Decentralisation

Abstract

A system such as Bitcoin operates using a proof-of-work-based consensus mechanism that many individuals have falsely claimed to limit the ability for the system to scale. As a result, alternative proposals based on proof of stake are misleadingly being promoted as scaling solutions. Yet, it will be demonstrated that proof of stake is not a scaling solution but rather a means of reintroducing ownership and equity control through a back-door creation of a digital bearer share. Here, an equity system based on anonymous holdings is constructed that allows the digital control of a corporate entity outside the provisions of regulatory controls.

Craig Wright

Keywords: decentralisation, proof of stake, equity, Howey test

Decentralisation

A methodology of decentralisation that was never a part of Bitcoin has evolved in the last decade. The OED defines decentralisation as the process of putting something into smaller parts. Consequently, we can say that the majority of public companies is decentralised. Here, the control of the organisation is split between multiple shareholders. The equity stake provides voting rights, and acts to allow different entities to have different levels of control based on the different types of share offers. Ishiguro and Yamada, in a study of decentralisation, demonstrated how more distributed ownership of companies leads to lower rates of CEO overconfidence and lower rates of tax avoidance.[1]

Consequently, a decentralised ownership structure has benefits when considering the corporate agency in management. Yet, as with the political problems from too many fractional parties, overly loose control of corporations also leads to problems. In the management and control of corporations, the legislative structures that have developed over the past centuries have created accounting and reporting controls that, while not perfect, limit the ability of corporate executives to defraud shareholders and investors. The distinction in the blockchain world is an argument that blockchain warrants a full return to bearer-share equity holdings.

Of note, one of the primary systems developed for this is called proof of stake (PoS). In a proof-of-stake system, owners of digital assets maintain the right to vote on the system and be paid. This payment is probabilistic and is related to the locking up of tokens for some time. In this manner, the system creates a multilevel structure where those who have more money and can lock away assets are rewarded over those with less. However, people with lower levels of investment are unable to lock away their money due to the need to pay for goods and services that are needed for daily survival.

The main benefit being touted for a proof-of-stake system over one using proof of work (PoW) relates to scalability. But, such claims are deceptive. The only measurement of scale that matters relates to the number of transactions that can be processed per second. Both PoS and PoW relate to the consensus methodology used by the system (the nodes) in forming an agreement and the method used to exchange information. In each case, PoW and PoS have

[1] Takehide Ishiguro and Akihiro Yamada, “Overconfident CEOs, Decentralisation, and Tax Aggressiveness: Evidence from Japan,” *International Journal of Economics and Accounting* 10, no. 2 (2021): 181–203.

no relationship to the number of transactions processed or the methodology to exchange these. For example, the hash puzzle solution in Bitcoin can be solved using a separate system that only sees the block header and never validates transactions. This innovation was a key part of the invention within Bitcoin and allowed the specialisation of services. Consequently, the argument about consensus methodology is a red herring designed to have people look at alternative processes and ignore the scaling problem.

Proof of stake thus ignores scaling and focuses on an alternative issue of concern to some people but is designed to have regulators and other individuals tasked with managing financial systems look a different way than the developers of the systems would like. The reason for this is simple. Proof of stake is equity-based. Holders of a system are rewarded under what the American Howey Test will recognise as an "investment of money in a common enterprise with a reasonable expectation of profits to be derived from the efforts of others."[2] So breaking this down, we have (1) an investment of money, (2) in a common enterprise, (3) with the expectation of profit and (4) to be derived from the efforts of others.

