EUROPEAN BLOCKCHAIN ASSOCIATION

Staking Infrastructure Provider

Position Paper

EUROPEAN BLOCKCHAIN ASSOCIATION E.V.
VR 208150
Oskar-von-Miller-Ring 36
80333 Munich, Germany
europeanblockchainassociation.org

Contacts:
Julius Schmidt
Chair of Staking Infrastructure Working Group
js@eublas.org
+49.170.79.37.555

Awa Sun Yin
Co-Chair of Staking Infrastructure Working Group
awa@eublas.org

Rebecca Johnson
Secretary to the Staking Infrastructure Working Group
rlj@eublas.org
+49.176.60.99.94.89

DATARELLA STAKING FACILITIES DOKIA CAPITAL Staking Rewards ChainLayer Certus.One

StakeNow CRYPTIUM LABS cryptio CHORUS

EUROPEAN BLOCKCHAIN ASSOCIATION

Table of Contents

Executive Summary

The use of blockchain technology is increasing at an incredible pace, providing efficiency enhancements in key sectors, as for example the healthcare business and the financial industry. It can be taken for granted that by the end of this decade - probably much sooner - several core infrastructures around the world will have shifted to blockchain technology. Besides, a quickly growing new asset class has emerged that covers not only cryptocurrencies, such as BTC, ETH or USDT, but also tokenized securities, which are currently rather small in volume but may soon turn into one of the most relevant asset classes globally. With a market capitalisation of more than €241 billion as of June 7, 2020 public blockchain networks[1] are securing a significant amount of value already.[2]

Against this backdrop, a sound regulatory framework for blockchain networks is among the most important political goals of today. Providers of staking infrastructure (PoSIs) are a key component of the current and future blockchain ecosystem because they safeguard the integrity of transactions. The market for PoSIs securing blockchain networks is already worth several hundred million euro. Unfortunately, entry into this emerging high-tech market in the EU and capabilities for European union-based companies to innovate are being slowed down by a lack of regulatory clarity. Countries with looser environmental and financial infrastructure oversight regulations, such as China, are already well-positioned in the value chain for providing infrastructure to Proof of Work (PoW)[3] networks. There is a lot of interest from Asian PoSIs and mining pool operators in the security- and efficiency-driven Proof of Stake (PoS) space business model, which is currently most widely explored in Europe and North America.

This paper aims to give policy makers the tools needed to craft wise regulation of blockchain infrastructure that benefits the Union and its member states, and - by proxy - humanity at large. Our goal is to achieve a level of regulation that incentivises blockchain infrastructure providers to choose the EU over competing jurisdictions, as in particular China, Russia, or the USA. This will allow the EU to shape the development of globally relevant blockchain networks according to its values. If blockchain providers were incentivised to leave the European Union due to the legal and economic attractiveness of other jurisdictions, a loss of influence over the infrastructure of these critical networks would be the consequence. It should thus be a high priority to guarantee the security and independence of these networks and to make the operation of blockchain infrastructure in Europe as attractive as possible within sensible legal boundaries.

A carefully designed, sustainable and viable regulatory approach along the principles that underlie current infrastructure regulation in the Union will enhance the soundness of blockchain networks, increase user and investor confidence and eventually promote the EU as a safe haven of reliable blockchain infrastructures and attractive site for innovative new ventures to flourish.

With larger corporations entering the space, a sound regulatory framework for PoSIs is not only highly important but also a time-sensitive issue from both the perspective of token stakers as well as infrastructure providers'. The decisions taken by regulators over the next 12-18 months are likely to shape the distribution of Staking Infrastructure Providers globally and the degree to which this business is represented within the Union. Addressing these issues as well as improving broader education on this matter would allow us to

[1] The differences between private and public blockchains are set out in Appendix 2.
[2] https://coinmarketcap.com/charts/ (07.08.2020).
[3] Terms specific to distributed ledger and blockchain technology are set out in the glossary.

secure EU leadership in the space, attract more legal business into the Union instead of losing it to off-shore jurisdictions, thus reversing capital and talent outflow.

The Staking Industry: Facts and Figures

One core element of the governance structure of public blockchains is that no central entity controls the rules and transactions of the network and safeguards its robustness against fraudulent or malicious attacks. Instead, public blockchains have a specific procedure to verify the correctness of the transactions on the network. To this end, most modern blockchains rely on the PoS security model, which provides multiple advantages over the first-generation blockchain's PoW validation for two main reasons: (1) PoS allows transaction throughput to increase by orders of magnitude, which makes these blockchains suitable for industrial adoption; (2) PoS is significantly reducing energy consumption in comparison with PoW.[4]

"Staking" has already gained economic significance with a market capitalization of €7 billion and value creation since the beginning of 2020 has been app. €245 million.[5] When considering the announced transformation of major blockchain projects - in particular Ethereum - to PoS, this industry will surpass a market capitalization of €41 billion in the next 18-24 months, despite the current COVID-19 pandemic and recession.[6] Networks must thus rely on their infrastructure to be resilient, performant and secure. PoSIs are the trusted parties whose task is to secure these networks on the technical level.

The difference between PoS and PoW lies in the business model of the companies securing the network. While the fortune of PoW "miners" is mostly depending on the capital to acquire infrastructure and proximity to cheap energy, which gives an advantage to countries like China, the business model of PoS “validators” is hardware and software innovation-, security-, and efficiency-driven, creating highly-qualified jobs in the EU. This is based on PoS industry research and innovation in novel infrastructure architectures.

