Applications of Block-Chain Technology and Related Security Threats

Article *in* SSRN Electronic Journal · January 2002

DOI: 10.2139/ssrn.3205732

1 author:

Rejwan Bin Sulaiman
Glyndwr University
4 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Applications Of Blockchain Technology And Related Security Threats

A Comparative Study

Rejwan Bin Sulaiman
School of Computer Science and Technology
University of Bedfordshire
Vicarage St, Luton LU1 3JU

***Abstract*—Blockchain is one of the emerging technology of 21st century. It is getting common to the people helping them by providing better financial services without any centralised medium (banks, agencies etc.). Although it has a strong backbone of cryptography which ensures the data protection, however, security vulnerabilities are still the part of this system and they are continuously emerging. This paper will explore the deep analysis of various blockchain applications, related security threats and vulnerabilities, future trend and possible solutions that could promise the integrity of this technology.**

Keywords— Security, IOT, threats, privacy, bitcoin, Cybersecurity, privacy-protection

I. INTRODUCTION

Bitcoin is composed of a backbone of certain cryptographical instances which are referred as the blockchain. [1] At some stage, Bitcoin has banned in certain countries i.e. Russia, European states and other countries because of the lack of centralised infrastructure and also sudden changes in the value of bitcoins itself Blockchain technology is one of the emerging technology in an IT World and without any doubt, it has altered the financial infrastructure to a greater extent. But as far as the security aspects of this technology are concerned, it has been adopted by the wide range of public and people have developed their confidence towards this revolutionary technology. [2-4].

The blockchain technology emerges as an outstanding way of giving the opportunity of data storage in such a way that it can manage the data as well as transmit the data over the platform in a decentralised manner without the involvement of any third-party firm or related organisation. This technology has brought a big revolution in all private and public sector, however, while looking at its base it has started from cryptocurrency and over the period of time it has contributed to a larger extent in various credit assets etc. and even now it has grown up in an information system and other sectors of data transmission. Confidentiality, reliability, authenticity and availability are always being a big concern about this technology.

The blockchain is one of the technologies which is spreading very quickly, and many firms and organisations are getting familiar with the ultimate advantages of its applications in the near future. However, while considering all the positive aspects of this technology, there are security limitations and threats that could make this infrastructure invulnerable to attacks. [5] Over the time the ultimate possible weaknesses are getting exposed and the experts and researchers are working to put all their efforts to ensure the integrity of this technology. Delays in the data transmission and finite size of the blockchain have been in a serious consideration and possible solutions are implemented to reduce the risk caused by them [6-8].

II. BENEFITS INVOLVED IN SECURITY OF BLOCKCHAIN

The ultimate backbone of this technology for the users is to rely on the database which is deprived of any physical medium like banks or corporations. Below figure gives the technical infrastructure of blockchain technology:

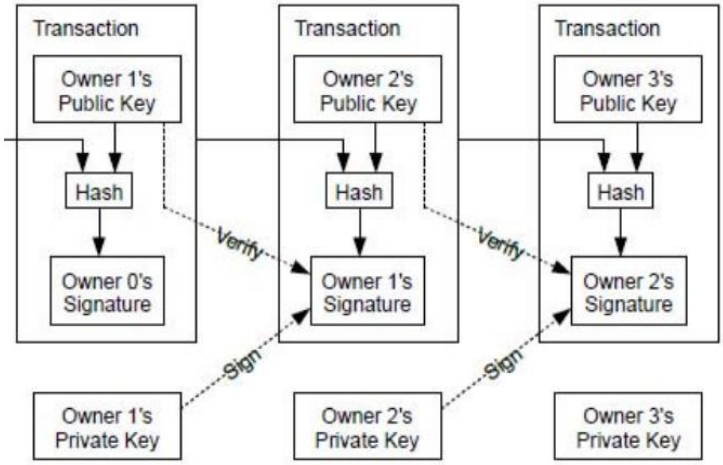

Figure 1: Blockchain system [1]

As shown in the figure above, there is a number of blocks which are responsible for the generation of data and provide the storage place. All the blocks are connected to each other in a consecutive order to form the centralised data model. As shown all the endpoint nodes of the users are involved in the authentication and management process of the data. And in case of addition of any new block required an authentication for over half of the total available users and the process of centralised synchronisation goes over the all user's platform once the new block is added. Afterwards, when the process of centralised synchronisation is established, the system won't allow making any alterations or formatting of the data [1].

