A study on using edge computing in block chain based secure storage management for IoT

Author:Parvathy Viswanath

Guest Lecturer, N.S.S. College Ottapalam

Abstract

By the advancements in the technologies like block chaining, edge computing and IoT has opened chances to combine all these together for a better world. When these technologies stand alone it can exhibit certain disadvantages. When edge computing combines with block chaining , it can facilitate mobile devices in offloading their mining tasks to cloud resources. According to the studies once they are integrated it ensures reliable access and distributed computation. But care should be taken for the security, scalability and resource management , so that the integration can be successfully made.This paper includes the study how they can be integrated to achieve the success.

Keyterms: Block chaining, Edge computing, IoT

Introduction

Block chaining is a technology that works well with multiple users and it can synchronies the replicated ledgers[1]. It works good with centralized ledgers, but working with decentralized ledgers that verifies and stores the records of transactions can works better. That is why edge computing and block chaining can be combined together [2].Privacy policies can be safeguarded by the decentralized nature and it can guarantee the security in a peer to peer systems. But by the intensive consumption of resources in the mining and the high resource utilization can lead difficulty in utilizing block chaining in IoT and other mobile services[2].

Edge computing is introduced as decentralized ledger at the edge of the network as an extension to cloud computing[3].This technique can be easily implemented in new technologies like 5G. It can provide all facilities as cloud like high computing and storage services. Once edge computing and block chaining is combined , it can provide a decentralized environment and secure storage for transactions.

This paper includes a study on the practical approach towards the implementation of a decentralized application and the protocols and operating environment to achieve this implementation of secure block chain data storage in edge computing platforms for IoT applications[4].

Need of integration

When all the three technologies are stood alone , they serve many advantages. Like block chaining , when it was introduced to provide security for bitcoin it claimed many stringent requirements for storage and this requirement can be fulfilled by the distributed ledger method like edge computing[4]. Whereas Edge computing was a

technology that faced some malicious attacks and this technology can be made smarter and wiser by combining it with IoT .Hence by combining all the three ensures high storage, accurate transactions and consistent connections in edge computing environment.

Problems faced when block chaining integrated with IoT

Apart from the advantages discussed above, there are some problems when both technologies are integrated. Some of them are

Integrity

As when data is travelled from one place to another , need of integrity is high. When the factors like reliability, accuracy or integrity are compromised ,it may affect the whole transmission of data. According to the studies, the attacks like selfish mining attacks or stub born mining attack can affect the integrity of data when all these technologies are combined[5].

Anomality

Sometimes combining all the three technologies can create anomalous issues and we may not be able achieve all the advantages of this combinations. Several techniques to avoid these problems were introduced like change address , multiple inputs , usage of some centralized services [6].These integration can also lead to the disclosure of user's identity and it can be solved by either linking back multiple address owned by same participant[7] or the whole service can be controlled by a centralized entity[8]

Integration of block chain with edge computing for IoT

This integration can be achieved by designing the configuration in different layers to use block chaining operations in different layers outside the application layer containing IoT devices .This design can be achieved by three different layers for – edge , cloud and device layers. When all these layers are combined it follows edge computing architecture with a P2P connectivity in every layer. But it requires additional storage and more computational capabilities. According to the study, it was found that the edge layer can be comprised of servers and storage facilities.Hence the requirements like additional storage can be included here . Apart from that the features like robustness can be added here along with the risk avoidance features[4]. Data storage for a very short time and communication in the form of messages among the different nodes are discussed in this layer. Whereas the features like long term data storage and level reporting and communication can be included in the cloud layer. Every resources in the cloud layer can be designed in the form of block chains so that the security , privacy and integrity of data in the system can be ensured.

In case of device layer , user devices can participate in the block chaining system and so it can exchange messages between the devices and these devices are assumed to be smart devices and those with sensors and actuators. These devices will collect information and share those with others and send them to the upper layers in layered architecture. Communication among the devices can be either centralized through edge servers or even can be decentralized. Communication between peer devices is done by making use of keys.In this layered design , when the device joins with the block chaining technology, more operations should be done by servers . So the server side should perform more operations and clients will perform basic operations only.

