Blockchain Technology: A Review of the Current Challenges of Cryptocurrency

Diego Valdeolmillos[1] , Yeray Mezquita[1(✉)] ,
Alfonso González-Briones[1,2(✉)] , Javier Prieto[1(✉)] ,
and Juan Manuel Corchado[1,2,3,4(✉)]

[1] BISITE Research Group, University of Salamanca,
Calle Espejo 2, 37007 Salamanca, Spain
{dval,yeraymm,alfonsogb,javierp,corchado}@usal.es
[2] Air Institute, IoT Digital Innovation Hub (Spain),
37188 Carbajosa de la Sagrada, Spain
[3] Department of Electronics, Information and Communication,
Faculty of Engineering, Osaka Institute of Technology, Osaka 535-8585, Japan
[4] Pusat Komputeran dan Informatik, Universiti Malaysia Kelantan,
Karung Berkunci 36, Pengkaan Chepa, 16100 Kota Bharu, Kelantan, Malaysia

Abstract. As a result of the 2017 boom in the cryptocurrency market, some governments around the world have begun to work in the direction of regularizing and supervising digital currency. People have gained trust in the use of cryptocurrency thanks to the security of the blockchain technology and of their economic ecosystem. This paper reviews the challenges faced by five different cryptocurrencies with the highest market capitalization. Furthermore, we analyze the blockchain technology that underlies them.

Keywords: Blockchain technology · Legal framework · Cryptocurrencies · Review

1 Introduction

The financial crisis of 2008 has shown that banks and centralized financial institutions have breached the trust of the people who deposit their money in them, by lending it while keeping very little in reserve. Bitcoin emerged in 2009 as an answer to those transgressions, the solution it provided was to have a currency without the need of a central authority [1].

The Bitcoin platform comprises a series of cryptographic protocols that totally transform the way in which transactions are made. Thus, this platform has brought the financial system one step closer to a true democratic economy constructed by the community. The Blockchain Technology (BT), on which Bitcoin operates, implements a distributed ledger across the peer-to-peer network of actors that participate in the system. This technology makes possible to validate and verify the transactions carried out within the Bitcoin platform. Thanks to this, a central body that acts as a trusted intermediary is no longer necessary [15]; the nodes of the blockchain network provide users with confidence and security in carrying out transactions.

The use of BT is becoming widespread among applications that require the use of digital records and transactions between non-trusted parties. These applications range from financial services to asset traceability and much more. Their incorporation of BT is innovative because it allows non-trusted parties to reach agreements called smart contracts [5].

In most cases, smart contracts make it possible to establish agreements in an autonomous way and without the need of intermediaries [14, 16, 18]. However, in some cases, due to the limited capacity of the blockchain to interact with the real world, the establishment of those contracts requires an external entity called oracle. The oracle is an intermediary between the data inside the blockchain and the data outside of it [17, 20].

BT-based platforms are a type of Distributed Ledger Technology (DLT) system, but not all DLT systems make use of BT. Every cryptocurrency has its own underlying DLT platform, with distinct features. The variations in the DLT platforms may include the algorithm they employ for consensus between the nodes of the network, the rate at which new coins are created, the maximum size of each block of data where transactions are stored, etc.

DLT can be used in a system to improve robustness against traditional cyberattacks. The problem resides in the fact that only a few consensus algorithms are used by the vast majority of cryptocurrencies leaving the door open to the appearance of new specific cyberattacks against this kind of platforms [26]. Despite it, the fact that the networks and protocols that underlies some cryptocurrencies are somehow safe and sound against those attacks, continue attracting new investors and capital to their market.

Considering the boom and the capitalization of the cryptocurrency market that occurred in 2017, some governments around the world have begun to work in the direction of creating measures for the regularization and supervision of digital currency. A prominent case is that of Malta, whose government has adopted a legal framework in 2018 in which systems based on DLTs are granted legal certainty [6].

This paper reviews some of the cryptocurrencies and the challenges they face. It is structured as follows: Sect. 2 provides background information on BT and some of their actual challenges. Section 3 analyzes five cryptocurrencies with the highest market capitalization. Finally, Sect. 4 concludes this review.

