www.ijmserh.com
Volume 4, Issue 1, January 2016
ISSN: 2349-6037
IJMSERH International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)
DOI: 10.15662/IJMSERH.2016.0401002

The Emergence of Blockchain: Security and Scalability Challenges in Decentralized Ledgers

Mohit Mittal

Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India

ABSTRACT: In the past decade, blockchain technology has garnered significant attention from a diverse array of industries. Despite the fact that blockchain technology was initially developed for the Bitcoin P2P cryptocurrency network, there has been a recent surge in interest in its potential integration with other service sectors. In the domain of machine-to-machine commerce, distributed ledger technologies, as seen in blockchain systems, have recently been hailed as potential platforms. A decentralised network architecture, security, immutability, and transparency are among the primary attributes of blockchains. The unalterable nature of blockchain ledgers enables members to rely on one another, thereby increasing performance and participation. Scalability and security are substantial challenges for blockchain technology. This study provides a comprehensive analysis of the emergence of blockchain technology and various methods for addressing the scalability issues associated with distributed ledgers.

KEYWORDS: Blockchain, Bitcoin, Ethereum, Proof-of-Work, Proof-of-Stake, Smart Contracts, Scalability Solutions

I. INTRODUCTION

A distributed ledger, or Blockchain, can facilitate the maintenance of secure and confidential electronic transaction records. All computers linked to the blockchain must monitor all actions executed for its functionality. The distributed ledgers facilitate this by documenting each participant's behaviour in the transaction at every node. Each partner validates their identification and acknowledges the terms as part of the transaction. This implies that, theoretically, no individual can alter the system or manipulate it unfairly. If a blockchain were to materialise, it could modify the data stored by all machines linked to the digital ledger. Moreover, blockchain is decentralized, signifying its capacity to function autonomously from any singular organization, whether governmental, organizational, or geographical. The network's distributed architecture and the storage of data across multiple devices facilitate the preservation of ledger integrity [1]. Blockchain block diagram is shown below in figure 1:

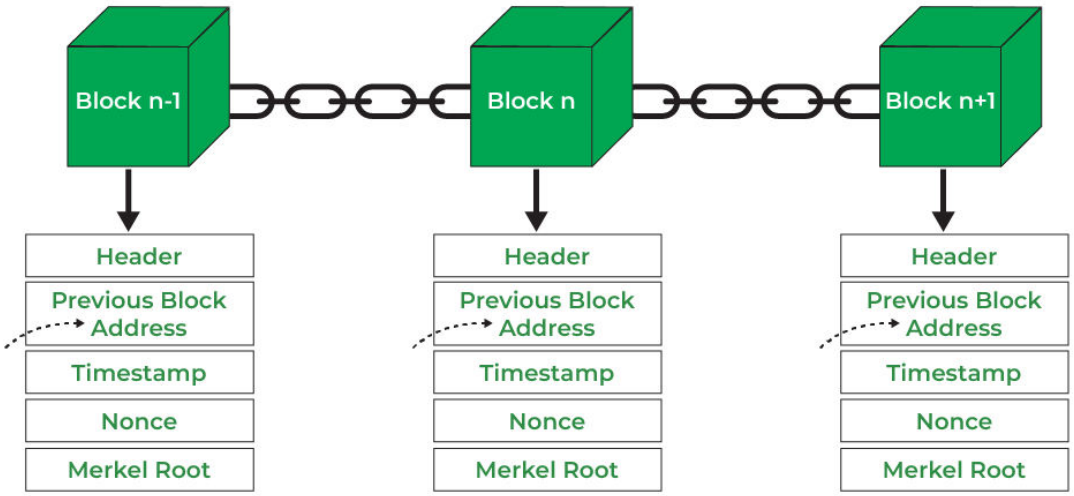

Figure 1: Blockchain Block Diagram

DOI: 10.15662/IJMSERH.2016.0401002

The Bitcoin blockchain is rapidly ascending in the realm of technological innovation. Bitcoin, having experienced significant expansion in its global user base over recent years, is presently the foremost implementation of this technology [2]. Nonetheless, few individuals comprehend the role of blockchain technology and its rapid ascent to prominence inside the bitcoin network. The rapidly gaining traction blockchain technology documents and analyses data while rendering alterations almost impossible. Due to its governance by the collective actions of all network participants, it lacks a specific regulator [3].

