CRYPTOCURRENCY SECURITY

Dr Arvind Kumar (Assistant Professor), Mohd Shaqib Visal, Mohd Anas

Galgotias University
Email: arvindkumar@galgotiasuniversity.edu.in
Shavisal5432@gmail.com
mohammadanasgour@gmail.com

Abstract

Security and privacy are two conditions that are closely linked to current trends in cryptocurrency, and this study offers a similar comprehensive review. Cryptocurrency adds security to transactions and controls the formation of additional currency units. Great growth for cryptocurrency market testing leads to the misuse of failures to benefit enemies. In this study, the review was designed to focus on safety and security standards of cryptocurrencies especially in Bitcoin. This study explains cryptocurrency agreements, their benefits, and communications within the framework.

KEYWORDS: *ATTACKS, BITCOIN, BLOCKCHAIN, SECURITY*

Introduction

In recent years, the global economy has certainly moved towards digital period. Everything is done by people in a digital way. Too hot a practice in the field of digital payment cryptocurrency. Like standard currencies, cryptocurrencies are used as a trading method but are designed with the intention of exchanging digital information. It is an extended digital of money that uses cryptography for security and thus makes it difficult compose. Meanwhile, it is not provided by central government officials therefore it is not removed from users. Cryptocurrency type a reliable and secure type of digital currency that people choose to use today. With no third-party involvement, cryptocurrencies offer a type of user authentication and sense of security while performing transaction.

When users create cryptocurrencies, all official and certified transactions are kept in a public directory. The ownership of the owners who own the funds is fully encrypted to ensure the integrity of the record keeping. Another reason is that people do not have to spend their money to do this work transaction. It is because people are mining cryptocurrencies receive their compensation from the network itself.

Also, people can keep their money in safe wallets for free only charge. People can do their jobs in an anonymous and very secretive way. As senders or recipients of cryptocurrencies, they cannot transfer money directly to their credit card accounts or any other accounts and users are not required to share their information anyone. Thus, Identity theft can be avoided.

In 2009, a passenger by the name of Satoshi Nakamoto published a book a research article related to a later theory that continued to bring disruption internet site. Since the release of Bitcoin digital currency, about 600 different cryptographic currency proposals have emerged. Among the several cryptocurrencies launched, Bitcoin is the most successful and popular digital currency. Contains a unique set of data structures can be used to save and operations that occur on its external network third party organization. The main method used in the development of Bitcoin is blockchain innovation, which is launched annually. 2008 and its real-time performance was achieved in 2009. Blockchain technology is being developed with decentralized installation strategies and does not involve any trusted authority. This amazing process has taken place in the ongoing development of cryptocurrencies. In these technologies, the exchange of digital resources took place in a separate area way. In addition, several cryptocurrencies have emerged in the real world such as Bitcoin, Ripple, Litecoin, Ethreum, etc. In all of these cryptocurrencies, legal entities can perform economic activities without any central authority. It was noted that Bitcoin is the best operating product in 2016 and in the same year, blockchain technology gained 10 billion of dollars in its financial market.

These cryptocurrencies do not require a central regulatory authority and operate independently. Bitcoin, like any other cryptocurrency, uses the concept of peer-to-peer technology, in any person who owns any unit of this currency may use it or spend anywhere and anytime without the contribution of any trustee third party. Bitcoin is listed as an open source, and no one has either he controls it. Bitcoin is integrated with the blockchain technology developed on it distributed area and thus single user authority was avoided. Later, there is not a single point of failure and transfer of funds between customers is done without the involvement of any third party. Therefore, the self-imposed police approach was created by combining a separate blockchain technology with a consent-based correction program that ensures that only valid transactions are made. blockchain system.

By using Bitcoin, users can complete electronic payments first transactions that transfer Bitcoins between users. Targeted address is calculated using cryptographic sequences hash functions in the user's public key. In Bitcoin, users can save a lot addresses by creating multiple keys are public and all of these addresses can be connected to their wallets. In order to use Bitcoins managed in the form of a digitally signed transaction, users must provide their own private key. it is a secret. User anonymity can be controlled by using the hash function public key as a welcome address and it is suggested that a Bitcoin address be different from all other transactions you receive.

