Avrupa Bilim ve Teknoloji Dergisi
Özel Sayı 29, S. 6-10, Aralık 2021

Araştırma Makalesi

www.ejosat.com ISSN:2148-2683

European Journal of Science and Technology
Special Issue 29, pp. 6-10, December 2021

Research Article

The Improvement needs in Blockchain Technology

Arif Furkan Mendi[1*]

[1*] HAVELSAN, Ankara, Türkiye (ORCID: 0000-0002-0750-4012), afmendi@havelsan.com.tr

(International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT) 2021 – 21-23 October 2021)

(**DOI:** 10.31590/ejosat.1009560)

ATIF/REFERENCE: Mendi, A. F. (2021). The Improvement needs in Blockchain Technology. *European Journal of Science and Technology*, (29), 6-10.

Abstract

Bitcoin's attack in finance has caused a new wind to blow in the stock market and with the emergence of many new crypto currencies, the crypto currency market has become a new financial area. Although Blockchain technology is the technological infrastructure of Bitcoin, awareness is not as high as Bitcoin. Despite it was found in 1992, its first use was in the shadow of Bitcoin, influenced by the fact that it was with Bitcoin in 2008. However, due to the features that it provides; Without Blockchain technology, the Bitcoin system would not work. As the dazzling offer of Bitcoin; through the decentralized structure, buyers and sellers can meet directly on a platform and make their purchases securely, without involvement of any third party. Verification in the system can only be done by approving by more than 50% of the participants. Thus, besides of no need for a central authority, it became almost impossible for any cyber attack to be successful. The continued success of Blockchain technology is vital for Bitcoin and other cryptographic currencies survival. Beside of all these advantages, there are some issues that need to be addressed for Blockchain technology. These can be listed as throughput, latency in processing, size and bandwidth, some security vulnerabilities, resource waste for adding a new block to chains, usability, and privacy. In this article, we will discuss these issues that need to be addressed for Blockchain technology.

Keywords: Blockchain, Blockchain Restrictions, Blockchain Problems

Blokzincir Teknolojisinde İyileştirilmesi Gerekenler

Öz

Bitcoin kripto parasının finans alanında yapmış olduğu atak, borsada yeni bir rüzgarın esmesine neden olmuş ve birçok yeni kripto para biriminin ortaya çıkmasıyla kripto para piyasası yeni bir finans alanı haline gelmiştir. Blokzincir teknolojisi Bitcoin'in teknolojik altyapısı olsa da bilinirliği Bitcoin kadar yüksek değil. 1992 yılında bulunmasına rağmen ilk kullanımı 2008 yılında Bitcoin ile birlikte olmuş ve bu sebeple Bitcoin'in gölgesinde kalmıştır. Fakat; blokzincir teknolojisi olmadan Bitcoin sisteminin çalışması mümkün değildir. Bitcoin sahip olduğu merkezi olmayan yapı sayesinde, alıcı ve satıcıları doğrudan bir platformda buluşturmakta ve herhangi bir üçüncü tarafın katılımı olmadan güvenli bir şekilde alışverişlerini gerçekleştirmelerine imkan sağlamaktadır. Sistemde doğrulama ancak katılımcıların %50'sinden fazlasının onayı ile yapılabilmektedir. Böylece merkezi bir otoriteye ihtiyaç duyulmamasının yanı sıra herhangi bir siber saldırının başarılı olması neredeyse imkansız hale gelmektedir. Tüm bu avantajların yanı sıra blokzincir teknolojisi için ele alınması gereken bazı sorunlar da bulunmaktadır. Bunlar; verimsizlik, işlemlerde gecikme, boyut ve bant genişliği, bazı güvenlik açıkları, zincirlere yeni bir blok eklemek için kaynak israfı, kullanılabilirlik ve gizlilik olarak sıralanabilir. Bu yazımızda blokzincir teknolojisinde geliştirilmeye ihtiyacı olan bu hususları tartışacağız.

Anahtar Kelimeler: Blokzincir, Blokzincir Sınırlılıkları, Blokzincir Problemleri

1. Introduction

Blockchain technology is defined as a distributed database that maintains an ever-growing list of transaction records, protected from threats such as theft or destruction. It consists of blocks holding the stacks of individual operations. Each block contains a timestamp and a link to the previous block (Nakamoto, 2008). It is necessary to correct the misconception that Bitcoin and Blockchain, commonly known in society, are the same or similar concepts. In today's internet world, many areas such as multimedia transfer data. Blockchain technology is a distributed database that allows us to transfer assets to which we attribute value. With the Bitcoin crypto currency, which was proposed by a secret writer named "Satoshi Nakamoto" in 2008, the world began to talk about the existence of a new international currency. While Bitcoin was originally thought of only as money, it was noticed that later on the Blockchain technology at the base of Bitcoin could be a more general use area.

