A Review on Blockchain and its Future Scope

[1] Priyanka Agarwal, [2] Kanchan Kumari, [3] Pratham Sharma

[1] Asst. Professor
Electronics and Communication Engineering
Arya Institute of Engineering and Technology, Jaipur
[2] Asst. Professor
Electrical Engineering
Arya Institute of Engineering, Technology and Management, Jaipur
[3] Research Scholar
Computer Science Engineering
Arya Institute of Engineering and Technology, Jaipur

Abstract: Blockchain is a technology with desirable properties such as decentralization, autonomy, integrity, immutability, verification, fault tolerance, anonymity, control and transparency. In this article, we begin to explore blockchain technology, specifically its history, quantitative comparison of consensus algorithms, cryptographic details from a general cryptography perspective, hash functions used in blockchain, and more. Complete list of blocking programs. Additionally, this paper focuses on blockchain security. Specifically, we evaluate blockchain security from risk analysis to lower blockchain security risk categories, analyze actual blockchain attacks and vulnerabilities, and summarize recently developed blockchain security measures. Finally, challenges and research directions are presented to achieve a more scalable and secure blockchain system for mass deployment.

1. Introduction

Blockchain is a decentralized technology . Profuse of digital legal tender administration like Bitcoin, Ethereum, Ripple, and Litecoin are the example of blockchain technology. In fact, this technology is widely useful and can be used for various applications. Block chains are distributed digital ledgers of cryptographically signed transactions which are grouped into blocks. Each block is cryptographically linked to the previous one Going through a validation and consensus decision. As new blocks are added, older blocks .It becomes more difficult to improve. Blockchain takes a big role in security . so today we have to discussed about the security in blockchain .

2. Proposed Methodology

Blockchain is controlled by the coordination of a group of machines (computers) (computer nodes). Block the software. There is no node policy that determines which buttons can display the following blogs in blocking mode. Any node keeps a copy of the block and can propose new ideas to other mining sites. All friends can bid on the new transaction, and the transaction request eventually spreads among the nodes that join the group. When mining nodes join new competitors, they have untapped business. Waiting can get a combination of the old system. New system (paid by the user sending the transaction in the form of a transaction fee). Each business checks whether the mining point is valid, as other nodes will not accept fraudulent blocks.

3. Blockchain Security Issues and Challenges

Blockchain has a complex and rigid structure. However, this is in technology there are problems and challenges after v.r.t for security. Except the couple In Bitcoin, costs are always possible to include at least one attack surface wallet attacks (e. g. client-side security), network attacks (e.g. DDoS, hacking and hijacking) and mining attacks (e.g. , 50%, procurement and bribery).

4. Security Management

The use of a distributed ledger means that information is shared among all counterparties network. On the one hand, this can have a negative effect confidentiality; on the other hand, it has a positive effect on accessibility by many Nodes participating in Blockchain make it more secure and durable.
Some common safety concerns are:

A. Basic Management

A private key is a direct way to allow work from an account if accessed by an opponent, it will damage the wallet or safe assets with this button. Potentially different private keys can be used to sign and encrypt messages more handouts. An attacker who obtains the database encryption key can read basic information. Private keys are usually used a reliable random function, tuff , if not impossible, to rebuild . If the user loses the personal(private) key, then all assets connected with that key are lost. If the personal(private) key stolen, the attacker will gain full control(access) to all assets managed by that personal(private) key and once the criminal steals the key and refers(sends) the funds to another account, it can't be recovered.

B. Cryptography

Blockchain transactions are always generated cryptographically and private key. In the case of cryptography, strict policies and procedures should always be in place People, processes and technology are tracked when they manage keys. Software used to generate cryptographic keys must generate strong keys cannot be opened easily.

C. Privacy

Privacy is an additional issue arising from the use of Blockchain technology. Inside invalid entry, all counterparties can download the log book they can explore the entire transaction history not a member. In the authorization brochure, the use of authorized representatives' or smart contract capabilities can compromise privacy agent or author access to smart contracts.