Saleh references proof of stake in the context of a blockchain without waste.[3] However, as we will demonstrate, this is deceptive and in error. PoS is merely a system for hiding equity ownership. The use of Pseudononymy allows a large stakeholder to pretend to be many smallholders and thus hide the consolidation of control in a corporation or other entity. PoS is a way of reintroducing bearer shares after these were made illegal in the United States and other countries.[4] PoS is a methodology that removes competition from a blockchain and does not aid in scaling. The consensus methodology is separate in any blockchain from the distribution of transactions. Consequently, the problems with the abuse of shell companies that occurred before the Panama papers exposed this practice have been reintroduced through an argument of “decentralisation”.[5]

The consequence is creating a system that allows for minority rule by a few oligarchs while hiding the ownership structure through the use of multiple keys.[6] In effect, the ability

[2] https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets

[3] Fahad Saleh, “Blockchain without Waste: Proof-of-Stake,” *The Review of Financial Studies* 34, no. 3 (2021): 1156–90.

[4] Adrian ŢUŢUIANU, “LEGAL REGIME OF BEARER SHARES.,” *Valahia University Law Study*, 2018.

[5] Carl Pacini and Nicole Forbes Stowell, “Panama Papers and the Abuse of Shell Entities,” in *Corporate Fraud Exposed* (Emerald Publishing Limited, 2020).

[6] Tom Barbereau et al., “Decentralised Finance’s Unregulated Governance: Minority Rule in the Digital Wild West,” *Available at SSRN*, 2022.

for an individual to hold multiple keys and ensure that these are not linked to identity creates a form of digital *Freeport*.[7] Removing money-laundering controls and identifying the individuals acting to stake transactions and validate these on the network may pose multiple individuals by splitting their ownership into as many keys as they like. The minimum balance required for staking sets a lower limit on this ability to hide and favours large players.

(1) An Investment of Money

The first component of the Howey test on any PoS system is simple, and applies to many other systems that will be excluded from other aspects of securities legislation. For example, in a proof-of-stake system, the investment in a digital asset requires an exchange of money or monetary value. Therefore, such an investment can be easily determined to fall under the first part of the Howey test.

(2) In a Common Enterprise

Next, all individuals acting in a proof-of-stake system do so under a common set of rules and consensus mechanisms. Through this, the various parties follow the dictates of the issuer (for instance, the creator of the system or the development group maintaining any changes) and act under the rules of the system. The necessity for all transactions and nodes in any blockchain network to maintain a common set of rules creates a common enterprise. This condition is again true of any blockchain.

(3) With the Expectation of Profit

The economics of a proof-of-stake system is derived from encouraging large holders to invest in the system. This incentive is based on the payment of both *proposers* and *validators* and allows multiple parties to act under an equity stake to expect payment and profit.[8] The primary distinction between corporate shareholdings and the differentials between different classes of shares is the introduction of Pseudononymy or anonymously issued tokens. In this, a token is merely a database or ledger entry. The issue of tokenised equities has been a mainstay of financial enterprise since the 1980s. However, the development of computer-

[7] Paul Michael Gilmour, “Freeports: Innovative Trading Hubs or Centres for Money Laundering and Tax Evasion?,” *Journal of Money Laundering Control*, 2021.

[8] Giulia Fanti, Leonid Kogan, and Pramod Viswanath, “Economics of Proof-of-Stake Payment Systems,” in *Working Paper*, 2019.

assisted trading and the dematerialisation of securities occurred decades ago.[9] As such, arguments proposing that digital assets are new tradable assets are false and misleading. Rather, digital assets, including bitcoin and Ether, are merely tokenised offerings existing on a ledger. The difference is that the ledger is distributed and held by multiple parties. The ownership of individual tokens remains controlled by individuals just as an individual controlled any share certificate.

This section distinguishes greatly between proof-of-stake and proof-of-work blockchains. In a proof-of-work system, nodes compete against one another for payment irrespective of the holding in the underlying digital asset. In this, the system uses a unilateral contract developed and announced by the issuer of the system that pays nodes for validation services. The payment is not related to the increase of a token value or the speculation associated with holding such a token. While the operator of a node in a system such as Bitcoin can speculate, this is superfluous to the operation of the node itself.

