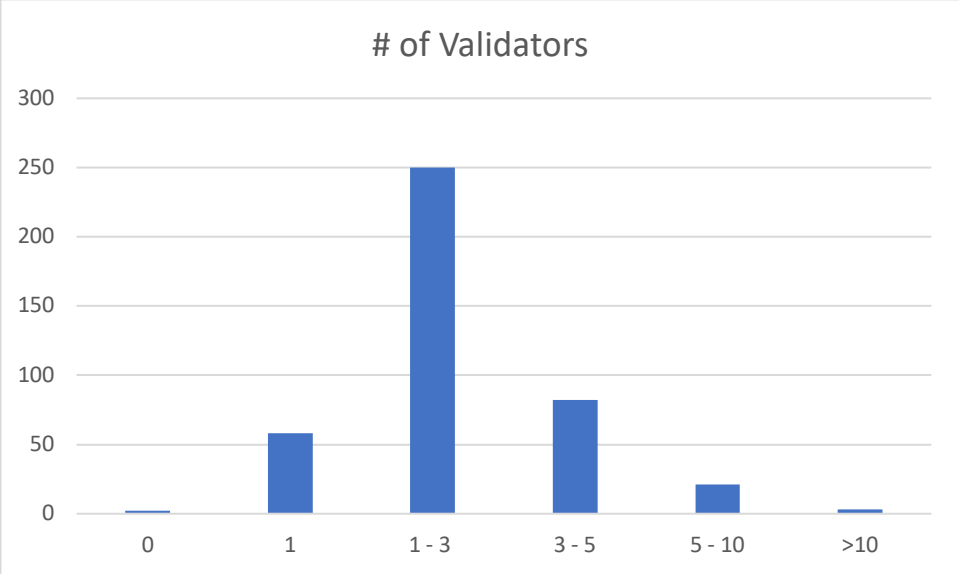
Appendix 11: Question 2.5 Year of first investment into the Cosmos ecosystem



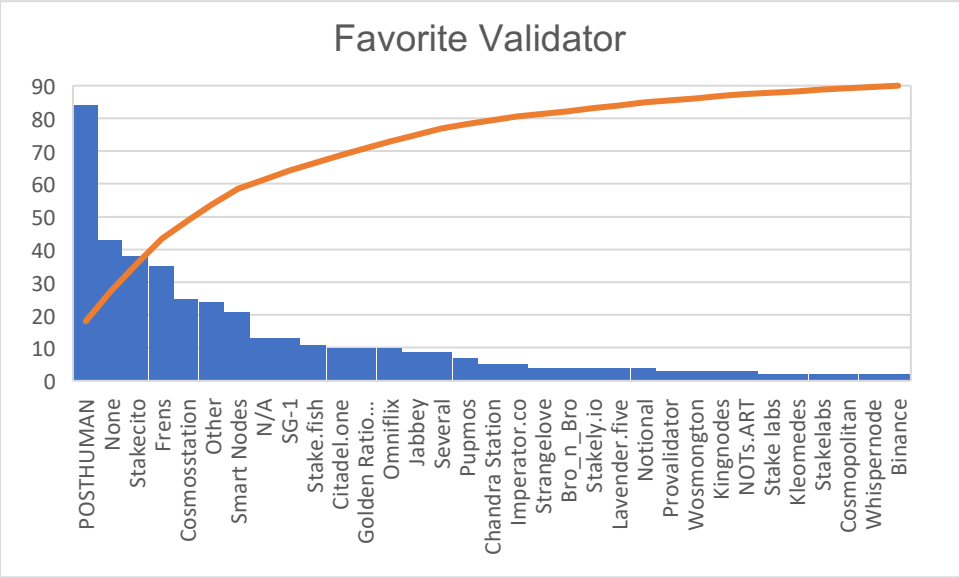
Appendix 12: Question 2.6 Daily hours spent on PoS network



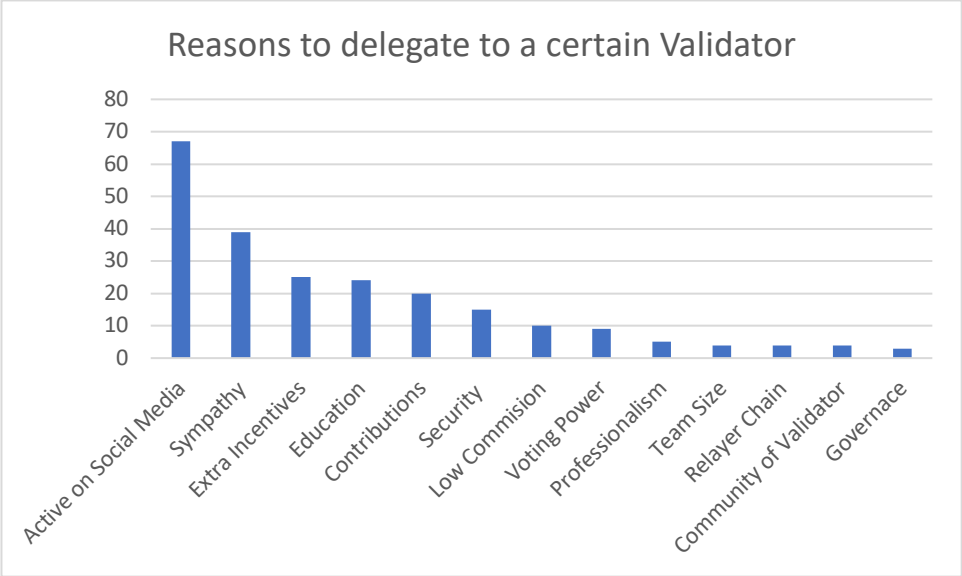
Appendix 13: Question 3.1 Validator selection criteria