Cryptocurrencies, especially Bitcoin, are widespread worldwide. Since cryptocurrency is a widely distributed model with a lot of space, hackers and malicious users find this program as an easy way to fraud. transaction. Also, there are a number of security risks to cryptocurrency protocols, as well as within networks. Therefore, there is more debate around the world as security and privacy issues for cryptocurrencies are still being investigated. In addition, the attacks, especially on blockchain networks such as netsplit, double spending, ease of use, Finney attacks, etc., are discussed in books focused on miners or mining ponds.

This study presents a comprehensive study focusing on the security and security features of Bitcoin and other cryptocurrencies and their key concepts. This includes threats to user security and transaction anonymity, leading to the use of crypto currency in real-world applications and services. In recent years, researchers have done just that and proposed a number of security solutions to address the current security and privacy issues in Bitcoin, which have been discussed in this study. And focuses on security issues and countermeasures related to key components of cryptocurrencies.

Particularly, the main contributions of this research are as follows –

1. This function introduces the basic concepts of Bitcoin, its functionality, and related ideas, its operation. Students must have a clear definition as well a solid foundation on cryptocurrencies and basic concepts to better understand the security issues and the challenges they face the world of cryptocurrencies.
2. Systematic presentations and discussions are made with various threats based on security and privacy, which occurs directly or indirectly by Bitcoins. In addition, exploring the potential for various threats that the enemy could gain.
3. The effectiveness and shortcomings of existing solutions were discussed which deal with security threats and enable secure privacy Bitcoin, thus providing a technical perspective on these challenges in practice with cryptocurrencies.
4. The security challenges in the Bitcoin network have been discussed, explained the challenges of open research in blockchain technology

This research seems to help interested readers:

1. Provides insight into security and privacy concerns and it’s scope and impact.
2. Recognize the potential harm of these threats.
3. Giving good guidance on this topic and finding ways to get it back contain these threats.

Different Attacks on Cryptocurrencies

The Bitcoin network is vulnerable to various stages of attack due to the concept of double decay which is the main cause of many attacks on the network. Double use is a form of attack that occurs when someone attempts to transfer two conflicting actions from the same address.

Bonneau et al. (2015) discussed the various risks and security opportunities in Bitcoin, which cast doubt on financial stability, performance of the protocol, as well as the application of the various solutions proposed in relation to the above issues, which include changing boundaries as limits. on block size and performance, inter-block time, monetary policy, etc., and the emergence of alternative cryptographic jigsaw puzzles and help mankind by solving real-life situations.

Karame et al. (2012) reported the costs incurred in the calculation transactions and increased security resulting in delays in the whole process is about 10 minutes. Cryptocurrencies include higher levels of safety and there will be delays in performance. Therefore, they should not be used for quick transactions when time is of the essence. Following the same idea, if these are made for quick payments with reducing security, which will increase performance, will be in place The issue of double spending can make cryptocurrencies less secure. Vas and Lunagaria (2014) define the concept of proof of work (PoW), and its use in blockchain ensures that the block initiated by miner compares the pattern to the following block. Moreover, they talked security threats related to blockchains such as time-jacking problems, attacks on wallet software, "> 50%" attacks, double spending, and selfish mines.

Conti et al. (2018) mentioned aspects of the Bitcoin protocol as well also discussed their effectiveness. This work casts doubt on the practical potential of cryptocurrency and finds risks in its basic PoW-based compact and blockchain protocols. Such people performance in Bitcoin is threatened by these at risk, that is, if if killed, it could cause much damage