Blockchain technology is often seamlessly integrated with existing systems, as all stakeholders must consent to any modifications before implementation. Businesses are intrigued by blockchain technology for purposes that extend beyond the practical uses of Bitcoin [4]. The order and purchasing departments of firms have commenced utilizing the Blockchain network for inventory tracking and finance transfers, as it conserves time and digital currency. The Ledger money transfer software, developed by Santander, a prominent European banking institution, will eliminate intermediaries and their corresponding fees. By eliminating intermediaries and processing fees, it fundamentally transformed the banking sector and resulted in substantial savings for banks. Its connection with contemporary technologies could transform the operational methods of numerous businesses. It may also be applicable in domains such as data security, electoral processes, patient record management, logistics, and digital asset authentication, all of which could see enhanced efficiency and reduced fraud.

Moreover, it is essential to analyze a Distributed Ledger Technology (DLT) based blockchain security framework to identify various vulnerabilities, including endpoint vulnerabilities and public/private key security issues. This is particularly applicable in contemporary cooperative networks, where decentralised ledgers enable data exchange and device authentication, and where each node retains an identical copy of the data. Security issues, including device spoofing, false authentication, and double-spending, may occur if an attack compromises a blockchain node [5].
Moreover, in contrast to bitcoin's cash-equivalent tokens, which are indistinguishable from financial assets, the "contract," which is once again reflected in cryptocurrencies, is the sole blockchain system that has incorporated minuscule computer programs directly into the public ledger. Bitcoin may be replaced by alternative assets like as bonds or loans [6]. Due to the proliferation of several applications, the Ethereum self-executing platform is presently valued at over one billion dollars. The fourth significant advancement, sometimes referred to as "proof-of-stake," is presently the most discussed notion in blockchain theory [7]. By necessitating the system with the greatest processing power to render decisions, a mechanism known as "proof of work" guarantees the privacy of contemporary distributed ledgers. Entities of this nature are referred to as "mine operators," and they manage extensive data centers in return for remuneration in bitcoin. Contemporary data security techniques have made data centers redundant, substituting them with complex financial instruments that offer an equal or superior level of protection. Proof-of-stake systems are expected to become operational later this year.

Fifthly, blockchain scalability is imminent. It will be implemented shortly. All machines connected to the network now perform every transaction within the blockchain ecosystem. The operation is time-sensitive. A scalable blockchain accelerates the process by effectively distributing the workload across the participating computers and forecasting the requisite number of workstations for validating each activity, all while maintaining security. The challenge resides in identifying a solution to this issue that does not compromise the blockchain's established security attributes. We anticipate a scalable blockchain to possess sufficient efficiency to support Internet of Things technologies and interface with the banking sector's cash-on-delivery intermediaries, like VISA and SWIFT.

A distinguished team of computer scientists, cryptographers, and mathematicians has collaborated for a mere ten years to construct this cutting-edge environment. Upon the acknowledgement of the comprehensive effects of these discoveries on society, circumstances are likely to become peculiar. Connected automobiles, autonomous drones, and self-driving cars will utilize blockchain technology for payment processing. Enhanced reliability beyond the capabilities of the existing infrastructure will enable international money transfers to decrease from hours to just seconds, ultimately achieving a duration of just a few seconds. These and other changes imply a significant reduction in transaction costs. There will be rapid, substantial, and unpredictable consolidations and disaggregation of existing markets as transaction fees fall below discernible thresholds. Auctions were generally more regional and localized compared to the globalized, standardized formats observed on platforms such as eBay today. The system experienced swift transformation as the expense of contacting individuals diminished [8].

DOI: 10.15662/IJMSERH.2016.0401002

Numerous feedback loops were initially triggered by the advent of electronic commerce in the late nineties, and it is expected that blockchain will elicit a similar response.