Appendix 14: Question 3.2 Average selected Validators per chain

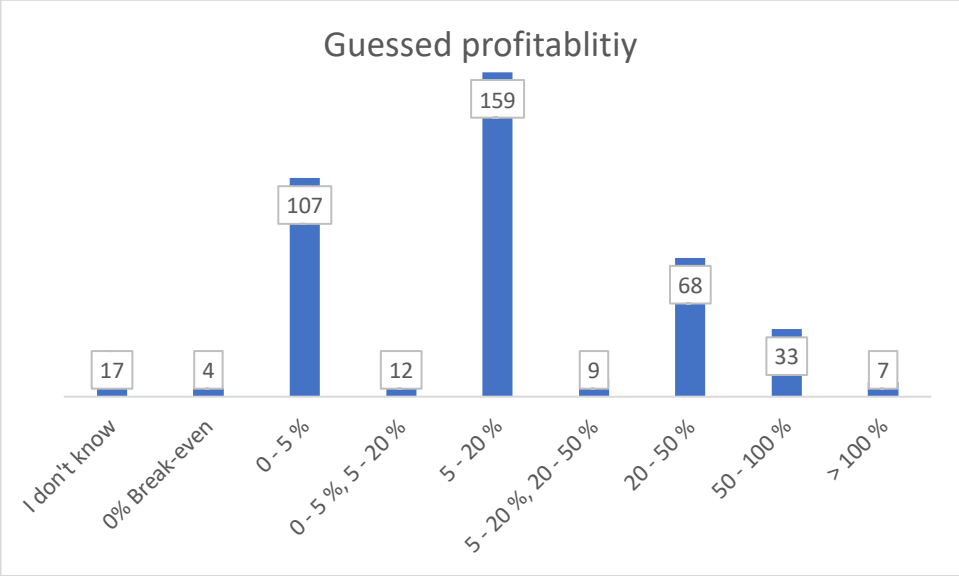


Appendix 15: Question 3.3 Favorite Validator

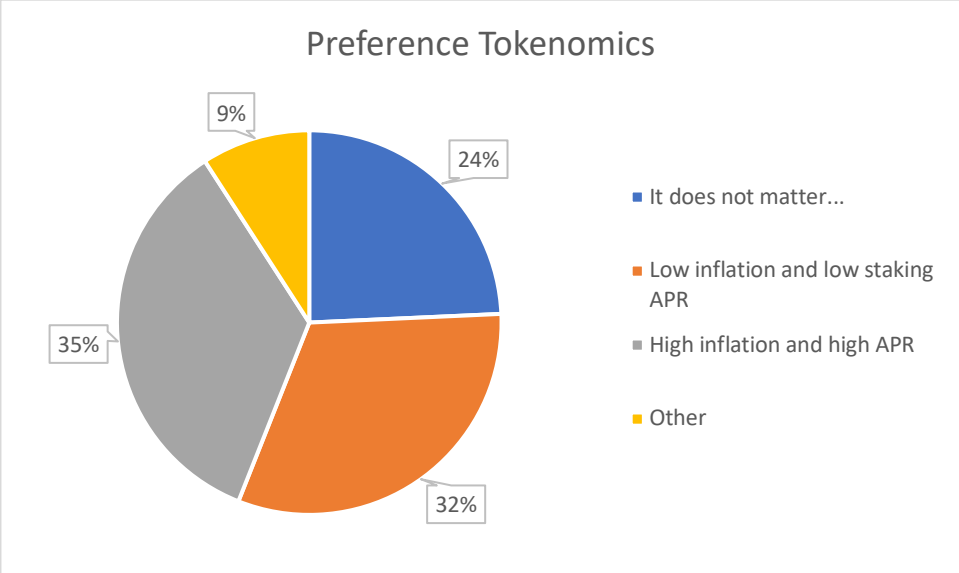


Appendix 16: Question 3.3 Reason of Validator

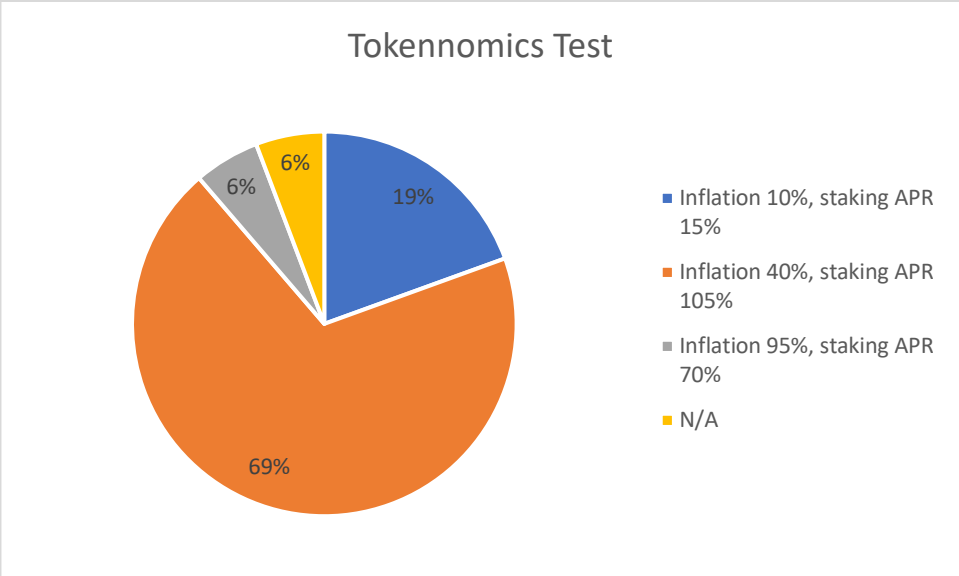
Appendix 17: Question 3.4 Additional wishes form Delegators



