Blockchain and Bitcoin Security in IT Automation

Sikender Mohsienuddin Mohammad

Wilmington University

Abstract

In recent days, the technologies referred to as Blockchain and Bitcoin have gained much interest from society. These activities are increasing relevancy in the era of digitization and which forms a digital economy in the United States and all over the world. Currently, the automation of IT has deployed the use of technology atomization process through robotics hence machine production, the development of the framework of artificial intelligence, the Blockchain, and Bitcoin referred to as the open systems, the concepts of big data, algorithms of software, and the neural networks. In the implementation of enterprise, it is not easy to access the possibilities of assessing adequately and the consequences, which includes the opportunities of a qualitative change. In the last century, the invention of the essential ingredients that are key in the cryptography and its use in the hash functions have been underway and have also included the sensitivities that will enable Blockchain and Bitcoin to be successful. In recent years, technology has become available for the systems of payment, and other applications that revolve around bold issues, and the contracts are smart. The essay will discuss the automation trends and consequences of Blockchain and Bitcoin in the various sectors of the economy, including the industries. The paper will also comment on the analogies associated with the payments that may lead to a deeper understanding of the properties of Blockchain and Bitcoin.

Keywords - *Bitcoin, Blockchain, Distributed, Decentralized, Cloud computing, Authentication, Cryptocurrency*

Introduction

There has been a rising need for financial technology which will be used in the next generation, increasing recently. Ongoing studies have been carried out on Blockchain and Bitcoin to enable electronic cash to be used securely (Baur et al., 2018). It can be done by enhancing the peer to peer communication and without involving any third party. Blockchain and Bitcoin are ledgers that are public and are used for transaction purposes preventing hackers when a transaction is underway, which requires virtual cash (Conti et al., 2018). They deploy the use of a distributed king of databases that entails a list of data records which keep on growing daily. They are designed to avoid and disable any tampering that may be arbitrary by the user and operator of the peers that are being distributed (Kiayias et al., 2017). The records of transactions are encrypted by the use of a rule and operated using a computer that runs the software of Blockchain and Bitcoin (Vidal et al., 2018). However, Bitcoin is a currency that is electronic and uses the technology of Blockchain.

Using these technologies provides enhanced and quality security as compared to just store data in a central database. In the aspects of storage of data and management of data, any damage that may be as a result of an attack on the database is prevented and hence ensuring the security of data (Yanga et al., 2019). However, the technology has an attribute of openness that can provide data transparency when it is implemented to an area requiring the data to be disclosed. Moreover, due to all the strengths the technologies have, it is utilized in a diversified area, which includes the sector of finance, and the IoT environment that is referred to as the 'Internet of Things' and the applications are also expected to incur expansion in the future (Reyna et al., 2018). Many environments of IT has implemented the use of a technology referred to as cloud computing because it is efficient and readily available.

The paper tends to investigate the base technology, including the trends and survey of Blockchain and Bitcoin. The study will also consider the environments of cloud computing since techniques use it to enhance peer communication. It also focuses on the technology of Blockchain and Bitcoin (Puthal et al., 2018). It surveys them by creating an analysis of the tech that is generic and the trends of research, including the solutions for using Bitcoin more safely. The research results serve as essential data that is based on Blockchain study hence aiding in the understanding of the security problems that may be associated (Gaetani et al., 2017). The future of the technology of Blockchain can be fostered for further developments by developing an understanding of the trends of the security of Blockchain.

Literature review

This section will discuss the concepts of Blockchain and Bitcoin that are basic and the research that are currently existing. It will also discuss the study of the use of Blockchain and Bitcoin that are specific:

Blockchain:

Blockchain is a technology that allows its members to store a ledger that contains transaction data and helps them create an update of the accounting to maintain integrity whenever a transaction occurs. Members have been able to verify the transaction readability since the technology of the internet and encryption was advanced (Zhang et al., 2018). Therefore, the issue of an arising failure on a single point has been resolved hence eradicating the dependency of a third party that is authorized. The characteristic of blockchain is that it is P2P based, which means that it is broke free. It means that the system does not handle any unnecessary transaction fees through the P2P without having authorization from a third party (Joshi et al., 2018). When people own their information for transactions, hacking becomes difficult and therefore saving the expense of security. Any transaction done is approved automatically, and mass participation performs the recording hence assuring prompts (Nakamoto, 2019). Also, the implementation, connection, and expansion of the systems can be quickly made using a record of the transaction and the open-source. They are accessed openly to make the transactions become public and reduce the costs of regulation (Vidal & Ibanez, 2018).