Smart contracts, when utilized with blockchain technology, provide immediate and efficient management of data transfers among many participants under specified criteria. Figure 2 illustrates the functioning of a smart contract. This sort of contract is otherwise analogous to ordinary contracts, except for the enforcement of the consensus. The parties involved in a smart contract are as bound to adhere to its stipulations as they would be in a conventional legal agreement. While rules govern traditional conversations, smart contracts are enforced by their corresponding programs. An increasing number of individuals are choosing smart contracts because of their dependability and transparency. This contract is examined by numerous individuals to guarantee its accuracy. With their assistance, transitioning online services from one provider to another is effortless.

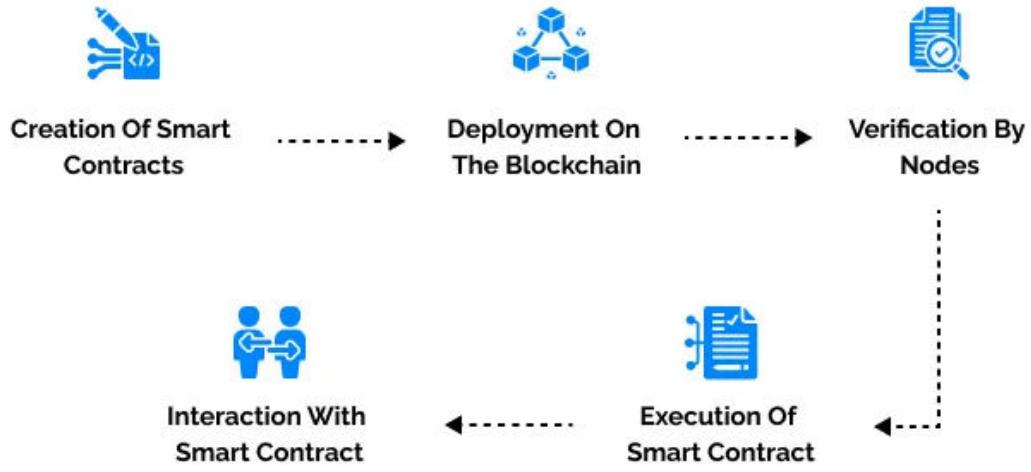

Figure 2: Working of Smart Contracts

II. RELATED WORK

The majority of contemporary businesses have implemented blockchain technology to enhance the security of their data. It is one of the most recent technologies that is garnering the most traction in the field of digital protection. This chapter investigates a diverse array of strategies, procedures, and approaches that have been implemented in the blockchain industry to mitigate security and data sharing concerns.

In their empirical study, Vasek et al. [9] examined the prevalence and impact of distributed denial-of-service (DDos) attacks on operators in the bitcoin economy. They discover that currency exchanges, mining pools, and wagering operators are significantly more susceptible to attacks than other services. Additionally, the likelihood of DDoS attacks is significantly higher in large mining pools than in small pools. This study examined three of the most prevalent methods of anti-DDoS protection; however, there are additional options. Additionally, certain forms of DDoS attacks are not protected by protections like Cloudflare. Danny [10] introduced and analyzed the issues with bitcoin, such as the 51%-attack, double spending, dust transactions, and code-based assaults. All of these attacks enable the network to be manipulated for personal benefit.

Herrmann et al. [11] conducted an analysis of the bitcoin system, with a particular focus on the double-spend protection procedure, and identified a vulnerability in specific usage scenarios. They also assessed the potential for double-spending assaults on bitcoin. People anticipate that the features will be analyzed in order to resolve or defend the numerous assaults that are being discovered. However, there may be a parameter setting in this work that leads to the desired, but unrealized, attack properties of their attack. In order to identify such a setting, additional investigation of

DOI: 10.15662/IJMSERH.2016.0401002

the parameter space would be necessary. If the detection mechanism they developed is extensively implemented throughout the network, this configuration may not exist at all.