2   Background

BT has been created with the intention of replacing the current, centralized financial system. The authors of [13] claim that BT is capable of replacing intermediaries while ensuring the security of platforms. BT offer resistance to traditional cyberattacks, but as this technology gains widespread adoption, they are being developed new attacks specifically for hacking it.

Distributed Denial Of Services (DDOS) attacks are the most common. A kind of DDOS attack is the Malleability attack, produced when an attacker create a copy of a transaction but with another ID, which makes the user spend double for it [26]. This attack occurs when a system that make use of a blockchain, like a bitcoin exchange,

have flaws in the implementation of the code that allows the trading of cryptocurrencies.

The eclipse and sybil attacks have similar bases. In both, the attacker gains control of a large number of IP addresses of the network and surrounds the victim with them. In Eclipse attacks, the victim is not allowed to obtain transactions they are interested in, it has been successfully carried out in the Ethereum blockchain by Researchers from the University of Boston. In a Sybil attack, the victim is influenced by the voting power of the attacker nodes and the information they send to it, which makes the victim vulnerable to double spend attacks.

A 51% or majority attack occurred when a single entity owns the majority of the voting power of a network. An attacker who wants to take advantage of this condition can create a fork of the main chain with the transactions it wants to be done. The small cryptocurrencies are at risk because their networks are composed of few nodes.

The more proven a BT-based platform is against the attacks previously mentioned, the more trust the users give in the cryptocurrency it underlies. As a result of that trust its economic ecosystem will grow, which will translate into an increment in the value of the cryptocurrency [13].

Some of the differential aspects of a BT based platform are: the consensus algorithm that the peers of the network use to add new blocks to the blockchain; the way in which the network is governed; and its capability to execute code that does or does not allow to deploy Turing-complete Smart Contracts in the blockchain.

Relating to the consensus algorithm, there is an increasing number of them and their own variations. The most widespread algorithms are the most proved, that's why they, or a their variations, are shared by the vast majority of the cryptocurrencies [2].

In the Proof-of-Work (PoW) algorithm, to add a new block to the blockchain a cryptographic problem must be solved. The computational cost and the difficulty of solving the problem, the energy spent on searching for its solution (work) and the simplicity of verifying it, are enough reasons to encourage the nodes that wants to add new blocks (miners) not to cheat by adding illegal transactions.

Proof-of-Stake (PoS) is a consensus algorithm, in which miners take turns at adding new blocks. The probability of a miner to receive the turn to add a block depends on the amount of coins deposited as escrow (Stake). This algorithm assumes that a node is going to be honest in order to avoid losing the escrow.

The Practical Byzantine Fault Tolerance (PBFT) the process of adding a new block is called a round. In each round a node is selected to propose a new block, the block needs to receive 2/3 of the votes of all the nodes in the network in order to be valid.

Currently, every consensus algorithm has its own risks and vulnerabilities. For example, PoW wastes a massive amount of energy to produce new blocks. It is very limited in terms of scalability and its mining pools are centralized [23]. In the case of the PoS algorithm, its Nothing at a Stake theory causes to occur forks more frequently in the blockchain than with other consensus algorithms [3]. In the case of PBFT the main risk is that it is a permissioned protocol and not a truly decentralized one [4]. In Table 1 it has been done a comparative between the mentioned algorithms and their three most important characteristics: scalability, consistency and decentralization.

Table 1. Comparison of the consensus algorithms.

Consensus algorithm	Scalable	Consistent	Decentralized
PoW	No	Yes	Yes
PoS	Yes	No	Yes
PBFT	Yes	Yes	No

When there is no consensus in the governance of a blockchain among all the nodes of the network, there is a risk that a hard fork will be produced, splitting the community of the platform. An example of this is when the DAO hack of Ethereum occurred, creating two different blockchains: one called Ethereum classic while the other just Ethereum [7]. This was in effect, a breach of Ethereum's immutability and it left a sizeable minority of the community bitterly dissatisfied.

The possibility of executing Smart Contracts within a blockchain system supports the development of decentralized Applications (dApps) [19, 25]. This feature, if available on a platform, can help grow the economical ecosystem of a cryptocurrency by adding use cases in which the cryptocurrency is used in the form of dApps. This helps attract more users and investors who are eager to use the cryptocurrencies.