The blockchain is designed in a way that it develops a list that is structured and is capable of saving data in a form that is similar to a database that is distributed. The design also makes the manipulation in an arbitrary way difficult since the participants in the network verify and save the blockchain (Gandal et al., 2018). A header and a body are structured in every block. The cash values are located on the header, which includes the current and previous blocks. Searching of block data is done in the database by deploying the method of an index. The hash value of the block next is added as a practice since the block itself does not contain the hash value (Baur et al., 2018). It becomes difficult to alter and falsify the data that is registered in the database because the stored hash values on every paper in a particular block are affected by the importance of the previous block. Although altering data may seem to be possible, that is, if an average of 52% of the peers is hacked under the same period, the scenario of an attack occurring is challenging in reality (Lu, 2018).

The verifications that are based on a key and the function of a hash in public can be decrypted since they are all used in the provision of security in the system of blockchain. The electronic signatures of the ECDSA algorithm verify the generated signatures when a transaction is done between peer individuals and proves that the transaction data is protected and has not been altered by any means (Zheng et al., 2017). One can discover the person who sent and has sent how much to the peer by using the public key that is rendered anonymous as the information of the account will be generated and displayed (Kiayias et al., 2017). The core ensures anonymity since there is no stipulated way of finding the information that is penetrating towards the owner (Conti et al., 2018).

The hash function does the verification of the block data that contains the details of transactions (Nofer et al., 2017). It ensures that no detail is interfered with and finds a value of nonce to generate a new block. It also guarantees that the integrity of the data being transacted is protected during a transaction of bitcoin. The key that is based on the public contains encryption that verifies the integrity of the details of the deal on the hash value of the data being transacted (Kiayias et al., 2017). The hash value is accumulated by the root hash value and is contained in every aspect of a transaction done. It enables the determining of whether the data of bitcoin was interfered with since the value of the root hash will change when any of the benefits are altered in the process of developing the data (Zheng et al., 2017).

Studies are underway to enhance security when one uses all the characteristics of the blockchain. The part that is crucial in the protection of blockchain is the one that is related to the personal key that is used in encrypting the data (Lin & Liao, 2017). Studies are also carried out on how the secret key will be protected. The private key that is stored in a peer's system will be attempted to be obtained by the attacker by deploying different kinds of attacks to hack the bitcoin. An attacker can hack Bitcoin since data leaking may occur if the attacker gets the personal key (Conti et al., 2018). To handle the problem, the studies done deploy the use of both software and hardware securities in the approval of any ongoing transactions.

Since bitcoin is always traded on a broader population, it becomes vulnerable to be infected by malware since it uses devices like smartphones and PCs. The malware is made to penetrate through various ways into the machine-like mails, USB drives, or even applications with relatively weak security (Halpin & Piekarska, 2017). Therefore, they must be detected and given the necessary treatment since they can interfere with the peer's device. Security needs are significantly growing and at a broader perspective that includes the trade of items used in gaming since most of them use bitcoins (Park, 2017). Therefore, it has led to studies on malware detection and treatment in the gaming environment.

