The Dominance of DPoS over PPoS: Analysis of Security, Scalability, Efficiency for Blockchain Networks

Hamilton Holt

Department of Computer Science, Binghamton University

CS301: Ethical, Social, and Global Issues in Computing

Dr. George Weinschenk

March 8, 2023

Abstract

This research paper shows that Delegated Proof-of-Stake (DPoS) outperforms Pure Proof-of-Stake (PPoS) as a PoS algorithm for blockchain networks, as DPoS offers higher levels of security, scalability, and efficiency resulting in a more sustainable and equitable computing technology for the stability of future global financial systems. The paper analyzes various technical aspects, such as Algorand's PPoS model, Ethereum's transition from Proof-of-Work to Proof-of-Stake, and the Roll-DPoS consensus algorithm. PPoS has several disadvantages, such as a lower fairness quotient, limited reliability and performance, and vulnerability to forking attacks and fraudulent activities. In contrast, DPoS allows for increased protection against vulnerabilities that could compromise the system. DPoS enables networks to handle more transactions at faster speeds. DPoS's more equitable distribution of power results in a more fair decision-making process. DPoS-based networks consume less energy than PPoS-based networks. The paper also discusses the social impact of DPoS, highlighting its potential to foster greater involvement from token holders, promote quicker transaction confirmation, and reduce centralization in blockchain networks.

The Dominance of DPoS over PPoS: Analysis of Security, Scalability, Efficiency for Blockchain Networks

Proof-of-Stake (PoS) addresses the vulnerability of the 51% attack, which affects investors or users in Proof-of-Work (PoW) currencies (Do et al., 2019, p.90). DPoS involves a group of nodes to validate transactions, while PPoS allows any node with a stake in the network to validate transactions. Delegated Proof-of-Stake (DPoS) outperforms Pure Proof-of-Stake (PPoS) as a PoS algorithm for blockchain networks, as DPoS offers higher levels of security, scalability, and efficiency resulting in a more sustainable and equitable computing technology for the stability of future global financial systems. In blockchain technology, DPoS offers the highest level of security to ensure the integrity and reliability of the system. Vulnerabilities in blockchain algorithms can compromise the integrity of the system, leading to financial losses and data breaches. Though favored for achieving a higher degree of decentralization, DPoS continues to outperform PPoS.

Alternative Technology

PPoS applies to blockchain technologies, including Algorand's. Dimitri (2022), a professor at the University of Siena who does research papers on blockchain and cryptocurrencies, best known for his work as an economic consultant at a start-up incubator at Siena's Innovation Park for Life Sciences. According to a recent research article by Dimitri, Algo randomly selects users to participate in block proposal, selection, and certification (9:2). The number of Algos held by the user over the total money supply determines the probability of selection. The research article says that users can stake a portion of their money holdings to gain eligibility for block validation and governance voting sessions. The probability of the selection of a user, shown by the equation:

$$\pi ib = aib / Ab, \quad (1)$$

where aib represents the number of Algos held by user i, Ab represents the total supply of Algos in the system, and Ib represents the number of users in the system. The equation operates as a lottery, where the probability of selection resembles the ratio of individual-bought tickets over the total number of organizer-sold tickets (9:3). The user's utility function, given by the equation:

$$U(a0; E(a1)) = \delta E(a1) - a0 \text{ with } 0 \leq a0 \leq A0, \quad (2)$$

where $0 \leq \delta \leq 1$ represents the user's discount factor and A0 represents the number of Algos introduced in the system before certification of the first block. The expression reflects the user's tradeoff between spending Algos immediately on goods/services and retaining Algos in the wallet to enhance the likelihood of drawing one of the three roles and acquiring additional Algos (9:6). In equilibrium, the aggregate money demand, shown by the equation:

$$A0 = I0a0 = 3\delta(r-t1+t1n) / (1-\delta)((I0-1) / I0)^3, \quad (3)$$

as I0 increases, A0 increases at decreasing rates due to an externality effect. In the non-linear relationship, I0 portrays A0 increasing up to I0=4, reaching a maximum and then decreases towards a0=0 (Dimitri, 2022, 9:14). The non-linear relationship, perhaps due to the tradeoff between using Algos for transactions versus staking currency units.