According to all the technical aspects of the database of the blockchain, point to point network strategy and other cryptographic measures, it ensures the best possible security

solution to the users in terms of the overall operation of the system as well as it keeps in consideration the bandwidth utilised in the distributed database strategy [9]. In terms of security point of view, blockchain technology has brought tremendous advantages among which some are as follows:

A. Strategy of anti-tamper

One of the great things about the blockchain technology is that it is tamper-proof which doesn't allow any alteration of the data and this is achieved by the structure of data used in blockchain as well as the method of building up that data. Following figure demonstrate the real operation behind the mechanism of its anti-tamper strategy:

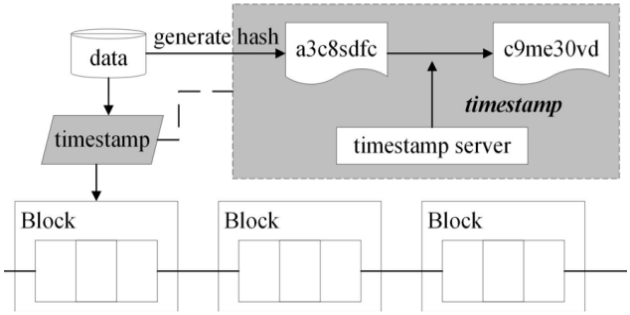

Figure 2: Anti-tamper operation of the blockchain[10]

As elaborated in the figure above, whenever any transaction is added to the combined form of blockchain topology in its centralised data infrastructure, at the same instance another timestamp will be noticed as well [10][11]. And interestingly any alteration of data that is performed earlier will no longer be allowed. And in any case of addition of transaction, it must be decided mutually by agreement method. In simple, the acceptance of the number of users are required to write the data in the block format and usually, this number goes up to 50 percent. In case of data monitoring process, the over networking nodes are required to take in consideration for the purpose of possessing strong processing power for its operation.

B. Recovery procedures

Blockchain technology utilises the certain protocols which are open source and they are involved in the monitoring of the data and secondly, it synchronizes the storage data over the all end-user platform. This strategy is quite different than the one used in a conventional database system where it provides storage and monitoring of the data in one or multiple locations whereas in blockchain topology, all the users have the complete information about the data and they keep all the possible records of the generated data. However, in this case, redundancy is one of the factors that can be an issue to a certain level but on the other hand integrity of the overall network is enhanced and due to this random attack will no longer create a massive damage to the overall network system of the blockchain. [12][13]

C. Confidentiality

Blockchain ensures the maximum protection to the data by considering the privacy factor by utilising the asymmetric method of data encryption and this method is quite secure than other as it let the users create their own private key [14][15][16]. And the public is distributed across the network which is used for the purpose of user identification and the interesting thing about this terminology is the hash value which is not concerned in anyhow with the actual user identity, thus ensuring the user's confidentiality and privacy. The scope of this strategy can be monitored on the base of the fact that user's private key cannot be known by anyone else and it is impossible to generate the private key while using the public key.

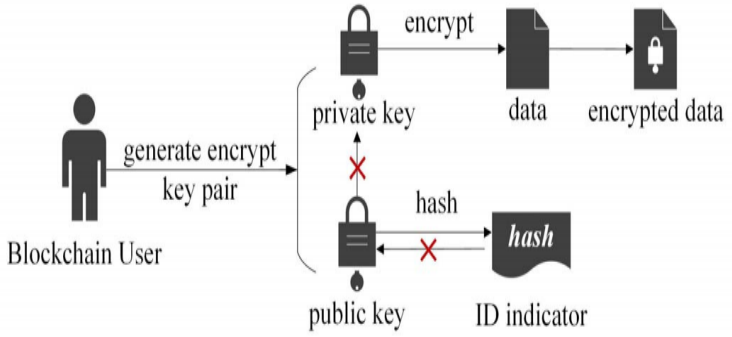

Figure 3: Confidentiality in the blockchain[14]