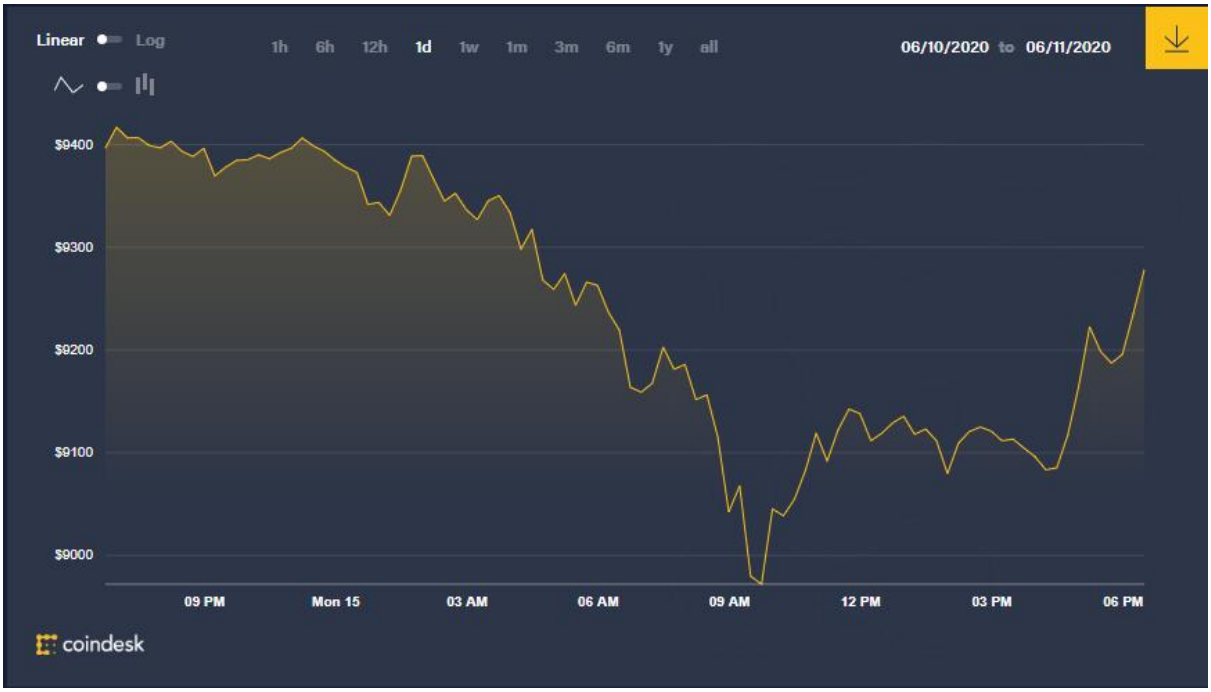
One of the aspects of bitcoins strengths is that it becomes a difficult task to falsify and interfere with the ledgers because many peers share the transaction ledger. The recorded data is taken to the majority of the ledgers making it practically impossible to hack unless the hacker can alter and falsify over 52% of the accounting of the peer's even if all the data in some of the ledgers are interfered

with (Dai et al., 2017). Concerning the increasing power of computers, some concerns are raised that 51% of the accounting can be interfered with and falsified simultaneously. To do away with this problem, some studies suggest that there should be an intermediate process of verification or the operation to be designed (Puthal et al., 2018).

Bitcoin:

Bitcoin is a type of currency that is digital. In 2009, Satoshi Nakamoto proposed the bitcoin to enhance peer-to-peer transactions without having authority at the center to manage and issue the currency. The database that is based on P2P is used in the trading of bitcoin and is based on the cryptology of the public key (Halaburda, 2018). In 1998, bitcoin became the first cryptocurrency to be implemented. The transaction information for bitcoin is disclosed on a network in a way that all the transacting peers are capable of verifying the transaction, therefore, limiting the issuance of currency (Aste et al., 2017).

The peers who are participating in the network have a blockchain that is the same, and blocks stores the data for the transactions made in a way that is the same with the storage distribution of the information being transacted (Vidal & Ibanez, 2018). Although involved threats are many on the transactions in an electronic means, bitcoin can cope with them if implemented professionally (Reyna et al., 2018). A good example is when a person tries to generate a receipt that is falsified from an account of another person to his own, he or she can be blocked by being verified with the personal key of the sender (Halaburda, 2018). If, at the same time, multiple parties intend to use bitcoin, elimination will be done to the chain that loses in the peer competition. The following chat is a 24 hour activity chart for the users of bitcoins primary index:



Source: https://www.coindesk.com/price/bitcoin

The components that are basic in bitcoin is the address of the bitcoin. It means where the bitcoin comes from and belongs (Giechaskiel et al., 2018). The peers of bitcoin confirm the transactions that indicate the bitcoin flow between the addresses and the block in which the transaction is located. The transaction of bitcoin is the key to the process of bitcoin (Benchoufi & Ravaud, 2017). It indicates the input that holds the bitcoin, and the address of the bitcoin becomes the output. The transaction of the bitcoin requires that all bitcoins located in the information should be transferred to the production whereby the inputs and outputs are needed to be in a single form (Henk & Bell, 2019).

Each electronic currency that is used in bitcoin is made up of signatures that are in an electronic forum and the form of a chain. The owner's coins are carried to the next chain with the previous transactions' hash value (Nofer et al., 2017). The electronic signature is taken to the subsequent owners' public key. The ownership chain is confirmed by the signature whereby the receipt evaluates the signature. In the process of confirmation, a problem tends to arise whereby the receipt cannot assure that one among the owners of bitcoin has not used it in multiple times (Conti et al., 2018). When this occurs, a reliable central authority is introduced to verify all the transactions made double to resolve the problem.