Blockchain technology will be approved by the common decision of all participants in the system to the parties who do not know each other, or to the untrusted parties, and prepare a record for everybody interested. Blockchain is a way to create and protect reality (The Economist, 2015). In the most general terms, Blockchain technology eliminates the need for a central control mechanism and trusted authority; propagates encrypted data to all participants in the network in a distributed database structure rather than central trust. Blockchain technology is commonly known as technology under crypto money like Bitcoin. However, the usage area of this technology is not limited to financial applications, on the contrary, it is much wider and more diverse. Although it originated in 1992, it was first used with Bitcoin in 2008. We can say that the interest in Blockchain technology is increasing, especially with the spread of Bitcoin. The reason for the interest in Blockchain is that it allows users to make secure transactions without the need for any trusted central authority. Blockchain technology enables providers and clients to securely transact directly with each other without the need for a third party's approval. In order to make this transaction between the parties secure, the entire process in the system is kept in a distributed database using cryptography. In order for the data in this distributed database to be manipulated, the relevant manipulation intervention must be done and recorded on the data on all computers. In order for any cyber-attack attempt to be successful, more than 50% of the computers in the system must approve this change on the data, making the probability of the attacks to be successful almost impossible. Advantages such as security, no-intermediation, transparency in data acquisition make Blockchain technology attractive.

When we examine the "Emerging Technologies" report of Gartner, which guides the sector with technology analysis they provided, we see that Blockchain technology has passed the "Peak of Inflated Expectations" and is moving towards the "Trough of Disillusionment" stage (See Hypcecycle curve in Figure 1). This shows us that it will take between 5 and 10 years for the technology to reach the productivity field. The fact that Blockchain technology is in a downtrend in the Hypecycle curve means that it will not reach the threshold in the short term. This is mainly because the technology is fairly new and there are still unresolved issues. With the studies to be carried out between 5 and 10 years, it will be ensured that the capabilities of technology are understood in real terms, and it will reach the maturity point by eliminating its deficiencies.

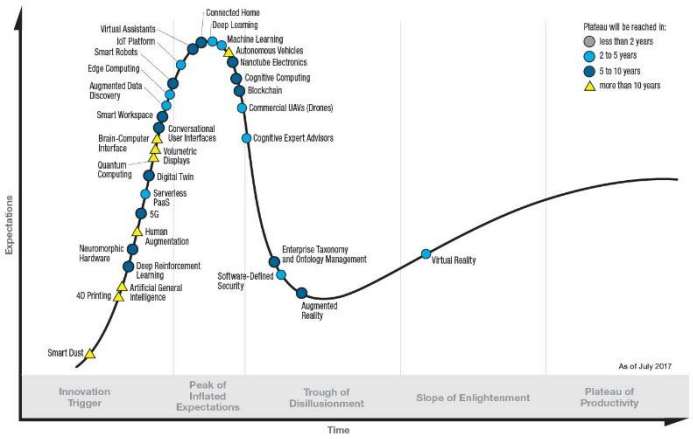

Figure 1. GARTNER Hype Cycle for Emerging Technologies (Kasey Panetta, 2017)

Beside of the advantages, there are some issues that need to be addressed for Blockchain technology in order to reach productivity area. These can be listed as throughput, latency in processing, size and bandwidth, some security vulnerabilities, resource waste for adding a new block to chains, usability, and privacy. In this article, we will discuss the issues that need to be addressed for Blockchain technology.

2. Material and Method

Blockchain technology enables providers and clients to securely transact directly with each other without the need for a third party's approval. In order to make this transaction between the parties secure, the entire process in the system is kept in a distributed database using cryptography. Without Blockchain technology, the Bitcoin system would not work. As the dazzling offer of Bitcoin; through the decentralized structure, buyers and sellers can meet directly on a platform and make their purchases securely, without involvement of any third party. Verification in the system can only be done by approving by more than 50% of the participants. Thus, besides of no need for a central authority, it became almost impossible for any cyber attack to be successful. The continued success of Blockchain technology is vital for Bitcoin and other cryptographic currencies survival. Beside of all these advantages, there are some issues that need to be addressed for Blockchain technology. Hence, these can be listed as throughput, latency, size and bandwidth, some security vulnerabilities, resource waste for adding a new block to chains, usability, and privacy.