Decker et al. [12] conducted an analysis of the multi-hop broadcast mechanism employed by bitcoin to propagate transactions and blocks through the network in order to update the ledger replicas. This blockchain research is crucial and beneficial in enhancing its security. The information stored in the ledger is not synchronized with a non-negligible probability by the synchronization mechanism of this work. This issue not only results in a long-term inconsistency that is not observed by a significant number of nodes, but it also renders the system less resilient to attacks.

Wilkinson et al. [13] developed an open-source software project with the objective of conceptually demonstrating that cloud storage applications can be enhanced to be more efficient, secure, and decentralised. Some individuals utilize blockchain as a software connector. This work has developed a novel model in which a blockchain can function as the foundation for a distributed application, MetaDisk. MetaDisk operates autonomously as a peer-to-peer network of nodes that execute open-source code. This work offers a comprehensive overview of a novel data platform; however, it does not offer protection against Sybil attacks and the security threats that underlie the Storj platform.

Karame et al. [14] examined a diverse array of scenarios to ascertain the probability of a double-value attack being successful. We discuss the concept of information concealment, which results in this issue, despite the fact that there may be numerous costs that an extended detection period cannot identify. The only solution to this problem is to extend the detection period. In the context of a situation necessitating a prompt payment, Bamert et al. [15] proposed a partial resolution to the problem of repetitive charges. Babaioff and colleagues' research indicates that the incentives offered to nodes to transmit information to all networks are inadequate [16]. Miners are accountable for fee-related operations and request them by generating blocks that contain transactions. In the present system, this is the strategy that is most prevalent. Bitcoin mining frequently necessitates the utilization of specialized hardware and consumes an excessive quantity of energy.

Becker et al. [17] investigated the impact of bitcoin and conventional currencies on the ecosystem in which they operate. They concluded that the network's maintenance and protection against attacks are costly, despite the relatively modest fees associated with bitcoin transactions. As we have observed, the processing capacity that is accessible within a network is subject to fluctuation. The relative anonymity of bitcoin transactions is another contentious issue that has been raised. The inability to maintain confidentiality is illustrated by the fact that the details of each transaction are accessible to all network participants and that each transaction is recorded in a copybook. Conversely, Nakamoto maintains that the confidentiality is solely an alias, as the identity of the account holder and the identity of the account are maintained as separate entities. Reid et al. [18] conducted an analysis of the claim and determined that it is feasible to ascertain the owner's information by reconciling the confidentiality of the various accounts that were involved in the transaction.

The transaction chart was analyzed by Shamir et al. [19] using a variety of global information, including an estimate of 78% of outbound bitcoins and an in-depth investigation of the busiest regions of the transaction chart. Furthermore, the authors estimated the quantity of bitcoin that was sent out. Elias [20] examined the legal and moral implications of Bitcoin's lack of anonymity. Subsequently, a cryptocurrency known as ZeroCoin [21] resolved the issue of anonymity in Bitcoin, thereby facilitating the establishment of a decentralised coin blending service that operated on zero knowledge. Hanke et al. [22] proposed transaction procedures for bitcoin contracts and facilitated transactions between dealers and their consumers. CommitCoin [23] is an additional carbon dating method that is predicated on the commitment technology of blockchain.

However, there are few references to double spending and 51% attacks on bitcoin, and we were unable to identify any conversions. This issue is addressed in the Bitcoin Wiki by a warning that states, "Transactions should not be considered valid until a specific number of blocks in the blockchain confirm or confirm the transaction [sic]." [S] It is impossible for a single transaction to control the entire network due to the decentralization of the blockchain. Fergal Reed et al. [18] characterized the perpetrators as conducting an excessive number of comparisons between users and public keys, as well as matching information from outside the system with users. The topological structure of these networks has been investigated using data from bitcoin transactions that were publicly accessible.

www.ijmserh.com
Volume 4, Issue 1, January 2016
ISSN: 2349-6037
IJMSERH International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)
DOI: 10.15662/IJMSERH.2016.0401002

III. BLOCKCHAIN CHALLENGES

Blockchain and other nascent technologies present distinct challenges. This section addresses the primary challenges linked to this breakthrough, including its potential future applications, which may clarify its slow acceptance. The term "blockchain" has existed since 2009, and the underlying technology is genuinely revolutionary. The cluster of workstations in the ledger has authenticated and recorded all transactions, rendering it an immutable ledger.