Solutions for blockchain and bitcoin security in automation:

Monetary damages can occur if the data of the user is disclosed in the environment of cloud computing. These may arise from the sensitive information of the user having leaked. The study of the security in transmitting and saving data, which

includes confidentiality and integrity in the environments of cloud computing are underway, this is according to Lu, (2018). However, the reviews on the anonymous and protection of the private data are not sufficient to ensure the integrity of information is preserved. The technology of blockchain represents anonymity (Park, 2017). If it is combined with the environment of cloud computing, blockchain can be enhanced and become a service that is convenient and provides security that is strong to its users (Park, 2017). If the method of blockchain is adopted in the saving of the information of the user in the environment of cloud computing, the anonymity of the user can be guaranteed. When using blockchain on cloud computing, an electronic wallet is installed in the system (Henk & Bell, 2019). . If the deletion of the electronic wallet is not done correctly, the user's information is left. The user information that is left behind can be used unanimously to guess the information of the user by an attacker (Dai et al., 2017). A proposal is made of a program that is capable of installing and deleting the electronic wallet in a secure way to resolve the problem.

The biggest problem is posed on the falsifying case of the ledger or the bitcoin and creating a double transaction of the blockchain by the user. Such a security problem requires a very secure wallet (Dai et al., 2017). Although the PC with an electronic wallet installed in it generally uses it, verification of the security of the electronic wallet in the devices is required as specific devices like mobile phones have become popular recently (Zheng et al., 2017). A transaction occurs based on the mobile device time value, therefore, making it easy to confirm the security of the transaction. It is only possible to do this if the time stamp accuracy and integrity generated in the mobile device are guaranteed (Joshi et al., 2018). Since the vulnerabilities tend to differ in accordance with the language of programming used and the platform that was used for the development of the environment of the electronic wallet, the base technology must also be verified (Baur et al., 2018). An electronic portfolio that is secure must be developed by being able to minimize and check and problems that may occur at every step of analyzing, planning, implementing, ensuring the quality, and maintenance (Gandal et al., 2018).

If an attacker infringes the system, the electronic wallet should be equipped with measures to secure restoration. Also, the system should be able to restore the self-protection verification for an installed binary and offer the remaining data protection that it requires (Zhang et al., 2018). It must ensure the utmost security for the data in the electronic wallet and also the setting necessary for using the electronic wallet. It should also be able to delete the data remaining in it in a secure way when it is no longer in use and must be discarded consequently.

To ensure that the electronic wallet is used securely, the user should install it on the PC, and the platform of the electronic wallet establishes a secure environment. The user then downloads the software for an electronic wallet and installs it in the PC to be able to use bitcoin with blockchain (Baur et al., 2018). The platform's public key is taken to the electronic wallet when the completion of the installation process is achieved. The platform then receives the distributed certificate from the electronic wallet when the development process is underway (Yaga et al., 2019). It then verifies if the document and the electronic wallet are valid. By using the method of Diffie-Hellman, the key is exchanged between the platform and the electronic wallet, whereby each of them owns the key that is shared (Gaetani et al., 2017). The electronic wallet and the platform are henceforth encrypted with the shared key when the user sends a request of a transaction that involves bitcoin. The ledger data that contains the stamp for the time between the two platforms also are encrypted. The certificate of the user is deleted once the request for disposal is completed (Puthal et al., 2018). The electronic wallet, therefore, receives a message for confirmation that the document is discarded securely. Also, all the relevant files are deleted to ensure that the data remaining are removed safely.

The case of authentication does not guarantee integrity since leaking is a problem that it faces by attackers taking advantage of the key that is personal in attacking the blockchain. It does not even protect residual information since the verification of the complete removal of the electronic wallet is not done (Conti et al., 2018). Availability is not provided in the incidents of a security case since the service is rendered unavailable due to the malware infection. Therefore, it does not protect the residual information since verification is not done. “The fact of the improved blockchain does not ensure integrity and availability since the double transaction remains vulnerable,” according to Yaga et al., (2019). The protection of privacy protects the information that is personal to the peers taking part in the transaction. The residual protection of information checks that the removal of the data of the user is done correctly at the point of terminating the transaction and removing the program (Dai et al., 2017).