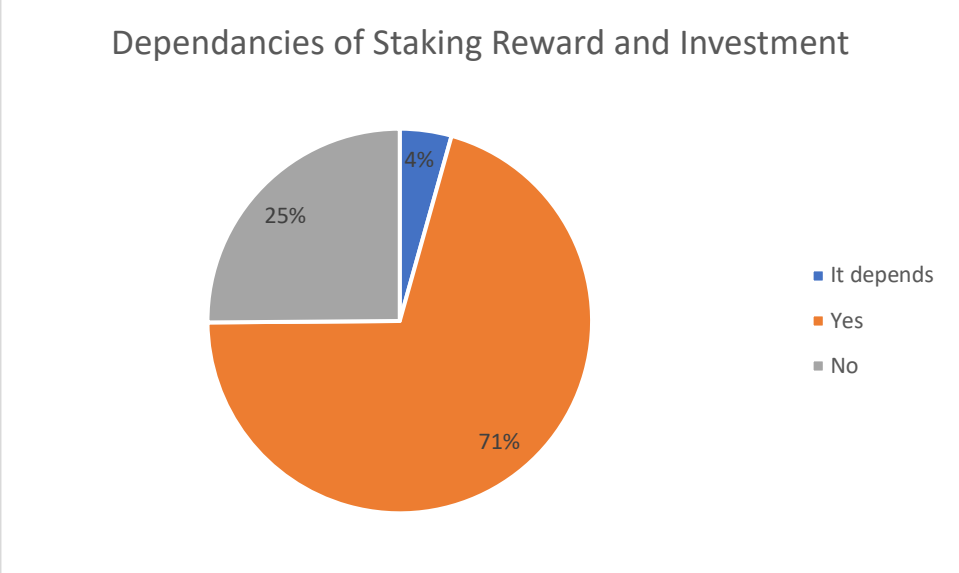
Appendix 18: Question 3.5 Guessed profitability of Validators



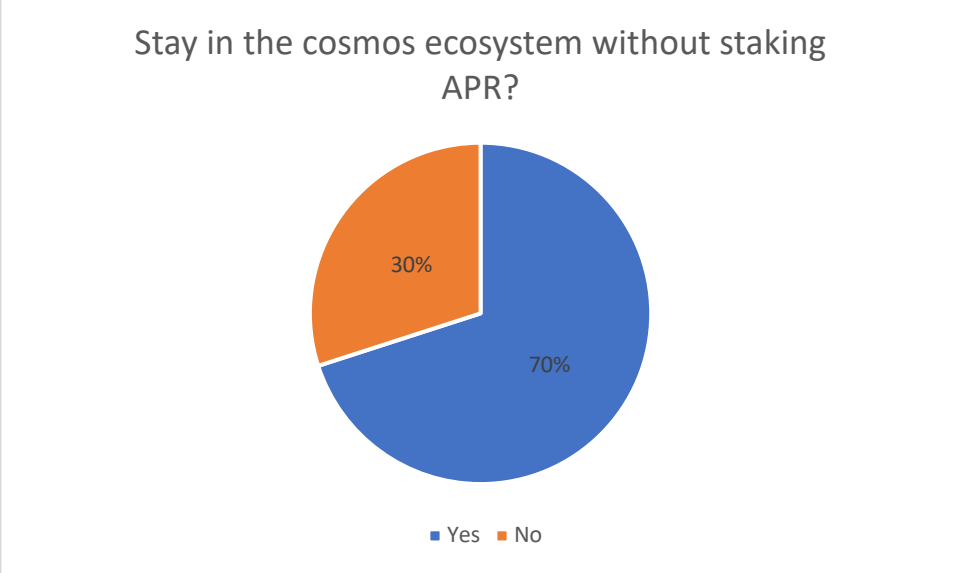
Appendix 19: Question 4.1 Preferred tokenomics



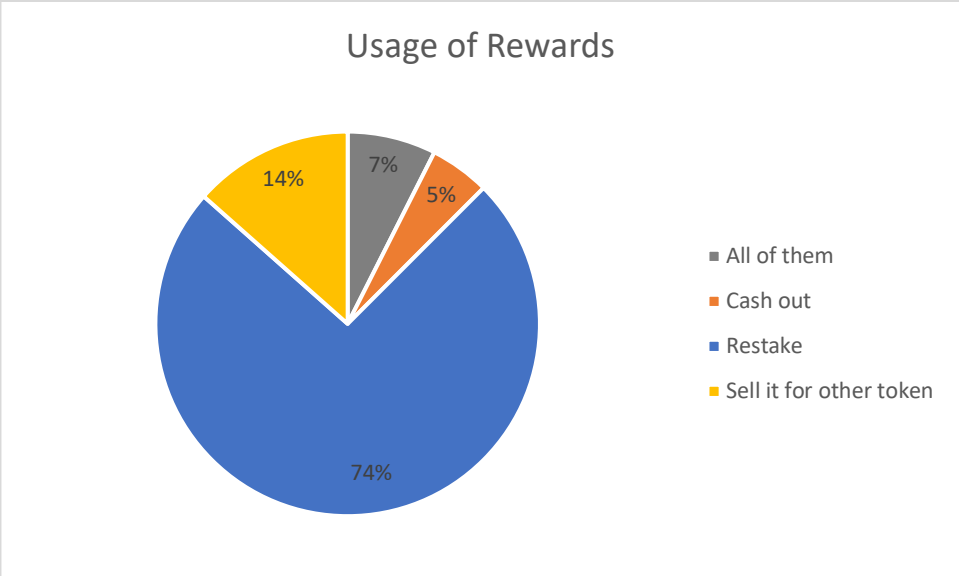
Appendix 20: Question 4.2 Tokenomics test



