Research Journal of Computer and Information Technology Sciences _____ISSN 2320 – 6527
Vol. **10(1),** 23-26, June **(2022)** *Res. J. Computer and IT Sci.*

Review Paper

Security and Privacy of Blockchain Technologies

Punyaban Patel[1*] and Riyam Patel[2]
[1]Department of Computer Science and Engineering, CMR Technical Campus, Kandlakoya, Hyderabad, India
[2]Department of Computer Science and Engineering, SRM Institute of Science and Technology, Kattankulathur, Chennai, India
punyaban@gmail.com

Available online at: www.isca.in
Received 14th Novembre 2020, revised 17th October 2021, accepted 7th January 2022

Abstract

Probably for about a decade, Blockchain technology (BCT) has prompted significant attention around the world. Since the technology was coined, the focus of the researcher switched to investigate the technology's insights. Second, Nakamoto invented the digital currency or cryptocurrency concept. The foundation of these cryptocurrencies is decentralised networks and the blockchain technology behind these currencies. While several investigation for blockchain on the security and privacy concerns have been performed, there is still a lack of systematic review on the safety and security of the blockchain technology. Here, with regard to various developments and applications, the security, confidentiality and the privacy of the blockchain along with its effects have been addressed.

Keywords: Blockchain Technology, Cryptocurrency, Security, Privacy, Distributed Techniques, Internet of Things (IoT)

Introduction

Crypto currency in both academia and industry has already become a buzzword. With its money, Bitcoin enjoyed a tremendous success[1]. In the capital market. A blockchain is essentially a list verifiable by cryptography. One of the reasons for the excitement around the blockchain is that there are no fairness in cryptographic databases, which is an important for any type of database running in an antagonistic situations and environment.

As a public ledger, Blockchain can be considered, and in a list of blocks all committed transactions are stored. This chain can grows if new blocks are continuously added to it.[2,3] In general, blockchain technology has core features of decentralization, confidentiality, persistency, and auditability. Blockchain can massively save costs and increase productivity with these characteristics. Since it makes it possible to make transfers funds without any bank or intermediary like agents or brokers, blockchain can be used in various types of services related to finance such as online payments, remittances & digital assets.

This paper is organised as the Section 1 contains Introduction, Section 2 contains Concepts of Blockchain Technology, Section 3 contains Security and Privacy of Blockchain, Section 4 contains Challenges, Section 5 contains Futures of Blockchain Research, and Section 6 concluded the paper.

Concepts of Blockchain Technology

Blockchain can be defined as an immutable distributed digital ledger that is secured and protected with advanced cryptography, duplicated between peer nodes in the peer-to-peer network, and uses a consensus protocols or mechanism to agree on the transaction log while decentralizing power. The paper explains the following concepts with this definition as the key concepts for unwrapping the blockchain, distributed, cryptography, scattered, immutable, digital ledger, peer2peer network background.[1,2,3]

Like a ledger in accounting, a ledger in digitise form may be database or digital file, or even a blockchain-like database in distributedform, whichis consensually synchronized and shared across multiple sites. Here, the transactions are electronically documented.In a way that ensures the transaction log is computationally impractical to modify.Blockchain transaction ledger is very special to other kind of ledgers. Double-entry book keeping implemented a simple method to recognize and eradicate mistakes, where two entries are register separately for each transaction; thus, the ledger is balance atconstantly.

There is a triple entry accounting implemented by Griggin 2005, an alternate to old-styledual entry accounting system, which is secure and safeguards transactions based on encryption to make it difficult to change them[1]. To permanently store blockchain transactions, Blockchain implements the concept of triple entry accounting, ensuring that the sender has the authorization to use public-key cryptography to execute non-reversible transactions. The cryptographic hash functions and the public key cryptosystems concepts has been used in block chainto verify the user's authority to perform transactions in order to accomplish consensus among these nodes on block chain.There are two keys called public and private in the public key cryptography. This two keys that convert the original text into a cypher text using the private encryption key.

The sender generates a pair of public-private key, and the private keyis kept confidential to encrypt the data; where the public key is distributed to everyone to verify that the original owner or sender is signed digitally.To verify ownership in blockchain, this form of public key cryptography is used when token or coin are transferred from sender to receiver.[3]

An important concept called cryptographic hash function is also used in blockchain to ensure data integrity, which is a one-way function that maps strings of arbitrary length using a mathematical algorithm into a bit string of fixed length called hash. The hash functions used in block chain, there are three properties required: (i) the same input should always result in the same output hash, (ii) provided that the hash no algorithm can produce the original input, and (iii) minor input changes lead to extremely different output hash.Bitcoin uses the hash function of SHA-256, while Lite coin uses Scrypt, and Ethereum uses Ethash when its block data is hashed.