The trends in the Blockchain and Bitcoin security technologies

Blockchain is a technology that is filled with the utmost potentials for transforming everyday’ business sectors. In the past years, reports have indicated that huge drops have been recorded on the values for the case of the bitcoin cryptocurrency. The report also shows that the programs that are pilot fails to mention the actual values (Reyna et al., 2018).

However, Walmart and IMB, which are the most prominent players, continue to push along with it with the confidence that it is capable of proving values that are real for the needs of an organization of the solutions of that innovates around record-keeping and transactions recording securely (Vidal & Ibanez, 2018). In the continuing years, we are likely to see the use of blockchain growing and making headlines continuously, although they may seem to be hyperbolically less. The following trends are likely to be achieved:

The technology becoming more substance with less hype and scams:

In the arena of blockchain, we are likely to see the more considerable and mature endeavors. Big businesses like Walmart develop solutions that will mean everyone involved in the product supply will adequately trace the items back to the farm where they are harvested by the use of a database that is distributed and cannot be tampered with (Gandal et al., 2018). . Amazon announced its projects for blockchain with several initiatives that aim to enable its customers to take advantage of supplying the technology of ledger in their projects (Zheng et al., 2017). With Amazon and Walmart, which are the most prominent players adopting the blockchain technology, it means that the technology can bring real value.

Blockchain continues to gather pace in its convergence with the Internet of Things:

In 2018, a report indicated that the use of the technology of blockchain in securing data in the technology of IoT was doubled. The trend seems to continue in the years that are coming, as more and more organizations are adopting the potentials of a distributed, and the technology of ledger that is encrypted in their fields (Joshi et al., 2018). It means that to break the powerful encryptions of blockchain, the attacker must have a large amount of the power of his or her computer to gain access to a single node. The nature they have, which are decentralized, means that the attackers cannot bypass the security by gaining access to a single node (Gandal et al., 2018).

Blockchain offers increases in the industries of financial services:

The trades of financial services mainstreams were not shaken by the emergence of the technology of blockchain and its potentials that are there to disrupt the thriving of the businesses. It, therefore, seems that they are likely to be at the forefront of the wave that may come next if it arises (Gaetani et al., 2017). In a society where most people are unbankable in developing a market in particular, it seems hard because the institutions do not have the ability or are unwilling to connect their services to the system (Baur et al., 2018). Therefore, enhancing start-ups may lead the way of the functions of innovation that is built around blockchain and digitizers that are resistant to currencies that are fraud and improve the mechanisms of data transfer (Kiayias et al., 2017).

Increased opportunities for investment brought by blockchain technology:

The technology of blockchain has rendered it possible for tracking and investment offers. The offers range to all the assets that have been provided the investors on institutions and preserving wealth (Conti et al., 2018). Regulations are therefore put in place before considering the opportunities of investment that is brought by the technology, which will render it safe enough for the daily investors to take place in their investments. When the regulations are in place, the individuals who invest regularly will be able to purchase the shares that are backed up digitally and sell them again when they want their funds to be liquidized (Lu, 2018). Additionally, the smart contracts that are designed based on the blockchain design reduce the middlemen reliance such as brokers when a transaction is being established, therefore lowering the entry costs and attached barriers.

Bitcoin will always hold the place of big business:

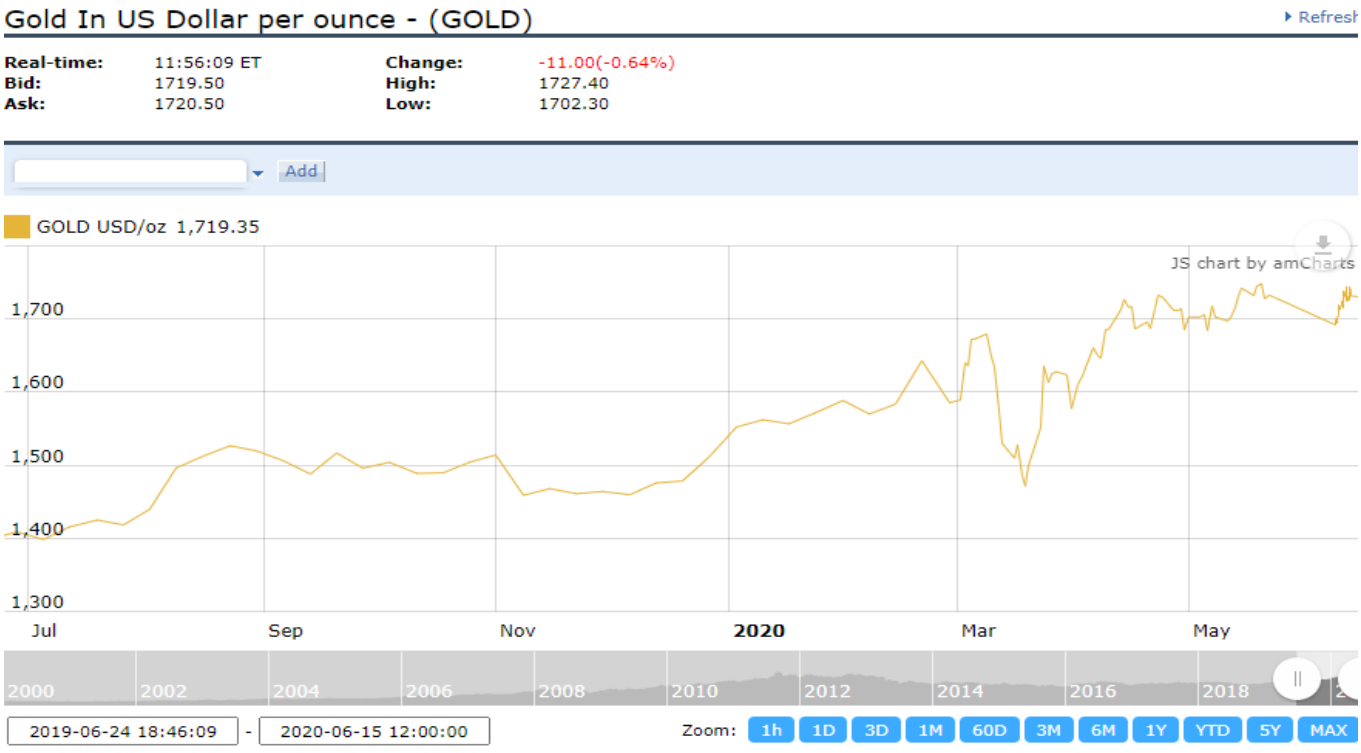
The price of bitcoin is used as a benchmarker since their cost is relatively much higher than the way they were in the previous years. Also, the volumes of trading on exchange indicate that there is an appetite that is healthy for investment speculation according to Reyna et al., (2018). Possible futures are therefore considered for the improvement of bitcoin in a way that it will offer advanced utility, enhance the security, and speed of operation. In 2017, the value of the assets of crypto circulation came close to three-quarters of a trillion-dollar worldwide (Baur et al., 2018). In 2018, the period continuation was observed that was relatively stable (Halaburda, 2018). When the people came to know about the cryptocurrencies and the offers it holds, it grew a foundation for an ecosystem of crypto that is valuable and began to emerge.

Discussion

The emergence of blockchain was a scheme that was distributed in enhancing transactions of any data. The data was supposed to be secured in the storage location and verification to be done without requiring a central authority (Henk & Bell, 2019). In other words, the blockchain notion was coupled tightly with proof that is well known for work, based on a hash mechanism of bitcoin. In recent days, blockchain has developed and has surpassed the hundred mark of blockchain alternatives (Krueckeberg & Scholz, 2019). Some of the other options are the simple bitcoins variants, others differ significantly on the design and the provision of the functions that are different, and the security is guaranteed (Baur et al., 2018). The following graph indicates the selling of Gold coins in US dollar for the bitcoin company interactive chart for the year 2019-2020:

Source: https://www.kitco.com/charts/interactive-charts/?utm_source=kitco&utm_medium=banner&utm_content=20110407_iCharts_chdata&utm_campaign=iCharts

It indicates that the community of researchers is searching for a simplified, scalable, and a blockchain that is deployed on technology. Reports also show an abiding interest in the blockchain use across different applications by various industries (Benchoufi & Ravaud, 2017). Everyone's expectation that blockchain will bring changes that are considered to several systems and large businesses.



The core of blockchain technology is to distribute trust and enhance privacy and security to the highest levels. They, therefore, have the potential of making them either fail or succeed (Krueckeberg & Scholz, 2019). The special issue tends to collect the ongoing research efforts that are the most relevant ones in establishing the privacy and security of the blockchain (Nakamoto, 2019). Many users are always grateful for the community of blockchain, especially on matters vast and the vivacity of its participation. An article by Ilias Giechaskiel et al. (2018) called "when the 'Crypto' breaks in the cryptocurrencies," which addresses the security of bitcoin under the primitives that are broken, they present an analysis of the primitives that are cut on bitcoin and its effects. The study ends up raising various suggestions for the plan of migration of bitcoin. It also provides an insight for the advancing cryptocurrencies in the case of the primitive cryptographies that are weakened (Giechaskiel et al., 2018). It, therefore, helps in tackling the critical security issues on the access to the blockchains that are contemporary.