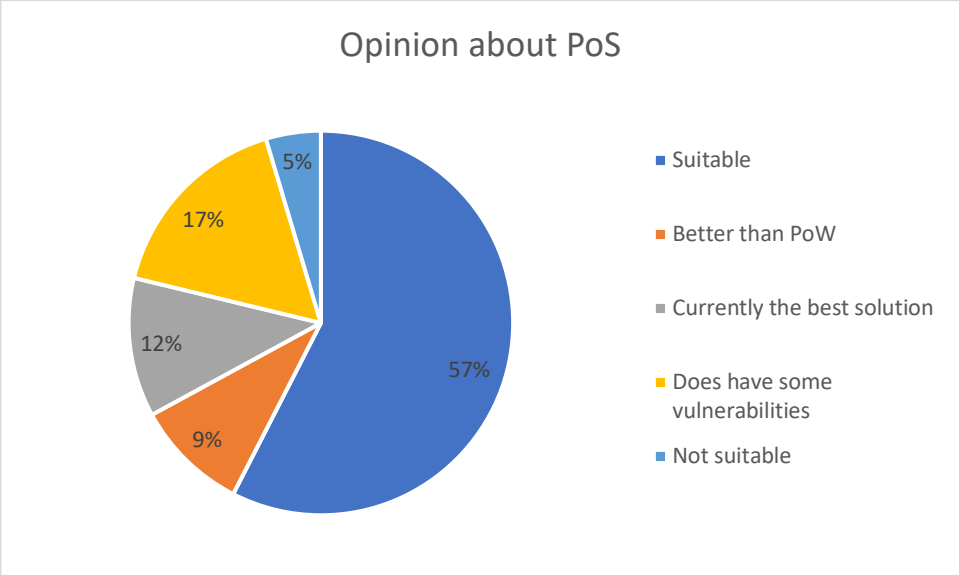
Appendix 21: Question 4.3 Dependencies of staking reward and investment



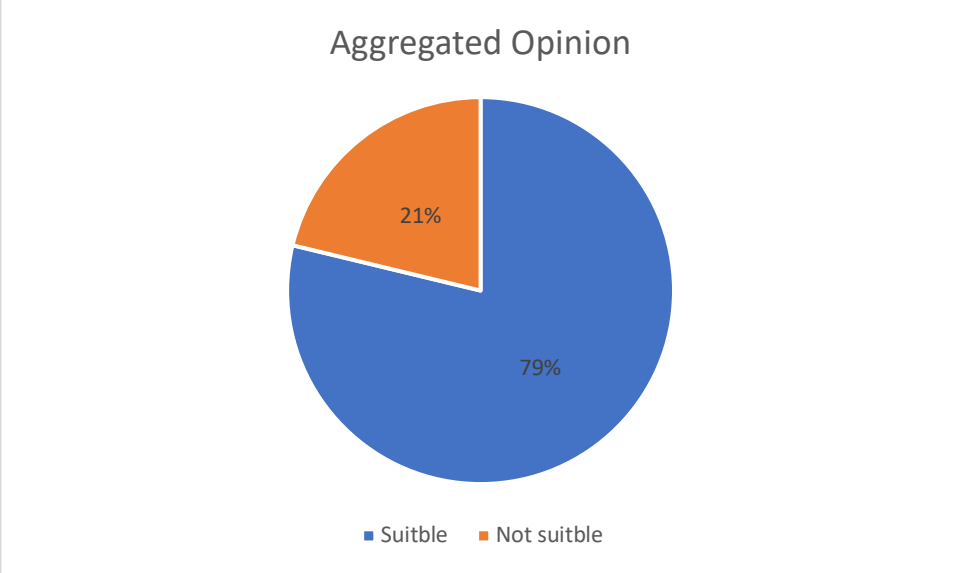
Appendix 22: Question 4.4 Stay in Cosmos without staking APR



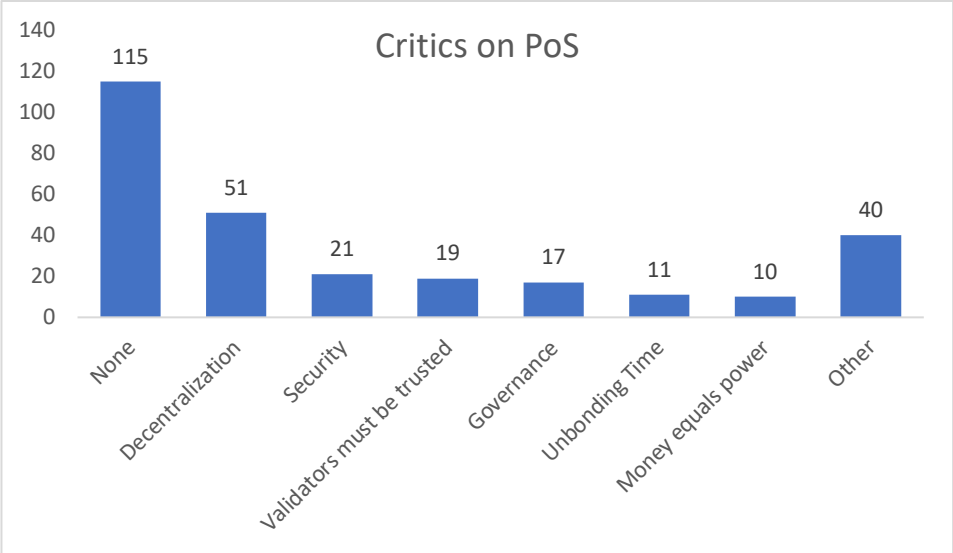
Appendix 23: Question 4.5 Usage of rewards



