Feature Article

Decentralization: The Failed Promise of Cryptocurrencies

Leonardo J. Valdivia
Universidad Panamericana, Facultad de Ingeniería, Zapopan, Jalisco, 45010, México

Jafet Rodriguez
Universidad Panamericana, Facultad de Ingeniería, Zapopan, Jalisco, 45010, México

Carolina Del-Valle-Soto
Universidad Panamericana, Facultad de Ingeniería, Zapopan, Jalisco, 45010, México

Miguel Alcaraz
Universidad Panamericana, Facultad de Ingeniería, Zapopan, Jalisco, 45010, México

***Abstract*—Cryptocurrencies promise to revolutionize the financial market due to two main features: security and decentralization. In this article, the authors analyze whether cryptocurrencies are fully decentralized—in other words, whether the transaction processing is distributed among different entities. In addition, they present the consequences that a possible centralization entails.**

Blockchain provides the means to be part of the global market for anyone interested. This participation comes with the benefits of a high degree of trust, authenticity, and transparency.[1] It is a solution that allows peer-to-peer interaction over a decentralized network without the need for a trusted intermediary. This is achieved through a local database with its own replicated dataset that makes each peer capable of notifying others when data is modified and ensures that all peers maintain the same data.[2]

Digital Object Identifier 10.1109/MITP.2018.2876932
Date of current version 27 March 2019.

Cryptocurrency is a blockchain transaction of a digital asset. Contrary to the current banking system, in cryptocurrencies, there is no central bank that manages the money supply. Instead, the control of cryptocurrencies works through blockchain.[3]

In this article, we analyze whether cryptocurrencies are truthfully decentralized, with decentralization defined as "delegating part of the power exercised by a central agency to different entities."[4] From this perspective, decentralization is fractioning parts of control among several entities, whereby the cryptocurrency is sustained not under the criterion of one entity but of several. In other words, cryptocurrencies base their support on the confidence that the community of

Published by the IEEE Computer Society

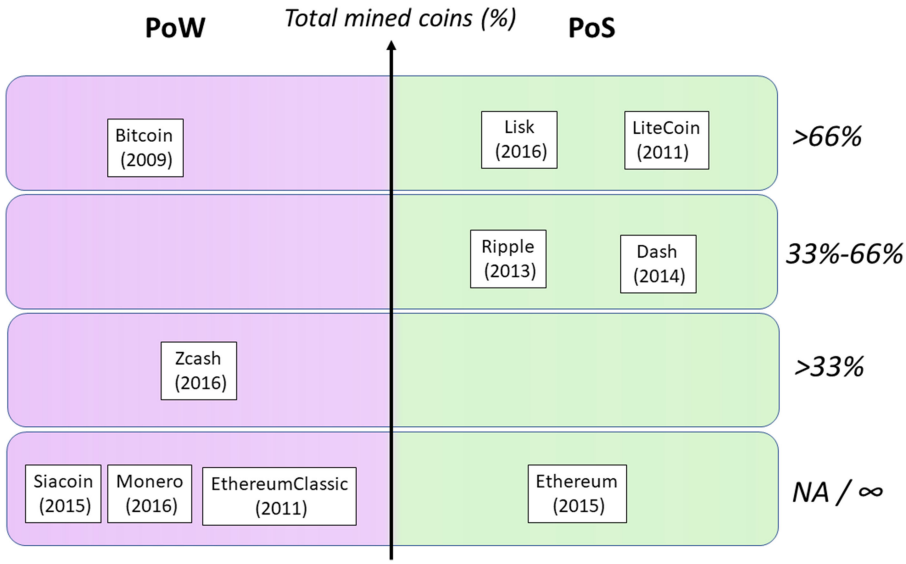

Figure 1. Comparison among the ten most used cryptocurrencies: type of consensus algorithm and supply fullness.

investors gives them and the consensus of all is required to have a working system.

BLOCKCHAIN

As the name implies, blockchain consists of a series of blocks chained together, where a block is a record of new transactions, and the chain is a reference to the block that came immediately before it. The primary objective of the blockchain protocol is to create a secure platform with the features described below.[5]

- Immutable. It is complicated to alter any block.
- Distributed system. A copy of all the blocks is stored with all its members.
- No centralized server. Blockchain does not depend on a central authority that dominates the system, which improves security.