Providers of staking infrastructures (PoSIs) set up and maintain hardware and IT security for other token holders. Those token holders delegate the rights to "stake" their tokens to this infrastructure and to earn staking rewards while securing and governing a PoS blockchain. Most PoS systems have sophisticated economic incentive models for agreeing on how the blockchain is maintained and preventing bad actors from manipulating the data in blocks. The PoSIs automatically receive a cut of the staking rewards paid out to the actual token holder in exchange for providing the infrastructure.

Many public blockchains are shifting from the PoW to the PoS security model. Unlike PoW, where the business model of infrastructure providers heavily relies on how much capital the infrastructure provider can deploy in the form of single-purpose hardware, the business model of PoSIs is a function of how securely and efficiently they operate.

[4] https://blog.stakingrewards.com/research-report-breaking-down-differences-between-pow-and-pos/
[5] Table 1: Current staking market capitalization and value creation
[6] Table 2: Future staking market capitalization and value creation

Proof of Stake and the Staking Infrastructure Provider Business Model

In a PoS network, just as in a PoW network, the distributed ledger (or blockchain) is simultaneously maintained over a diverse and geographically distributed network of disparate computers or servers called "nodes". The ledger contains all the transactions, denominated in the native cryptocurrency and associated assets/tokens that have ever occured in the blockchain network. Transactions are organized in the form of cryptographically linked, sequential groups of transactions called “blocks”. This is very similar to a spreadsheet of which every participant in a network holds the exact same copy and which simultaneously gets updated across the whole network.

The PoS process comes into play when a block containing new transactions is added to the chain. PoSIs are special network computers (nodes) responsible for validating new blocks and appending them to the blockchain. Hence, together with other PoSIs, they ensure the blockchain's security by monitoring its accuracy, establishing validity and guaranteeing availability. It is the PoSI's responsibility to verify that there are no irregularities in the upcoming block of transactions and to propose a block of transactions which contains only valid transactions. The PoSI who has successfully provided this service to the network has its work reassessed by its network peers and is then remunerated with "staking rewards".

These rewards are typically denominated in the native token of the blockchain the PoSI secures. Because of this reward, many PoSIs compete to add the next block. PoS systems use two main mechanisms to appoint the specific PoSI which performs this operation for the current block of transactions and ensure that this is done in an honest manner.

Two metrics are commonly used at determining who is allowed to validate the next batch of transactions: A pseudo-random lottery for selecting the next PoSI allowed to validate a transaction, and the "stake weight" of the validator for assigning block validation slots. PoSIs who have more tokens are said to have a greater "stake weight". In systems that assign block validation slots based on stake weight, the number of assigned slots is proportional to their stake weight. Selection by account balance would result in (undesirable) centralization, as the single richest member would have a permanent advantage. Instead, several different methods of selection have been devised.Many PoS blockchains use a selection process that combines these two concepts. Such a combination is called “Stake-Weighted Random Selection”, which in essence is a type of fair lottery where PoSIs can increase their odds by increasing the amount of tokens that they have "at stake".

In order to motivate PoSIs to participate honestly in the validation process, there are rewards and penalties in most PoS-models. Rewarded tokens are paid to the validators via "block rewards" (i.e. newly minted tokens by the network) as well as "transaction fees" (paid by the users of the network). In case of malicious or negligent behavior by the PoSI, such as validating two blocks at the same time or being offline for too long, the stake of a validator can be automatically forfeited in a process referred to as “slashing”.

“Slashing” is the reason why Proof of Stake networks are called Proof of Stake networks. In order to participate in securing the network and to be paid for this service, validators are required to put up collateral "stake" which can be forfeited programmatically if their actions break the programmatic rules that define the

blockchain protocol which they secure. Conversely, if PoSIs perform reliably and honestly, they are rewarded according to the amount of risk (stake) that they have on the line. As a result, running a PoSI business requires deep technical knowledge of the underlying blockchain, research into novel and suitable infrastructure architectures, setup and maintenance of secure and reliable IT infrastructure as well as the acquisition of sufficient PoS tokens to qualify as a PoSI (many networks have minimum requirements).

Delegation of Staking Rights

The right to validate and add blocks, hence to secure the validity and utility of the blockchain, is attached to every PoS token. In many PoS blockchains, token holders who want to contribute to the blockchain's security, yet do not want to act as a PoSI, can delegate these rights to a PoSI, thereby increasing the PoSI's stake. Delegating is not the same as transferring ownership. Delegators only transfer the right to stake their tokens without transferring ownership of the token itself. The original holder remains the legal owner of the tokens at all times and receives all the benefits of the staking validation. Token holders are incentivized to participate in the PoS process in order to earn rewards and to avoid the dilution of their funds due to the inflationary character of the rewards earned through staking.

The amount of rewards generated by the token holder through the PoSI's service is the ratio between the size of the holder's stake and the total stake of the PoSI. For their services, the PoSIs charge a competitive fee on the holders rewards. It is important to note that PoSIs offer their services to parties already in possession of stake-able assets which must be purchased on a token exchange. These upstream exchanges are regulated and usually adhere to KYC & AML regulations. Information with regards to the rewards, risks and characteristics of PoS networks are available through publicly accessible websites operated by third parties, whose content is not controlled by the PoSIs, thus reducing information asymmetries between the involved stakeholders.