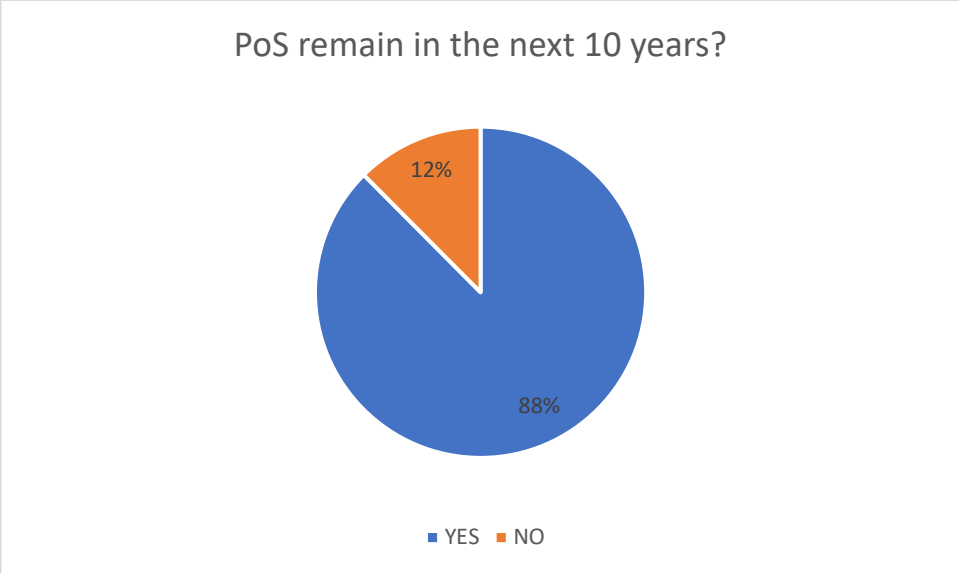
Appendix 24: Question 5.1 Sustainability of PoS



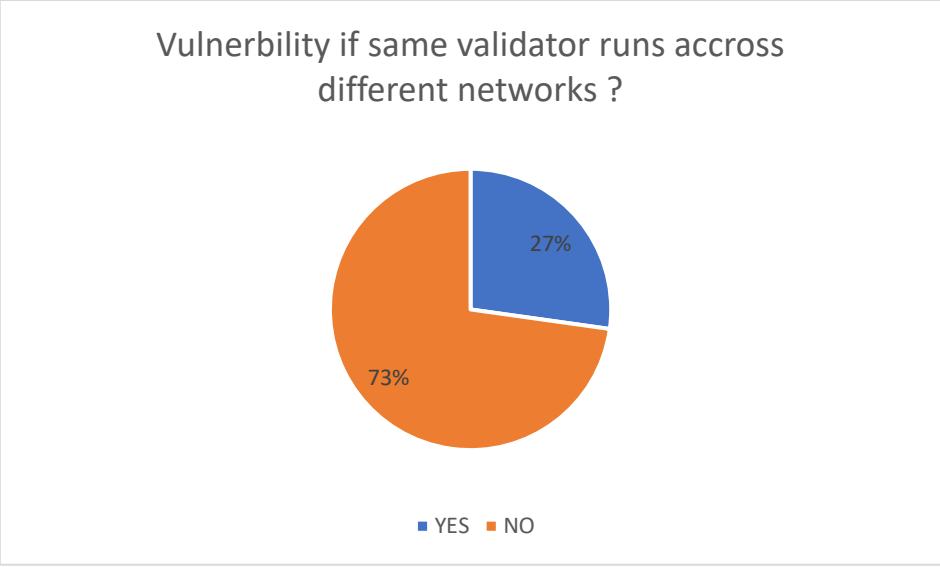
Appendix 25: Question 5.1 Aggregated opinion



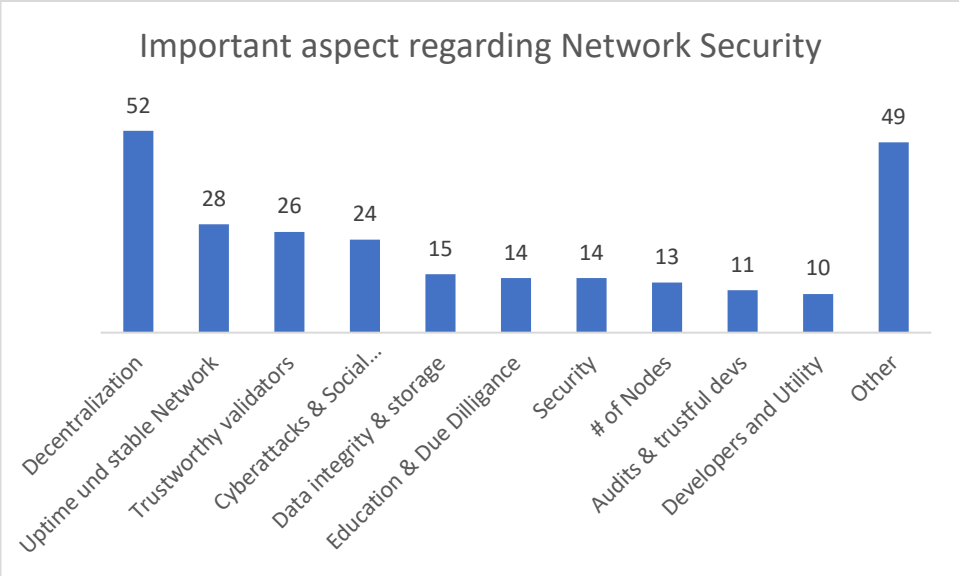
Appendix 26: Question 5.2 Critics on PoS



