DIGITAL CURRENCIES GOVERNANCE GROUP

Decentralized finance and the evolution of staking

A Digital Currencies Governance Group Whitepaper

2024

DIGITAL CURRENCIES GOVERNANCE GROUP

Introduction

PREPARED BY
Martinho Lucas Pires

Decentralized Finance (DeFi) proposes to be the new architecture of the financial sector, by setting up automated applications running in protocols based distributed ledger technology allowing for the provision of financial services (such as lending, collateralization, custody, among others) and ancillary activities to said services (such as settlement and redemption). Key to the success of DeFi is the liquidity available in those protocols and the security of the distributed ledger (or blockchain) that supports the protocol.

Staking is essential to both security and liquidity of DeFi, although its concept is subject to some confusion that can harm its use and success. This paper discusses the role of staking in decentralized finance, its characteristics and risks, and the challenges staking poses from a regulatory policy perspective.

Staking: a functional definition

Understanding Blockchain Technology

Distributed ledger technologies such as blockchain securely and transparently store data across a network of computers by having blocks contain a list of transactions, and then organizing and linking blocks chronologically to form a chain. Permissionless blockchains, which account for most protocols used in DeFi, are decentralised, meaning that they run not only in separate and independent nodes, but are also updated and managed ("validated") by different participants in the network. Therefore, no single entity has control over the entire network, which enhances both security and transparency, since any attempt to alter the data or the functioning of the protocol would require consensus from the network's validators and users. The distributed nature of the blockchain also means that there is no single point of failure, and if one computer on the network goes down, the others can continue to operate as normal.

Consensus Mechanisms

For a decentralized blockchain to work properly it must have in place a consensus mechanism. Consensus mechanism can be described as the methods through which a protocol validates the insertion of new information in the network. This activity is performed by different actors of the network, according to the rules set out in the protocol's code. The purpose of consensus' mechanisms is to combine functional efficiency of the network while maintaining equilibrium among its participants, so that no participant can have more validating power than other participants and, consequently, jeopardize the network's decentralized basis.

The consensus mechanism of the Bitcoin network and of several other protocols – such as, originally, the Ethereum network – was the proof of work concept (or PoW). In a PoW network, those participating in the validation process (also known as "mining" – which, in turn, makes the validators the "miners") are in a competition to solve a mathematical puzzle. Once a miner solves the puzzle, it will create a block and insert it into the network, and the process will restart once again. Mining of a block also generates new Bitcoin, which is awarded to the successful miner and thus serves as a powerful economic incentive for making the network function and to keep it secure. PoW depends heavily on computing power, which leads to more energy consumption to support the processing units used in the mining process and makes the network subject to attacks from miners that can harness more than 51% of computing power. The significant environmental impact of PoW has led to negative scrutiny by policy makers and activists.

More important for our topic is the other consensus mechanism known as Proof of Stake (or PoS), which is adopted by most of the largest networks by market cap (like Solana, Cardano, Avalanche…), including, since 2022, the Ethereum network. PoS networks requires validators to commit an amount of the blockchain's native assets to the network as collateral. Only then can they participate in validating activities, such as block creation, verification, finalization and other technical functions. Validators earn rewards, in the same asset, in return for committing the tokens to the protocol. Usually, there is a minimum portion to commit, the amount being defined in the protocol's code – for example, 32 ETH is the minimum to become a validator in the Ethereum network.

Therefore, instead of computing power, a PoS system puts the emphasis on the commitment that a validator makes to the network through its tokens.

The number of tokens held, the duration of the holding and other factors may play a part, depending on the protocol's code, in allowing a validator the opportunity to participate in technical activities related to the protocol. To control a majority of the network it is necessary to topple the amount locked in staking – consequently, the value is staked in the network, the safer it is from an attack. Furthermore, PoS is less energy-intensive than PoW, as it does not require computational power, thereby reducing environmental impact.

The staked amount is locked in the network and can be released at the time of request or after an unlocking period. If an actor stakes an amount in the network, and then proceeds to act against the rules of the protocol, its stake can be blocked and kept by the network itself. This is an incentive to compliance with protocol rules that adds up to the security that staking aims to provide to decentralized networks.

In sum, staking can be defined, in line with the best practices provided by the Proof of Stake Alliance and the International Association for Trusted Blockchain Applications, as the method of joining and acting in a PoS consensus mechanism through the commitment of a protocol's native tokens to the issuing network[1].