III. BLOCKCHAIN APPLICATIONS INVOLVED IN CYBER SECURITY

As the fact that blockchain technology was pursued while keeping in consideration of the Bitcoin evolution. At the root level, blockchain system is quite transparent, open source as well as it allows the equal distribution. Relying on the blockchain technology goes to the fact that it uses the complex cryptographic algorithms that ensure the maximum protection and doesn't involve any conventional medium in the middle of its operation. Due to its excellent security insurance, it has become popular not just only in cryptocurrency sector, but it has also gained a huge importance in management of assets and credits, and over the time it is evolving in various other sectors as well which typically involve finance sector, banking, engineering, medical sector etc. and the importance of its application are getting common day by day.

The scope of this technology can be determined by the taking in consideration of financial sector where blockchain provides best possible clearing and other payment solutions without any alteration in the normal conventional system. No doubt this technology has played a big role while increasing the ultimate efficiency of the business operation. Similarly, in the medical sector, this technology is being used to electronic records of medical data over the various hospitals and clinics and it also provides a solution to various information database management. The same trend can be observed in the energy sector and others as well. Due to the advancements in the security field, this has led improvement and great innovations while in the building process of blockchains and ultimately this can be used as a best possible solution for the major privacy and other issues involved in cybersecurity.[17] There is a number of blockchain applications that are in use, among them some are as follows:

A. Domain name system security

The major function of the domain name system is to issue the name of the servers based on the IP address and vice versa and to accomplish this strategy it follows the hierarchical design and the major operation is managed over the centralised DNS based server. Due to this adoption, several attacks could be possible which are originally based on the servers and among them, the most considerable one is the hijacking of DNS server, another DDoS attack etc. While considering the scenario above there are several studies available based on the blockchain DNS and this constitute of building the domain name system while considering the blockchain used in Bitcoin technology [17][18]. The overall secure communication is achieved by mapping the DNS with the hash, in such a way that it could give the user flexibility of using this system by performing their tasks which typically includes registration, data transfer and data checksum over the system. In this case, the node is always responsible for providing the storage place to the two generated keys by the asymmetric method i.e. private key and public key and other than that it also records the domain names. This situation which combines the domain name system with the blockchain technology results in the better encryption in the working of the blockchain system. This also results in providing a better security solution as this strategy makes the system decentralised and there is longer any central place which could provide any favourable place for the attacker, as the storage of data has no any central unit to be a target. Based on the blockchain topology which is built upon the DNS system and this makes every single node of the system to act as the DNS server and as the result of this, there will be no threat of getting any attacks like Hijacking attacks and other related sniffing attacks.

B. Signatures with no key strategy

While considering the environment, where it is required to deal with the big amount of data at a time, this results in the problem of publication of the key and also the alteration and other updating issues. Since the advancement in the computer industry which typically includes the massive development in the quantum computers, it can cause the breaking down the conventional system of asymmetric algorithm standards. To while considering this strategy, the researcher has come up with the solution to cope with this issues and threats by introducing the topology of keyless signature infrastructure (KSI) [19][20][21][22]. This keyless system takes the full benefits of taking in consideration of timestamp that can be used in blockchain technology. So, while looking at the operation of this keyless infrastructure, it utilises and stores the available state of the data, the overall system as well as the value of the hash. Afterwards, the KSI system will add a consecutive monitoring of the hash values while considering the timestamp and this results in adding more security in terms of any unauthorised to access or any other type of attack that can possibly happen to the OS and also on various applications. So, this type of monitoring the system there is not required to perform the maintenance of the keys as well as the revocation process. This helps the KSI to secure the big amount of data at a time. From the implementation point of view, it has a various application that is being used in a number of areas which typically includes nuclear sector and also commonly in flood prevention system that is widely adopted in the United Kingdom.