A particular technology has eclipsed all others in significance; nevertheless, its complex implementation obstructs progress. Addressing a specific array of difficulties is essential to accelerate technology adoption. Almost every area of the economy is currently employing blockchain technology, including finance, healthcare, e-commerce, and supply chain management. If this technology were integrated with other emerging technologies, everyone would receive something completely novel.

- **Scalability**

The biggest challenge in implementing it is making it scalable. Bitcoin (about 3-7 transfers per second) and Ethereum (roughly 15-20 operations per second) have substantial latency in the amount of data transmitted, despite the fact that trading groups can handle a large amount of information per second without being overwhelmed. As a result, blockchain is unsuitable for a wide range of applications. It is feasible that Ethereum's Plasma and Bitcoin's Lightning Network will provide new options for low-cost, accidental exchange support. Blockchain technology must accelerate before it can be used for mass modification.

- **Interoperability**

The next major issue that needs to be addressed is exchange, which is one of the main reasons why organizations have yet to adopt this innovation. Because most blockchains cannot send or receive data from other distributed ledger systems, they can only function autonomously and cannot participate in multiple peer interactions. Several projects have been initiated to address and remedy the issue. Ark employs a Smart Bridges architecture to reduce the connectivity gap between nodes. This project is driven by a global effort to facilitate cooperation.

- **Energy Consumption**

The Proof-of-Work technique is used by the platform to validate activities and establish confidence before they are added to the cluster. To analyze, validate, and, most importantly, protect the entire system, this system requires a significant amount of processing power to manage complicated mathematical procedures. The Ethereum co-founder has suggested transitioning from Proof-of-Work to Proof-of-Stake to address this issue. When implemented, this strategy reduces energy consumption since players are less inclined to solve complex riddles.

- **Security Challenge**

One of the most important aspects of this discussion is security. Each distributed ledger claims to be secure, and we all know that. However, much like any other new technology, blockchain has very few security holes that need to be addressed. Exploitable network vulnerabilities include a 51% attacks rate on connections. This assault allows hackers to access control of the network and use it in their own manner. They also have the power to change how transactions work and stop other people from mining their own blocks. This leads an increase in protocol layer security. Many of its security flaws have already been pointed out to us. On the other hand, only a few circumstances have robust mechanisms in place to deal with all this. Because of this, no one believes they can be used for an extended period without risk.

IV. BLOCKCHAIN SCALABILITY SOLUTIONS

For blockchain to achieve widespread adoption, scalability issues must be resolved. Bitcoin and Ethereum, two prominent systems, exhibit throughputs of merely 7 and 15 TPS, respectively, which is grossly insufficient for real-time applications. One of the founders of Ethereum,
Vitalik Buterin asserts that blockchain implementations involve trade-offs among the three fundamental characteristics of security, scalability, and decentralization. Figure 3 exemplifies the trade-off situation referred to as the Blockchain Trilemma. A compromise is unavoidable as only two of the three traits can be selected. Given the impossibility of compromising the network's security, the majority of scaling solutions seek to reduce the blockchain's decentralization.

www.ijmserh.com
Volume 4, Issue 1, January 2016
ISSN: 2349-6037
IJMSERH
International Journal of Multidisciplinary and Scientific Emerging ResearcH (IJMSERH)
DOI: 10.15662/IJMSERH.2016.0401002