The possibility of deploying Turing-complete Smart Contracts appeared with Ethereum [8]. This kind of blockchains are called second generation blockchains and experience the same scalability problems as the first generation blockchains, platforms that do not allow the development of Turing-complete smart contracts. However, some of these BT-based platforms support the development of simple non-Turing-complete smart contracts, like in the case of Bitcoin [21].

The third generation of blockchains has come about to increase the number of users and uses of BT-based systems. These blockchain platforms aim to provide solutions to the scalability problems of previous generation blockchains and allow for the mass adoption of dApps in the daily life of people. Examples of third generation blockchains are Tron, Cardano and EOS.

Right now, investors are speculating with the value of the coins in order to increase their income by exchanging cryptocurrencies of different types. That's why, the more people store their wealth in a cryptocurrency, the more difficult to let single fortunes control the fluctuations of its value [24].

3   Cryptocurrencies and Technologies

Part of the value of cryptocurrencies lies in the characteristics of the BTs on which they are based and in the economic ecosystem that supports them. For this reason, this section describes the distinctive characteristics of five currencies with the highest market capitalization, listed by CoinMarketCap [9].

Bitcoin (BTC). Bitcoin was the first use case of the BT. It has gained trust among cryptocurrency users as it has proven, indisputably, the security of its technology. This explains why it is the most used cryptocurrency in the world. However, it has some downsides too; its consensus algorithm is PoW, meaning that it wastes a lot of energy when adding new blocks to its blockchain and it is not scalable.

Ether (ETH). The Ether cryptocurrency is supported by the Ethereum blockchain. It was the first use case in which smart contracts were deployed and the most used Smart Contract platform. The value of this cryptocurrency comes from the fact that its underlying BT offers the possibility of developing dApps that will help the Ether economic ecosystem grow [8]. The problem with Ethereum is that it uses the same kind of consensus algorithm as Bitcoin, making the dApps impossible to escalate in terms of number of users and mainstream adoption by the people. Also, its high fees are a big problem in the way to deploy a dApp capable of handle micro-payments.

Ripple (XRP). This cryptocurrency is housed in the Ripple blockchain. It is scalable, being able to handle up to 1500 transactions per second, which means it has the potential to replace international payment systems like VISA and costs a fraction less. Ripple makes use of the Ripple Protocol Consensus Algorithm (RPCA). It is a variant of the PBFT which makes use of collectively trusted subnetworks of a larger network of validators [10]. The downside of this Consensus algorithm is that it is more centralized than its competitors. This is not a real problem form this platform, because the XRP cryptocurrency was designed a method of helping banks facilitating cross-border money transfers operations between them.

EOS. The EOS cryptocurrency based BT is one of the third generation blockchains. It has a scalable and feeless blockchain while it makes possible to deploy dApps within it. EOS's consensus algorithm is called delegated Proof of Stake (dPoS), a variation of the PoS in which the nodes of the network vote for their representatives according to their stake of funds, which will be the ones that add blocks to the blockchain. This algorithm doesn't have the Nothing at a Stake problem because, under normal conditions, the block producers cooperate to produce blocks rather than compete, making it impossible for any forks to occur [11].

Tether (USDT). Tether is one of the so-called stable coins. It is called that way because it is a non-volatile and stable cryptocurrency used as a dollar substitute in digital environments. To maintain a one-to-one reserve ratio between this cryptocurrency token and its associated real-world asset, the fiat currency, the USD reserves of Tether Limited, should be equal to or greater than the number of USDT in circulation. Tether is backed up by the Bitcoin blockchain via the Omni Layer protocol. This protocol is a software layer that enables next-generation features in the Bitcoin blockchain [12]. It provides off –chain scalability without the need to change the underlying BT.

To do a comparative analysis of the described currencies, we have created a table which includes a selected set of features of the technologies that underlie them, see Table 1. Distinctive features of the technology have been chosen, such as the consensus algorithm of the BTs; the scalability provided by the BT; and whether it is possible or not to deploy smart contracts within its BT. To show the activity of the ecosystem built around those cryptocurrencies, other features have been obtained from Coin Metrics, like the number of completed Transactions Per Second (TPS) and addresses that were active on January 28th, 2019, [22].