C. Security for the storage of data

Since for a long time, it's being very common about the number of incidents that have happened in the past due to the leaking of data to an unauthorised access in the central database which provides the data storage facility and this didn't happen in the small corporation rather it has affected certain organisations at national level which typically includes the area of finance, medicine and so on and the loss of privacy in these areas could cause a great destruction as it deals with the most sensitive part. According to one of the solutions that have been proposed is the use of blockchain technology which can be utilised to secure and the management of the hash value which typically includes the data of users identity, medical history and another appointment schedule in the medical sector [23][24][25]. With the use of the multi-signature procedure, there is the possibility of enhancing the security factor which can restrict certain access by creating an access list/rules and that rules can only let the users do any changes of updates when the permission of access is granted by the blockchain networking system. By implementing this strategy has greatly affected the medical industry in terms of providing better healthcare to the people by keeping and managing the record of all the doctors, staff and patients efficiently. This terminology is not just limited to the medical sector, but it has also explored its application in other areas as well i.e. certification of IoT devices [26][27], decentralisation of the data used in cloud [28] and most importantly in secure transmission process of data [29], as all these sectors are greatly improved by the use of blockchain technology.

IV. SECURITY VULNERABILITIES IN BLOCKCHAIN TECHNOLOGY

Due to the recent emerging of this blockchain technology, it has resulted in carrying out research work based on its advantages and many other useful and secure parameters. After doing a careful analysis of various applications of blockchain technology, it will be clear of the fact that this technology is still at its beginning stage and it still required several amendments and alterations to implement this technology in more broader scale and applications. No doubt, blockchain technology is evolved as the outstanding way of providing the best optimization in various sectors, however, the fact of the security risks and other vulnerabilities are still the part of the system. Despite its feature of decentralisation, it has already created certain issues which require a serious attention. Following are some of the possible risks involved in the blockchain technology:

A. Practical limitations

There is a number of technical points which restrict the blockchain technology to be a fully reliable component for the data management. One of the aspects that must be considered is the limited capacity of the blocks that are involved in the blockchain and because of this, there is a number of applications which doesn't allow this technology to be implemented. At the early stage, each block capacity was given the value of 1MB to prohibit attacks especially the one based on DDoS attacks. And there always be an argument between the size of the blocks i.e. smaller or bigger. Although the big blocks can result in giving more storage capacity to accommodate more records and data, however

on the other side overall management and operation of these nodes of blockchain is interrupted. While, the smaller blocks give a more reliable solution of data management without the involvement of any organisation, however in that places where it requires to deal with the big data, smaller blockchain is unable to accommodate enough storage space for the data records.

The operation of blockchain technology involves the distributed system for the storage of records and data, however, at the same time, it is giving more exposure to the attacker to access the data in various ways. While considering the fact that in the blockchain operation, the system keeps the copy of each data at all the user's end which is involved in the process, so it can be clearly noticed that attacker will get several ways to get access to the records which can be quite destructive. The worth thing to consider about the blockchain terminology is that it doesn't allow any user to make any alteration or changes in record or data, however even because of these secure parameters, an attacker can still find its way to attack the system which typically includes the methods of data mining and other various ways which can result in retrieving of the sensitive data which typically includes data about the network infrastructure, user personal information etc.

Another major issue about the blockchain technology to be considered is the risk of corporative attack which is based on the consideration of an assumption that most of the nodes involved in the blockchain technology work smoothly and securely. However, if one or multiple nodes involved together to operate the 51% of the computing process of the overall blockchain infrastructure, they can combine altogether and can cause an attack on the system which can result in the alteration of the various contents available in the blocks and other than that it may cause severe attacks which can cause a massive destruction on the wider scale, like DDoS attack is one of the common to be considered.

