Comparing Proof of Stake Protocols for Security and Scalability on Investments

Thomas M Bonagura

Department of Computer Science, Binghamton University

CS-301 Ethical, Social, and Global Issues in Computing

Dr. George Weinschenk

March 28, 2022

Abstract

The rise of blockchain technology and cryptocurrencies has left investors confused about what they should put their money into. Starting with Bitcoin and its use of Proof of Work - POW - new protocols began being developed using Proof of Stake - POS - as their way to mine cryptocurrency. Investors often struggled to invest in these new technologies due to the blockchain dilemma and which coins can overcome the average problems of blockchain technologies. The blockchain dilemma includes the scalability, safety, and true decentralization of cryptocurrency coins. Algorand - ALGO - and Cardano - ADA - are two coins that offer many solutions to this blockchain dilemma. Both coins use different protocols in their POS consensus, Algorand with the Byzantine Agreement and Cardano with Ouroboros Protocol, to give investors and coin users what they desire. In this article, I will provide why Algorand solves the blockchain dilemma, allowing for investment security and scalability, more efficiently and better than Cardano by comparing each of their algorithms and the code that goes into these coins' consensus protocols.

Comparing Proof of Stake Protocols for Security and Scalability on Investments

Security and scalability rank as important aspects for determining the value of an investment for the modern innovation of blockchain technology. Blockchain technologies utilize different consensus mechanisms to validate, or mine, cryptocurrency on their ledgers. The popular and earliest cryptocurrencies, including Bitcoin and Ethereum, currently use a consensus mechanism known as Proof of Work (POW). Although the most popular consensus at the time, this form of validation on the blockchain uses large amounts of resources, computing power, and energy, creating the need for more resourceful and scalable protocols. Newly developed Proof of Stake (POS) and branches such as Delegated Proof of Stake (dPOS) functioned to address these energy concerns and became adopted by a large number of cryptocurrencies including Cardano. Proof of Stake addressed the lack of efficiency in validating transactions in addition to being significantly less energy-intensive. Fortunately, there is always a need for improvement in new technology, and the developers of a cryptocurrency known as Algorand created a more secure and scalable branch of the Proof of Stake consensus mechanism called Pure Proof of Stake (PPOS). Using Algorand's Pure Proof-of-Stake (PPOS) algorithm as opposed to Cardano's Proof-of-Stake (POS) algorithm as a consensus mechanism on the blockchain achieves better validation of cryptocurrency exchanges, which serves to allow for superior security for investors and scalability of the cryptocurrency. Algorand's Pure Proof of Stake, by using Byzantine Agreement protocol for selection and sortition, allows for the safety of investors. The Byzantine Agreement allows targeted attacks to become obsolete due to ensured honest majority while also allowing for scalability due to high transaction speed. While Proof of Stake is better than Proof of Work protocols, Pure Proof of Stake simply allows for the most benefits for its investors.

Alternative Technologies

Consensus mechanisms in cryptocurrencies are what give coins their value. Bitcoin, the first of its kind, utilized POW to validate the exchanges on the blockchain. Proof of Work allows the nodes to agree on transactions and everything else that happens within the blockchain. These nodes perform “work”, a race of trials and error of different blocks with mathematical algorithms to validate the block and receive the reward (Minimalism, 2018, para. 6). By having this competitive race to validate everything on the chain, Proof of Work is very energy-intensive and requires expensive hardware, leading to the development of different consensus mechanisms that do not deplete physical resources. Proof of Stake was next in the development of consensus mechanisms, not requiring an intense amount of hardware and energy usage to mine coins. A comparison of Algorand’s Pure proof of stake with the use of the Byzantine Agreement with Cardano’s protocol is crucial for investors to determine the scalability and security of these different cryptocurrencies. Cardano is one of the cryptocurrencies that utilizes a POS protocol, adopting the Ouroborus consensus protocol. Cardano’s mechanism is most similar to a Delegated Proof of Stake (dPOS), where a leader node is elected by parties within the slot and then is allowed to create the block of transactions (Gazi et al., 2019, p. 6). The block leader, after being selected based off probability in relation to weight, the process uses Global Random Oracle to create a sort of randomness. Cardano’s unique protocol also limit’s the amount of staking power if a threshold is met to protect against manipulation (Arielfavio et al., 2021, para 13). Algorand, however, utilizes the Byzantine Agreement (BA) and cryptographic sortition. Although the randomized function has certain resemblances, the BA protocol ensures Algorand’s security and scalability for investors.