5. Mass Attack (51% Attack)

The possibility of mining a block grounded on the work done by miners . Because of this mechanism, people want to mine more blocks and merge them into a "mining pool", a where most of the computing power is stored. Since it has 51% computing power, it can monitor this block. This can create security issues in the chain. If any mortal has above than 51% data crunching capacity , they can be met with the one shoot value faster than others, meaning it has the right to opt which block is allowed.
After this attacker:

1. Changing transaction data can lead to double blind attacks.
2. ii. Stop the block that checks the transaction.
3. iii. Stopping miners from mining any block.

A. Distribution of Denial of Service:

Distributed Denial of Service resulting from distributed registration behavior remain a concern. For example, if a bad person decides to send out a lot of spam Network transactions can increase or decrease service processing time, as a check point for the authenticity of fraudulent transactions. In March 2016, the Bitcoin network slowed down. Because of Bitcoin wallets run a higher then average number of spam transactions This cost causes miners to prioritize this process when calculating new blocks. In an allowed directory, a node can ignore or even agree block the sender of spam transactions for example. However, if the attacker can take control A large number of clients can seriously damage the network by pushing large volume of transactions is not relevant. The distributed nature of Blockchain architecture introduces its future Malware is hard to turn off.

B. Wallet management:

Wallet management refers to the processes and technologies used by the wallet the software works with the keys assigned to it. The wallet must be protected by software unauthorized access to the key, if stored in both cases, as well while working with the software. Losing access to a given wallet can prevent financial institutions from authorizing it transactions or moving assets. It can be difficult for an organization to wait.

6. Conclusion

Distributed Ledger Technology (DLT) or Blockchain, disruptive technology now has the capacity to change our business, culture and sophistication. Distributed Ledger Technology (DLT) eliminates the need for third-party arbitrators by providing a non-financial/non-financial system to ensure integrity. This technology offers a new digital management system that will accelerate the transformation of business services. The big news is that this is a technologically advanced method to help ensure secure operation without the need for central government. This technology will have a huge impact on the communications industry, including users and mobile service providers. This could be a source of revenue growth for these service providers. Therefore, the roles and responsibilities of communication users, operators and service providers regarding security in the distributed ledger technology (DLT) environment need to be defined.

References

[1] Anand, S.R. and Tanguturi, R.C. (2019), “Blockchain based packet delivery mechanism for WSN”, International Journal of Recent Technology and Engineering, Vol. 8 No. 2, pp. 1112-1117.

[2] Bathula, A. and Basha, S.K. (2019), “Blockchain technology with internet of things in the real time network stream”, International Journal of Recent Technology and Engineering, Vol. 8 No. 4, pp. 682-689.

[3] Cole, R., Stevenson, M. and Aitken, J. (2019), “Blockchain technology: implications for operations and supply chain management”, Supply Chain Management, Vol. 24 No. 4, pp. 469-483.

[4] Coyne, J.G. and McMickle, P.L. (2017), “Can blockchains serve an accounting purpose?”, Journal of Emerging Technologies in Accounting, Vol. 14 No. 2, pp. 101-111

[5] Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where is current research on blockchain technology?—a systematic review. *PloS one*, *11*(10), e0163477.

[6] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., ... & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and sustainable energy reviews*, *100*, 143-174.

[7] 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.

[8] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)* (pp. 137-141). IEEE.

[9] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)* (pp. 137-141). IEEE.

[10] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017, June). Blockchain technology innovations. In *2017 IEEE technology & engineering management conference (TEMSCON)* (pp. 137-141). IEEE.

[11] Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.

[12] Michael, J., Cohn, A. L. A. N., & Butcher, J. R. (2018). Blockchain technology. The Journal, 1(7), 1-11. Sharma, R., Kaushik, M. and Kumar, G. (2015) “Reliability analysis of an embedded system with multiple vacations and standby”, International Journal of Reliability and Applications, Vol. 16, No. 1, pp. 35-53.

[13] Kaushik, M. and Kumar, G. (2015) “Markovian Reliability Analysis for Software using Error Generation and Imperfect Debugging” , International Multi Conference of Engineers and Computer Scientists 2015, vol. 1, pp. 507-510.

[14] R. Sharma and G. Kumar, "Working vacation queue with K-phases essential service and vacation interruptions," International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, India, 2014, pp. 1-5, doi: 10.1109/ICRAIE.2014.6909261.