Why Proof-of-Stake is an Improvement for Blockchains

1. **Requires Orders of Magnitude Less Energy**
   Much ink has been spilled about how "blockchains" waste energy. This is limited to systems using the Proof-of-Work security model. Since PoS doesn't require mining, the energy consumption and CO2 emission is drastically improved.
2. **Sophisticated Economic Incentives Built-in**
   For example, centralisation cartels can be prevented by improved game-theoretic design and 51% attacks can be made incredibly expensive. These characteristics are generally more difficult to implement in PoW systems.
3. **Faster Finality and Processing of Transactions**
   Finality measures how long one has to wait to be given a reasonable guarantee the transaction written in a blockchain is irreversible. For a block in a Proof-of-Work system to be considered final, a lot of time has to pass (E.g. Bitcoin around 60 minutes). Proof-of-Stake mechanisms allow much faster finality. Fast finality provides a superior user and developer experience and may be necessary for mass adoption of blockchain.
4. **Upgradeability and Built-in Governance**
   Stakeholders of many PoS networks may participate in network upgrades by evaluating, proposing, or approving amendments by on-chain-voting. Many PoS architectures have formal upgrade & self amendment mechanisms which allow networks to propose and adopt new technological

innovations or correct programming errors smoothly as they emerge. These aspects enable protocols to remain state-of-the-art long into the future. They also permit orderly upgrades to protocol in response to factors such as emerging regulation. Provisions for on-chain governance in PoS systems also allow for more stakeholders to participate directly in securing the network (in comparison to PoW which is dominated by large scale mining operations located outside the EU).

5. **Transparency**
   Nearly all PoS systems have source code and governance which is completely open and transparent. All metrics/data about staking providers are generally public and accessible to anyone through a block explorer[7].

It should be noted that PoS blockchains are an emerging technology and there is still much room for development and innovation in staking protocols. There are already many different types of PoS with each having their own benefits and drawbacks.

Evaluation of Current and Future Economic Significance of Staking

The Proof-of-Stake ecosystem is already sizable today and is expected to continue to expand with many highly anticipated networks set to launch with, or transition to, Proof-of-Stake in 2020 (examples include Ethereum, Cardano and Dfinity).

To illustrate the significance of this industry, the following analysis based on current market conditions and expected valuations of high-profile Proof-of-Stake blockchains is presented:

Blockchain Networks with Staking	**Launch Date**	**Market Capitalization** as of 07.06.2020[8]	**Value created by Staking Rewards p.a.** (based on market capitalization taken on 07.06.2020)[9]	**Staking-Reward paid**
EOS (EOS)	Q1 2018	€2,313,283,421	€40,945,116	1,77%
Stellar (XLM)	Q4 2014	€1,397,252,405	€13,972,524	1%
TRON (TRX)	Q2 2018	€1,014,167,788	€34,177,454	3,37%
NEO (NEO)	Q3 2017	€725,349,423	€13,491,499	1,86%
Tezos (XTZ)	Q2 2018	€1,802,722,455	€102,034,090	5,69%
Cosmos (ATOM)	Q1 2019	€495,090,949	€40,646,966	8,21%
TOTAL CURRENT VALUE		**€7,747,866,441**	**€245,267,649**	**3,65%**

[7] See glossary for "block explorer" definition.
[8] https://www.stakingrewards.com/assets/proof-of-stake
[9] https://www.stakingrewards.com/

Table 1: Current staking market capitalization and value creation

Blockchain Networks with Staking	**Expected Launch Date**	**Market Capitalization** as of 7/6/2020[10]
Ethereum (ETH)	Q3 2015 (PoS in 2020)	€23,499,027,895
Binance Chain (BNB)	Q2 2019 (PoS planned)	€2,380,984,998
Dfinity (DFN)	2020	€1,638,000,000 (Source)
Telegram (GRAM)	2020	€1,547,000,000 (Source)
Polkadot (DOT)	2020	€1,092,000,000 (Source)
Cardano (ADA)	Q1 2016 (PoS in 2020)	€1,950,635,137
ChainLink (LINK)	Q2 2019 (Staking in 2020)	€1,334,476,716
Future Planned PoS Network Value		**€33,442,124,746**
TOTAL VALUE (current + future)		**€41,189,991,187**

Table 2: Future staking market capitalization and value creation

For this analysis, the EBA only considered projects with an expected market cap above €250 million. In addition, there are many live Proof-of-Stake blockchains with lower valuations, e.g. Algorand (€106 million) and Terra (€116 million). Furthermore, a variety of other blockchains that will have some form of staking are in development. Many raised considerable funding from traditional venture capital investors, examples include Solana, NEAR, Ava Labs, Celo, Oasis, etc. As such, these estimates can be considered conservative.

The total value created through staking rewards in 2020 by the six largest protocols accounts for about €245 million at current market capitalization. If one assumes an average 10% commission fee charged by staking infrastructure providers for their services, the revenues of this industry would be estimated to be €24.5 million in 2020. These numbers are based on current market capitalization which may change significantly in the coming months. Additionally, some of the expected PoS launches might be delayed which would have a material impact on these estimates.

[10] CoinMarketCap

PoSIs Under the Current Regulatory and Fiscal Rules

VAT Exemption for Staking Rewards

While staking may qualify as "service for consideration" within the scope of Article 2(1)(c) of Directive 2006/112/EC (VAT Directive), it should be considered as VAT exempt pursuant to Article 135(1) of the VAT Directive.

One key "value add" that public blockchains offer is security through the decentralization of infrastructure. The networks pay infrastructure providers for their service through block rewards and transaction fees. This leads to a competitive market regarding the right to provide such infrastructure. PoSIs charge their delegators differently for their services. Delegators can choose freely to delegate their tokens to any PoSI participating in the network at any time and in any jurisdiction. The delegators' origin is usually impossible for the PoSIs to identify.