2.1. Throughput

Throughput is the first problem that is needed to be solved. If we look at the number of transactions that can be performed for a second, Bitcoin network can perform seven transactions at a time (7tps). For Ethereum, another Blockchain-based crypto currency, this number ranges from 3 to 20 (Vitalik Buterin, 2016). On the other hand, this number is quite high in other transaction processing networks such as VISA (2.000tps) and Twitter (5,000tps) (Yli-Huumo et al., 2016). When the frequency of operations in the Blockchain rises to similar levels, the efficiency of the Blockchain network needs to be increased so that the competition can be achieved.

2.2. Latency

The speed of adding a block on the chain is one of the important criteria at the point of preference. Approximately 10 minutes are needed to verify bitcoin transfers (Bitcoinwiki, 2018). This period is quite long for transferring formalization. In order to achieve effective security and becoming safer against double-spending attacks, this long time is necessary. Double spending problem is, spending the same coin for multiple times (Investopedia, 2018). Bitcoin provides protection against double spending by verifying each transaction inserted into the chain to ensure that the inputs of the process are not previously spanned. This is causing the delay in Blockchain which is a big problem right now. Making a block and confirming the transaction should happen in seconds, while maintaining security. VISA takes only a few seconds to complete a transaction which is a huge advantage compared to Blockchain (Yli-Huumo et al., 2016).

2.3. Size and Bandwidth

A block size in Bitcoin is currently set at 1M (Eyal et al., 2015). In addition, the size of a Blockchain in the Bitcoin network is over 50MB. Blockchain is predicted to grow 214PB in each year (Yli-Huumo et al., 2016). Thus, if Bitcoin reaches the throughput level of VISA, there will be a problem related with size and bandwidth. The number of transactions included in each block is also limited by the bandwidth of nodes participating in leader election which is current bandwidth per block is 1MB for Bitcoin. If it is considered that a block is created every ten minutes with an approximate size of 1MB, so there is a limitation in the number of transactions that can be handled. In order to control more transactions, the size and bandwidth issues have to be solved on Blockchain.

2.4. Waste of Resources

On the Blockchain network, successful transactions between the endpoints are taken to a list identified as "Unconfirmed Transaction Pool" in nodes called "Miner". The validity of the blocks is checked here and the appropriate blocks are kept waiting to be added to the chain. Miners compete to form a list of unconfirmed operations that does not exceed a certain size, called a "block." It tries to find a special conditional "Hash" code for each block, which can be found in a large number of trials that can not be computed with a standard formula, which depends on all transactions placed in that block and references the previous valid block. The miner, who finds this value first, publishes the hash value it finds for the block, and the experiment it makes to reach this hash, at the end of the mistakes, it publishes another numerical value network called "Nonce" which allows it to reach that hash. This is the first time that you complete this process and the miner has joined the first block in the process queue and receives the reward. This calculation intensive processing that miners have realized is called "mining". This consensus method is referred to as "Proof of Work (PoW)" because it requires a lot of CPU power and validation of a valid hash and nonce find operation (Tasca & Tessone, 2018).

Consensus methods varies according to different Blockchain technologies and needs, each idea unity mechanism brings advantages and disadvantages based on different features. For this reason various methods of consensus are available according to the needs of the Blockchain system. Although there are various ideas of consensus models, the Proof of Work method is the most widely known and widely used.

According to the research conducted by Cambridge University in 2021, it has been revealed that the electricity consumption of Bitcoin mining, which is around 121.36 terawatt-hours (TWh), is higher than the consumption of Argentina as a country (Figure 2). In fact, it has been revealed that if Bitcoin were a country, it would be one of the 30 countries that consume the most electricity in the world (Criddle, 2021).