B. Threats involved in cryptography

As the whole structure of the blockchain technology relies on the cryptographic standards and methods, while in this strategy of cryptography the certain issues associated with the blockchain technology is not resolved that mainly includes the problems associated with the management of the private key. In the current scenario of various applications of the blockchain, it utilises the private key to check the owner's identification while performing payment etc. Major risk involved in this strategy is the private key that is being used by the user and the point to be considered that user is the only owner and knows the fact of its key without the involvement of any third-party organisation i.e. bank. So, in this case, the user is the only one who can take care of its private key. The issue will arise if the user loses its key and this can result in a destructive situation for the user as it will not able to get access to its various assets that are based on blockchain without knowing its private key.

As the blockchain technology is implemented on the wider scale, and due to this it creates certain vulnerabilities and weaknesses which are usually based on the cryptographic algorithms. The point to be considered is the fact that blockchain uses the complex algorithm i.e. RSA etc. to carry out its cryptographic operation. However, during the implementation or maybe afterwards certain security weaknesses can be added creating a backdoor for the attackers, even possibly to the algorithm itself. And this adoption of vulnerability in the system can cause severe destruction to the overall blockchain infrastructure or maybe some of its applications. Due to the emerging of the quantum computing, it is causing the probability to crack the algorithms that are involved in the asymmetric cryptography.

C. Issues with the opensource strategy of Blockchains

Blockchain technology is involved in most of the applications that are associated with the upper-layer and it manages and operates various applications and its association with the users. To understand this strategy, it can clearly analyse its application used in the number of various sectors i.e. medical records, finance and other telecommunication sectors where the data is not just generated but also stored and transmitted over the blockchain system. Due to the opensource nature of the blockchain system, it results in giving the favourable environments to the attacker and hacker to exploit the various vulnerabilities of the system and this ultimately result in the massive destruction in terms of data privacy and access.

D. Management of blockchains in terms of security

In case of blockchain system, it is quite clear that it uses the distributed data strategy for the purpose of storing data, so to achieve that there involves the continuous flow of data quite frequently to keep the whole system in operation. As the blockchain structure involves the storage of the copy of data at every user's side. And at the time when any transaction is made to a block, it will simultaneously update all the copies of data at user's end. So, the users which are based on the wider geographical regions use this blockchain system, the quick processing of data results in the improvement of management of records and data transmission.

Another thing about the security of blockchain is the consideration of anonymity technique which may cause problem towards the attack. According to the operation of blockchain for the other users, they compute a hash value from the public key generated by the certain user. But the key thing to consider is the feature of securing the privacy of the users where it is impossible to keep the track of the real identity of the users as according to the rules and regulations of the cybersecurity.

V. CONCLUSION

Due to the advancements in the blockchain technology, there have been high hopes for this technology by the individuals and the organisations. Its applications have been adopted in various areas and even it has emerged into the field of ICT as well and other than that due to its unique infrastructure it is also being used in the finance sector. However, along with these advancements, there are many associated issues that are being considered on the priority basis by the researchers and the experts.

No doubt that this technology has brought a great revolution and its applications are continuously expanding and the advancements are in the pace such that it is emerging itself into the already existing technology and coming up with the better infrastructure for the business operation. And at the same time, it is also a challenging in the field of network security. This paper has

explored a comparative research on the blockchain technology and related issues while opening the future doors of considering those issues and come up with the best possible solutions in terms of introducing standards and other parameters so that its application could be adopted on the wider scale.

REFERENCES

[1] N. Satoshi, "Bitcoin: A peer-to-peer electronic cash system," Consulted,2008, pp:1-9.

[2] G. Varriale, "Bitcoin: how to regulate a virtual currency," International Financial Law Review, 2013, 32(6), pp: 43-45.

[3] D. Swartz N., "Bursting the Bitcoin bubble: The case to regulate digital currency as a security or commodity," Tul. J. Tech. & Intell. Prop.,2014, 17, pp: 319-335.

[4] N. Wenker, "Online Currencies, Real-World Chaos: The Struggle to Regulate the Rise Bitcoin," Tex. Rev. L. & Pol., 2014, 19, pp: 145-184.

[5] M. Swan, "Blockchain: Blueprint for a New Economy," O'Reilly Media, Inc.; 2015.

[6] Bitcoinwiki; 2015, https://en.bitcoin.it.