Table 2. Comparison of the features of the described cryptocurrencies.

Cryptocurrency	Consensus algorithm	Scalability	Smart Contracts	Transaction count	Active addresses
Bitcoin	PoW	No, ∼7 TPS	Non-Turing-Complete	307.917 K	636.805 K
ETH	PoW	No, ∼7 TPS	Turing-Complete	568.564 K	242.449 K
XRP	RPCA	∼1500 TPS	Not yet	455.801 K	5.986 K
EOS	dPoS	Yes, ∼10 k TPS	Turing-Complete	6.33593 M	91.347 K
Tether	Omni Layer protocol over Bitcoin	Yes, off-chain scalability	Not yet	20.244 K	10.819 K

By looking at Table 2, one may infer that the number of active addresses of a currency is related to its position in the market capitalization ranking. However, XRP is an exception to this rule. The reason for this is that it is not used by individuals, but by large corporations, like banks. Also, the currencies that are most used are the ones whose underlying BT makes use of a PoW consensus algorithm.

It is possible to explain why ETH has more daily transactions than Bitcoin due to the use of dApps. Furthermore, the high transaction count of the EOS platform is explained by the activity of the dApps deployed within it and its dPoS consensus algorithm, which can handle a large number of TPS.

In [22] you can see that the EOS cryptocurrency has an upward trend in the number of active addresses, this means that over time users gain trust in the technology that underlies this currency and as a result the number of active addresses increases.

4   Discussion

The rise of BT has contributed to the appearance of a great number of different cryptocurrencies. Each one of them is supported by a DLT platform, whose technology builds user trust in the cryptocurrency and therefore contributes greatly to its value.

The cryptocurrency capitalization market is growing because more investors are putting their money in it. Some countries, like Malta, have seen the potential of cryptocurrency as the main financial service of the future and have started to create legal regulations in order to offer investors a legal framework that covers cryptocurrency activities.

Although BT is a solution to improve security of the data in a traditional system, it is being targeted by new and specific types of cyberattacks. The most popular consensus algorithms, shared by the majority of the cryptocurrencies, are being modified and updated in order to face the specific vector attacks that are aiming to hack BT based systems. It is shown in the analysis carried out in this paper.

The major problem actual consensus algorithms are facing actually is the impossibility to obtain a platform globally scalable, consistent and fully decentralized. All of them have flaws in some of the listed points. Also, another problem is the governance of the network that underlies a BT platform.

Some of the cryptocurrencies are offering their users the possibility of developing and deploy Turing-complete implemented dApps within their economic ecosystem, bringing more functionality to it apart from the trading of assets. This is a measure that not all the cryptocurrencies allow, for example, from the five analyzed, just two of them allow it.

The two cryptocurrencies with most market capitalization make use of the PoW consensus algorithm. Their number of active accounts and transactions per day indicate that this algorithm offers everything their actual ecosystems need. If the ecosystem would grow, in terms of active accounts or number of transactions realized due to the massive adoption of dApps, there are different consensus algorithms like in the case of EOS or XRP.

The fluctuations in the price of the cryptocurrencies due to speculative movements of capital, difficult their use in the daily life of people. But, because the deflationary nature of the cryptocurrencies, if people store their wealth in cryptocurrencies, they would be more robust against the speculative movements made by single great fortunes.

References

1. Nakamoto, S.: Bitcoin: a peer-to-peer electronic cash system. (2008)
2. Zheng, Z., et al.: An overview of blockchain technology: architecture, consensus, and future trends. In: 2017 IEEE International Congress on Big Data (BigData Congress). IEEE (2017)
3. Martinez, J.: Understanding proof of stake: the nothing at stake theory. https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027. Accessed 27 Jan 2019
4. Witherspoon, Z.: A hitchhiker's guide to consensus algorithms. https://hackernoon.com/a-hitchhikers-guide-to-consensus-algorithms-d81aae3eb0e3. Accessed 27 Jan 2019
5. Casado-Vara, R., Corchado, J.M.: Blockchain for democratic voting: how blockchain could cast off voter fraud. Orient. J. Comp. Sci. Technol., **11**(1) (2018)
6. Parliamentary Secretariat for Financial Services (Digital Economy and Innovation, Prime Minister Office), Malta a Leader in DLT Regulation. https://www.fff-legal.com/wp-content/uploads/2018/02/FSDEI-DLT-Regulation-Document.pdf. Accessed 21 Jan 2019
7. Mehar, M.I., et al.: Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. J. Cases Inf. Technol. (JCIT) **21**(1), 19–32 (2019)