The greatest benefit of this technology is decentralization: The information of all blocks is stored in multiple computers around the globe. Consequently, to change the data of an existing block, it is necessary to change at least 51% of the copies stored. This means that not one single company or entity has full control over the process, improving security.

The most critical part is the validation; once an operation is verified, it is not possible to modify it.

For example, supposing a banking company has all its information stored in a particular branch, a hacker could focus all efforts on attacking only that branch to alter the data. On the other hand, if the banking information is stored in multiple locations, it does not matter if an attacker changes the data in one section since it is backed up in other places. The banking system can check all branches, and the majority must contain the same information—in other words, the attacker needs to alter the same information to at least 51% (the majority) of the banking branches.

Cryptocurrencies

Cryptocurrencies are an application of blockchain technology, and therefore, they share the main features (immutable, distributed systems, and decentralization); additionally, they are defined as digital assets designed to be anonymous and secure.[4] Cryptocurrencies are based on transactions; a transaction is a set of information that defines metadata and the digital bits to be transferred. A person expects his or her transaction to be encrypted and then confirmed by a number of peers, whose confirmations give him or her sufficient confidence that it will not be reversed. Each transaction is broadcast to the network to be validated. The most critical part is the validation; once an operation is verified, it is not possible to modify it.

Currently, two procedures are most commonly used to verify everything is correct by consensus and deterring attacks: Proof of Work (PoW) and Proof of Stake (PoS). The difference between them consists of providing a complicated math problem for a computer to solve (PoW) versus selecting a participant that owns an extensive amount of the currency (PoS).

Figure 1 shows a map where the coordinates indicate where a cryptocurrency is located on a spectrum going from well-matured coins (difficult to mine) to newer coins (easy to mine).[6–8] On the left, we have cryptocurrencies that use PoW as their algorithm to validate blocks. On the right, we have cryptocurrencies that use PoS.[9] At the vertical axis, we use the percentage of mined coins to date compared to the maximum capacity of coins for that currency. If that particular coin does not have a maximum capacity, then it is mapped only on its block time in the lower part of Figure 1. This can help us check the maturation of a currency over time and, if compared with the quantity of mined coins on a given timeframe, can be used as a measure of popularity.

However, is it possible to create a fully distributed platform? Are PoW and PoS algorithms truly decentralized? What are the consequences of a possible centralization?

PROOF OF WORK

In general, PoW is an approach to solve a crypto-puzzle to validate a new block in the chain. Depending on the application, the crypto-puzzle can be different, but like many cryptographic algorithms, this puzzle uses a hash function as a building block. A hash function is a procedure that converts a variable-size message into a fixed-size message (hash value), and it has two main objectives: detect intentional or accidental changes to data and verify if two messages are the same.[10]

Therefore, when a new transaction occurs in the blockchain, it has to be authenticated by all the participants. This is done by solving the crypto-puzzle (hash function). The first one who solves the problem wins and shares the solution with the other participants to validate it, and if it is valid (at least 51% of the participants agree), the block is added to the chain.

With PoW, decisions about essential changes that will be implemented within the system can be made jointly. The majority of votes come from miners, developers, and other influential members of the community, preventing the appearance of one or more leaders. However, some drawbacks are related to the waste of computing power and electricity when continuously generating random assumptions. Besides, the constant appearance of new coins can negatively influence its value.

Therefore, this algorithm has two central problems:

- The complexity of the hash function is directly proportional to the computing power. In other words, the more complex the hash is, more computing power is needed to solve it. With more computing power, it is faster to solve the puzzle.
- All the participants who did not solve the hash function lose time and money (in the form of electricity used by their computers).

Centralization and its Consequences

This section analyzes the two main problems of the PoW algorithm described in the previous section. Additionally, an analysis of how this algorithm could end up centralized is presented.