Support

Technical Details

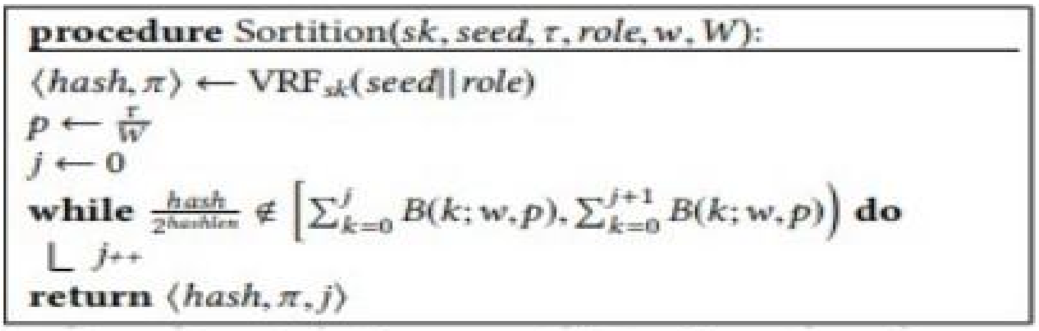
The efficiency of transactions and security are important aspects when investing in a cryptocurrency. As opposed to Cardano's Ouroboros protocol, Algorand uses unique cryptographic sortition and the Byzantine Agreement for the Proof of Stake selection process, resulting in Pure Proof of Stake (Kastelein, 2017, para. 7). With normal POS protocols, there are higher risks of "bad actors" within the transactions of the blockchain and targeted attacks. On the other hand, researcher **Richard Kastelein (2017), accomplished writer and founder of Blockchain News (2015),** explains that the validators of the block in Algorand are not chosen traditionally, but instead chosen randomly and suddenly with the use of a randomized hash. This untraditional and innovative selection process is unpredictable due to randomized probability functions, making Algorand's transactions practically immune to manipulations (Kastelein, 2017, para. 3).

Often with Proof of Stake protocols including Cardano's, each individual is given a weight that coordinates with the number of coins held. With Algorand, the more coins held leads to the higher probability of being selected for a role: either a committee member for a phase or choosing for block proposal. **H. U. Kumar and Raghavendra Prasad S. G, professors and researchers at RV College of Engineering in India,** provide that an individual's probability, *p,* is determined by the formula *wi* (individual weight) divided by combined weight, or *W* (calculated by *W*= ∑*iwi*) (Kumar et al., 2019, p. 497). However, the actual use of this probability and an added factor of randomization is what separates Algorand from the others. Algorand utilizes the Verifiable Random Function, or VRF, for the sortition process. **Founder of Algorand and Professor at MIT Silvio Micali (2019)** dives deeply into the importance of this protocol in his presentation at *TEDxMilanoSalon*. Micali elaborates on the safety provided by

Algorand's randomness in consensus due to VRF. He asks a silly question, "Whom should I bribe… Should I bribe you, him, or some lady in Shanghai?" [Micali, Translated Tedx Speech]. This statement is to provoke the thought that with true randomness, manipulation on a blockchain is impossible.

Figure 1

Pseudocode of Cryptographic Sortition Provided by Kumar et al (2019).