Requirements for the integration

When these technologies are combined , some of features must be ensured in order to get all advantages of this combination. As storage capacity is the biggest concern both edge computing and blockchain should complement each other .Other features that must be included are:

- Low latency :

  The computations and transactions between the peer devices can lead to some delays and these delays must be optimized in order to have a balance in the combination. So it is important to find out what all transactions are carried out and where are the computations held in order to reduce latencies.

- Data Integrity

  A large amount of information are stored when we combine technologies , some reliable mechanisms must be followed to check the actions of both data owners and data users. Data modification must be accurate as we store them in a decentralized environment.

- Authenticity

  The transactions and communications are done between different types of devices , the validity of devices connected to this environment must be checked. Hence all transactions must be strictly authenticated.

- Adaptability

  The architectural design should be made flexible and so that it can support all changing environments. As in future a greater number of devices are expected to get added in to the networks with different technologies. If this feature is included it can be implemented in the future with acceptable throughput.

- Anonymity

  By considering all other requirements, user should be able to perform all transaction without getting worried about losing their identity[9]. Identity is not considered mandatory for authentication[10]

- Access policies

  Some access policies mut be followed in order to control which information should be sent and who all can access them.

How requirements can be implemented by this architecture

When the architecture that was discussed above is followed , it can fulfill almost all requirements like low latency can be achieved by providing the edge server closer to the end devices and that is what we achieve in edge computing. Data integrity concerns can be solved as the way it is done in cryptocurrencies and some smart contracts can be signed by the data owners and users for that purpose. Each transaction can be validated in order to ensure the whole system's authenticity. As the architecture is designed in layers , any number of layers can be added in the future and more number of features can be added in each layer too. Some high security cryptographic mechanisms or tools like zerocoin[4] can be used to achieve anonymity of every transactions.

Conclusion

This paper included the study about combining different technologies like block chaining and IoT in edge computing platform. Many advantages can be achieved by this combination and these can be achieved only when this is done with all the conditions are met. More practical implementation must be done to apply this

combination. The solutions to the problems faced can be explained and resolved in future.

References

[1]Kubendiran, M.; Singh, S.; Sangaiah, A.K. Enhanced Security Framework for E-Health Systems usingBlockchain. J. Inf. Process. Syst. 2019, 15, 239–250.

[2]Xiong, Z.; Zhang, Y.; Niyato, D.; Wang, P.; Han, Z. When Mobile Blockchain Meets Edge Computing. IEEE

Commun. Mag. 2018, 56, 33–39.

[3]Satyanarayanan, M. The emergence of edge computing. Computer 2017, 50, 30–39.

[4]Blockchain-Based Secure Storage Management with Edge Computing for IoT

Baraka William Nyamtiga 1, Jose Costa SapaloSicato 2, Shailendra Rathore 2, Yunsick Sung 3

and Jong Hyuk Park 2,*

[5]Conoscenti, M.; Vetro, A.; De Martin, J.C. Blockchain for the Internet of Things: A systematic literature
review. In Proceedings of the 2016 IEEE/ACS 13th International Conference of Computer Systems andApplications (AICCSA), Agadir, Morocco, 29 November–2 December 2016.

[6]Yang, R.; Yu, F.R.; Si, P.; Yang, Z.; Zhang, Y. Integrated Blockchain and Edge Computing Systems: A
Survey, Some Research Issues and Challenges. *IEEE Commun. Surv. Tutor.* **2019**, *21*, 1508–1532

[7] Koshy, P.; Koshy, D.; McDaniel, P. An. analysis of anonymity in bitcoin using p2p network traffic. In
International Conference on Financial Cryptography and Data Security; Springer: Berlin, Germany, 2014.

[8]Valenta, L.; Rowan, B. Blindcoin: Blinded, accountable mixes for bitcoin. In *International Conference onFinancial Cryptography and Data Security*; Springer: Berlin, Germany, 2015.

[9]Brickell, E.; Li, J. Enhanced privacy ID: A direct anonymous attestation scheme with enhanced revocation capabilities. In Proceedings of the 2007 ACM Workshop on Privacy in Electronic Society, Alexandria, VA, USA, 29 October 2007.

[10]Jiao, Y.; Wang, P.; Niyato, D.; Xiong, Z. Social welfare maximization auction in edge computing resource allocation for mobile blockchain. In Proceedings of the 2018 IEEE International Conference on Communications (ICC), Beijing, China, 16–18 August 2018.