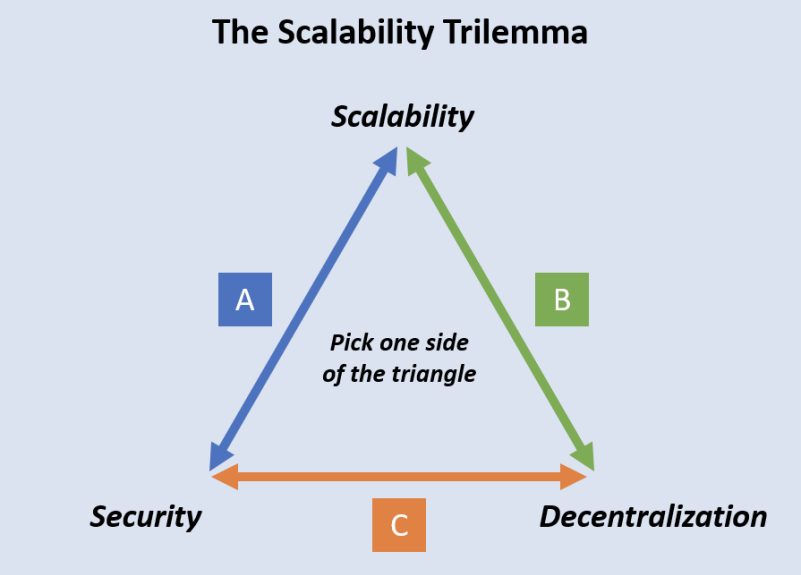

Figure 3: Blockchain Trilemma

Directed acyclic graphs (DAGs), consensus optimization algorithms (SOAs), and sidechains are approaches employed to attain scalability. These solutions are exclusively applicable to the Ethereum and Bitcoin platforms. The term "sharding" refers to the dividing of the blockchain network into smaller, more controllable segments. Among the available options, sharding provides the most effective solution to the scalability issue.

DAG distinguishes itself from traditional blockchain systems. A tree-based structure connects transactions rather than a chain-based structure that links blocks of transactions. The nodes conducting validation ascertain the validity of the transactions. The IOTA, Spectre, DLattice, and CoDAG blockchain systems are prominent examples that utilize Directed Acyclic Graph (DAG) technology. The tree structure of the DAG eliminates the necessity for dedicated nodes to achieve consensus, facilitating rapid transaction confirmation. The primary disadvantage is the tree structure's susceptibility to attacks. A parasite chain originating from a section of the tree can disrupt the overall network's functionality and lead to device malfunctions.

Blockchain systems depend on consensus procedures. Enhancements to scalability and reductions in processing requirements for traditional consensus mechanisms like as Proof of Work (PoW) and Proof of Stake (PoS) are feasible. Delegated Proof of Stake (DPoS), a variant of Proof of Stake, diminishes consensus cost and enhances transaction throughput by assigning transaction validation to a limited group of trusted nodes. Altering the blockchain protocol may enhance its scalability. To enhance scalability, one alternative is to transition from a single-layer blockchain to a multi-layered architecture, with each layer designated for specific functions. Merkle trees and compressed block headers exemplify efficient data structures that can diminish the blockchain's footprint and enhance its performance.
Sidechains offer an intriguing opportunity for enhancing the scalability of blockchain systems. A sidechain functions autonomously after its initiation, notwithstanding its connection to the primary blockchain. Implementing sidechains to manage a portion of transactions can enhance the scalability of the primary blockchain. A supplementary blockchain known as the Liquid Network operates concurrently with the Bitcoin blockchain. Digital assets created and managed by users can be exchanged instantaneously and economically over the Liquid Network.

V. CONCLUSION

A blockchain is a distributed, shared, and secure ledger that simplifies the process of recording and tracking resources without the necessity of a centralized, trusted authority. It enables two parties to communicate and exchange resources in a peer-to-peer network, where the majority makes distributed decisions rather than a single centralized authority. The blockchain-based framework facilitates the timely and dependable exchange of information, thereby improving

DOI: 10.15662/IJMSERH.2016.0401002

traceability. The participants' participation and performance are improved as a result of the immutable nature of blockchain ledgers, which allows them to trust one another. Blockchain technology faces two significant obstacles: security and scalability. This paper examines the emergence of blockchain technology and the development of a variety of approaches to address scalability concerns in distributed ledgers.