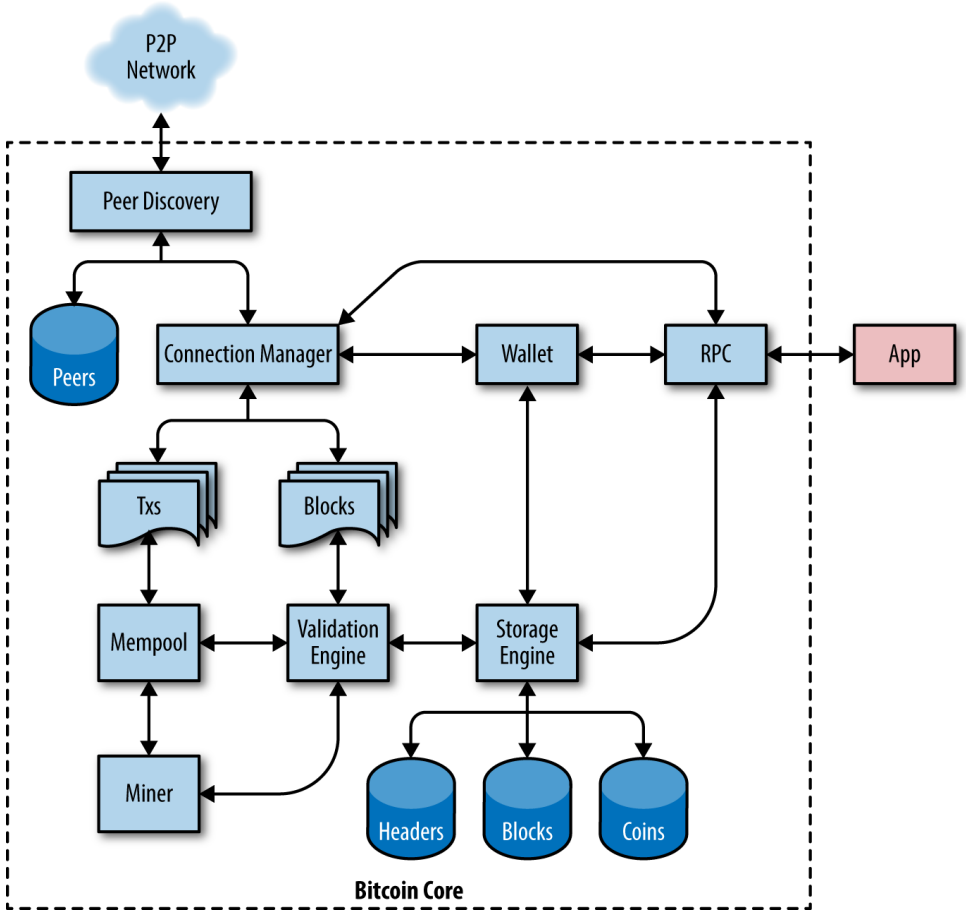
Blockchain Architecture

Cryptocurrencies can be defined as digital and digital assets is designed to serve as a trading platform through the cryptography industry to not only to build some additional units but also to provide a secure approach in exchange and verify the authenticity of the work. These are segregated and mainly operate through a separate human system known as a blockchain, which is an open and accessible website for everyone. The blockchain acts as a distributed ledger.

Blockchain is a pillar to ensure crypto currency transactions and makes them secure. It continues to create new records so-called squares; these squares are connected and secured with cryptography help. Blockchain behaves like a linked list where each piece contains a hash pointer and points to the previous block, too it can also include the timestamp and interchangeable data. By definition, The blockchain is unchanged and weak if someone wants to change data available in blockchain. The blockchain is managed by a shared and trusted system at a public meeting authorizing the addition of new blocks. Once these blocks are added, and the data is made part of the system, it cannot be changed because the corresponding hash of the block will change. and every subsequent hash needs to be replaced accordingly.

In general, blockchains are much safer. They are often the subject of a relevant framework in the discussion involved with the great Byzantine adaptation to failures related to internal functioning. Agreement of land redistribution was achieved through the establishment and implementation of blockchain, and it faces many problems, such as the issue of double expenditure which includes a professional or dedicated dedicated server. Square time is defined by time taken for the system to generate and add a block to the blockchain. A few blockchains build a block every 7 seconds. When the block is re-created added, the entered

information becomes visible, and at the same time, the exchange currency occurs. So a short square footage will lead to faster trading.