Computing power The PoW algorithm depends on the processing power; therefore, it is fair to say that a person who owns a computer with high processing power has more chances to solve the crypto-puzzle faster than others. However, some applications such as Bitcoin (the most famous application using PoW as an algorithm) need such high computing power that it is incredibly difficult to find it on just one machine.

One way to measure the amount of computing power is known as the hash rate (hash operations per second). Currently, the Bitcoin network requires around 24.4×10^{18} hashes per second to work.[11] To put this in perspective, a commercial computer is around 30×10^{3} hashes per second.

Accordingly, some private companies have created mining pools to try to solve the computing power issue. A mining pool is built as a series of computers that share their processing power over a network; they can split the rewards (if

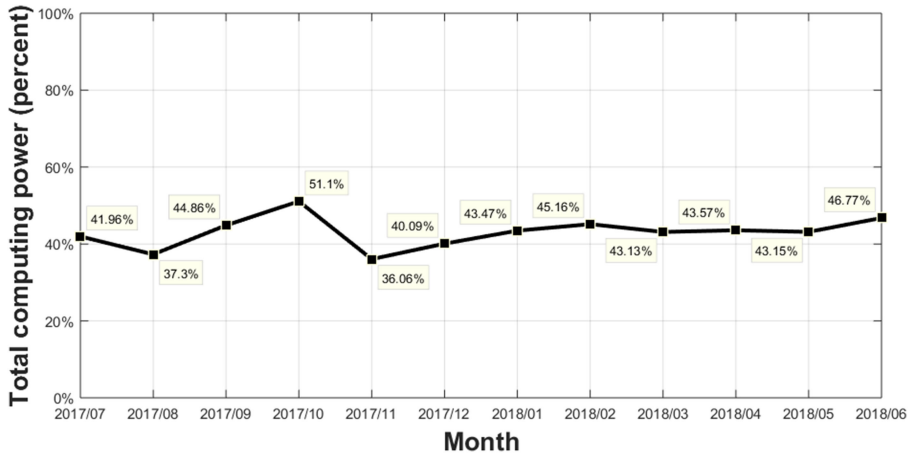

Figure 2. One-year historical data of the combined computing power of the top three mining pools.

any) according to the resources used to solve the crypto-puzzle.

Hence, theoretically, a mining pool can be big and powerful enough to control all transactions (they would always solve the crypto-puzzle before anyone else). Unfortunately, this is happening. Figure 2 shows the one-year historical data of the three biggest mining pools, and they have between 40% and 50% of the computing power needed in the Bitcoin network.[12]

Figure 2 confirms how the PoW algorithm tends to centralize. This is a logical conclusion if an increasingly advanced and expensive technology is required, given that companies with more significant resources will have more possibilities to outperform the competition.

The disadvantages of centralization are explained below.

- Security (performance). According to Figure 2, it is only necessary to focus a malicious attack in a few companies (the biggest pools). Moreover, if the three biggest mining pools are attacked, almost 45% of the processing power required for the Bitcoin network is at risk; therefore, it is probable that an attack results in a network failure.
- Security (transaction). If a company can control the majority of the mining power (51%), it would have the ability to reverse new transactions.
- Wallet security. With PoW, it is possible to have private wallets. However, users find maintaining local wallets cumbersome and do not want to download the entire blockchain during client installation. They prefer to use the services of wallet providers, who store wallets online, regardless of how the mining is done.[13]
- Fees. If only a few companies can offer the mining service, they can include fees for the transaction, as there is no competition.
- Availability: If one of the mining pools is down, the service is interrupted.

It is important to mention that even a group with 51% of the mining power does not have total control over the chain. Currently, it is very complicated to change previous blocks—the older the transactions are, the more difficult it will be to replace them. However, it is possible to change new blocks to reverse transactions. An attack probability on many mining pools might be low because attackers may try to redirect mining capabilities to a competing group. However, there is the fact that an attacker who has a processing power equivalent to 10% of the blockchain has a 50% chance of making a successful attack by delaying communication between several sub-groups for at least 20 min.[14]

Moreover, there is another problem with the PoW algorithm that affects everyone, even those who do not use blockchain or cryptocurrencies: energy consumption.