[1] INATBA and POSA

Staking in DeFi

Staking brings liquidity and security to DeFi – the former, by enabling the issuance of new tokens that can be used in the market, and the latter, by safeguarding a network against external attacks. It is an activity that can be performed individually, by token holders, directly with the PoS protocol, or collectively, through a pool, or performed indirectly via a staking service provider.

There are different types of staking practices and services in DeFi, which makes a taxonomy necessary to understand the technical and economic variety available.

Types of staking

DIRECT V. INDIRECT STAKING

One distinction concerns the degree of technical connection of the participant (the token holder) with the network, if it is direct (no intermediary) or indirect (through an intermediary). In the first case, the token holder stakes the tokens directly with the network and participates in the consensus mechanism. In the second case, the token holder stakes the tokens with a third-party node that will participate in the consensus mechanism on its behalf. Hence, in the first case, the token holder is a validator, while in the second case it commits its tokens to a validator that shall participate in the consensus mechanism.

Indirect staking is usually called "delegate proof of staking" and it is a form of allowing smaller stakeholders to participate, albeit indirectly, in the validation process of the network, thus enhancing collective commitment to the protection of the blockchain. Most PoS networks allow for both systems to co-exist or opt for the delegated proof of staking mechanism, such as Ethereum, Cardano and Solana. In this case, validators provide a staking service to token holders, who remain – as in direct staking – owners of their respective tokens and entitled to a reward proportional to its holdings.

INDIVIDUAL V. COLLECTIVE STAKING: DIRECT STAKING V. STAKING POOLS

Another distinction concerns the structure of staking. In one case, staking is a sole effort, either executed directly or indirectly (through a staking service provider) by an individual in the network, while in the other case staking is a collective effort, exercised by many token holders that pool their assets together to be able to participate in the validation process and distribute rewards. This form of collective enterprise is called a staking pool – for example, in delegated proof of staking networks such as Cardano, token holders commit their staking to the pool of a specific validator, that earns a fee of the validation rewards for managing such pool.

CUSTODIAL AND NON-CUSTODIAL STAKING

This distinction concerns also the technical structure of staking. Custodial staking is a service provided in which the token holder deposits its tokens with an entity that shall stake the latter on behalf of the former. They are usually offered by exchanges and trading platforms. Such custody entails a transfer of ownership of the tokens from the holder to the custodian, in exchange for the distribution of the rewards of the protocols and assumption of the risk of executing a staking service. The custodian also charges a fee that is deducted from the staking rewards. Differently, in non-custodial staking services, the user connects to the staking provider through its non-custodial wallet – the service provider is the developer of an application allowing the token holder to stake its tokens with a validator node or with the network's structure. Suffice to say that in non-custodial staking services there is no transfer of ownership and no fee to be paid.

RE-STAKING AND LIQUID STAKING

When a token holder commits its tokens to staking, it is contributing to the network's security. Re-staking service providers aim to allow token holders to allocate their staked tokens (or liquid representations of the tokens) to other protocols and applications. The aim is to increase, through this redistribution, the security of second and third protocol layers – blockchain networks built on top of a layer one. Examples of re-staking services are EigenLayer in the Ethereum network and Picasso in the Solana Network, in which token holders can re-stake their Ethereum or Solana in Actively Validated Services (AVSs) that support the security of other protocols.

Re-staking is a new development that is yet to be fully implemented in the market. At a much more developed stage is liquid staking. As the name suggests, the aim of liquid staking is not so much security, as in the case of re-staking (although, as discussed above, liquid staking tokens can be issued as liquid re-staking tokens and serve that purpose too) but liquidity. The purpose of liquid staking is to provide token holders that commit their tokens with a token-alternative (a derivative of the staked asset) to use in other DeFi protocols to generate yields or rewards. Famous platforms providing this service are Lido and StakeDAO, that issue derivative versions of native tokens (for example, stETH) that can be used for trading or yield generation in liquidity pools on other protocols, such as CurveDAO.