Conclusion

Since blockchain has achieved in doing away with the server that includes the central authority involvement, it has been able to facilitate transactions through shared storage of the records of purchases. It has finally approved the P2P network technology transactions. The structure of blockchain that is distributed utilizes the network of peer to peer and the resources of computing of the peers. Implementation of the technical measures that

includes the stack and work proofs have been put in place to enhance the blockchain security. Although enhancement of the blockchain security is always done, specific problems have been encountered continuously. Therefore there has been an arising need for a security study to be implemented that is active. The attacker carries on various attempts to gain access to the key that is personal and stored in the computer of the user or a smartphone to acquire the bitcoin. To protect the private key, there are studies in place to implement the use of tokens that are secure or enhancing storage security.

The paper has discussed the technology of blockchain and the core technologies that are related to it, including a survey of the studies that are up to date in addressing the areas that are further to be studied. To use blockchain in the United States, the current issues are taken into considerations in adopting the use of blockchain in the environment of cloud computing. Various problems are attached to blockchains, including transaction security, electronic wallet, software, and studies to cater to all the issues. The user's information should be anonymously ensured when using blockchain in the environment of cloud computing.

The user's data should be deleted completely when the service is being removed. If the information is not correctly deleted and is left behind, the information of the user can be guessed from the information that is remaining on the system. Therefore, the paper has discussed the methods of enhancing security by the presentation of a process of use of blockchain that is secure and the protocols of removal. When taking into account the environments in which the information to be transmitted is massive, there is a need to study the efficiency of blockchain in handling such information besides considering the security.

References

[1] Aste, T., Tasca, P., & Di Matteo, T. (2017). *"Blockchain technologies: The foreseeable impact on society and industry*". computer, 50(9), 18-28. https://discovery.ucl.ac.uk/id/eprint/10043048/1/Aste_BlockchainIEEE_600W_v3.3_A.doccceptedVersion.x.*pdf*

[2] *Baur, D. G., Hong, K., & Lee, A. D. (2018). "Bitcoin: Medium of exchange or speculative assets?*". Journal of International Financial Markets, Institutions and Money, *54*, 177-189.

[3] Benchoufi, M., & Ravaud, P. (2017). "*Blockchain technology for improving clinical research quality"*. Trials, 18(1), 335. https://trialsjournal.biomedcentral.com/articles/10.1186/s13063-017-2035-z

[4] Conti, M., Kumar, E. S., Lal, C., & Ruj, S. (2018). "*A survey on security and privacy issues of bitcoin"*. IEEE Communications Surveys & Tutorials, *20*(4), 3416-3452. https://arxiv.org/pdf/1706.00916.pdf?utm_source=securitydailynews.com

[5] Dai, F., Shi, Y., Meng, N., Wei, L., & Ye, Z. (2017, November). *"From Bitcoin to cybersecurity: A comparative study of blockchain application and security issues*". In *2017* 4th International Conference on Systems and Informatics (ICSAI) (pp. 975-979). IEEE.

[6] Gaetani, E., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017). "*Blockchain-based database to ensure data integrity in cloud computing environments"*. https://eprints.soton.ac.uk/411996/1/BC_1.pdf

[7] Gandal, N., Hamrick, J. T., Moore, T., & Oberman, T. (2018). "*Price manipulation in the Bitcoin ecosystem*". Journal of Monetary Economics, *95*, 86-96. https://par.nsf.gov/servlets/purl/10066235

[8] Giechaskiel, I., Cremers, C., & Rasmussen, K. B. (2018). "*When the crypto in cryptocurrencies breaks: Bitcoin security under broken primitives*". IEEE Security & Privacy, *16*(4), 46-56. https://ora.ox.ac.uk/objects/uuid:37b766d5-c749-41e7-bb24-8d10cde6133f/download_file?safe_filename=SP_SPSI-2017-01-0027.R1_Giechaskiel.pdf&file_format=application%2Fpdf&type_of_work=Journal+article