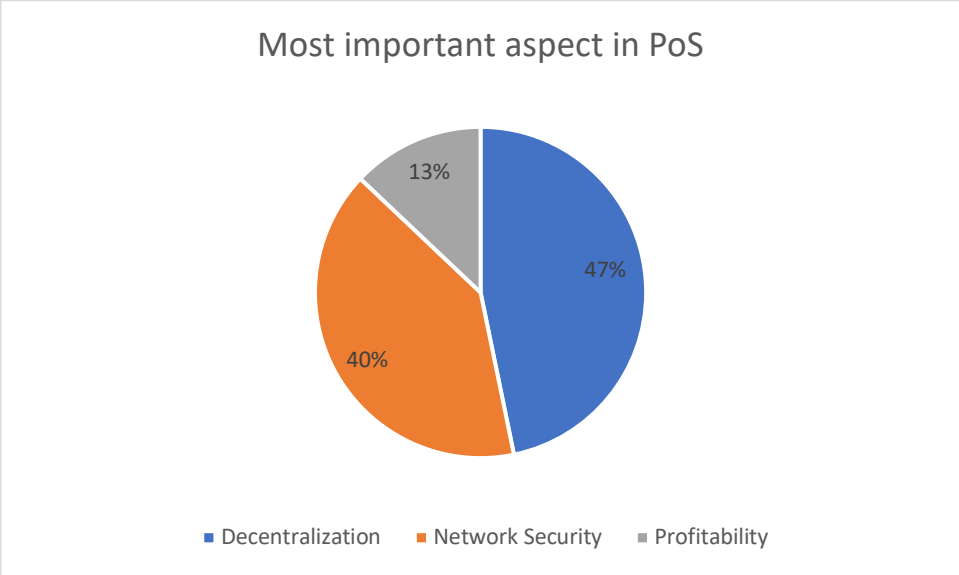
Appendix 27: Question 5.3 PoS remain next 10 years



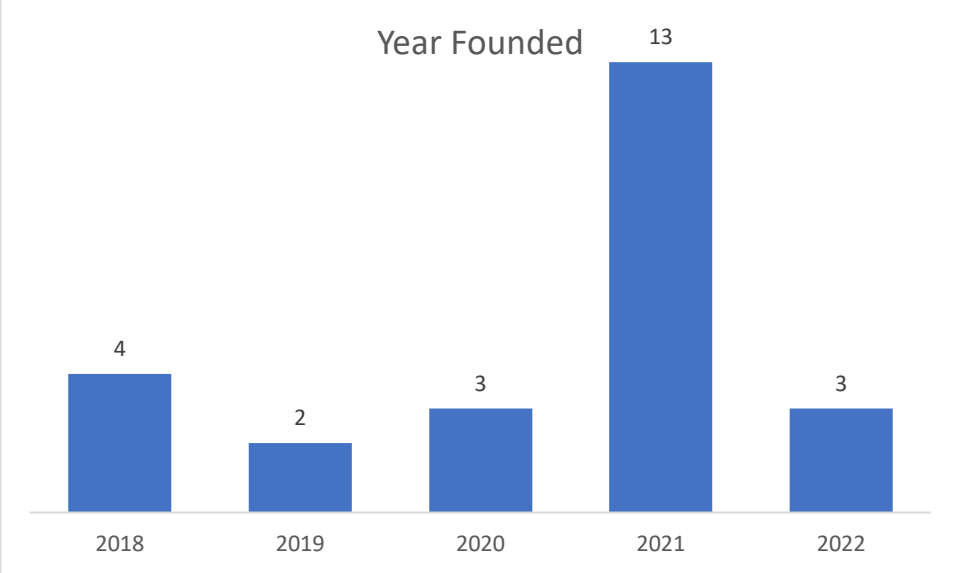
Appendix 28: Question 5.4 Vulnerability if Validator runs across different networks.



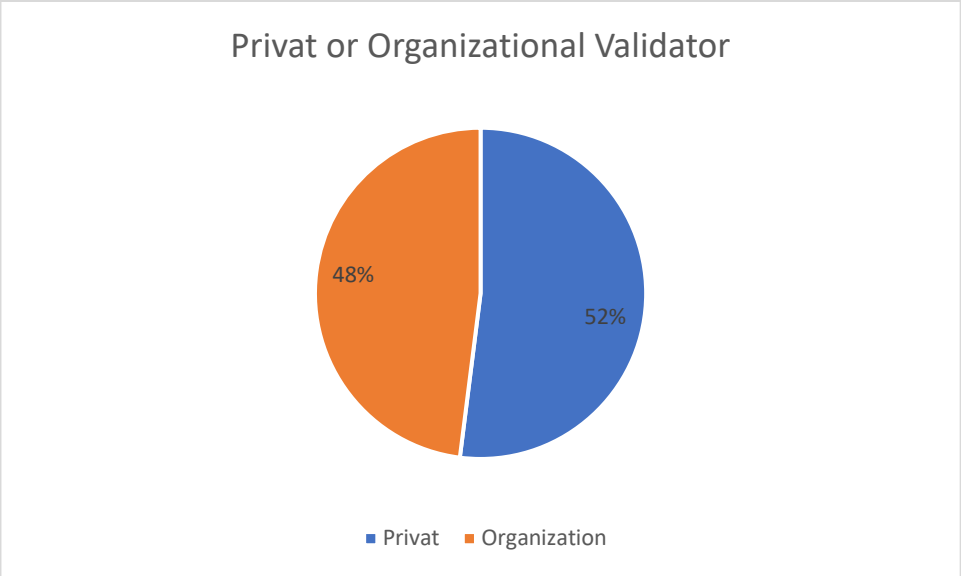
Appendix 29: Question 5.5 Important aspects regarding Network Security