Activities that are often confused with staking

There are other activities and services in DeFi that are often called staking, although they are different from staking as defined by the best practices in this field, and therefore different than the definition this paper has adopted. The key distinctive element has to do with the disconnection between the deposit of tokens with a custodian or program and the participation in the consensus mechanism of a PoS protocol in these activities. It is essential, to be considered staking, that the deposit is done in the context of a validation process in a blockchain.[2]

Earn programs

Earn programs are services, usually provided by exchanges or custodians, in which users deposit tokens with the service provider and receive interest in the form of more tokens or other assets. Such deposits are used by custodians to support their activities, such as lending or staking in protocols. In earning programs, there is no connection between the deposit of tokens and participation in the consensus mechanism of a PoS network, even if the rewards are paid in the same token as the one staked.

Yield farming

Yield farming concerns participation in DeFi protocols by becoming a liquidity provider (LP). A token holder deposits its tokens in a liquidity pool, a vault or other application to generate more liquidity and, with that, receive rewards in the form of the same token or other tokens, based on their annual percentage rate. This is tool on which decentralized exchanges (also known as DEXs) rely heavily to operate without intermediaries. However, like in earn programs, provision of liquidity is not associated with participation in the consensus mechanism and does not add to a PoS network's validation process. As much, it provides liquidity balance for DEXs, but it is not part of a consensus mechanism.

Crypto lending

In crypto lending, there is a traditional lending operation by which someone deposits tokens, either as collateral to borrow from a protocol or as liquidity for the protocol to lend the tokens to a third party. Again, this is a commercial service provided by a decentralized network that does not concern the consensus mechanism of a PoS network.

[2] That is why the POSA suggests the use of expressions such as "consensus staking" to distinguish staking from activities that may be technically similar but functionally different.

Importance

There are three ways in which staking is an essential tool for DeFi.

The first concerns staking as a tool for supporting the security and decentralization of a blockchain protocol. As discussed, it is through staking that the network remains decentralized and protected from malicious attacks affecting the ledger and its constitution. In this sense, staking serves a technical safeguard function. If a validator acts maliciously, its stake can be taken by the network, which is another incentive for complying with the protocol rules.

The second way in which staking is important for DeFi concerns not only its role as a technical component of the protocol's functioning, but how its role as a governance tool. Decentralized networks are subject to complex governance arrangements in which a variety of stakeholders with different and, sometimes, competing interests – nodes running the ledger, validators, developers, investors and others – participate.

In PoW networks, the amount of computing power is a crucial element in determining the "corporate" or "political" power in governance discussions concerning protocol maintenance or updates[3]. In PoS networks, it is the number of native tokens that are staked that end up defining the corporate power of validators and investors, by distributing and weighting voting power in the decision-making processes related to protocol governance.

In this governance sense, staking is seen also as commitment by the validators to the network and a way to call for their participation in protocol decision-making through economic incentives, since the more tokens are staked the more token rewards (and, hence, votes) validators and delegators will receive. By differentiating voting power among staked contributions, PoS systems invariably acknowledge the importance of the economic investment made by validators in the network. Some decentralized networks only allow validators to vote if they lock their native tokens and receive governance tokens. This is the case, for example, of CurveDAO.

[3] See the blocksize wars and the role it played on Bitcoin, but also other issues, such as, for example, love.

Besides governance and security, staking plays an important role in the generation of liquidity. Staking is a process within consensus mechanisms, that are not only about security and governance but also – given the economic game-theory logic that underpins decentralized networks and their structures – about minting the native tokens of the network. The tokens may have a value due to their market utility (for example, because they allow for governance participation) but one part of said value is connected to their staking potential and the consequent capacity of unlocking more tokens (therefore, increasing token circulation).

A tokenomics problem with liquidity in PoS concerns inflation. The more tokens are generated, the more supply there is in the market. There is, then, an inflationary character to staking, that can affect the annual percentage rate of staking rewards. One way to control this inflation is by enabling the burning of tokens, which allows for the management of issuance. Another way is to incentivize the staking and locking of at least part of newly issued tokens in the network and locked. This puts tokens out of circulation and can help reduce inflationary levels of PoS systems.

Staking is also important for DeFi since it allows for the creation of new tokens and new forms of liquidity and market generation, through re-staking and liquid staking. The secondary market for liquid staking tokens, propelled by platforms such as Lido and Curve, together with DEXs such as Uniswap, enables validators and delegators access to new rewards and participation in different networks, which can also increase the security, participation and commitment to an entire decentralized ecosystem.