Support

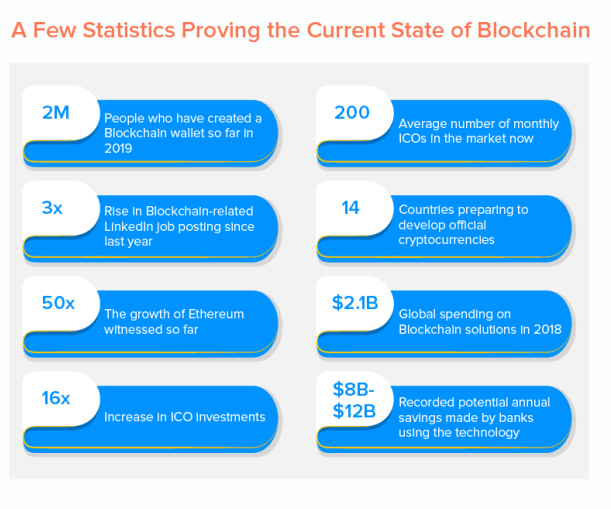
Technical Details

Blockchain technology has a non-linear relationship, another factor that highlights its transformative power. Oxford and Georgetown graduate Bettina Warburg (2016) is the co-founder of Animal Ventures, which establishes business strategies for blockchain, artificial intelligence, the industrial Internet of Things, and digital platforms. Depending purely on technology rather than political and economic institutions alters how people exchange value and

reduces mutual trade concerns (TED, 2016, 0:35). Figure 1 illustrates the economic impact of the blockchain (Chirag, 2022, para.4).

Figure 1

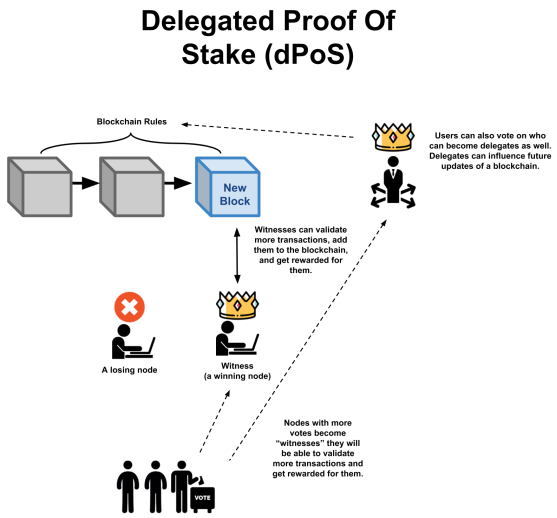
Statistics of Blockchain's Economic Impact



Ph.D. student Do (2019) from Hong Kong University of Science and Technology published a paper on the Symmetry of Extending Properties in Associative Rings where he presents the right-left symmetry of the CS and max-min CS conditions on nonsingular rings and generalization to nonsingular modules. According to a recent conference paper by Do et al., coin holders vote for a select group of witnesses to secure and execute transactions on the network as part of the DPoS consensus method. Figure 2 illustrates how voting works in a DPoS blockchain ("The DPOS consent system—Delegated proof of stake," 2019, sec.3).

Figure 2

DPoS Content System



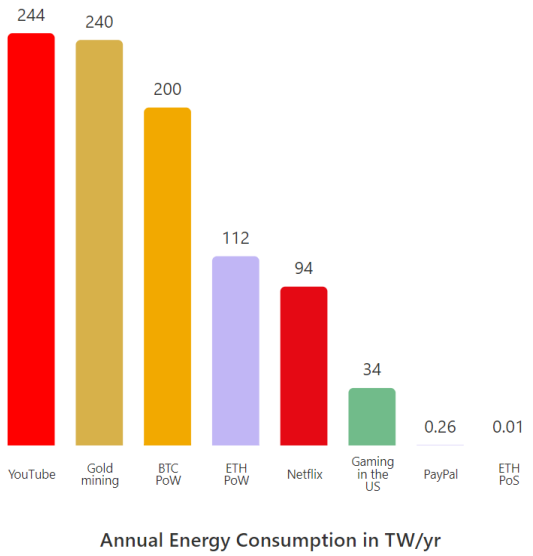
The conference paper says that the DPoS mechanism addresses the main issue of a naive PoS system such as the lack of a stakeholder, long-range attacks, and weak subjectivity. DPoS maximizes the performance of blockchains, notably scalability, while drastically lowering the cost of network administration and maintenance. EOS, WAVES, and Steem represent just a few DPoS-based blockchains that have scaled up to hundreds of transactions per second (p.91). The top 21 chosen delegates will serve as block producers who validate transactions, develop new blocks, and manage the network. Block producers receive rewards for their efforts (Do et al., 2019, p.92).