Energy consumption One consequence of the absurd processing power required for Bitcoin mining is energy consumption. With more processing power, more energy is needed by the miners. According to Tosh *et al.*, the annual

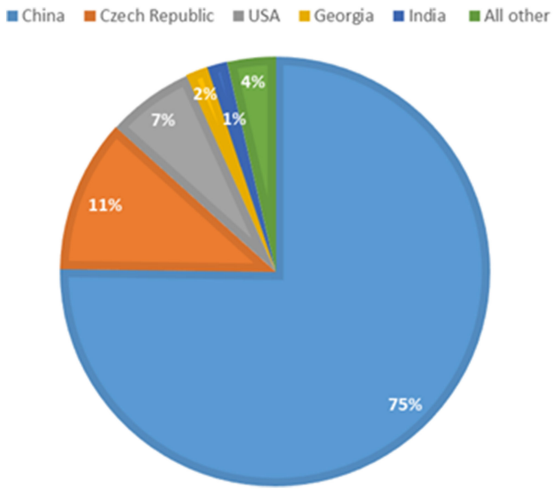

Figure 3. Hash rate power distribution by country.

estimated electricity consumption of Bitcoin is 15.77 TW, which is 0.08% of the world's electricity consumption.[15]

Figure 3 shows the world distribution of the hash rate. China is the country where most of the mining pools are located, and as a result, the hash rate power is centralized there.

The centralization of energy consumption entails some disadvantages:

- Social problems: Due to the high consumption, the energy generation costs may rise, affecting whole populations. Additionally, the stability of the electrical grid could also be affected.
- Pollution (especially with centralization in China): In China, 87% of total energy generation is produced by fossil fuels.[16]
- Governments: Blockchain technology, especially cryptocurrencies, is not regulated by many countries; therefore, a restrictive regulation in a country with a high hash rate will affect the network directly.

In order to solve the problems presented above, a new algorithm was created—PoS. The next section analyzes this algorithm to realize if it is truly decentralized.

PROOF OF STAKE

This algorithm was created as an alternative to PoW, and its uses focus mainly on cryptocurrencies. PoS has the same objective as PoW: to provide a consensus between many actors (miners). Unlike PoW, in which the probability of mining a block (solve the crypto-puzzle) depends on the processing power of the miner, in PoS, it is necessary to have a stake in the currency to participate. Usually, this comes to prove the ownership of a certain number of cryptocurrency units (coins).[17]

Therefore, in PoS the validator and creator of a new block depends on the number of coins owned, also defined as stake (someone who possesses 10% of the total coins in existence can mine 10% of the blocks).[18]

The PoS algorithm solves one of the biggest problems of PoW: energy consumption. Since it is not necessary to validate and create a new block as fast as possible to win (like PoW), the hardware costs are much lower than the costs associated with the PoW system. However, this algorithm has two main problems:

- It benefits wealthy people: Everyone with traditional money can buy cryptocurrency; therefore, the more cryptocurrency one has, the more blocks one can mine.
- Security: The wallet (wealth information) of the miners must be online in order to participate in the creation of new blocks.

This model does not require advanced computer equipment, costs are lower, and there is no pressure on the price.

However, one of the disadvantages of accumulating coins is that selling them is counterproductive because one loses stake. Besides, instead of using the cryptocurrency as a form of payment (what should be its main purpose), it is used to have more in the stake. That means that the users who possess the most also have more significant power to decide on the changes that are implemented in the system. The former contradicts the principle that cryptocurrencies should not have a central authority.

Centralization and its Consequences

This section analyses the two main problems of the PoS algorithm described in the previous section.

PoS BENEFITS WEALTHY PEOPLE As mentioned before, this algorithm is environmentally friendly, especially when compared to PoW. However, PoS also requires resources such as hardware, electricity, and Internet connection; therefore, it also has real-world costs (much less than PoW).

Hence, people who own more coins have a cheaper cost than people with smaller stakes. For example, let us assume that two people have identical computers, but one person has twice as much cryptocurrency units as the other—then the costs of mining are the same (same energy consumption, same hardware cost, etc.). However, the person who owns more coins has twice the chance of being selected to create a new block. Thus, with the same hardware investment, one person wins more money (for each built block the miner rewarded) than the other, just because one person previously had more stake.