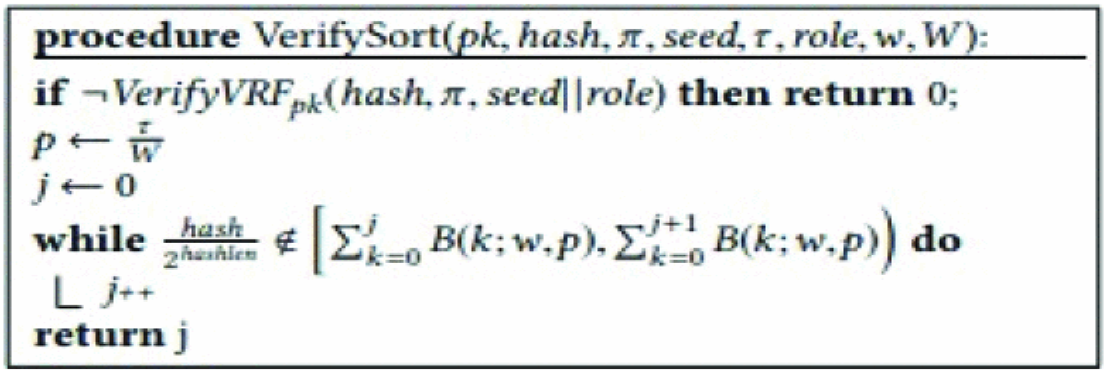
```
procedure Sortition($sk, seed, \tau, role, w, W$):
  $\langle hash, \pi \rangle \leftarrow \mathrm{VRF}_{sk}(seed||role)$
  $p \leftarrow \frac{\tau}{W}$
  $j \leftarrow 0$
  while $\frac{hash}{2^{hashlen}} \notin \left[\sum_{k=0}^{j} B(k; w, p), \sum_{k=0}^{j+1} B(k; w, p)\right)$ do
    $j$++
  return $\langle hash, \pi, j \rangle$
```

Pseudocode 1 :CryptograhicSortition Algorithm

Lepore et al. (2020) describes the Verifiable Random Function as a randomized number generator that uses the public seed and the node's role (Lepore et al., 2020, p. 16). As shown in Figure One (Kumar et al, 2019), the Sortition function takes parameters including *sk* (secret key), a seed, τ (the threshold for a specific role), roles including the block proposer or member of a committee, and the weight variables discussed above (Kumar et al., 2019, p. 498). Within the Sortition function, the user conducts <hash, π><-VRFsk(seed||role), with hash being the number of users selected and π being the proof obtained by VRF output. **Crisitian Lepore et al., a cryptographic and computer science expert at the University of Milan,** showcases that there is a do-while loop is run as part of the functionality, helping to determine the value of *j*. After running through the functionality, sortition returns three values: a random number (new hash), π proof that the output is correct, and a number *j* that expresses the probability of a node becoming a committee member (Lepore et al., 2020, p. 17). The seed parameter is a public random value that is selected. The seeds are published at round r, which is determined by the VRF function having the seed from the previous round. In addition, *sk* in the process must be chosen before the seed is made each round, leading to the use of another function (Kumar et al., 2019, p. 498).

Figure 2

Pseudocode of VerifySort Provided by Kumar et al.