Science writer Fairley (2019) received the Society of Environmental Journalists Award for reporting on the environment for a series of articles on solar energy history, technology, politics, and impact. He is best known for his writing on energy, technology, and the environment. According to a recent magazine article by Fairley, Ethereum has made an effort to combat concentrated power even though PoW mining uses a lot of electricity by using a memory-intensive PoW algorithm for mining ether, which discourages the usage of ASICs (para.12). The PoW method used by Ethereum has not stopped the exponential rise of processing

power devoted to ether mining, and the ensuing energy consumption has sparked a backlash from environmentalists (para.13). To address the growing environmental concerns, Ethereum has planned to transition from its current PoW consensus algorithm to a PoS algorithm known as Ethereum 2.0 (para.27). The transition to PoS represents a major step towards achieving a more energy-efficient and sustainable blockchain platform. Figure 3 illustrates the difference in energy consumption between Etherium PoW and Etherium PoS (Sarkar, 2022, para.3).

Figure 3

Energy Consumption for Various Industries



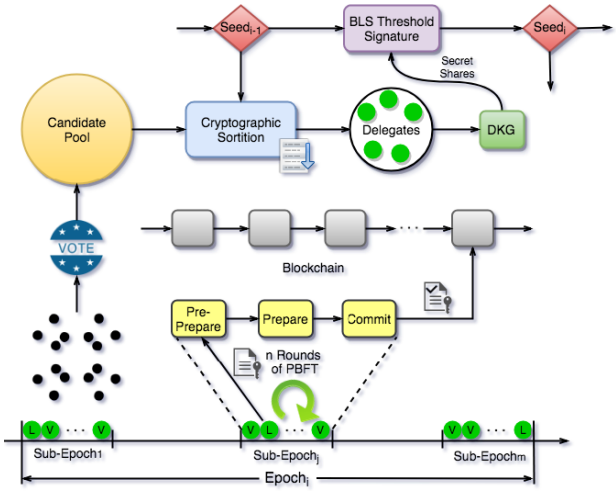
DPoS eliminates the need for mining and allows the network to operate with delegates selected by the community instead of anonymous miners (Fairly, 2019, para.10).

Fan (2018) is an associate professor at the Institute of Computing Technology of the Chinese Academy of Sciences who researches secure machine learning, decentralized trust computing, and edge computing. He is best known as a founding member and head of cryptography at IoTeX, a startup empowering the future machine economy with an innovative combination of blockchain and IoT. According to a recent conference paper by Fan & Chai,

DPoS concentrates block manufacturing in the hands of a small group of somewhat trustworthy delegates. The randomized DPoS consensus technique known as Roll-DPoS uses a random beacon and a cryptographic hash function; Roll-DPoS chooses a predetermined number of block producers at random from a candidate pool. (p.482). The conference paper says that Pedersen's DKG protocol becomes utilized by the chosen block producers to create epoch-specific private key shares, signing messages using the short-lived ECDSA and BLS threshold signature methods in the Practical Byzantine Fault Tolerance procedure. Figure 4 illustrates a flow chart for the exact process of the Roll-DPoS algorithm (p.483).