Therefore, given the fact that the more cryptocurrency wealth is accumulated, the higher the profit margin will be, any investor would try to increase his or her crypto-wallet funds for better profits. Then, a bigger crypto-wallet would grow faster than a smaller one.

It is important to note that the current cryptocurrency global wealth is around $300 billion—this number is far away from the traditional global wealth that is approximately $84 trillion.[19] However, cryptocurrencies went from $160 million to $300 billion in just one year. With this growth rate, cryptocurrencies become an attractive investment opportunity for wealthy people. According to the annual wealth report, 21% of ultra-rich people (billionaires) increased their investments in cryptocurrencies in 2017.[20] Then, people with such an amount of money can take more risk and buy more cryptocurrency coins.

This makes it clear that the PoS algorithm would be centralized due to the people with the economic capacity to buy more. Moreover, if one company or person owns more than 50% of cryptocurrency units, it is possible to control the transactions, since it will always be chosen to create a new block. This centralization causes the same problems as those explained in Section "Proof of Work," such as performance security, transaction security, fees, and availability.

PoS security The main feature of PoS may become its greatest weakness because the algorithm chooses the miner based on the amount of coins in his or her public wallet. Therefore, there is a deterministic algorithm. In theory, it is possible to know which wallet will be picked as the next validator; therefore, a hacker can focus his or her efforts on attacking this wallet, being able to alter the new block, delete the transaction, or change the order of the blocks.

This leads to a very dangerous attack; if hackers can edit the information of a block, they can alter it in such a way that enables them to be the new validator. Then, the attackers can earn money without the need to invest in the cryptocurrency.

Paradoxically, one solution to this problem is centralization: having a limited number of trusted "judges" that keep a copy of the blocks that were initially received. When they receive an alternative version of one block, it will indicate a problem in the chain. Therefore, a chosen few are responsible for validating all transactions. This configuration mirrors how the current banking system works. This provides an extra layer of security but encourages centralization.

CONCLUSION

Based on the analysis done in this paper, we can see how eventually cryptocurrencies shift from decentralization to centralization. Initially, they all start decentralized, but as time passes, both algorithms begin favoring a select group. In other words, in the case of PoW, the participants with more computing power can win faster, and eventually, the problems to solve are so incredibly complex that only the most powerful are capable of keeping pace. Therefore, the same happens with PoS, since the participants with a massive collection of the cryptocurrency coins are selected to continue mining.

Another important aspect is the popularity; popular currency will attract more attention. This attention will be especially evident on organized miners with high hashing power. This, in turn, will generate centralization. Comparatively, a newer currency with a low percentage of total coins mined will attract another kind of miners—those who are more adventurous and want to discover the newer currencies before they are famous. The profile of these miners makes them have lower hash power and work as a more granulated force, just as the Bitcoin designers expected. Nevertheless, as we have exposed, eventually these currencies will fall in the other spectrum as increasingly more blocks are mined.

The most important decisions regarding the direction a cryptocurrency will take are considered and voted by a diversified network of investors, without a person or group able to control such decisions. However, within the cryptocurrency ecosystem, there are small centralized groups that promote the accumulation of mining power. With these dual affirmations, the propagating nature of decentralization is combined with the efficiency of centralization.

Therefore, the main consensus and validation algorithms (PoW and PoS) used in cryptocurrencies cannot guarantee decentralization. On the contrary, the more mature the cryptocurrency, the more centralized it becomes. Additionally, it is important to note that a centralized cryptocurrency cannot guarantee security, because if an entity controls the network, it also takes control over new transactions, even being able to reverse transactions. For now, the promise of having a secure and decentralized cryptocurrency cannot be fulfilled.