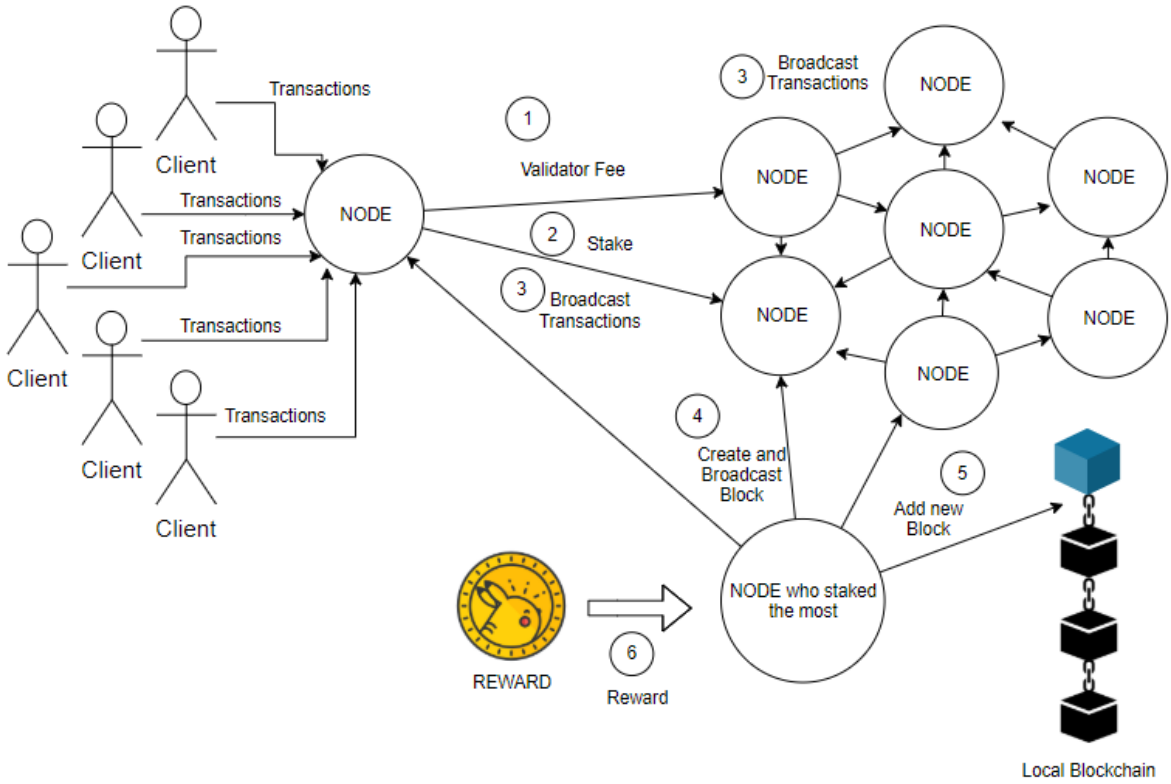


Proof-of-work (PoW) in Cryptocurrencies

The concept of the PoW system is used to prevent cryptocurrency system abuse, such as banning service attacks, spam, double spending, and many other attacks. This concept is used to build a distributed unreliable compatibility, when the system requires a specific function, i.e. a computational function, from a computer requesting a service. This "job" is usually in the process of processing time by the applicant computer. Cynthia and Moni came up with the idea of doing your own "job." application for admission. A key factor and perhaps the reason why PoW is a concept most of the cryptocurrency systems have been able to rely on since then the establishment is a balance between when it comes to the actual work of calculation, and when it comes to validating it. The concept goes with many other words — computational puzzle, CPU costs work, cryptographic puzzle. Although its basic concept is very similar to that of the CAPTCHA, it differs from it and is intended for it people solve faster than computers. In PoW lines, varied other concepts are proposed, such as local evidence, bandwidth evidence, and proof of ownership.