Risks

Although central to PoS networks, staking poses certain risks for participants in blockchain and, in certain cases, to an entire ecosystem and market. These risks have to do with the technology aspects of staking, as well as with its governance and liquidity elements.

Technical risks

Staking poses the same type of technical risks that other technological applications do. Therefore, risk considerations should be assessed by considering the programming of the staking platform, e.g. the smart contracts used – either by the main network or by applications providing staking services or enabling delegated staking. Security breaches, bugs, and other programming malfunctions may facilitate exploitation by malicious actors and increase the possibility of external attacks.

Liquidity risks

Staking can significantly affect liquidity in the event of a market downturn. If the tokens are locked, it is not possible for token holders to retrieve and sell them in the market to ease their losses and adapt to shifts in market trends, leading to impermanent losses. This in turn can generate market risk from contagion of lost positions to other safer assets.

Governance risks

Staking can be problematic from a governance perspective. One of the main critiques to PoS systems concerns centralization risks. Validators could compete for voting power by acquiring more tokens or by congregating different delegated pools to establish voting blocs through their combined stake. The case of Steem – where two thirds of governance tokens were acquired by another protocol that, in fact, attempted to take over the protocol – is an example of how this can lead to drastic changes in a blockchain.

Delegation risks

In the case of delegated staking, there may be counterparty risk given that tokens are locked with a validator that manages the delegated pool and that the delegator does not control. If the validator performs an invalid function and is “slashed” (penalized), delegators may lose their tokens, and if the validator’s node is attacked or down it may also affect the position of delegators. In terms of governance, delegators may also be used as support for certain validators.

Re-staking and liquid staking risks

Re-staking and liquid staking pose the same risks – technical, political, delegated – than normal staking, and increase the risk of general staking. This is so because new staking layers are created on top of the first, which makes both layers (the first and the second) permeable to each other’s risks.

Regulatory challenges

Staking poses challenges from a regulatory and policy perspective.

The main regulatory challenge concerns the treatment of staking under existing rules and laws, be them specific to crypto-assets or not. As discussed, staking concerns a technical activity for securing a blockchain network, enabling the validation of blocks and the minting of new tokens. This activity is central to the development of a decentralized network. In this sense, staking is not subject to any kind of specific regulation – in the EU, according to recital 26) of the Regulation 1114/2023 (Market in Cryptoassets Regulation or MiCAR), tokens generated by staking (in the context of a consensus mechanism) are outside of the regulatory perimeter.

The problem arrives with the provision of remunerated staking services by intermediaries. In this case, staking services can be confused with other services (regulated under MiCA), such as custody of crypto-assets. It is unclear, for example, if assets in custody can be used for staking, and if so, under what rules. In other ways, staking through staking pools can also be seen as a form of collective investment contracts. More problematic is the provision of staking services by intermediaries that manage the tokens and the rewards – what is known as staking programmes – and that can be considered an investment service. That, at least, is the understanding in the United States of American according to its Securities and Exchange Commission, as seen in the case of SEC v. Kraken Exchange. In this situation, staking service providers that work as intermediaries may be considered financial service providers and require a new form of license.

There is also the challenge of distinguishing between the provision of a staking service and a similar activity such as earn programs, crypto lending and yield farming. As discussed above, these activities are not staking because they are unrelated to the validation and development of a blockchain protocol. These services merely generate rewards for its clients in exchange for the possibility to use their tokens for other purposes – such as lending, or liquidity provision.

Here, the exception of MiCAR, for example, is no longer valid but there are also unclear regulations to apply to these services – again, custody rules do not specify whether the custodian can or not stake the tokens, there are no specific rules for crypto lending, and yield farming may fall under the fully decentralized exception. In the case of e-money tokens and asset-referenced tokens there is a specific prohibition, under MiCAR, for crypto service providers to pay interest.

Another challenge that staking poses, expertly identified by a group of European scholars, concerns its use as a governance tool under the context of decentralized activity. In the EU, but also in other jurisdictions, the exercise of an activity in a manner that is considered "fully decentralized" exempts the service provider from regulatory scrutiny. The problem, then, is to understand what fully decentralized means (an issue that is being widely discussed in the EU and its Member States). Given the centralization risk of PoS systems, staking may be used by few validators to fully control the network, either directly or indirectly, while claiming that the network is fully decentralized and not controlled by any single group or entity.