REFERENCES

1. N. Kshetri, "Blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manage.*, vol. 39, pp. 80–89, 2017.
2. P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Secur. Privacy.*, vol. 16, no 4, pp. 20–29, Jul./Aug. 2018, arXiv:1801.03294.
3. B. A. Tama *et al.*, "A critical review of blockchain and its current applications," in *Proc. IEEE 2017 Int. Conf. Elect. Eng. Comput. Sci.*, 2017, pp. 109–113.
4. F. A. Ahmad, "Bitcoin: Digital decentralized cryptocurrency," in *Handbook of Research on Network Forensics and Analysis Techniques*, Hershey, PA, USA: IGI Global, 2018, pp. 395–415.
5. R. Chatterjee and R. Chatterjee, "An overview of the emerging technology: Blockchain," in *Proc. 3rd Int. Conf. Comput. Intell. Netw.*, 2017, pp. 126–127.
6. A. S. Hayes, "Cryptocurrency value formation: An empirical study leading to a cost of production model for valuing bitcoin," *Telematics Informat.*, vol. 34, no. 7, pp. 1308–1321, 2017.
7. WhatToMine. Available at: https://whattomine.com/, 2018.
8. "All coins," CoinMarketCap. Available at: https://coinmarketcap.com/coins/views/all/, 2018.
9. A. Kiayias *et al.*, "Ouroboros: A provably secure proof-of-stake blockchain protocol," *Annual International Cryptology Conference*. New York, NY, USA: Springer, 2017, pp. 357–388.
10. D. Gupta, J. Saia, and M. Young, "Proof of work without all the work," in *Proc. 19th Int. Conf. Distrib. Comput. Netw.*, 2018, p. 6.
11. "Hash rate," Blockchain Luxembourg. Available: https://blockchain.info/es/charts/hash-rate.
12. "Hashrate distribution," Blockchain Luxembourg. Available: https://www.blockchain.com/en/pools
13. A. Gervais *et al.*, "Is bitcoin a decentralized currency?," *IEEE Secur. Privacy*, vol. 12, no. 3, pp. 54–60, May/Jun. 2014; doi:10.1109/MSP.2014.49.
14. A. Laszka, B. Johnson, and J. Grossklags, "When bitcoin mining pools run dry," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2015, pp. 63–77.
15. D. K. Tosh *et al.*, "Consensus protocols for blockchain-based data provenance: Challenges and opportunities," in *Proc. 8th Annu. Ubiquitous Comput., Electron. Mobile Commun. Conf.*, 2017, pp. 469–474.
16. "Fossil fuel energy consumption," *World Bank Group*. Available: https://data.worldbank.org/indicator/EG.USE.COMM.FO.ZS?end=2014&locations=CN&start=1971&view=chart
17. J. Spasovski and P. Eklund, "Proof of stake blockchain: performance and scalability for groupware communications," in *Proc. Int. Conf. Manage. Emergent Digital EcoSystems*, 2017, pp. 251–258.
18. "Proof of stake," *Bitcoin Wiki*. Available: https://en.bitcoin.it/wiki/Proof_of_Stake, 2018.
19. "Total Market Capitalization, CoinMarketCap. Available: https://coinmarketcap.com/charts/, 2018.
20. "The wealth report," *Knight Frank*, 2018. Available: https://www.knightfrank.com/resources/wealthreport2018/the-wealth-report-2018.pdf

Leonardo J. Valdivia received the M.S. degree in telecommunications engineering and the Ph.D. degree in embedded systems. After spending three years working on software for the automotive sector, in 2013, he started working for the railway sector, specifically in safety and security integration. At present, his research interests include blockchain applications. Contact him at lvaldivia@up.edu.mx.

Carolina Del-Valle-Soto received the Ph.D. degree in information technology and communications. Her skills are focused on the application and development in the areas of telecommunications,

specifically wired and wireless networks, programming, and security. Contact her at cvalle@up.edu.mx.

Jafet Rodriguez received the Master of Science degree in computer science with a specialization in computer graphics. His main research interests include human–computer interactions, computer graphics, extended reality, apps, and video games applied to rehabilitation, education, and commercial products. Contact him at arodrig@up.edu.mx.

Miguel Alcaraz is a Professor with Universidad Panamericana, Guadalajara, Mexico. He works in algorithm design and its applications in image processing and social network design. He received the Ph.D. degree in optics for designing and prototyping a holographic printer. He has worked on image transference and compression algorithms for images. Contact him at malcaraz@up.edu.mx.