Proof-of-stake (PoS) in Cryptocurrencies

Unlike PoW which creates a broad consensus based on the amount of calculation work performed by the service applicant, in the verification system (PoS), the next block holder is selected based on in the combination of random selection and wealth or age. Although PoS uses more power than PoW, PoW is stillis a very popular scheme because it offers better consistency in this regardthe computer will be created by the creator of the next block. The most popular cryptocurrencies use the PoW system or the integrated PoW / PoS system.



Digital signature

A user who signs a digital transaction must have two keys: public key and secret key. The process is that the secret key is used to sign transactions are also kept confidential. After signing the transaction, i transactions are advertised in the full network; confirmation is possible with a public key sent by a user. Standard digital signature system involves two phases as mentioned: the signing and verification phase section. For example, user Bob is willing to send another user Alice a message, and wants no one else to read the message to it .

1. In the signing phase, Bob secretly records his data with his secret key is kept private, and sends Alice the encrypted result and the original data.

2. In the verification phase, Alice verifies the value with Bob's public key, and thus Alice can verify whether the data is easily tampered with or not. The elliptic curve signature algorithm is a digital signature system widely used in blockchains.

Smart contract

A smart contract is a computer program, or digital document, for the purpose of simplifying, validating, and forcing negotiations and contracting.

Smart contracts act as a ledger and allow for reliable operation transaction. The flow of work is similar to the fact that each block in the blockchain contains its own ledger, thus avoiding the need for any third party. In this way, smart contractors achieve their goal of providing security and trust higher than standard contract law and reducing other contractual burden. Algorithms that tolerate Byzantine errors have enabled security in partition, which has facilitated the construction of intelligent contracts. In addition, the programming languages used to build blockchains have several degrees of Turing perfection as a built-in feature, which allows for the construction of complex complex concepts.

The hash algorithm converts an invalid amount of data into a hash code of fixed length. The hash code will be changed depending on the data, i.e. the same hash code will be the result of the same data, but changing the data just a little bit will completely change the hash code. A hash function is a computer program that captures input data of any size, uses the function in it, and then output the output size data.

Different Security Algorithms

Different defense algorithms are analyzed for visualization and security issues, and solutions have been introduced.

- **SHA-256**

The Secure hash algorithm (SHA) is very complex in comparison with algorithms, such as SCRYPT. This algorithm is widely used by different cryptocurrencies and Bitcoin itself. Increasing the security of this Algorithm, the processing of data blocks is done almost free of any errors. However, it leads to slowing down the transaction, and thus minutesv used instead of seconds to measure time. For money mining to be is effective when SHA-256 is used, hash standards at GH / s level or higher quality is required. That is why it is not easy for all miners to dig again use the network at this high hash level.

- **SCRYPT**

As stated in the description of SHA-256, SCRYPT is much higher free and fast algorithm. In this review, it is noted that new cryptocurrencies on the market use SCRYPT over SHA-256 due to its ease of operation and speed. SCRYPT requires a few resources than SHA-256 and does not require its own dedicated machine jobs so many miners prefer to dig in SCRYPT-based cryptocurrencies rather than SHA-256 based. Hash ratings this algorithm lies in the range of KH / s or MH / s, which can be achieved with the operation of a single computer.

Some people doubt its authenticity again safety levels because of their time to do quick work, but no one has them proved this practice so far.

- **Crypto Note**

It is a protocol pertaining to the OSI model system framework. It is an important protocol behind many cryptocurrencies and is one of them reasons for the emergence of ideas like Bitcoin though both of these are separate from each other. An important difference between this dual technology blurrier than CryptoNote because of its the blockchain is almost unknown. On the other hand, non-CryptoNote blockchains do not see well. Although CryptoNote currencies use a a public and shared book keeps a record of all activities, the balance of its corresponding currency, does not follow blockchain also does not disclose the identity of the recipient or i sender. A value estimate can be made available, however actual value, origin, or location is not available. The rate is always higher than the actual value, and the sender only once the activity receiver knows the full set of data. This database can also downloaded by one person with one or both private keys.