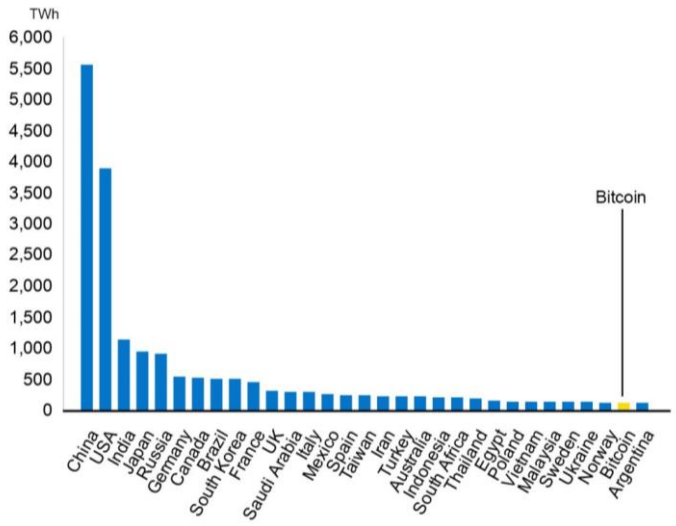

Figure 2. The Amount of Consumption of Bitcoin Compared to the Electricity Consumption of Countries

Bitcoin mining wastes serious amounts of energy, which is $15million/day (Yli-Huumo et al., 2016). This waste is about PoW effort. There are alternative methods such as Proof of Stake (PoS), which you have to have money in your electronic wallet to make money. Your winnings will be directly proportional to the amount of money you hold in your prize purse. It means the more money you have in your wallet, the more rewards you will get. Such energy saving methods should be preferred to prevent waste of resources.

2.5. Security

Security is the main reason Blockchain has gained popularity in recent years. The vast majority of crypto currencies, primarily Bitcoin, use the Proof of Work (PoW) method for verification on the network. In the PoW method you win as many blocks as you mine. In addition, in this verification method, the first person to solve the algorithm needed to insert the block string receives the reward. This type of mining requires investors to take an active role in validating the data blocks, which ensures that transactions are validated and new crypto money is generated. If you do not actively work for block verification in this mining type, you will not receive any awards. Since the prize is awarded to the first person who solved the new block, and because the processor power is needed to solve the block algorithm, those with the highest processor power are most likely to receive the reward. This has led to the institutionalization of the mining process and the establishment of large mining farms where millions of high-capacity processors operate (Figure 3).

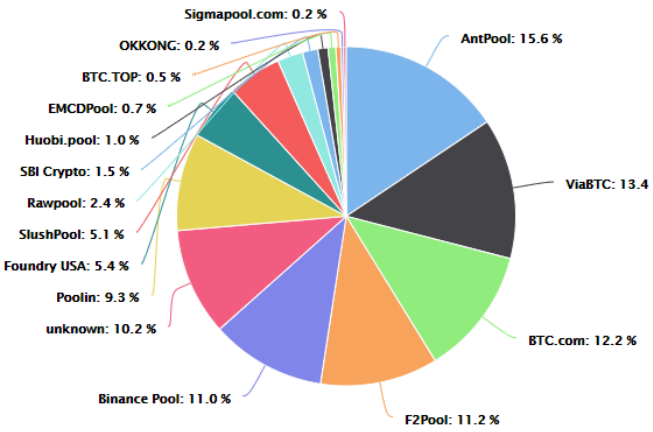

Figure 3. Bitcoin Mining Pool Hashrate Distribution (*Bitcoin Pool Stats*, 2021)

It has become impossible for users to make bitcoin mining with their desktop computer now in their homes. This situation hurts the idea that many crypto currencies like Bitcoin are not connected to a center which is the first exit idea. Verification in the system can only be done by approving by more than 50% of the participants. If more than 50% of the nodes in the network are being controlled by a single user, there is a possibility that manipulation can be done by that user. In this condition, Blockchain's central approach will be corrupted, and network control will belong to a single part. Especially when we look at the Bitcoin mining pools, we see that the pools are under the control of certain companies. It is not seen as a distant dream that one of these companies has more than 50% of the network. Therefore, further investigation of security is required to resolve this problem.

2.6. Usability

It is difficult to use Blockchain application API's like Bitcoin API provided for application development. There is a need to develop a more developer-friendly API for Blockchain. At the point of application of the technology, we see that there are no standards yet. The open source system is preventing many different software groups from creating a standard for different ideals to be constructed differently. All companies use their own infrastructures and the system they build, there is no standard infrastructure. To solve this problem, in the coordination of the LINUX Open Source Code community; a group of 54 companies including technological institutions such as IBM, Cisco, Fujitsu as well as financial institutions such as "J.P. Morgan" Accenture have established an open source community called "Hyperledger" (Hyperledger, 2018). The community continued to market the "Fabric 1.0" version in July 2017 after working on it. In February 2018, Sawtooth continued to market version 1.0. Apart from these versions, Iroha, Indy, Burrow are also available. They aim to produce a mature version after evaluating the feedback they give after using the different versions and the developers use. This consortium, which are continuing their efforts to bring them to the mature level, are required to create a giant infrastructure that will provide money transfers between the companies and the sectors. With this infrastructure, it is thought that awareness can be created in the internet world and finance field. The work that Hyperledger has done is intended to correct the usability issue.

