PriMera Scientific Engineering
Volume 5 Issue 1 July 2024
ISSN: 2834-2550

PriMera Scientific Publications

Article on How to Secure Node in Block Chain Technology

Type: Mini-Review
Received: June 12, 2024
Published: June 26, 2024

Citation:
Dr. Shilpa B Sarvaiya. "Article on How to Secure Node in Block Chain Technology". PriMera Scientific Engineering 5.1 (2024): 46-48.

Dr. Shilpa B Sarvaiya*

Head, Department of Computer Application (MCA), Vidya Bharati Mahavidyalaya, Amravati

***Corresponding Author:** Dr. Shilpa B Sarvaiya, Head, Department of Computer Application (MCA), Vidya Bharati Mahavidyalaya, Amravati.

Abstract

The technology of Block chain is fundamentally a record of the distributed database or it is a public ledger of all the dealings or proceedings that are executed digitally and shared with other entries that are participating. Every transaction made in the public ledger is certified by mutual agreement of all the contributors in the arrangement. And after the entry of the information, it can never be erased. Each transaction made in the system can be easily verified and recorded in the case of Block chain technology.

I propose a secure protocol system for Nodes or Blocks present in the Block Chain network.

The numbers of Node will be connected into single network which will be called as Block.Entire data will be passed through this Networks therefore more possibility to hack this network by the inturder and that may cause a major defeat. Accordingly by implementing this propose system it is possible to avoid this loss.

In Block Chain network node communications consistently get coped and illegal operation performs if it happened then there will be a probability to go for massive catastrophe. So ,that security in protocol of Block need to be improve and implement so that the proposed article will help to cross check the sender and receiver node which keep the security up and maintain the variation in data handling.

How to Secure Node in Block Chain Technology

A Block Chain is appending only, cryptographically secured, distributed and replicated store of records. In other words we can say that Block chain is a decentralized computation and information sharing platform that enables multiple authoritative domains, which do not trust each other, to co-operate, co-ordinate and collaborate in a rational decision making.

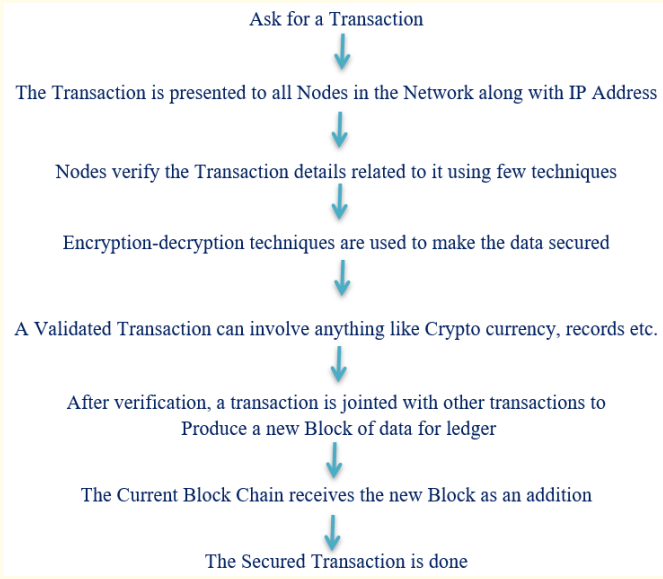

Figure 1: The working of Block Chain.

Limitations

- In ability to process large amount of transactions within the own Block Chain Network.
- No incentives for being Non- mining Full Node.
- Growth of ledger makes it difficult and expensive for them to maintain Full Node.
- Lack of proper documentation.
- Security Vulnerabilities arises due to bugs.

Conclusion

Each transaction is stored on a block connected to the others using hashing techniques, which gives Block Chain a tighter securities. It stores transactions using the SHA-256 hashing algorithm.

The fact that Block Chain databases are kept on every Node of the Network creates a storage problem, as the volume of transactions rises, more storage space will be needed.

Block Chain Technologies decentralized structure makes it impossible to tamper with data; any change will be reflected across all Nodes, making it impossible to commit fraud. As a result transactions can be said to be tamper proof.

Block Chain Technology plays an important role in next generation technologies. So, data security plays an important role in this Platform. Here signals is send in the form of data to the Block in which the data is get transfer for one Block to another. In mean over the network if data or signal is get altered by intruder then it will highly impact on transactions. It will cause a big damage to the Block or node so to overcome this some work is get proposed in which the encryption-decryption techniques are used to make the data secured.

To improve this Sender side and Receiver side conformation and encryption scheme in which the data is get transfer to the user with highly encryption and key transfer technique so that the data in network is remain secured consistently. Subsequently system

will also check for the sender side and receiver side terminal. On condition that the sender side terminal is right as well as receiver side terminal is also right then cross verification of sender and receiver done as well otherwise reject the command for connecting the nodes and Blocks so that the article take part in maintaining the data security additionally perform their responsibility in respect of any types of attacks.

References

1. Y Liang., et al. "A Multi-blockchain Scheme for Distributed Spectrum Sharing in CBRS System". IEEE Transactions on Cognitive Communications and Networking (2023).
2. Liu B., et al. "Blockchain based data integrity service framework for IoT data". In 2017 IEEE International Conference on Web Services (ICWS). IEEE (2017): 468-475.
3. Storj: A Decentralized Cloud Storage Network Framework (2018) v3.0 https://github.com/storj/whitepaper.
4. C Sun and R Jiao. "Discrete Exclusion Zone for Dynamic Spectrum Access Wireless Networks". IEEE Access 8 (2020): 49551-49561.
5. CCSA TC5, "Research on Blockchain Based Solutions for Wireless Network Architecture". 2021B94
6. Y Liang., et al. "Interference-Based Consensus and Transaction Validation Mechanisms for Blockchain-Based Spectrum Management". IEEE Access 9 (2021): 90757-90766.
7. S Wang and C Sun. "Blockchain empowered dynamic spectrum sharing: Standards, state of research and road ahead". TechRxiv preprint TechRxiv: (2022).
8. Kosba A., et al. "Hawk: The blockchain model of cryptography and privacy-preserving smartcontracts". 2016 IEEE Symposium on Security and Privacy (2016): 839-858.
9. Zecheng Li., et al. "B-DNS: A Secure and Efficient DNS Based on the Blockchain Technology". IEEE Transactions on Network Science and Engineerin 8.2 (2021): 1674-1686.
10. Liu H, Han S and Zhu Z. "Blockchain technology toward smart construction: Review and future directions". J. Constr. Eng. Manag 149 (2023): 03123002.