There is one important difference which is PoW based on hash algorithm. SHA-256, a CPU-bound function, is used in Bitcoin, while CryptoNote uses CryptoNight, which is a memory-bound function that can be easily downloaded. Miners have their limitations based at the speed of calculating what is happening. CryptoNote code has never existed derived from Bitcoin and thus has many different algorithms available used in internal operation, such as the recalculation of the size of new block.

- **ECDSA**

ECDSA is a cryptographic algorithm used by various blockchain networks and widely used by Bitcoin. This algorithm ensures that money is used only by its trusted owners.

Some key concepts related to this algorithm:

Private Key: A randomly generated number that is supposed to be kept as a secret and is only known to the person that generated it. In the case of Bitcoin, the person having the private key which is connected to the money on the ledger that is available to everyone can spend that money.

Public key: This is deeply connected to its corresponding private key with the difference being that this does not have to be kept as a secret. This key can be derived or computed from the corresponding private key, but a private key cannot be retrieved from a public key. This is majorly used to find out whether the digital signature is authentic or not without making use of the private key. In the case of Bitcoin, these keys can be found in either of the two states: compressed or uncompressed.

Signature: It is a number that acts as proof of operation once the signing takes place. This is generated mathematically by two numbers, one being the hash of the transaction that will be signed and the second being the private key itself. The signature consists of two parts s and r. If one has the public key, then using a predefined algorithm, anyone verifies whether the signature was formed by the hash and the private key and this process does not include private key at all. Signatures are 71, 72, or 73 bytes of length and possibly 25%, 50%, and **25% respectively.**

Challenges in Security

Although blockchain is an innovative and effective technology, it is associated with a number of problems and challenges. In the research activities, the authors present the following challenges for the use and adoption of this blockchain technology.

Bandwidth and Size

The size of Bitcoin has grown steadily since the year it was created, i.e. since 2009 and has reached approximately 269.82 GB in the final of September 2019. If output performance is increased, blockchain size can increase by 214 PB annually. Therefore, this problem leads to the existence of a barrier to the number of unmanaged activities. If transaction value is higher, then size and bandwidth issues should be appropriate resolved.

Useability

A complete analysis of the Bitcoin flow and the Bitcoin user group in the network will provide the right percentage of usability. In addition, the Performance appraisal test will demonstrate the usability of the application. Therefore, addressing the usability problem is a challenge from researchers.

Privacy

It has been noted that blockchain has many potentials for 51% attack where one participant will have full control over additional hash-rate components of network mining. Otherwise, that business will have it the ability to update or change the blockchain. This issue remains the same an important safety challenge for researchers.

Wasted Resource

To dig Bitcoin, additional resources are needed due to the use of PoW system. Alternatively, the PoS system can be used. In the PoW program, mining depends on the miners and the work done by them. In the case of the PoS system, The amount of Bitcoin mined by the miner is calculated as the resources used. So, the problem with wasted resources must be solved in order to produce more on the blockchain network.

Delay

To achieve security efficiency, most of the time is spent on one block itself avoid double-edged attacks. Therefore, to avoid security attacks, most of the time is spent on performing tasks successfully. However, this is a matter remains a research challenge to satisfy participants.

Outturn

In recent years, the outflow of the Bitcoin network has increased to seven activity per second (tps). When out of competing applications is higher, and the growth of blockchain transactions is higher, and then up the use of blockchain networks should be a challenge.

Conclusion

One of the most popular cryptocurrencies is not only Bitcoin has attracted the best people, who are fascinated by the concept of blockchain segregation but it also entices people to misuse blockchain communications. There there are 5,563 different cryptocurrencies in the world, and the number is growing daily. However, Bitcoin has always been superior to all the others there it comes into use, and that makes it a major target for black hat hackers committing various wrong acts against similarity. The review led to findings, such as how Bitcoin-related agreements work, including PoW and making the whole concept separate so every user needs to do it they agree on a transaction, and this keeps the users safe. However, these set rules become a hole and a point of violation exploitation by people with malicious intent. Potential attacks Bitcoin is being discussed and ways to combat it are being developed. I existing research works on Bitcoin negotiating different ways for others cyberbullying can be minimized and addressed. However, there comes with full Bitcoin security and secure blockchain operation, no process can guarantee that. The concept of blockchain segregation has caused problems related to privacy as well features of anonymous users.