Conversely, in proof-of-stake-based systems, the profit is derived from the ownership aspect of the asset itself. A node operator on a PoW system does need not to own any asset and can sell anything they earn for the validation service without any expectation of speculative price rise. In PoS, the token holder is explicitly incentivised to stake the token for repayment and, hence, the expectation of profit or ownership of the token. Therefore, a PoW system fails the third part of the Howey test. Equally, any and all PoS systems pass the first three parts of the Howey test without further analysis.

(4) To Be Derived from the Efforts of Others

Finally, the system is directly related to the efforts of other parties. In joining a PoS consensus system, the token holder has a presumption of other efforts being conducted through other individuals. Firstly, software development is conducted by development groups that may or may not be rewarded by the PoS system issuer. Even without this aspect of the system, there is a necessity to involve the efforts of others. Every proof-of-stake system is designed to provide “decentralised control”. By definition, every blockchain system requires an interaction between multiple parties and every token holder that is speculating benefits

[9] Michael J. Reynolds and John Campion, “The Contribution of Western Legal Systems to the Developing Law and Regulation of Eastern European Financial Markets,” *European Business Law Review* 3, no. 4 (1992); J. Thomas English and Georg Maier-Reimer, “Recent Developments in Securities Law: Introduction,” *Int’l Bus. Law.* 20 (1992): 211.

from the efforts of others. The distinction between PoW and PoS systems comes down to the expectation of profit merely from holding the token. It exists not merely through commodity-based gains one would expect in Bitcoin but rather through a direct payment made in the form of a dividend. As such, they can be no cogent argument that any PoS system fails to meet all four of the Howey test requirements. Proof of stake is, by nature, a form of equity.

Pseudonymity

The more interesting aspect is related to the reasons for creating such a system and linking this needlessly to pseudonymous ownership. The Bitcoin white paper noted that identity was firewalled from the blockchain. However, this does not remove the possibility of having identity systems or linking them into any exchange. It is possible to have a pseudonym linked to an identity-related key that meets all AML and KYC requirements and stops the issue of bearer share formed tokens. However, this is also outside of the aims and goals of many people in the falsely named “cryptocurrency” industry.

The limit of stake requirements changes the nature of how voting works in a system such as Ethereum 2.0. Smallholders in the system cannot be rewarded with a minimum staking requirement. This system requirement limits the ownership of the system to a small number of large investors. In effect, it magnifies the ownership power of the top investors and stakeholders in the system. For instance, if a stake required 1000 coins as a minimum stake and the system had 100 million coins, the Pareto-based distribution of ownership in such a system would cut off 60-80% of the owners of small amounts allowing only the large ownership stake to vote. A large holding entity like the Ethereum Foundation would amplify its network control in such a scenario. Even holding only 35 to 40% of the network would give it 50% voting control.

Next, if in a staking system requiring 1000 coins and individual held 10 million total coins, the ability to split this into 10,000 separate addresses would enable the illusion of decentralisation while maintaining strong overall system control. By dividing keys and holding these as separate legal entities, such as Panama based shell companies, a set of validating and proposing nodes would be able to act in concert as a single boating entity despite being spread across 10,000 separate legal entities. The purpose is to recreate the problems when the corporations implement multiple shell companies to bypass money-laundering controls.

Scaling

Scaling is a very simple topic of defining that has been made difficult in order to mislead people as to the nature of what is required. Scaling is directly related to the number of transactions processed in any particular period. For instance, the number of transactions per second or the number of transactions per day equally measure the scalability of a blockchain-based system. The solution to the hash puzzle in Bitcoin relates to the blockheader. Because of the use of a Merkle (binary) tree structure, the entire set of transactions remains the same size whether a block contains one transaction or 100 trillion. Consequently, the consensus methodology in Bitcoin and other proof-of-work systems is unrelated to the issue of scaling.