2.7. Privacy

Blockchain is a Peer-to-Peer (P2P) ledger for transactions. Public key cryptography is used to transact. A public and a private key are provided to a user in the system: The private key is used to sign transactions, while the public key is used as an address in the system. Therefore, there is no need for real-world IDs for transactions: it's a form of "Pseudonymity". Data transparency is provided with pseudonymity; every transactions and its associated values are visible to everyone in the system. Because Blockchain is a distributed network without the need for a trusted party, all transactions are transparent and publicly disclosed. Users on the network have some privacy-related problems because they can see the entire transaction flow, although nodes can not see the private information associated with the identities. Although the sender and field addresses are public keys instead of open names, all operations are public keys and it is theoretically possible to go out of a known process and follow the actions of any participant. However, this is not the case in particular in scenarios where financial actors are involved. When we look at the researches related to the solution of this problem, many conflicting studies emerged. Koshy and colleagues analyzed a traffic pattern in Bitcoin and discovered that some subsets of Bitcoin addresses can be mapped to an IP address simply by observing transaction relay traffic (Koshy et al., 2014). Feld and colleagues created a tool to traverse the Bitcoin network and generate statistics based on it. With the tool, the average peer list contains addresses that are mostly located in the spouses' own autonomous systems. Therefore, the authors claim that transaction linking may be possible.

In addition, various studies have been done to increase the privacy and the use of various address mixer algorithms has been presented. Herrera-Joancomartí offers one of them. He proposed a mix of services to solve the anonymity reduction. Some trials are examined to see the services. A proposed mixing transaction enables the users to move Bitcoins from sender's address to client without a clear trace linking between addresses. Such transactions can help to improve anonymity when transaction linking becomes more challenging (Herrera-Joancomart´, 2015). There are more examples like CoinParty, a decentralized mixing service for Bitcoin based on a combination of decryption mix-nets with threshold signatures (Ziegeldorf et al., 2015). One of the most remarkable applications is the ZeroCoin (EZC) plug-in, which has been proposed to hide the transaction value and address balances at Bitcoin for increased privacy. ZeroCoin acts as a temporary currency to block the traceability of money, but does not hide the transaction and balance number of Bitcoin addresses. Suggested improvements include mixing Bitcoins before they reach a destination from a variety of sources, and mixing EZC style payments before they need to be recycled back to Bitcoin (Androulaki & Karame, 2014). The examples listed show that Blockchain is lacking in data privacy. In order to overcome these shortcomings, we can say that there are still open points and that the number of works needs to be increased.

3. Results and Discussion

With Bitcoin's attack in finance, a new wind began to flow in the stock market, and with the emergence of many new crypto money, the crypto money market has become a new area of finance. Although Blockchain technology is the technological infrastructure of Bitcoin, awareness is not as high as Bitcoin. Despite it was found in 1992, its first use was in the shadow of Bitcoin, influenced by the fact that it was with Bitcoin in 2008.

However, due to the features that it provides; Without Blockchain technology, the Bitcoin system would not work. As the dazzling offer of Bitcoin; through the decentralized structure, buyers and sellers can meet directly on a platform and make their purchases securely, without involvement of any third party. The reason for the interest in Blockchain is that it enables providers and clients to securely transact directly with each other without the need for a third party's approval. In order to make this transaction between the parties secure, the entire process in the system is kept in a distributed database using cryptography. In order for the data in this distributed database to be manipulated, the relevant manipulation intervention must be done and recorded on the data on all computers. In order for any cyber-attack attempt to be successful, more than 50% of the computers in the system must approve this change on the data, making the probability of the attacks to be successful almost impossible. Advantages such as security, no-intermediation, transparency in data acquisition make Blockchain technology attractive. Beside of all these advantages, there are some issues that need to be addressed for Blockchain technology. These can be listed as throughput, latency in processing, size and bandwidth, some security vulnerabilities, resource waste for adding a new block to chains, usability, and privacy. In this article, we will discuss these issues that need to be addressed for Blockchain technology. Throughput is the first issue that needs to be handled. In order to compete with big actors of finance sector like VISA, Blockchain network needs increase it current level from 7 tps to higher level. In similar manner, latency is another point that should be improved to rival with companies like VISA. Size and Bandwidth of the system will be a problem when the usage of the system is increased. Thus, the limitation in that case needs to be disappeared. Because of PoW validation method, energy consumption is pretty high. Therefore, alternative consensus methods or improvement in PoW method is needed to avoid energy waste. Also because verification in the system with PoW method can only be done by approving by more than 50% of the participants, the majority of the mining pool being seized by a single user may damage the concept of decentralized structure. Usability of the system is needed to be developed in order to have a standardized user-friendly infrastructure. Lastly, although Blockchain serves users to a transparent system that all transactions could be seen by participants, it may lead a lack in data privacy. the privacy of the data should be developed for situations such as deciphering the addresses of the participants.