8. Buterin, V.: A next-generation smart contract and decentralized application platform. white paper (2014)
9. CoinMarketCap. https://coinmarketcap.com/. Accessed 16 Feb 2019
10. Schwartz, D., Youngs, N., Britto, A.: The Ripple protocol consensus algorithm. Ripple Labs Inc White Paper 5 (2014)
11. Cox, T.: EOS.IO technical white paper. GitHub repository (2017)
12. Omni Layer. https://www.omnilayer.org. Accessed 30 Jan 2019
13. Hawlitschek, F., Notheisen, B., Teubner, T.: The limits of trust-free systems: a literature review on blockchain technology and trust in the sharing economy. Electron. Commer. Res. Appl. **29**, 50–63 (2018)
14. Casado-Vara, R., González-Briones, A., Prieto, J., Corchado, J.M.: Smart contract for monitoring and control of logistics activities: pharmaceutical utilities case study. In: The 13th International Conference on Soft Computing Models in Industrial and Environmental Applications, pp. 509–517. Springer, Cham, June 2018
15. González-Briones, A., Valdeolmillos, D., Casado-Vara, R., Chamoso, P., Coria, J.A.G., Herrera-Viedma, E., Corchado, J.M.: Garbmas: simulation of the application of gamification techniques to increase the amount of recycled waste through a multi-agent system. In: International Symposium on Distributed Computing and Artificial Intelligence, pp. 332–343. Springer, Cham, June 2018
16. Casado-Vara, R., Chamoso, P., De la Prieta, F., Prieto, J., Corchado, J.M.: Non-linear adaptive closed-loop control system for improved efficiency in IoT-blockchain management. Inf. Fusion **49**, 227–239 (2019)
17. González-Briones, A., Castellanos-Garzón, J.A., Mezquita Martín, Y., Prieto, J., Corchado, J.M.: A framework for knowledge discovery from wireless sensor networks in rural environments: a crop irrigation systems case study. Wirel. Commun. Mob. Comput. (2018)
18. Casado-Vara, R., de la Prieta, F., Prieto, J., Corchado, J.M.: Blockchain framework for IoT data quality via edge computing. In: Proceedings of the 1st Workshop on Blockchain-enabled Networked Sensor Systems, pp. 19–24. ACM, November 2018
19. Casado-Vara, R., Prieto, J., De la Prieta, F., Corchado, J.M.: How blockchain improves the supply chain: Case study alimentary supply chain. Proc. Comput. Sci. **134**, 393–398 (2018)
20. Curran, B.: What are Oracles? Smart Contracts, Chainlink & "The Oracle Problem". Accessed 15 Feb 2019
21. Kaiser, I.: A Decentralized Private Marketplace: DRAFT 0.1
22. Coinmetrics. https://coinmetrics.io. Accessed 20 Jan 2019
23. Beikverdi, A., Song, J.S.: Trend of centralization in Bitcoin's distributed network. In: 2015 IEEE/ACIS 16th International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD). IEEE (2015)
24. Knowledge@Wharton, How the Blockchain Will Impact the Financial Sector, 16 November 2018. http://knowledge.wharton.upenn.edu/article/blockchain-will-impact-financial-sector/. Accessed 23 Jan 2019
25. Casado-Vara, R., Prieto, J., Corchado, J.M.: How blockchain could improve fraud detection in power distribution grid. In: The 13th International Conference on Soft Computing Models in Industrial and Environmental Applications, pp. 67–76. Springer, Cham, June 2018
26. Bryck, A.: Blockchain attack vectors: vulnerabilities of the most secure technology. https://www.apriorit.com/dev-blog/578-blockchain-attack-vectors. Accessed: 26 Mar 2019