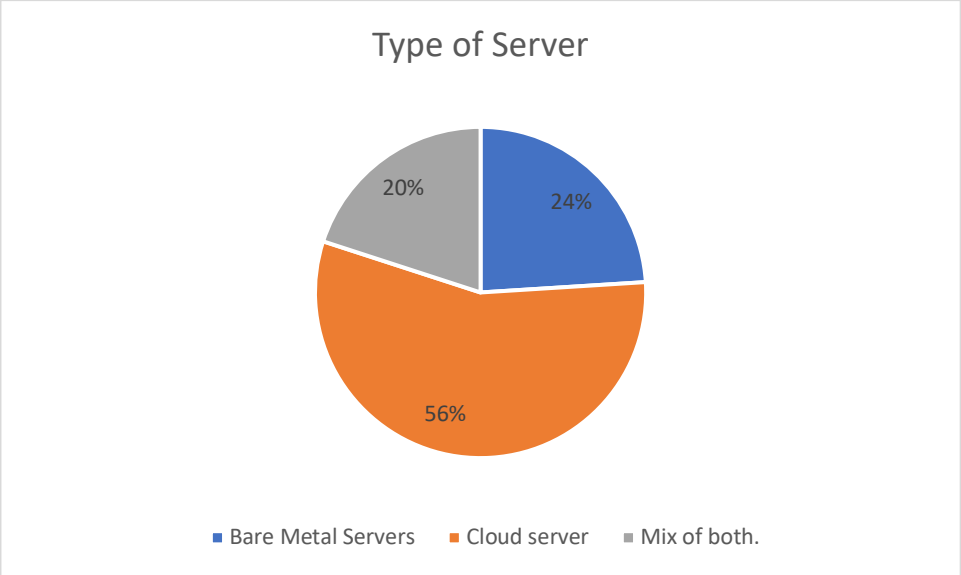
Appendix 30: Question 5.6 Most important aspect in PoS



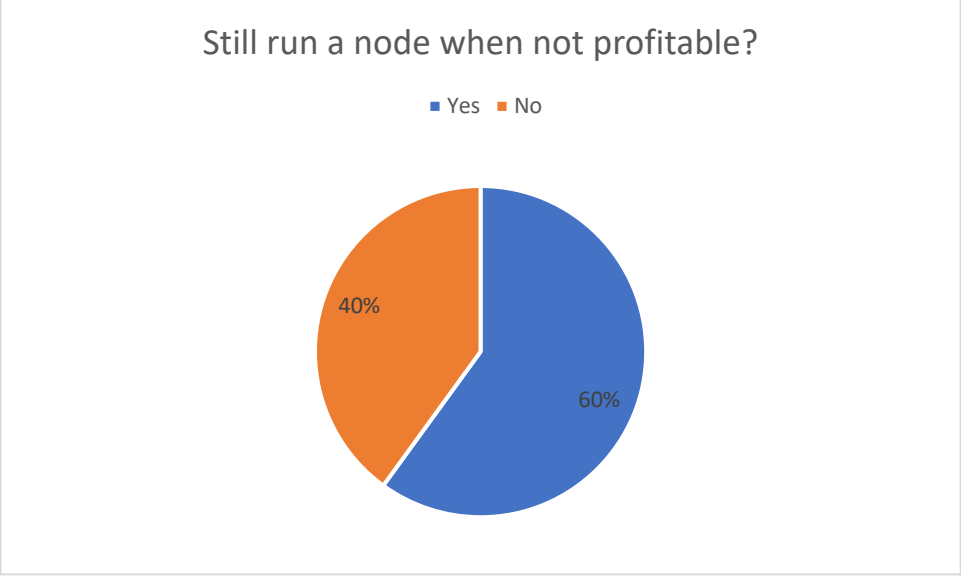
Appendix 31: Question1.2 Founding year of Validator



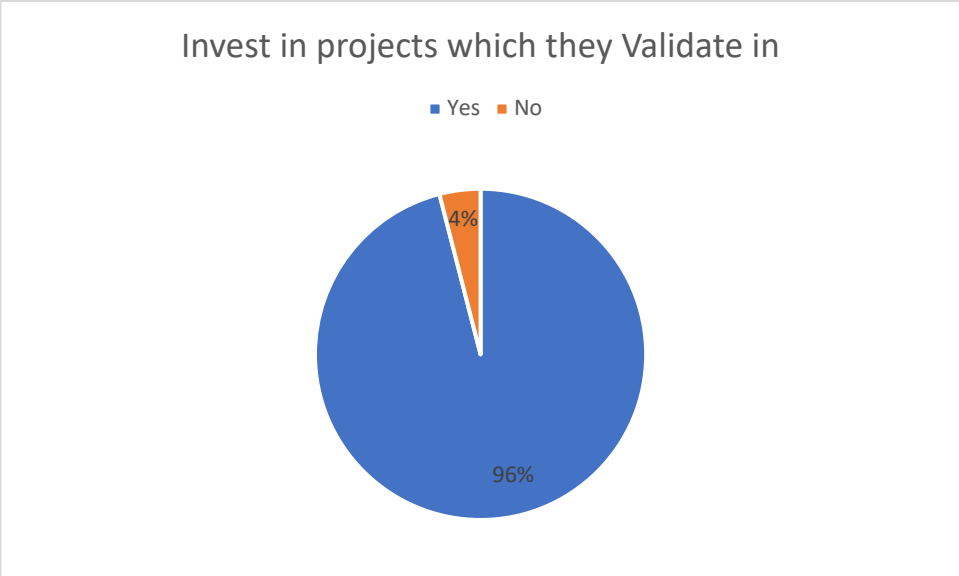
Appendix 32: Question 1.3 Privat or Organization