Requiring PoSIs to charge VAT on every transaction would lead to a competitive disadvantage for EU-based PoSIs who, by definition, compete on a global scale with players from every possible legal system and might even impede EU based PoSIs from successfully competing in the global staking industry. If the implementation of associated regulation isn't carefully tailored to enable Union-based competitiveness in the global staking industry, this could in turn lead to two potential outcomes: Delegators choosing non EU PoSIs and/or PoSIs moving away from the Union. Both outcomes are undesirable for the EU as well as the PoSIs since staking is a very profitable and seminal industry for the coming years.

The German Ministry of Finance (BMF) took this ruling as an opportunity to clarify follow-up questions regarding the VAT treatment of Bitcoin in relation to further transactions. With regard to mining, the relevant Decree[11] states that "miner services are non-taxable transactions. The so-called transaction fee, which the miners may receive from other users of the system, is paid voluntarily and is not directly related to the services provided by the miners. Nor is remuneration in the form of the receipt of new Bitcoin by the system itself to be regarded as remuneration for the miner services, since the miner services are not provided within the framework of a service exchange relationship. This requires the existence of an identifiable service recipient in addition to the service provider."

No Obligation for PoSIs to Apply AML/CTF rules

Staking companies should not qualify as obligated entity under Article 2(1)(g) or (h) of Directive (EU) 2015/849 (AMLD5)

Article 2(1) of the AMLD5 qualifies two services provided in connection with crypto assets as relevant for AML/CFT purposes: (1) "Providers engaged in exchange services between virtual currencies and fiat currencies" i.e. cryptocurrency exchanges and (2) "Custodian wallet providers" i.e. cryptocurrency wallet services (where the service provider holds its users' private keys). These new provisions bring legitimacy

[11] BMF Decree of 27 February 2018 - III C 3 - S 7160-b/13/10001 BStBl. 2018 I p. 316.

and clarity to the European cryptocurrency industry and counter the real risks of misuse of the technology. While we have not observed signs from financial supervisors to consider staking as a relevant service under the AMLD5, we would like to emphasise the technical characteristics of PoS networks relevant to the assessment of the application of the AMLD5, based on which we consider that PoSIs do not qualify as obligated entities:

1. Buying PoS tokens in exchange for Fiat money:
   To be able to participate in the staking process, PoS tokens of the respective network have to be purchased through a regulated exchange with respective licenses and KYC / AML5 compliance before they can participate in the process.
2. Earning staking rewards:
   Earnings through staking can only be paid out either in the native token of the PoS system or associated settlement tokens (not fiat money).
3. Selling PoS tokens in exchange for fiat money:
   Fiat conversion is only possible through regulated exchanges with respective licenses and KYC / AML5 compliance.
4. PoSIs have no control or custody over the private keys or wallets of their delegators at any point in time.
5. Due to the technical design of PoS public blockchain protocols, PoSIs can not control who uses their infrastructure and have no data regarding the origin and nature of their delegators.

Due to the above mentioned points the Staking Infrastructure Working Group assumes that the described AML5 regulations do not apply to PoSIs. A mandatory implementation of KYC measurements would lead to a competitive disadvantage for European PoSIs.

Improving Industry Standards & Customer Protection

Potential Risk Mitigation Measurements

The Staking Infrastructure Working Group is actively improving and developing industry standards. The primary objective of these measures is to provide reliable and secure infrastructure as well as keeping users informed about the risks inherent to staking. These risks include malfunctions in the blockchain software, attacks on the infrastructure and network as well as internet and power outages and finally hardware defects.

Since there are currently no definite quality criteria and certification or audit schemes for the industry, the Staking Infrastructure Working Group is currently evaluating the following optional risk mitigation measurements:

1. Accessible educational content on how these networks work and their implications on a security and economical level for users. Specifically the EBA seeks to inform stakeholders about the possible risks involved with staking.
2. General terms and conditions (voluntary):
   Clarify and define liabilities between customers and infrastructure providers.
3. ISO infrastructure certificates (voluntary):

Provide transparency and regular external audits on the security of the infrastructure provided by PoSIs.

4. Insurance:
   Protect customers and validators against potential financial losses particularly through the acquisition of a group insurance contract covering the operations of all member PoSIs.
5. European staking infrastructure provider certificate (voluntary):
   - Develop a European certificate to prove that PoSIs uphold minimum industry standards and undergo regular audits. Infrastructure Providers would thereby be able to differentiate themselves in the market on the basis of proven adherence to quality standards.
   - One proposal currently in discussion within the EBA envisions that PoSIs would sign bilateral contracts with the European Blockchain Association committing to uphold basic and specific security, and reliability practices. The EBA would in turn inspect a certain percentage of the PoSIs each year and be able to levy contractually enforceable fees for non-compliance in the event that a PoSI did not meet the standards. The PoSIs would receive a credential issued by the EBA to prove to their customers that they uphold minimum industry standards and undergo regular audits. The Certified Staking Infrastructure Providers would thereby be able to differentiate themselves in the market on the basis of proven adherence to quality standards.

The development of standards on a European level offers the opportunity to define international standards. Furthermore, it increases the overall security of public blockchain infrastructures and fosters the role of Europe as an industry-leading region. A large and diverse set of validators is critical to the security of decentralized PoS networks. The measures above are to be considered voluntary because a move to mandatory standards would increase the barriers to entry for less mature PoSIs (individuals, small entities) which would in turn shut out a large set of potential validators stakers with limited resources. At this time we don't recommend such a binding requirement as it would invariably lead to lower decentralisation and network security overall as well as the loss of many PoSIs to jurisdictions with looser regulation.

The Staking Infrastructure Working Group is interested in cooperating with national and European institutions to define such standards.