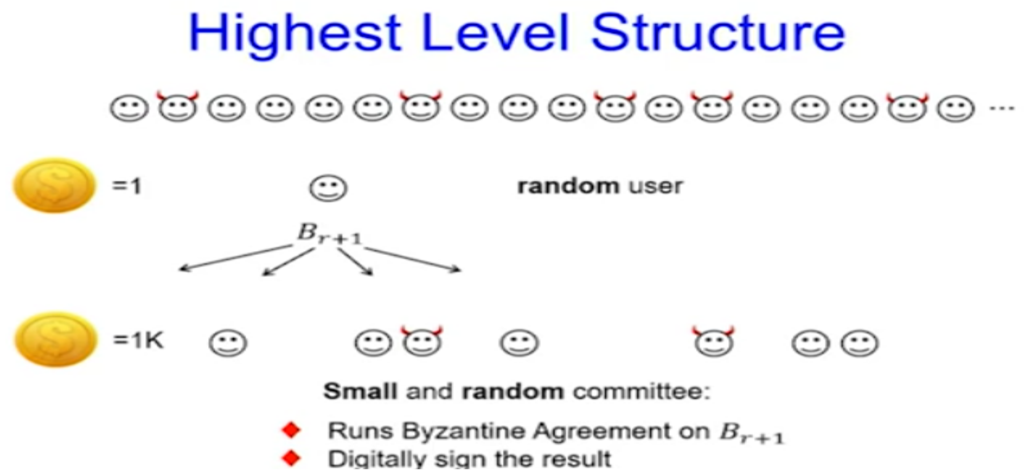


```
procedure VerifySort($pk, hash, \pi, seed, \tau, role, w, W$):
if $\neg VerifyVRF_{pk}(hash, \pi, seed||role)$ then return 0;
$p \leftarrow \frac{\tau}{W}$
$j \leftarrow 0$
while $\frac{hash}{2^{hashlen}} \notin \left[\sum_{k=0}^{j} B(k;w,p), \sum_{k=0}^{j+1} B(k;w,p)\right)$ do
    $j$++
return j
```

VerifySort is the function used in Algorand's selection process to allow every node in the process to verify the *j* value (Lepore et al., 2020, p. 17). Computing the Seed value requires the special key value of every user in the selection process. In VerifyVRF, the program checks if round r of the cryptographic sortition is complete. It then proceeds to check the timestamp for the round r-1-(r%R), and the secret keys are used from the last block which was created by the time before the block r-1-(r%R) (Kumar et al., 2019, p. 498). This function ensures the validity of the decisions made by VRF. Overall, VRF and the Verify Sortition functions work together to create a truly random and fair proposal process. These functions also help to ensure security and honesty on the blockchain.

Figure 3:

Image Displaying Structure of Byzantine Agreement by Sathya Peri from Medium.com



Small and random committee:

- Runs Byzantine Agreement on B_{r+1}
- Digitally sign the result

The Byzantine agreement is a crucial aspect of the security and efficient validation that Algorand provides over Cardano. **Peter Gazi (2019), with use of his PHD in cryptography and full time research position at IOHK,** and his co-writers explain how Algorand immediately finalizes these blocks by running the Byzantine Agreement before proposing the next block(p. 156). Once leaders are selected to propose a block using the algorithms above, BA forced the program to rely on a new subset of users each round (Lepore et al., 2020, p.17). In addition, Cardano and many other POS cryptocurrencies utilize epochs, time slots for transactions. Gazi (2019) demonstrates how Algorand does not have epochs and tells how creating and processing a sidechain certificate for each block is overly demanding, instead, Algorand utilizes the BA functionality (Gazi et al., 2019, 156). In each step of the BA, a committee member must cast a vote for some procedure and all the users must count the votes to ensure validity(Kumar et al. 2019, p. 498). Users who receive more of the threshold votes will vote for the particular value in the proceeding step(Kumar et al. 2019, p. 498). Silvio Micali (2017) describes the process as promoting a global democratic process, using mass agreement by many nodes to promote decentralization(13:07). Figure 3 demonstrates how Algorand's protocol maintains honest agreement and consistency throughout the transactions and rounds.