4. Conclusions and Recommendations

To summarize, the continued success of Blockchain technology is vital for Bitcoin and other cryptographic currencies survival. One of the most important issues in ensuring the continuity of this success and taking it further is raising the maturity level of technology. The higher the maturity level of the technology, the easier it will be to embody its capability. Thus, with the applications to be developed, it will be possible to prove how much of the advantages promised by the blockchain technology can be gained. In order to experience all these positive developments, it is seen that there are problems that need to be solved. The number of efforts to remove these restrictions should be increased. In addition, with the increase in the number and application of new types of applications being developed, technically problematic points related to technology will become clearer and faster to be removed. This will speed up the maturity of technology and increase the value of crypto currencies like Bitcoin.

References

Androulaki, E., & Karame, G. O. (2014). Hiding transaction amounts and balances in Bitcoin. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8564 LNCS*, 161–178. https://doi.org/10.1007/978-3-319-08593-7_11

Bitcoin Pool Stats. (2021). BTC.Com. https://btc.com/stats/pool

Bitcoinwiki. (2018). *Block*. Bitcoinwiki. https://en.bitcoin.it/wiki/Block

Criddle, C. (2021). Bitcoin Consumes More Electricity than Argentina -. *BBC News*. https://www.bbc.com/news/technology-56012952

Eyal, I., Gencer, A. E., Sirer, E. G., & van Renesse, R. (2015). *Bitcoin-NG: A Scalable Blockchain Protocol*. https://doi.org/abs/1510.02037

Herrera-Joancomart´, J. (2015). Data privacy management, autonomous spontaneous security, and security assurance. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8872*, 3–16. https://doi.org/10.1007/978-3-319-17016-9

Hyperledger. (2018). *Hyperledger Community*. https://www.hyperledger.org/announcements/2017/07/25/hyperledger-adds-cisco-as-a-premier-member

Investopedia. (2018). *Double-Spending Definition*. https://www.investopedia.com/terms/d/doublespending.asp

Kasey Panetta. (2017). *Top Trends in the Gartner Hype Cycle for Emerging Technologies, 2017 - Smarter With Gartner*. https://www.gartner.com/smarterwithgartner/top-trends-in-the-gartner-hype-cycle-for-emerging-technologies-2017/

Koshy, P., Koshy, D., & McDaniel, P. (2014). An analysis of anonymity in bitcoin using P2P network traffic. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8437*, 469–485. https://doi.org/10.1007/978-3-662-45472-5_30

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 9. https://doi.org/10.1007/s10838-008-9062-0

Tasca, P., & Tessone, C. J. (2018). Taxonomy of Blockchain Technologies. Principles of Identification and Classification. *ArXiv*. https://doi.org/10.2139/ssrn.2977811

The Economist. (2015). *The great chain of being sure about things - Blockchains*. https://www.economist.com/briefing/2015/10/31/the-great-chain-of-being-sure-about-things

Vitalik Buterin. (2016). *Privacy on the Blockchain*. https://blog.ethereum.org/2016/01/15/privacy-on-the-blockchain/

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on Blockchain technology? - A systematic review. *PLoS ONE*, *11*(10), 1–27. https://doi.org/10.1371/journal.pone.0163477

Ziegeldorf, J. H., Grossmann, F., Henze, M., Inden, N., & Wehrle, K. (2015). CoinParty: Secure Multi-Party Mixing of Bitcoins. *Proceedings of the 5th ACM Conference on Data and Application Security and Privacy*, 75–86. https://doi.org/10.1145/2699026.2699100