In producing arguments related to scale and associating these with changes to the consensus mechanism, those individuals seek to mislead regulators and others who are less technically knowledgeable. Unfortunately, the misinformation surrounding blockchain-based technologies has led to multiple problems when it comes to understanding how Bitcoin works. First, scaling Bitcoin or any blockchain is simply a basis of increasing the number of transactions per second. This outcome is, by necessity, always related to increasing the block size. More transactions require more data storage.

Concluding Decentralisation

Every listed corporation or tradable security is by definition decentralised. When public companies are required to report the beneficial ownership of large holders, the level of decentralisation is increased. When corporations are allowed to maintain secret shareholdings and operate using bearer-share instruments, the ability to bypass regulatory controls and act outside of ethical behaviour increases. Many regulatory controls have been implemented over the years because of corporate failures, including WorldCom, Enron, etc. The reasons come down to transparency.

The creation of proof of stake was related directly to the development of a system that had no relationship to solving the scaling problems within Bitcoin or other blockchain systems; rather, it is a way of hiding ownership and control of equity. In a proof-of-work-based system, the requirement for the nodes involves a constant reinvestment and upgrading of the system to ensure that each node provides a competitive service and innovates. Proof of stake allows existing equity holders to maintain control. That is, they can maintain equal shareholding without reinvesting in the network. A principal work system requires constant reinvestment, which needs to be maintained by the system owner. Others do not provide the investment for you. This requirement differs significantly from proof of stake where an equity holder need only rely on the innovation of others and can continue to operate without innovating or investing in the network.

Facebook is more decentralised than any blockchain-based network. But, equally, Google, Amazon, and most Fortune 500 companies maintain tens of thousands if not millions of shareholders in the registry. In arguing for decentralisation, misleading claims are constantly proposed to confuse people and stop any investigation into the real issues at hand. Bitcoin was always designed to scale and to do so through increasing the block size. The arguments are not delivered to promote a blockchain-based system but rather to hijack the system and enable money laundering and the facilitation of crime.

The argument around decentralisation a simple. There are 3 to 4 nodes controlling the majority of mining activity on any blockchain. Consequently, arguments about decentralisation because of Sybil systems proposing to be nodes without solving problems or acting in the consensus mechanism are a little more than misleading statements designed to hide the true nature of the system.

References

Barbereau, Tom, Reilly Smethurst, Orestis Papageorgiou, Johannes Sedlmeir, and Gilbert Fridgen. “Decentralised Finance’s Unregulated Governance: Minority Rule in the Digital Wild West.” *Available at SSRN*, 2022.

English, J. Thomas, and Georg Maier-Reimer. “Recent Developments in Securities Law: Introduction.” *Int’l Bus. Law.* 20 (1992): 211.

Fanti, Giulia, Leonid Kogan, and Pramod Viswanath. “Economics of Proof-of-Stake Payment Systems.” In *Working Paper*, 2019.

Gilmour, Paul Michael. “Freeports: Innovative Trading Hubs or Centres for Money Laundering and Tax Evasion?” *Journal of Money Laundering Control*, 2021.

Ishiguro, Takehide, and Akihiro Yamada. “Overconfident CEOs, Decentralisation, and Tax Aggressiveness: Evidence from Japan.” *International Journal of Economics and Accounting* 10, no. 2 (2021): 181–203.

Pacini, Carl, and Nicole Forbes Stowell. “Panama Papers and the Abuse of Shell Entities.” In *Corporate Fraud Exposed*. Emerald Publishing Limited, 2020.

Reynolds, Michael J., and John Campion. “The Contribution of Western Legal Systems to the Developing Law and Regulation of Eastern European Financial Markets.” *European Business Law Review* 3, no. 4 (1992).

Saleh, Fahad. “Blockchain without Waste: Proof-of-Stake.” *The Review of Financial Studies* 34, no. 3 (2021): 1156–90.

ȚUȚUIANU, Adrian. “LEGAL REGIME OF BEARER SHARES.” *Valahia University Law Study*, 2018.