About the EBA and Staking Infrastructure Working Group

The European Blockchain Association (EBA) e.V.[12] has been established to combine, synchronize and leverage blockchain-related activities of European corporations, startups, venture capitalists, and scientific institutes. It is structured as a decentralised semi-autonomous organisation backed by a comprehensive governance model[13].

The EBA considers staking to be a fundamental topic for the future of blockchain technology as most new blockchains rely on a Proof-of-Stake security model. In order to face the problems connected with staking, the ‘Staking Working Group’ was founded by the undersigned EBA member organizations as a with the goal of addressing the needs of Staking Infrastructure Providers in a collaborative approach.

[12] https://europeanblockchainassociation.org/sample-page/structure/
[13] http://bit.ly/EBA-Governance-Process

Appendix 1: Glossary

Feel free to refer here for an extended look at PoS industry terminology:
https://www.stakingrewards.com/glossary

Active Validator Set
The active validator set refers to all validators of a network who are currently authorized to engage in the validation process.

Bakers
In the Tezos blockchain, network validators are called Bakers[14].

Block Explorer
A block explorer is a website linked to an underlying blockchain or distributed ledger node and which makes the entire history of the ledger visible, searchable and transparent to anyone with a web browser.

Block Height
Block height can be referred to as the number of a certain block. The block height states the number of blocks between the respective block and the very first block of the underlying blockchain (called "genesis block").

Block Proposer
The validator of the active validator set, who proposes the most recent block, which then has to be approved by other validators of the active set.

Block Reward
Conducting operations on a blockchain such as validating new blocks makes one eligible to receive additional, newly generated tokens of the underlying network. This has an inflationary effect on the network's native token supply.

Commission Rate
A fee charged by the Stacking Infrastructure Provider for their service. The fee is based on the staking reward paid out by the protocol.

Consensus Algorithm
Set of rules and processes that define how nodes of a decentralized network can reach an agreement on the true current state of the network.

Decentralized Network

Blockchains are a type of decentralized network, removing any centralized form of decision making thanks to various types of consensus algorithms. The nodes involved in the network interoperate and collaborate with each other to execute these consensus algorithms without the need for any central decision-making source, thus making it a decentralized network[15].

[14] **https://wheretobuytezos.com/tezos-info/what-is-baking-tezos-xtz**
[15] https://www.stakingrewards.com/glossary/decentralized-network

Delegator
Token holders who want to participate in the process, but do not run a validator node are called delegators. Delegators transfer ("delegate") the rights associated with their tokens (e.g. validating new blocks) to a validator, who performs these operations. Rewards generated through these operations are then split proportionally to everyone's stake between the validator and it's delegators.

Endorsement Rewards
In some PoS networks (e.g. Tezos), validators of the active set earn additional rewards by endorsing the most recently proposed block. Endorsing means verifying that the block was properly proposed.

Fork
Forks are additional instantiations of a live network. One has to differentiate between two different types of forks: Soft Fork & Hard Fork (both defined in this glossary) Note that forks and governance are orthogonal concepts. They may be related, but not necessarily. Forks occur at the specific point in time that a network software upgrade/change becomes widely deployed on a live network.

Governance
Governance refers to a system for designing, proposing, enforcing, and implementing changes to a blockchain network protocol irrespective of the PoS or PoW security model. Many distinct mechanisms exist which can be classified based on the level of formality in the decision making process, how binding decisions on network participants are and whether decisions are self-enforcing/executing at the level of protocol code. On-chain governance is a means of upgrading blockchain protocols using on-chain voting. This differs from off-chain governance which requires agreement of all stakeholders (core developers, node operators, miners, and users) to coordinate and agree to update their software.

With on-chain governance, anyone can propose a code change into the protocol and then token holders vote during an encoded voting period on whether or not it should be integrated. This system offers a voice to all token holders and provides an efficient way of settling disputes[16].

For illustration, consider the following examples:

- Tezos' on-chain governance is very formalised and very binding and self-enforcing. Stakeholders cast votes for or against alternative versions of the protocol software (code already implemented in a testnet) via a multi-step on-chain mechanism. When stakeholders approve changes to the node software nodes running the default clients are forced to automatically upgrade. Nodes which run customised clients need to adjust to the correct protocol hash in order to continue operating in the mainnet.[17]
- Cosmos' on-chain governance is less binding than Tezos', not self-enforcing, but fairly formalized since stakeholders vote on-chain on prose proposals (instead of testnet code). The process for adopting a prose proposal and covering that into implemented code once an on-chain vote has approved it is not specified or binding for participating PoSIs.[18]
- Bitcoin and Ethereum are examples of protocols that have a governance mechanism that is neither highly formalised nor binding as well as not being self-enforcing. Note that this doesn't mean that

[16] https://messari.io/article/on-chain-governance
[17] https://medium.com/cryptium/the-hitchhikers-guide-to-tezos-36f112662074
[18] https://medium.com/cryptium-cosmos/the-hitchhikers-guide-to-the-cosmos-37c0c4e9b8fc

there is no governance per se, it simply means that the mechanism has not been described in the actual network protocol code.

Hard Fork:
A backwards incompatible network software upgrade. Blocks created by nodes on the new protocol (post fork) are considered invalid by nodes on the old protocol (pre fork). These cause a chain-split.
Examples: Increase in block size from 10MB (old protocol) to 20MB (new protocol). Old nodes will reject blocks created by new nodes.

Nodes
The computers/servers that interact with the network via default or custom clients There are different kinds of nodes with different roles, such as archival nodes (storing the full history of the blockchain), consensus nodes (validating new blocks added to the blockchain) or seed nodes (storing network addresses to connect nodes with each other).