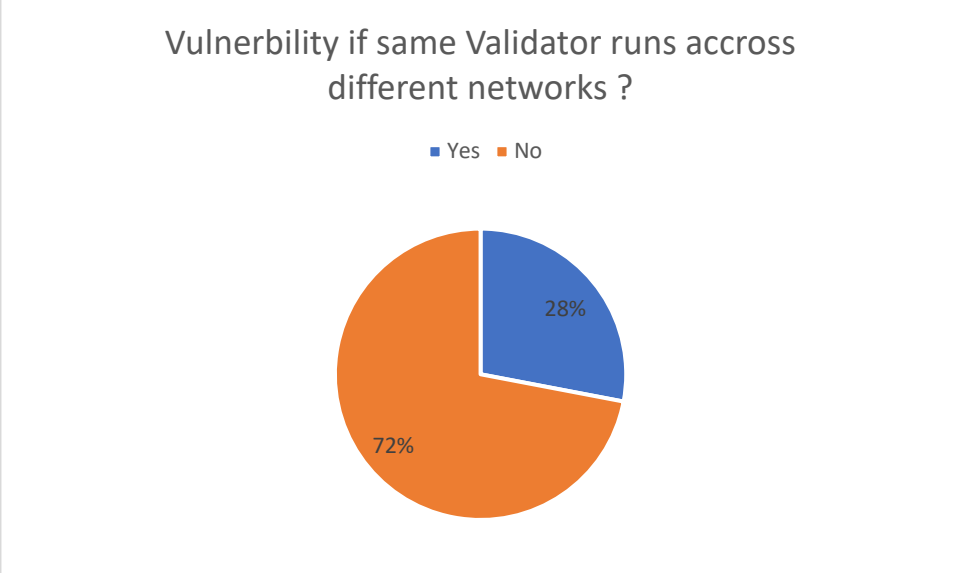
Appendix 33: Question 2.6 Type of server



Appendix 34: Question 3.2 Still run a node when not profitable?



Appendix 35: Question 3.6 Validators invest in projects which they validate?



Appendix 36: Question 4.4 Vulnerability if same Validator across several networks

Delegator Survey

1.General Information

1.1 Name
1.2 Age
1.3 Location
1.4 Field of work
1.5 Invested in projects outside of Cosmos ecosystem, if yes, which ones?
1.6 Portfolio size

< 5,000 $	5,000 – 20,000 $	20,000 – 100,000 $	100,000 – 250,000 $	250,000 – 500,000 $	500,000 – 1,000,000 $	> 1,000,000 $

2.Basic Questions

2.1 Do you stake your token?
2.2 How much % of your portfolio is staked?
2.3 Do you stake other coins outside of the Cosmos ecosystem?
2.4 Since when you are invested in cryptocurrencies and since when in the Cosmos ecosystem?
2.5 How many hours per day do you spent with research/claiming rewards/voting?

3.Validator Questions

3.1 On which criteria do you select validators?
3.2 To how many validators do you delegate on average per chain?
3.3 Who is your favorite validator and why?
3.4 What should a validator do in addition to have 100% uptime?
3.5 What do you think, how profitable is it to operate a validator node (in %)?

4.Tokennomics

4.1 Would you prefer low inflation and low staking APR or high inflation and high APR?
4.2 Select the best option:
- Inflation 95%, staking APR 70%
- Inflation 40%, staking APR 105%
- Inflation 10%, staking APR 15%

4.3 Do you select investment decisions based on staking rewards?
4.4 Would you stay in the Cosmos ecosystem if there would be no staking rewards anymore?
4.5 What are you doing with your rewards? Restake / sell / trade it to other projects?

5.POS Questions

5.1 What is your opinion about PoS? Is it suitable or does it have some vulnerabilities?

5.2 What is your biggest critics on PoS?
5.3 Do you think PoS will remain in the next 10 years? Explain why you think so.
5.4 Do you see vulnerabilities when the same validator has nodes across different chains?
5.5 What is the most important aspect regarding Network Security in your opinion?
5.6 Select which one is the most important aspect in your opinion: Profitability / decentralization / Network Security

Appendix 37: Delegator survey

Validator Survey

1.General Information

1.1 Validator name
1.2 Founded in year
1.3 Privat or organization
1.4 Size of team

2.Basic Questions

2.1 Which protocols do you currently offer for staking?
2.2 Voting power of each chain?
2.3 When did you set up your first node and when did you set up your last one?
2.4 How do you select which project you are going to validate?
2.5 Are you using your own servers or a cloud server and why?
2.6 Where are your servers located // which cloud provider do you use?
2.7 What is your average commission rate?
2.8 How often do you maintain the node?
2.9 What are your cost to set up one node?
2.10 What are your cost to maintain one node?

3. Motivational Questions

3.1 What is important for you as a validator when you validate?
3.2 Why are you a validator?
3.3 If being a validator wouldn't be profitable, would you still be a validator?
3.4 Which additional benefits do you bring to stakers and the network in general?
3.5 How would you attract more delegators?
3.6 Are you invested in the project which you validate?
3.7 Do you also delegate to other validators? If yes, to how many different validators on average per project?
3.8 What are you doing with your commissions, restake// sell// or trade it to other projects?

4. POS Questions

4.1 What's your opinion about PoS is it suitable or does it have some vulnerabilities?
4.2 What's your biggest critics on PoS?
4.3 Do you think PoS will remain in 10 years, explain why you think so?
4.4 Do you see vulnerabilities when the same validator has nodes across different chains?
4.5 How many other validators do you know or have contact to?
4.6 What is the most important aspect regarding Network Security in your opinion?
4.7 Select one //Profitability// Decentralization// Network Security

5. Cosmos PoS Questions

5.1 Do you have nodes outside of the cosmos ecosystem?
5.2 Does the Cosmos PoS ecosystem represent the general PoS environment in your opinion, if not what is different?
5.3 Do you see any potential dangers in the current or future validator sets?
5.4 To become an active node it requires a notable number of delegations; do you think this hurdle is big and justified?
5.5 Did you bootstrap your node with delegations from the foundation or did you self-founded it to get into the active validator set?

Appendix 38: Validator survey

Declaration of Sole Authorship

I, Zafercan Cakir, certify that I have written this paper independently and have not used any sources or aids other than those specified here. I have marked all statements taken from other works in word or sense and they have not been part of other study or examination achievements.

Date: _____ Signature: _____