Finally, there is also the problem of whether re-staking and liquid staking service providers are not offering financial services or selling financial products, since liquid staking tokens can be considered as a form of derivative that can be used for trading and investment. In the case of re-staking, since its focus is to guarantee the security of other PoS protocols built on top of other PoS layers, the situation may be clearer from a regulatory perspective. Still, questions remain.

Considerations for Policymakers

In order to allow for the development of PoS networks, to harness the benefits of blockchain and decentralized governance, and to protect the security and stability of such networks (thus reducing market risk and spillover effects in DeFi markets), it is necessary that policymakers consider the challenges posed by staking.

Clarity of Regulatory Frameworks

First, it is recommended that staking is subject to clear rules and regulations. This requires, first of all, that a clear understanding and definition, along the lines used by market best practices, is adopted by regulators and policymakers. In this way, there can be a clear distinction between staking and other forms of service provision, such as crypto deposits or crypto lending, and a better determination of applicable rules to each activity.

It is also important that staking is clearly cut out from rules regarding investment contracts and financial services, given that it is but a technical activity to generate protocol security and validity. While in the EU, for example, there is already an exemption under MiCAr for tokens generated through this process (as long as these tokens are not asset-referenced tokens nor electronic money tokens), more rules are necessary to clarify the boundaries of delegated staking through staking pools and provision of intermediation staking services or programs. Importantly, consideration should be given to the correlation between the rewards of delegators and the gains of validators or intermediaries for asserting that a financial contract exists.

From a tax perspective, it would also be important to understand how staking rewards should be treated, given their specific character as part of a validating activity. The Law Commission has published some reflections in the UK, and some Member States have adopted tax rules that incentivize long-term staking by exempting stakers from capital gains taxation if they hold to their tokens for a certain period of time.

Also, it should be clear whether staking tokens are subject to financial regulations, since they provide holders with governance rights (voting, management, rewards…) that may be like other instruments, such as shares. This is part of a wider discussion concerning the regulation of decentralized governance and decentralized autonomous organizations and where to draw the line between the use of a decentralized platform and the provision of a service through a digital platform, structured as a blockchain but managed by an identifiable group of people. This discussion will be central to the success of DeFi and should not be taken lightly nor at haste, given the complexities surrounding this market.

It is recommended that policymakers get to know the technology and its applications, understanding their benefits from a structural perspective and also the way in which they allow for new products and services in finance, which can propel the development of capital markets and free liquidity for public and private investment.

Private and public participation in staking

Given the potential of PoS networks and blockchain in general, as a form of public goods-like infrastructure, it would be important that policymakers and regulators attempt to understand and use the technology to comprehend its benefits of security and effectiveness in transacting value.

Although several initiatives are taking place around the world, it would be important to enable and incentivize the participation of “traditional finance” and public institutions in the DeFi ecosystem. Becoming a validator can be a way to participate in ecosystems and open the use of these networks for a broader audience. Delegation can also be a system, through staking pools or via intermediaries, that can also unlock the benefits of DeFi to more traditional institutions and bring crypto markets to mainstream adoption.

Conclusion

Staking is a fundamental component in the DeFi ecosystem, playing a crucial role in ensuring the security and stability of blockchain networks. By allowing users to lock their assets in a protocol to validate transactions and secure the network, staking not only fosters greater decentralization but also mitigates risks associated with malicious activities. As more participants engage in staking, the network's robustness increases, creating a more trustworthy and efficient financial system.

It is important to note, however, that staking poses challenges from a regulatory perspective due to the complexity and variety of technical and commercial arrangements on this. The current regulatory landscape is fragmented and often unclear. Consistent regulatory guidelines would provide the necessary framework to ensure compliance and protect investors, fostering an environment where innovation can thrive.

By bridging the gap between DeFi and traditional finance, regulatory clarity can unlock new opportunities for collaboration, driving the growth of a more inclusive and innovative financial ecosystem. This synergy between DeFi and traditional finance, underpinned by well-defined regulations, can lead to a more robust, secure, and accessible global financial system.

DIGITAL CURRENCIES GOVERNANCE GROUP

2024

Thank you!

Thank you for taking the time to read this report. If you have any questions or would like to discuss our findings further, please do not hesitate to reach out to us.

info@dcgg.eu

www.dcgg.eu

European Transparency Register Number: 658658339474-38