[9] Halaburda, H. (2018). "*Blockchain revolution without the blockchain?"*. Communications of the ACM, *61*(7), 27-29. https://dl.acm.org/doi/fullHtml/10.1145/3225619

[10] Halpin, H., & Piekarska, M. (2017, April). *"Introduction to Security and Privacy on the Blockchain*". In 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 1-3). IEEE. https://hal.inria.fr/hal-01673293/document

[11] Henk, M. A., & Bell, R. T. (2019). "*Blockchain: An insurance focus*". http://jp.milliman.com/uploadedFiles/insight/2016/2340PCP_Blockchain_20161108.pdf

[12] Joshi, A. P., Han, M., & Wang, Y. (2018). "*A survey on security and privacy issues of blockchain technology"*. Mathematical Foundations of Computing, *1*(2), 121-147. http://www.aimsciences.org/article/doi/10.3934/mfc.2018007

[13] Kiayias, A., Russell, A., David, B., & Oliynykov, R. (2017, August). "*Ouroboros: A provably secure proof-of-stake blockchain protocol."* In Annual International Cryptology Conference (pp. 357-388). Springer, Cham. https://coinnws.com/wp-content/uploads/2019/08/cardano-whitepaper.pdf

[14] Krueckeberg, S., & Scholz, P. (2019). "*Cryptocurrencies as an asset class"*. In Cryptofinance and Mechanisms of Exchange (pp. 1-28). Springer, Cham. https://www.researchgate.net/profile/Peter_Scholz7/publication/325057131_Cryptocurrencies_as_an_Asset_Class/links/5d026bef92851c874c6436af/Cryptocurrencies-as-an-Asset-Class.pdf

[15] Lin, I. C., & Liao, T. C. (2017). "*A survey of blockchain security issues and challenges*". IJ Network Security, *19*(5), 653-659. http://ijns.jalaxy.com.tw/contents/ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf

[16] Lu, Y. (2018). "*Blockchain and the related issues: a review of current research topics*". Journal of Management Analytics, *5*(4), 231-255.

[17] Nakamoto, S. (2019). "*Bitcoin: A peer-to-peer electronic cash system"*. Manubot. https://git.dhimmel.com/bitcoin-whitepaper/

[18] Nofer, M., Gomber, P., Hinz, O., & Schiereck, D. (2017). "*Blockchain. Business & Information Systems Engineering", 59*(3), 183-187. http://www.cs.unibo.it/~danilo.montesi/CBD/Articoli/2017Blockchain.pdf

[19] Park, J. H., & Park, J. H. (2017). "*Blockchain security in cloud computing: Use cases, challenges, and solutions". Symmetry*, *9*(8), 164. https://www.mdpi.com/2073-8994/9/8/164/pdf

[20] Puthal, D., Malik, N., Mohanty, S. P., Kougianos, E., & Yang, C. (2018). "*The blockchain as a decentralized security framework [future directions]"*. IEEE Consumer Electronics Magazine, *7*(2), 18-21. http://www.smohanty.org/Publications_Journals/2018/MohantyIEEE-CEM_2018-Mar_The-Blockchain.pdf

[21] Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). "*On blockchain and its integration with IoT. Challenges and opportunities*". Future generation computer systems, *88*, 173-190. https://www.sciencedirect.com/science/article/pii/S0167739X17329205

[22] Vidal-Tomás, D., & Ibañez, A. (2018). "*Semi-strong efficiency of Bitcoin*". Finance Research Letters, *27*, 259-265.

[23] Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). "*Blockchain technology overview*". arXiv preprint arXiv:1906.11078. https://arxiv.org/pdf/1906.11078

[24] Zhang, Y., Deng, R. H., Liu, X., & Zheng, D. (2018). "*Blockchain based efficient and robust fair payment for outsourcing services in cloud computing*". Information Sciences, *462*, 262-277. https://ink.library.smu.edu.sg/cgi/viewcontent.cgi?article=5216&context=sis_research

[25] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). "*An overview of blockchain technology: Architecture, consensus, and future trends*". In *2017 IEEE international congress on big data (BigData congress)* (pp. 557-564). IEEE. https://www.researchgate.net/profile/Hong-Ning_Dai/publication/318131748_An_Overview_of_Blockchain_Technology_Architecture_Consensus_and_Future_Trends/links/59d71faa458515db19c915a1/An-Overview-of-Blockchain-Technology-Architecture-Consensus-and-Future-Trends.pdf