Figure 4

Overview of the Roll-DPoS Consensus Algorithm



Three phases make up the bootstrapping process for the Roll-DPoS protocol on the Ethereum blockchain. In step one of the process, miners propose themselves and register as prospective block producers in the community. The conference paper says that establishing a campaign website to draw support from the community accomplishes this. In step two of the process, community voting selects an initial pool of N block producer candidates. The conference paper says that voting occurs through submitting unique Ethereum transactions with the data field set

to vote and the value field set to 0. Choosing the N candidates with the most backing forms the initial block producer candidate pool. In step three of the process, the candidate pool provides the successive bootstrapping nodes for the first epoch to serve as the n block producers, indicated by:

$$BP^{(1)}1,..., BP^{(1)}n. \quad (4)$$

The conference paper says that a deterministic random bit generator (DRBG) selects the n bootstrapping nodes in a dispersed manner. Each candidate starts the DRBG using the initialization string:

$$DRBG(s0,pk^{(1)}1,..., pk^{(1)}N, 1), \quad (5)$$

where pk^(1)i represents the candidate C^(1)i's public key and 1 represents the epoch number of the first epoch. Each candidate continues to produce L-bit random numbers R's until the selection of n block producers (Fan & Chai, 2018, pg.484).

Ph.D. student Nair (2021) from T John Institute of Technology conducts research in blockchains, security of data, storage management, and theorem proving where she present new ways to improve the security and efficiency of blockchain technology. According to a recent conference paper by Nair & Dorai, the PPoS model has several shortcomings. The majority of stakeholders receive a big quantity of coins in PPoS since it has the lowest fairness quotient (pp.281). PPoS has limited reliability and performance, which varies over time. Having no equivalent to the total hash rate in PoW, the insecurity of systems using PPoS presents a serious challenge (pp.282). Nair & Dorai says that as a result, PPoS remains vulnerable to forking attacks and fraudulent activities carried out by individuals with very high stakes. DPoS, an extension of PoS, offers increased security as certain delegated miners must sign newly formed blocks to legitimize them (Nair & Dorai, 2021, pg.280).

Social Impact

DPoS represents a more fair method of decision-making. Token holders in DPoS-based blockchain networks may vote for validators, which results in a more equitable distribution of power across the network. PPoS, in contrast, concentrates authority in the hands of individuals who own the greatest number of tokens. This principle suggests that DPoS stands as a more equal form of computing technology. A small number of people holding all the authority due to the power concentration in PPoS-based networks can result in biased decision-making and the exploitation of the network by negative actors. In DPoS-based networks, the power distributed more equally among members guarantees that everyone has a say in decision-making, thus developing a more fair computing technology for all users.

The equity of DPoS supports the stability of future international financial systems. Stability in the financial system remains essential for economic prosperity at both national and individual levels. Power-based PPoS networks tend to grow unstable, which increases the risk of financial systems collapsing. DPoS-based networks, on the other hand, guarantee that everyone has a say in the decision-making process, lowering the likelihood of instability and guaranteeing that the financial systems stay steady and dependable. DPoS-based networks use less energy than networks using alternative consensus methods, such as PPoS-based networks. Environmental issues arise because PPoS-based networks use a significant amount of energy to keep the network operational. DPoS-based networks remain more sustainable and ecologically considerate since they consume a lot less energy to run.

DPoS stands as a superior PoS algorithm for blockchain networks due to its ability to deliver higher levels of security, scalability, and efficiency. Essential to the platform's integrity and dependability, security remains a top priority for each blockchain network. In DPoS-based networks, validators get chosen by token owners, who remain responsible for their activities.

Because validators remain motivated to behave in the network's best interests rather than their own, this accountability makes the system more secure. By risking losing their share in the network, unscrupulous actors get discouraged from trying to take advantage of the system. Scalability remains another important consideration for blockchain networks, as the network's success hinges on its capacity to process enormous volumes of transactions. Since the number of validators may get altered in response to the demand for transactions, DPoS-based networks remain more scalable than PPoS-based networks. Scalability guarantees that the network can handle a high number of transactions without getting overloaded and enables the network to adapt to changing conditions. Efficiency remains a crucial consideration for blockchain networks since the network's success depends on the speed of the transaction process. Due to the quicker and more simplified block manufacturing process, DPoS-based networks remain more effective than PPoS-based networks. As a result, transactions can undergo faster processing, enhancing both the user experience and overall network effectiveness.

Another benefit of the DPoS system lies in its ability to foster involvement and interaction from token holders. Token owners remain encouraged to stay involved with the network and take part in decision-making since they may vote for validators. Voting produces a community that remains more invested and involved, potentially resulting in a network that remains more resilient and lively. DPoS-based networks have the potential to confirm transactions more quickly than those using alternative consensus techniques like PPoS-based networks. DPoS's fast block production allows for quicker processing and confirmation of transactions. DPoS's fast block production remains crucial for networks like payment systems and decentralized exchanges that demand very rapid confirmation of transactions. In addition, DPoS can aid in lessening centralization in blockchain networks. The global distribution of

DPoS validators ensures the network's independence from any specific region. Such independence keeps the network robust and decentralized while preventing centralization.