Nominator
In Polkadot, nominators secure the relay chain by selecting good validators and staking DOTs (the native token of the Polkadot ecosystem) [19].

Nothing-at-Stake Problem

The Nothing-At-Stake problem is a phenomenon that occurs when the validating nodes in a protocol can generate and maintain multiple forks at no cost. This problem was not an issue when all networks relied on Proof of Work, where miners had to point the hashing power to a specific chain or could only support multiple ones in parallel by increasing the hashing power (additional hardware and electricity consumption). In PoS networks, as PoSIs do not require atypical computing power to generate digital attestations, maintaining multiple forks does not come with economic restrictions. A common way of preventing the nothing-at-stake problem has been for the protocol to adopt “slashing” mechanisms, which have the purpose of disincentivizing the PoSIs to cause and maintain forks (faults known as “safety faults”).[20,21,22]

Mechanisms such as Delegated Proof-of-Stake (DPoS) have been under significant scrutiny because they suffer from such problems: Any block producer in EOS may be signing at multiple block heights using the same keys, creating and maintaining multiple histories. The EOS for instance protocol does not have in-protocol a mechanism for detecting, accounting, and penalising such faults.

Pool Staking
Many Proof of Stake Networks have specific requirements for the number of tokens required to become a validator and/or be eligible for staking. Pooling funds together with other investors for staking is similar to the concept of pooling hashing power in mining pools. This way, investors can stake amounts even under

[19] https://wiki.polkadot.network/docs/en/maintain-nominator
[20] https://medium.com/cryptium/half-baked-is-always-better-than-double-baked-what-is-at-stake-in-the-tezos-protocol-6619ce4a5f87
[21] https://medium.com/cryptium/the-hitchhikers-guide-to-tezos-36f112662074
[22] https://medium.com/cryptium-cosmos/the-hitchhikers-guide-to-the-cosmos-37c0c4e9b8fc

the minimum requirements and achieve a higher reward frequency. Validators who accept delegations/votes can be seen as Staking Pools.

PoS - Proof-of-Stake
Process to appoint the node which gets to create the next block. These nodes are called Validators in PoS based systems. Validators are chosen with regards to the amount of staked tokens attributed to them. These tokens (also referred to as "stake") are locked in the network and are comparable to a security deposit since they can be forfeited in the case of misbehavior by the validator.
The amount of staked tokens determines the likelihood of the validator being chosen to create the next block. In order to not only favor the wealthiest ones, additional methods are included in the selection process such as a pseudo-random lottery.

PoW - Proof-of-Work
Process to appoint the node which gets to create the next block. These nodes are called Miners in PoW based systems. A miner is chosen based on the fact of how quickly it can solve a computational heavy puzzle. Solving this puzzle requires a certain capital expenditure by the miner in the form of specific hardware and energy. Malicious behavior by a miner is detected by other nodes and results in the miner not receiving any compensation for his/her operations. Hence, malicious behavior results in a miner having expenses, but not being compensated for his work and thus having to bear losses.

Proof-of-X
Set of requirements or rules that determine what entities are allowed to participate in consensus, in order words, a sybil resistance mechanism.

Process of declaring the node that gets to create the next block & append it to the blockchain. A node conducting these operations gets compensated for it in the form of block rewards and transaction fees. Proof-of-X processes are used to incentivize nodes to conduct these operations in an honest manner.

Self Amendment
This is usually an on-chain voting process by which a blockchain protocol can improve itself over time utilizing a formalized process for deciding on and implementing protocol upgrades. Many PoS systems are also Self Amending.[23]

Slashing
In the case of validator misbehavior (defined individually within each protocol), the total stake of the validator (Own Stake/security deposits and sometimes even Delegated Stake) gets slashed, meaning that a certain percentage of tokens is burned or distributed to a treasury. This is designed to incentivize security, availability and governance participation as well as prevent double-spend or spam attacks[24].

Staked Tokens / Stake
Rights of **t**okens that are assigned to a validator. This can either be the tokens of the validator itself and/or the tokens of delegators. Staked tokens are often referred to as “stake”.

Staking

[23] https://learn.tqgroup.io/files/self-amendment.html#introduction
[24] https://www.stakingrewards.com/glossary/slashing

Staking is a process where a holder of a Proof-of-Stake (PoS) crypto asset locks their funds in order to validate transactions. They are then compensated via protocol level inflation proportional to the amount staked as a percentage of the overall amount being staked. Staking is designed as an alternative to Proof-of-Work that maintains the long-term security and reliability of a protocol[25].

Staking-as-a-Service
Staking-as-a-Service exists because staking can be a complex process that the everyday token holder might not want to perform. To participate in the inflation rewards, users can delegate their funds to corporations that run validating nodes who then stake user funds. Inflationary rewards are returned to the holders with a fee taken by the service provider[26].

Staking-Infrastructure-Providers (**PoSIs**)
PoSIs are specific nodes that provide the technical infrastructure and maintenance required by the respective network.
In addition PoSIs perform operations on the underlying network in order to receive rewards & transaction fees.
PoSIs provide services such as acting upon voting and validation rights. PoSIs hold these rights either through delegation by their clients and/or through their own token holdings.

Stake Weight
Stake weight refers to the amount of tokens currently staked with a particular validator. In the context of on-chain governance this may also be expressed as "voting power". This weight is a function of the total amount of tokens that are attributed to a validator (their own tokens plus those delegated to them by others). The more tokens that are attributed to a validator, the higher the validators stake weight and ultimately the higher his/her voting power. In many blockchains, stake weight is an important factor in determining which validator is allowed to validate the next block.