In short, this review article is a function of privacy and security problems in different areas of cryptocurrency. After defining the architecture of Bitcoin and its segregation of performance, this review highlights privacy and authenticity that can be proven in different stages of operation, from creating transactions to add-on activities in the blockchain. This work explores the privacy issue affecting each user and anonymous users in a world where cryptocurrencies and their use are increasing clearly. Apart from that, the security challenges in the Bitcoin network are being discussed in order to highlight the open research challenges and hope that this research will do. encourage researchers to start research on this exciting site.

References

Andrychowicz, M., Dziembowski, S. (2015). On the malleability of bitcoin transactions. Financial cryptography and data security: FC 2015 international workshops, BITCOIN, WAHC, and wearable (pp. 1–18). Springer

Huckle, J(2016). Procedia Computer Science, 98, 461–466. https://doi. org/10.1016/j.procs.2016.09.074.

Ghosh et al (2020). Journal of Network and Computer Applications, 163, 102635. https://doi.org/10.1016/j.jnca.2020.102635

Nakamoto (2008). Bitcoin: A peer-to-peer electronic cash system. https://bitcoin.org/bitcoin.pdf.

Narayanan e al(2016). Bitcoin and cryptocurrency technologies: A comprehensive introduction. Princeton University Press

Conti M (2018). A survey on security and privacy issues of bitcoin. IEEE Communications Surveys & Tutorials, 20(4), 3416–3452. https://doi.org/ 10.1109/COMST.2018.2842460.

Chaudhary, R (2019). Blockchain-based secure energy trading SDN-enabled intelligent transportation. Computers & Security, 85, 288–299. https://doi.org/10.1016/j.cose.2019.05.006

Dorri A (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. IEEE.

Tschorsch (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084–2123. https://doi.org/10.1109/COMST.2016.2535718

Bonneau, J. (2016). Why buy when you can rent? Springer

Karame, G. O (2012, October). Double-spending fast payments in bitcoin. In Proceedings of the 2012 ACM conference on computer and communications security (pp. 906–917).

Vyas, C. A.(2014). Security concerns and issues for Bitcoin. The Proceedings of National Conference cum Workshop on Bioinformatics and Computational Biology. NCWBCB.

Chohan, U. (2017). Cryptocurrencies: A brief thematic review. https://doi.org/10.2139/ssrn.3024330

Cynthia, D., & Moni, N. (1993). Pricing via processing, or, combatting junk mail, advances in cryptology. CRYPTO'92: Lecture Notes in Computer Science No. 740 (pp. 139–147). Springer.

Markus, J., & Ari, J. (1999). Proofs of work and bread pudding protocols. Communications and multimedia security (pp. 258–272). Kluwer Academic Publishers.

Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017). From bitcoin to cybersecurity: A comparative study of blockchain application and security issues. 2017 4th International Conference on Systems and Informatics (ICSAI) (pp. 975–979). IEEE

Barkatullah, J., & Hanke, T. (2015). Goldstrike 1: CoinTerra's first-generation cryptocurrency mining processor for bitcoin. IEEE Micro, 35 (2), 68–76. https://doi.org/10.1109/ MM.2015.13.

Jindal, A. S SURVIVOR: A blockchain-based edge-as-aservice framework for secure energy trading in SDN-enabled vehicle to-grid environment. Computer Networks, 153, 36–48. https://doi.org/10.1016/j.comnet.2019.02.002

Shojafar, M. (2019). Energy-efficient adaptive resource management for real-time vehicular cloud services. IEEE Transactions on Cloud Computing, 7(1), 196–209. https://doi.org/10.1109/TCC.2016.2551747