The proof-of-work consensus mechanism is the most common algorithm,which is implement by every blockchain consensus mechanism to reach agreement on the accuracy of the data in the middle of nodes.The replicated data of the blockchain stored in the peer-to-peer network node, with the best effort basis messages are exchanged; nodes can leave and join according to the network will, when nodes are offline it accept the longest chain of proof-of-work as proof of what occurred[2,4]. A new broadcast transactions are accumulate by node on the network, whichcreatehashed transaction tree like data structure in a block wise, and then solve a hard proof-of-work based on hash by competing with each other.

Its initial node, who resolves the proof-of-work, communicate through the broadcasting the block to validate and connect to their current blockchain with a reply for others. When all transactions are valid then only node accepts the block; acceptance is shown by working to create the next block with the hash of the agreed block as a previous hash.

Security and the Privacy of Blockchain

The Security and the Privacy have been discussed as follows[6-8].

Security of Blockchain: Blockchain security has become an important concept because it requires data &the protection of data, whichis usedduring the transactions of cryptocurrency and the blocks towards various non-malicious and malicious attacks. In order to identify and protect risks, defence requires the introduction of different security measures, tools, and IT services. These are;

Manage vulnerabilities: In this strategy, Vulnerabilities can betest and maintained by identifying, modifying, authenticating the user, and by patching the gap.

Defence in penetration: Similar corrective measures are included in this approach implemented to safeguard information. Instead of enforcing a single layer of protection, it works on the concept of data security in multiple layers.

Minimum privilege: This technique decreases data accessibility tolowermost plausible level to strengthen and improve the level of protection.

Manage patches: It patches the administered portion such as code, program, and operating system in this approach by obtaining, checking, and installing patches.

Manage risks: Environmental threats are processed by the detection of the risk, estimation of the level of risk and the management of risk possibilities.

In order to preserve the privacy for block data or transaction data, Blockchain technology uses several techniques, regardless of the use or data in the block.The others blockchain concept that is most safe is that the longest chain is the legal one. Due to 51% percent dominant attack and fork problems, this dispenses with the safety risks.

Privacy of Blockchain: Blockchain security means having the right to share without spilling data from recognisable proof of data.Privacy is the right to disconnect or disconnect details along these lines from a lonely person or more than one, conveying all that needs to be carefully communicated. In the meanwhile, privacy helps customers to remain acceptable by discerningly revealing themselves without exposing the entire system to their behavior.

Storage distribution: The nodes that store the whole copy of the blockchain are complete nodes on the network. When paired with the append-only features of the blockchain framework, complete nodes also contribute to data redundancy. This data redundancy introduces two new aspects to the blockchain system: transparency and variability. The level of openness and variability in the network is defined by the level of consistency of the application with its data minimisation.

Stored data sorting: Blockchain offers the facility of storing all kinds of data. In blockchain modifications, privacy perspective for personal and corporate data. Despite the fact that personal data is subject to the rules on privacy, increasingly restrictive rules on privacy apply to organizational and sensitive data.

Permissioned versus Non-permissioned types of blockchain: With public or unauthorised blockchain implementations, all users are able to add data. The distribution of network control can be restore by permitting trusted intermediaries.

Public versus Private block chain: Block chain accessibility is remarkable from a privacy perspective. As each node store a copy of the complete blockchain, restricted data on a block can be encrypted for restricted and conditional access at an advanced level through approved users.

Append-only: It is not possible to change information from previous blocks within the undiscovered blockchain. In certain instances, the block chain's append-only feature does not restrict user corrections, especially if the information is documented incorrectly. Special consideration needs to be paid to this technology when assigning rights to data subjects.

Challenges

They still produce metadata, despite the deployment of private information technologies.Though the data itself is encrypted, the statistical analysis will disclose "some" information, which makes it possible to identify patterns.Furthermore, since the consensus mechanism is presently too costly, scalability is an emerging problem. A much faster transaction speed is expected when currency or any other value is transferred on a blockchain-based application. In the case of the Bitcoin network, energy usage remains one of the big problems with miners. Bitcoin hascapability of about 3.2 per second transactions, while Ethereum is currently capable of 2.8 transactions per second.

Because of the complicated consensus mechanism for each transaction, Bitcoin takes far too long (currently proof of work or proof of stake).[9, 13, 16]There are another attack called "Majority Hash Rate Attack" which can occur 51% attack. If an individual or a single entity controls 51% of the hash power, he or she may reverse transactions already sent, avoid transaction confirmation, and block all other miners from extracting them[14,15].