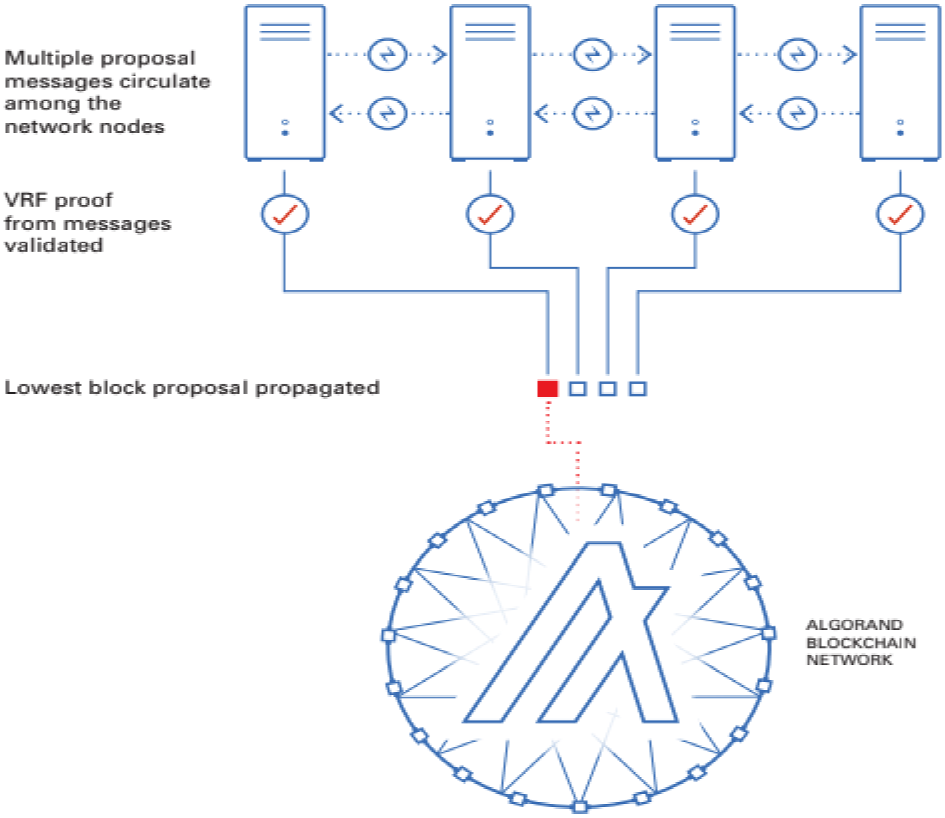
Social Impact

The people and financial institutions have been warring due to the increase in inequality of wealth and power all across the globe. Due to these issues, new technological innovations began being developed to combat the centralization of wealth. Blockchains, ledgers with full viewability, and decentralization began becoming published by developers worldwide. People are slowly adopting cryptocurrency as an actual investment and currency as opposed to fiat (the dollar). The lack of trust in new technology is what scares the average investor from pursuing life-changing innovations. Investors in the space either do not trust cryptocurrencies due to the lack of security and perceived hacking vulnerability, lack of scalability (transaction efficiency), or lack of true decentralization. As Silvio Micali intended and other Algorand enthusiasts believe, Algorand solves the *BlockChain Dilemma*. The blockchain dilemma is a belief that a singular blockchain cannot sufficiently apply decentralization, security, and scalability. Algorand utilized cryptographic sortition and Byzantine Agreement to ensure the validity of transactions while maintaining efficiency and decentralization.

For example, efficiency is very important to the scalability of a cryptocurrency. The VRF and Sortition functions discussed previously allow Algorand to produce blocks every 4.5 seconds. Algorand can also hold up to 5,000 transactions, which results in about 1,000 TPS (transactions per second) while also being one of the most used cryptocurrencies (Algorand Developer Team, 2021, para. 26). Cardano, on the other hand, only allows 250 transactions per second according to DayTrading.com. Based on these recorded speeds, Algorand is four times as fast as Cardano currently. Although Algorand is fast, some might question what makes it a safe investment for investors.

Figure 4

Soft Vote Part 1 by Algorand Developer Team


Multiple proposal messages circulate among the network nodes
VRF proof from messages validated
Lowest block proposal propagated
ALGORAND BLOCKCHAIN NETWORK

Algorand secures its blockchain and transactions by using new committee members for each round of sortition. Average Proof of Stake manipulation is virtually impossible due to player replaceability (Lepore et al., 2020, p. 17). Richard Kastelein (2017), after doing intensive research on Micali and Algorand, explains how bad choices of block proposers are simply dropped. If the block proposer is a bad choice, decided by the Byzantine Agreement, zero progress will be made and everyone is forced to agree on nothing. This prevents bad actors from infiltrating the decision-making and even prevents people from automatically choosing themselves for every proposal. These preventive measures, in addition to the algorithms discussed above, lead to a more secure and fair proposal and transactions for Algorand's blockchain. Cardano has no such method to prevent bad actors, only casual ways to prevent a 51% attack (same as Bitcoin).