REFERENCES

[1] Buterin, "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2014.
[2] Buterin, "On Public and Private Blockchains, Ethereum Blog," 2015.
[3] Buterin, "Ethereum: A Next-Generation Cryptocurrency and Decentralized Application Platform," Bitcoin Magazine, 2014.
[4] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://bitcoin.org/bitcoin.pdf
[5] Decker and R. Wattenhofer, "Bitcoin Transaction Malleability and MtGox," in Proceedings of the 5th USENIX Workshop on Bitcoin and Blockchain Technology (USENIX-Bitcoin '15), 2015.
[6] G. Wood, "Ethereum: A Secure DecentralisedGeneralised Transaction Ledger," Ethereum Project Yellow Paper, vol. 151, 2014
[7] Sompolinsky, Y., Zohar, A. (2015). Secure High-Rate Transaction Processing in Bitcoin. In: Böhme, R., Okamoto, T. (eds) Financial Cryptography and Data Security. FC 2015. Lecture Notes in Computer Science(), vol 8975. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-47854-7_32
[8] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292-2303, 2016
[9] Vasek, M., Thornton, M., & Moore, T. (2014). Empirical analysis of denial-of-service attacks in the Bitcoin ecosystem. In *International conference on financial cryptography and data security* (pp. 57-71). Springer, Berlin, Heidelberg
[10] Bradbury, D. (2013). The problem with Bitcoin. *Computer Fraud & Security*, *2013*(11),5-8.
[11] Herrmann, M. (2012). Implementation, evaluation, and detection of a double spend-attack on Bitcoin (Master's thesis, ETH Zürich, Department of Computer Science).
[12] Decker, C., & Wattenhofer, R. (2013). Information propagation in the bitcoin network. In IEEE P2P 2013 Proceedings (pp. 1-10). IEEE.
[13] Wilkinson, S., Lowry, J., & Boshevski, T. (2014). Metadisk a blockchain-based decentralized file storage application. Storj Labs Inc., Technical Report, hall, 1-11.
[14] Karame, G. O., Androulaki, E., & Capkun, S. (2012). Two bitcoins at the price of one? double-spending attacks on fast payments in bitcoin. *Cryptology EPrint Archive*.
[15] Bamert, T., Decker, C., Elsen, L., Wattenhofer, R., & Welten, S. (2013). Have a snack, pay with Bitcoins. In *IEEE P2P 2013 Proceedings* (pp. 1-5). IEEE.
[16] Babaioff, M., Dobzinski, S., Oren, S., & Zohar, A. (2012). On bitcoin and red balloons. In *Proceedings of the 13th ACM conference on electronic commerce* (pp. 56-73).
[17] Becker, J., Breuker, D., Heide, T., Holler, J., Rauer, H. P., & Böhme, R. (2012). Geld stinkt, Bitcoin auch–Eine Okobilanz der Bitcoin Block Chain. *INFORMATIK 2012*.
[18] Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. In *Security and privacy in social networks* (pp. 197-223). Springer, New York, NY.
[19] Ron, D., & Shamir, A. (2013). Quantitative analysis of the full bitcoin transaction graph. In *International Conference on Financial Cryptography and Data Security* (pp. 6-24). Springer, Berlin, Heidelberg.
[20] Elias, M. (2011). Bitcoin: Tempering the digital ring of Gyges or implausible pecuniary privacy. *Available at SSRN 1937769*.
[21] Miers, I., Garman, C., Green, M., & Rubin, A. D. (2013). ZeroCoin: Anonymous distributed e-cash from bitcoin. In *2013 IEEE Symposium on Security and Privacy* (pp. 397- 411). IEEE.
[22] Gerhardt, I., & Hanke, T. (2012). Homomorphic payment addresses and the pay-to-contract protocol. *arXiv preprint arXiv:1212.3257*
[23] Clark, J., & Essex, A. (2012). Commitcoin: Carbon dating commitments with bitcoin. In *International conference on financial cryptography and data security* (pp. 390-398). Springer, Berlin, Heidelberg.