Futures of Blockchain Research

Overall, blockchain research's boundaries are broad. We encouraged works that go far away from Bitcoin to explore the blockchains uses to resolve issues in what would seem to be completely dissimilar fields. Asan example,' for greater usability, transparency and accessibility via a Blockchain for IoT updates that provides a framework for the use of blockchains to protect one of the risk attack surfaces of the IoT. One of the most important, if elusive, questions in blockchain research is the sense of security in the application of a blockchain to a new issue[10,11].

Another emerging area called smart contracts, whichrequire considerable more research on privacy and security. Nevertheless, many significant subjects or fields of study have not been represented; from privacy-preserving signature aggregation to systematic testing of a new generation of smart contracts, the researchers will accomplish much.Therefore, if the fundamental trade-offs in security and privacy relating to scalability and decentralization are exist; it is possible that gametheoretical approaches can be used to discuss these.We hope that, what has been said in the early days about the price of Bitcoin can contribute to the majority of high-quality research on blockchain security and privacy. Another emerging area called the "smart contracts"where much more research is require in blockchain security and privacy[5,14].

Conclusion

Due to its peer-to-peer existence and decentralised structure, blockchain has recently become one of the most common topics in the field of information technology. These possessions make it possible to meet necessities in a variety of arenas and applications. It is unfortunate that., despite its various benefits, this technology still has security and privacy weaknesses, the most serious of which we discussed.In addition, Cybersecurity threats are emerging day-by-day, while older threats are quiet, lingering around and waiting to be abusedonce more. Blockchain technology is not going to be a key focus in cybersecurity, but it is a powerful and influential tool, that helps to toughenthe networks. If the mechanism, that is daunting, is a centralized structure with a single point of failure, then Blockchain will use its strengths well. If greater transaction speeds are feasible, Blockchain is a platform with a large range of applications, including smart grids and the Internet of Things, as well as a widely used blockchain framework and smart contracts[12].

References

1. Harry Halpin and Marta Piekarska (2017). Introduction to Security and Privacy on the Blockchain. *IEEE European Symposium on Security and Privacy Workshops (EuroS & PW)*, IEEE Computer Society, 1-3.

2. Y. Yuan and F. Wang. (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man and Cybernetics: Systems*, 48(9), 1421–1428.

3. Valenta, M., & Sandner, P. (2017). Comparison of ethereum, hyperledger fabric and corda. *Frankfurt School Blockchain Center*, 8, 1-8.

4. Zheng, Z., Xie, S., Dai, H.N., Chen, X. & Wang, H. (2018). Blockchain challenges and opportunities:a survey. *Int. J. Web Grid Serv*. 14(4), 352–375.

5. L. Bach, B. Mihaljevic, and M. Zagar. (2018). Comparative analysis of blockchain consensus algorithms in 2018. 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). IEEE, 1545–1550.

6. Neha Gupta. (2020). Security and Privacy Issues of Blockchain Technology. Advanced Applications of Blockchain Technology, Springer, 207-226.

7. Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10), 71.

8. Manimuthu, A., Rejikumar, G., & Marwaha, D. (2019). A literature review on Bitcoin: Transformation of crypto

currency into a global phenomenon. *IEEE Engineering Management Review*, 47(1), 28-35.

9. Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7, 117134-117151.

10. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., Enyeart, D.,Ferris, C., Laventman, G., Manevich, Y. and Muralidharan, S. (2018). Hyperledger fabric: a distributed operating system for permissioned blockchains. *In: Proceedings of the Thirteenth EuroSysConference*, Article No. 30, Pg.1-15, ACM, https://doi.org/10.1145/3190508.3190538

11. B. K. Mohanta, S. S. Panda, and D. Jena. (2018). An overview of smart contract and use cases in blockchain technology. 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE Xplore, pp. 1–4, IEEE - 43488. https://doi.org/10.1145/3190508.3190538

12. Kosba, A., Miller, A., Shi, E., Wen, Z., & Papamanthou, C. (2016). Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In 2016 IEEE symposium on security and privacy (SP), pp. 839-858. IEEE. doi:10.1109/sp.2016.55

13. Rosenfeld, Meni (2014). Analysis of hashrate-based double spending. arXiv preprint arXiv:1402.2009, February 2014.

14. Oleksandr Oksiiukand Iryna Dmyrieva (2020). Security and privacy issues of blockchain technology. IEEE Int. conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering, University College of London, pp. 531-535.

15. Nakamoto, Satoshi (2008). Bitcoin: A peer-to-peer electronic cash system. www.bitcoin.org.