[7] AM. Antonopoulos, "Mastering Bitcoin: unlocking digital cryptocurrencies," O'Reilly Media, Inc., 2014.

[8] Double-spending, https://en.bitcoin.it/wiki/Double-spending

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, K. Smolander, "Where Is Current Research on Blockchain Technology?- A Systematic Review," PLoS ONE, 2016, 11(10), pp: 1-27.

[10] D. Tapscott, A. Tapscott, "Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business, and the World," 2016.

[11] B. Gipp, N. Meuschke, A. Gernandt, "Decentralized Trusted Timestamping using the Crypto Currency Bitcoin," in Proceedings of the iConference 2015, Newport Beach, CA, USA, Mar. 24-27, 2015.

[12] G. Paul, P. Sarkar, S. Mukherjee, "Towards a More Democratic Mining in Bitcoins" In: Prakash A, Shyamasundar R, editors. Information Systems Security. vol. 8880 of Lecture Notes in Computer Science. Springer International Publishing, 2014. pp: 185-203.

[13] L. Wang, Y. Liu, "Exploring Miner Evolution in Bitcoin Network," In: Mirkovic J, Liu Y, editors. Passive and Active Measurement. vol. 8995 of Lecture Notes in Computer Science. Springer International Publishing, 2015, pp: 290-302.

[14] Zyskind, Guy, O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," Security and Privacy Workshops (SPW), IEEE, 2015, pp: 180-184.

[15] Kosba, Ahmed, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," Security and Privacy (SP), 2016 IEEE Symposium on. IEEE, 2016, pp:839-858.979

[16] Meiklejohn, Sarah, Claudio Orlandi, "Privacy-enhancing overlays in bitcoin," International Conference on Financial Cryptography and Data Security, Springer Berlin Heidelberg, 2015, pp:127-141.

[17] H. Weihong, A. Meng, Sh. Lin, X. Jiagui, L. Yang, "Review of blockchain-based DNS alternatives," Chinese Journal of Network and Information Security, 2017, 3(3), pp: 71-77.

[18] M. Ali, J. Nelson, R. Shea, M. Freedman, "Blockstack: Design and Implementation of a Global Naming System with Blockchains", Last visited on, 2016, 25(2).

[19] Tosh, K. Deepak, "Security implications of blockchain cloud with analysis of block withholding attack," Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE Press, 2017, pp:458-467.

[20] Liang, Xueping, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing. IEEE Press, 2017, pp:468-477.

[21] Jämthagen, Christopher, Martin Hell, "Blockchain-based publishing layer for the Keyless Signing Infrastructure," Ubiquitous Intelligence & Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People, and Smart World Congress (UIC/ATC/ScalCom/CBDCom/IoP/SmartWorld), 2016 Intl IEEE Conferences. IEEE, 2016, pp: 374-381.

[22] Emmadi, Nitesh, Harika Narumanchi, "Reinforcing Immutability of Permissioned Blockchains with Keyless Signatures' Infrastructure," Proceedings of the 18th International Conference on Distributed Computing and Networking. ACM, 2017 (46).

[23] Azaria, Asaph, "Medrec: Using blockchain for medical data access and permission management," Open and Big Data (OBD), International Conference on. IEEE, 2016, pp: 25-30.

[24] Yue, Xiao, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, 2016 (218).

[25] Ekblaw, Ariel, "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data," Proceedings of IEEE Open & Big Data Conference. 2016, pp: 1-13.

[26] Christidis, Konstantinos, Michael Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, 2016, pp: 2292-2303.

[27] Zhang, Yu, Jiangtao Wen, "The IoT electric business model: Using blockchain technology for the internet of things," Peer-to-Peer Networking and Applications, 2017, pp: 983-994.

[28] Wilkinson, Shawn, J. Lowry,T. Boshevski, "Metadisk a blockchainbased decentralized file storage application," Technical Report, Available: http://metadisk. org/metadisk. pdf, 2014.

[29] Rowan, Sean, "Securing Vehicle to Vehicle Communications using Blockchain through Visible Light and Acoustic Side-Channels." arXiv preprint arXiv:1704.02553 (2017).