Lastly, Algorand is a truly decentralized blockchain due to its almost democratic process (Micali, 2019, [Translated]13:07). There is no central figure to control the proposal and agreement protocols within Algorand itself. Algorand's transactions are completely run by the automatically selected committee and proposal, even denying the bad actors, as stated above. Decentralized finance allows transactions to be fully public and transparent on the blockchain. This includes transaction amounts, types, and times of these cryptocurrency transactions. Financial wrong-doings can be exposed and equality can repair itself.

The combination of these technologies and aspects puts Algorand's benefits over those of Cardano's. Algorand simplifies true decentralization while pursuing safety and efficiency. Cardano, although being a decentralized platform, does not reach the same investment securities and scalability that Algorand provides to the newly developing decentralized world. The Byzantine Agreement Protocol allows for more security through honest agreement.

Conclusion

Blockchain technology and cryptocurrency protocols have had drastic changes and improvements over the past couple of years. Research proving Algorand's superiority over other POS protocols showcased that the blockchain dilemma is closer to being solved every day. Algorand demonstrates safety and true randomness with the use of VRF and the Sortition function. Algorand also allows for security by having new committee members and utilizing the Byzantine Agreement every round of its selection process. As new cryptocurrencies, both scam and true investments, become developed, it is important to keep note of what can be accomplished with blockchain technology. While Cardano, or ADA, is a great investment, Algorand provides more scalability and safety in the ever-changing internet-world. Algorand’s transaction speed topped with security ensured by the Byzantine Agreement gives new investors a clear choice when choosing a cryptocurrency to put their money into.

References

Algorand Developer Portal. (2021). *Why Algorand?* Algorand. [Text and Diagram] https://developer.algorand.org/

Arielfavio. (2021, January 21). *Ouroboros how does the protocol work? (quick view)*. Cardano Forum. https://forum.cardano.org/t/ouroboros-how-does-the-protocol-work-quick-view/45206

Gazi, P., Kiayias, A., and Zindros, D. (2019). Proof-of-stake sidechains. *2019 IEEE Symposium on Security and Privacy (SP)*, 139–156. https://doi.org/10.1109/sp.2019.00040

How many transactions per second can be achieved on cardano vs Solana? Day Trading. (n.d.).https://www.daytrading.com/ada-vs-sol

Kastelein, R. (2017, January 6). *Move over bitcoin – mit cryptographer Silvio Micali and his public ledger algorand... the future of blockchain?* Blockchain News, Opinion, TV and Jobs. Via Communications of the ACM, https://www.the-blockchain.com/2017/01/05/mov

Kumar, H. U & R. P. S G. (2019). *Algorand: A Better Distributed Ledger.* Paper presented at 1st International Conference on Advances in Information Technology (ICAIT), Chikmagalur, India. (pp. 496-499)[Text and Image].10.1109/ICAIT47043.2019.8987305.

e-bitcoin-mit-cryptographer-silvio-micali-public-ledger-algorand-future-blockchain/

Lepore, C., Ceria, M., Visconti, A., Rao, U. P., Shah, K. A., & Zanolini, L. (2020). A survey on blockchain consensus with a performance comparison of POW, POS, and pure pos. *Mathematics*, *8*(10), 1782. https://doi.org/10.3390/math8101782

Minimalism. (2022, March 28). *Proof-of-work (POW)*. ethereum.org. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/

References

Micali, S. (2019, November). *A truly decentralized blockchain: Silvio Micali: Tedxmilanosalon*. [Video] TED Talk, from https://www.ted.com/talks/silvio_micali_truly_decentralized_blockchain

Peri, S. (2018, May 10). *Algorand, MIT Bitcoin Expo '18*. Medium. https://medium.com/mitbitcoinclub/algorand-mit-bitcoin-expo-380a68ebc2b3