Stake-Weighted Random Selection
In order to prevent networks from being solely run by validators with the highest weight, randomization is added to the validator selection. It is analogous to a lottery wheel: while names are drawn randomly, validators with a higher weight get to add more tickets with their name on it. This ultimately increases the chance to get chosen as a validator with a high stake weight, while keeping things fair for smaller validators who still have a chance to get chosen.

Soft Fork
A backwards compatible network software upgrade. Nodes on the old protocol (pre fork) consider blocks created by nodes on the new protocol (post fork) valid. Blocks created by nodes on the old protocol (pre fork) may not be considered valid by nodes on the new protocol (post fork) though. These don't cause a chain-split. Example: Decrease in block size from 10MB (old protocol) to 5MB (new protocol). Old nodes will accept blocks created by new nodes.

[25] https://messari.io/article/staking-as-a-service
[26] https://messari.io/article/staking-as-a-service

Sybil Attack
A Sybil Attack happens in case one participant of the network creates multiple nodes in order to gain an absolute majority of the network's voting power.

Transaction Fee
Using decentralized networks, that is sending transactions, incurs fees levied on to the user. These fees prevent the network from being spammed and are used to compensate validators for their work.

Validator
Validators are special nodes in PoS based networks. They provide the technical infrastructure and maintenance required by the respective network. Validators propose and validate new blocks and actively participate in the network's governance by either submitting or voting on new proposals (depending on network).

51% attack
A 51% attack occurs if a single node or colluding nodes control more than 51% of the network. This would result in these nodes controlling who composes & validates new blocks.

Appendix 2: PoS Technical Concepts

Consensus Mechanisms

The distinction between sybil resistance and consensus mechanism was not needed until the first public Proof-of-Stake networks were launched, prior to which the vast majority of networks relied on Proof-of-Work, where the notion of consensus was implied. However, the landscape of public blockchains started to shift in mid 2018, when the first Proof-of-Stake networks launched. Furthermore, a substantial set of new projects have announced plans to follow an architectural path that involves Proof-of-Stake.

Consensus is defined as the rules through which participants in a trustless network agree on the latest state of a set of values, such as which is the latest valid block. At the time of writing, the two most prominent families of consensus algorithms are Nakamoto Consensus (aka longest-chain consensus) and Byzantine Fault Tolerant Consensus (BFT). The main idea behind nakamoto consensus algorithms is that the chain with the largest accumulated amount of *work*, in this case hashing power or consumed computing power, is the canonical one. On the other hand, BFT consensus algorithms consider a set of values final, as soon as ⅔ of the participants have provided a cryptographic attestation on the validity of the value. Many PoS systems rely on a variety of consensus mechanisms which solve the Byzantine generals problem and thus can be considered Byzantine Fault Tolerant.[27]

[27] https://en.wikipedia.org/wiki/Byzantine_fault

Differences Between Private and Public Blockchains

Blockchain systems can be structured as “public” or “private”. The same distinction is made by using the terms “permissionless” and “permissioned”.[28] The difference between the two concepts lies in the way users may obtain rights on the respective blockchain. There are three rights that can be exercised on blockchains:

1. read: access data on blockchain
2. write: submit transactions to blockchain
3. commit: run consensus protocol and update state of network with new blocks

Blockchains are mainly distinguished by the right to *read* (a). While anyone can read data on public blockchains, similar to the internet, private blockchains work like intranets in the sense that only authorized entities enjoy access/reading rights.

Another difference lies in the right to execute “write” (b) and “commit” (c) operations on the blockchain. A "permissionless" blockchain has no restrictions for either of the two operations, while in a "permissioned" blockchain only authorized entities may perform "write" and "commit" actions.

In certain “permissioned” blockchains, the right to “write” and “commit*”* are separated from each other. In Public permissioned blockchains only a defined set of entities are allowed to “commit” blocks to the blockchain. Still, anybody has the right to *"read"* and execute transactions (“write”) on the network.

	read	write	commit
Public permissionless	anyone	anyone	anyone
Public permissioned	anyone	anyone or authorised entities	authorised entities
Private permissioned	authorised entities	authorised entities	authorised entities

While it is likely that both private and public blockchains will coexist in the future, the main drivers for innovation and disruption will be public blockchains, due to their open and permissionless nature.[29] However, in areas considered sensitive due to their overall economic or other relevance, discussions are ongoing as to whether public blockchains provide sufficient robustness given the relevance of the processes carried out on the blockchain.

Incentives & Penalties

Validators receive a portion of the annual inflation of the network, which is proportional to their voting power or weight among the global amount staked. This is to incentivise the honest and secure participation of validators in the network.

[28] S. De Angelis,G. Zanfino, L. Aniello, F. Lombardi, V. Sassone, Blockchain and cybersecurity: a taxonomic approach (University Southampton October 2019), 3-4
[29] Catalini, C., & Gans, J. (2016). Some simple economics of the blockchain (available here).

On the other hand, most protocols have many penalty mechanisms that aim to prevent misbehaviour or attacks on the blockchain. The most common issue is the nothing-at-stake attack. The nothing-at-stake problem is present in some Proof-of-Stake protocols, where participants are able to cause and maintain contentious forks (or history versions) at no cost.