Conclusion

DPoS offers unique features that distinguish it from other consensus mechanisms. DPoS provides enhanced security through its more balanced distribution of power and an accountable decision-making process. The number of validators can adjust according to transaction demand, enhancing scalability and making DPoS-based networks more adaptable to changing conditions. The accelerated block manufacturing process boosts efficiency by enabling faster transaction confirmations and improving user experience. DPoS indisputably surpasses PPoS as the superior PoS algorithm for blockchain networks. The unparalleled security, scalability, and efficiency provided by DPoS foster a more sustainable and equitable computing technology, ensuring the stability of future global financial systems. This research has significant implications for computer professionals. By adopting DPoS, token holders are encouraged to participate more actively, fostering a stable and decentralized ecosystem. The insights provided by authors such as Dimitri, Do, Fairley, Fan, and Nair show the potential impact of DPoS on industries that demand rapid transactions, like payment systems and decentralized exchanges. This shift could revolutionize these sectors and reshape the responsibilities and roles of computer professionals, highlighting the importance of understanding and implementing DPoS as an effective and sustainable blockchain solution. Addressing the challenges of ensuring trust and accountability among DPoS validators, striking a balance between centralization and decentralization, and designing and implementing fair, transparent, and ethical systems is vital for the success of DPoS networks. To ensure trust and accountability, it is essential to establish clear guidelines and protocols for validators, as well as to provide appropriate incentives that encourage honest

behavior. Balancing centralization and decentralization requires a thoughtful selection of validators and a careful distribution of power among them. Finally, the creation of fair, transparent, and ethical DPoS systems necessitates continuous evaluation and improvement of the underlying mechanisms, incorporating feedback from the community and stakeholders. By addressing these concerns, DPoS networks can unlock their full potential and revolutionize various industries.

References

Chirag. (2022). Beyond the Hype: The Real Impact of Blockchain on Economy. [Photograph]. Appinventiv. https://appinventiv.com/blog/real-impact-of-blockchain-technology-on-economy/

Dimitri, N. (2022). Proof-of-stake in algorand. *Distributed Ledger Technologies: Research and Practice*, *1*(2), 9:1-9:17. https://doi.org/10.1145/3550197

Do, T., Nguyen, T., & Pham, H. (2019). Delegated proof of reputation: A novel blockchain consensus. *Proceedings of the 1st International Electronics Communication Conference* (pp.90–98). New York. https://doi.org/10.1145/3343147.3343160

Fairley, P. (2019). Ethereum plans to cut its absurd energy consumption by 99 percent. *IEEE Spectrum*. *56*(1), 1:29-1:32. https://spectrum.ieee.org/ethereum-plans-to-cut-its-absurd-energy-consumption-by-99-percent

Fan, X., & Chai, Q. (2018). Roll-dpos: A randomized delegated proof of stake scheme for scalable blockchain-based internet of things systems. *Proceedings of the 15th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (pp.482–484). New York. https://doi.org/10.1145/3286978.3287023

Nair, P. R., & Dorai, D. R. (2021). *Evaluation of performance and security of proof of work and proof of stake using blockchain.* 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV) (pp.279–283). Tirunelveli, India. https://ieeexplore-ieee-org.proxy.binghamton.edu/document/9388487

Sarkar, A. (2022). *The Merge brings down Ethereum's network power consumption by over 99.9%.* [Photograph]. Cointelegraph.

https://cointelegraph.com/news/the-merge-brings-down-ethereum-s-network-power-consumption-by-over-99-9

TED. (2016). *How the blockchain will radically transform the economy | Bettina Warburg* [Video]. YouTube. https://www.youtube.com/watch?v=RplnSVTzvnU

The DPOS consent system—Delegated proof of stake. (2019). [Photograph]. *Cripto51*. https://www.cripto51.com/en/2019/07/21/the-dpos-consent-system-delegate-proof-of-stake/