In the traditional world dominated by Proof-of-Work networks, this was not possible as miners had to point the hashing power to a specific fork: should they wish to support multiple forks, they would have to scale their resources horizontally. However, in Proof-of-Stake, the computational power required to generate cryptographic attestations is not exorbitant. This results in low costs for PoSIs to cause and maintain different competing network versions. In order to disincentivise this behavior, as it diminishes the security of the network, the protocols have features to detect a fault, attribute it, and to issue a penalty – generally resulting in a loss of the assets placed as collateral. The most common misbehaviour is the signing of two different blocks at the same height. The punitive feature is commonly known as *slashing* and *slashing conditions*.[30][31]

The PoSI offers the client a service in which the client delegates validation and voting rights derived from virtual currencies to the PoSI. The PoSI uses these rights in accordance with the technical specification of the respective virtual currency in order to obtain an opportunity to perform operations for the underlying blockchain in proportion to the number of rights.

The virtual currencies are not transferred to the PoSI, but only the rights are assigned. The operations are based on the technical specifications of the respective virtual currency and are performed in a defined period. These operations include, for example, creating new blocks or their endorsement. The PoSI will receive revenue in the form of tokens of the respective virtual currency ("reward") for the performance of such operations. The PoSI either receives the full reward and then pays its client proportionately for their rights or the clients receive their reward directly from the blockchain. In both cases, the PoSI receives a remuneration. The business model therefore consists of two pillars of income: the reward derived from the own stake and the remuneration from clients.

Peer Selection Mechanism

While Proof-of-Stake mechanisms set the requirements for peers to become eligible to participate in consensus, they also describe the process and times in which the eligible peers are able to sign and produce blocks. There might be differences in the algorithm but the implication in practice is that validators or peers' likelihood of being selected or receiving slots is proportional to their voting power or staked weight.

For example, if a validator represents 2% of the global stake on the network, in the long run, this results in the validator receiving the equivalent to 2% of the signing or block production slots.
Some types of PoS allow for nodes with more stake to have more votes on the validity of the blocks.

---

30 https://medium.com/cryptium/half-baked-is-always-better-than-double-baked-what-is-at-stake-in-the-tezos-protocol-6619ce4a5f87

31 https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ#what-is-proof-of-stake

Sybil Resistance

In the context of blockchain and distributed systems, Proof-of-Stake (PoS) describes a family of sybil resistance mechanisms (security model). It sets the rules and requirements for peers in a trustless network to be eligible to participate in consensus. At the time of writing, Proof-of-Work and Proof-of-Stake are the two most prominent families. In Proof-of-Work, for participants to become eligible to produce blocks, they must compete with other participants in solving a mathematical puzzle. In Proof-of-Stake, peers become eligible to participate in consensus if a certain amount of wealth or value is placed as a collateral, which can be lost, should the participant deviate from the rules of the protocol. In return, participants are rewarded with a portion of the annual inflation of the network that is proportional to the stake they represent in relation to the global amount at stake.

Appendix 3: Working Group Members

Representative	Company	Company Description	Staked Tokens
Hendrik Hofstadt	Certus.One	DLT validator, Staking Infrastructure Provider.	7.277.166 ATOM 12.143.066 IRIS 11.430.583 LUNA (Source) _____ Total: 14.634.502 €
Peter van Mourik	ChainLayer	Staking Infrastructure Provider (7M XTZ Baker that is shutting down).	599.876 ATOM 1.223.387 LUNA 7.039.863 IRIS 4.636.928 WAN 2.156.193 KAVA (Source) _____ Total: 2.789.452€
Brian Crain & Felix Lutsch	Chorus One	Builds core infrastructure for blockchain protocols Staking Infrastructure Provider.	4.831.324 ATOM (Source) 6.191.409 LUNA (Source) 2.475.995 KAVA (Source) _____ Total: 10.521.200 €
Adrian Brink & Awa Sun Yin	Cryptium Labs	Swiss-made security oriented Proof-of-Stake infrastructure provider operated by protocol	23.001.263 XTZ (Source) 1.564.595 ATOM (Source) 11.261.250 IRIS (Source) _____

		researchers and engineers	Total: 36.544.412 €
Aurel Iancu	Dokia Capital	Staking Infrastructure provider	23.188.635 ATOM (Source) 20.272.352 IRIS (Source) 3.269.187 KAVA (Source) 7.195.711 LUNA (Source _____ Total: 43.959.275 €
Andrew Paulicek	HappyTezos	Staking Infrastructure Provider	8.753.474 XTZ (Source) _____ Total: 12.804.581 €
Kevin Leuthardt	KSquared GmbH	Startup (tax) advisor	-
Anja Raden	Legal Garage	DLT Lawyer	-
Daniel Liebert & Carlo van Driesten	StakeNow	Professional staking services for private and institutional clients.	2.127.596 XTZ (Source) _____ Total: 3.112.247 €
Julius Schmidt & Robert Dörzbach	Staking Facilities	Staking Infrastructure Provider	2.024.309 ATOM 2.075.127 XTZ 7.820.542 AION (Source) _____ Total: 7.081.248 €
Rebecca Johnson	Datarella GmbH	Blockchain solutions Provider	-
Gianpaolo Eramo	Staking Team	Staking-as-a-service company operating secure and performant block validation nodes. Staking Infrastructure Provider	6.456.700 XTZ (Source1-Source2) 58.138.829 IOTX (Source) 1.165.061 ICX (Source) 53.663.132 ONE (Source) _____ Total: 17.597.919 €
Gleb Dudka, Andreas Dittrich	T-Systems (Deutsche Telekom)	Building up staking-as-a-service offering. Europe's largest Telco.	Not yet live
Sebastian Burkhardt	-	Junior Lawyer with focus on DLT	-
Total Economic Value Staked as of 08.06.2020			**Total: 141.436.400 €**