ENHANCING DISTRIBUTED BLOCKCHAIN SYSTEM USING LOCAL SECRET SHARING

Mr. A. Sai Babu[1], N. Yamini[2], C. Sravani[3], D. Vishnupriya[4]

Article History: Received: 13.02.2023 **Revised:** 28.03.2023 **Accepted:** 15.05.2023

Abstract

Blockchain systems use a distributed ledger to record transactions, with the goal of having every node in the network have an identical copy. High storage costs are associated with blockchain systems since they are similar to repetition codes. It has been argued that distributed storage blockchain (DSB) systems that include secret sharing, private key encryption, and information dispersion techniques may increase storage efficiency. When peers fail because of DoS assaults, however, the DSB incurs high communication costs. Using a local secret sharing (LSS) system with a hierarchy secret structure consisting with one global secret and numerous local secrets, we suggest a novel DSB method. The recovery and storage communication costs are reduced using the suggested DSB method with LSS.

Keywords: Blockchain, DSB, secret sharing, LSS, secret, communication costs.

[1]Assistant Professor, Department of CSE, Sridevi Women's Engineering college, Hyderabad, Telangana, India
[2,3,4] UG Student, Department of CSE, Sridevi Women's Engineering college, Hyderabad, Telangana, India.

Email: [1]swecsaibabuyadav@gmail.com, [2]gyamini777@gmail.com, [3]sravani.ch369@gmail.com, [4]dasipriya30@gmail.com

DOI: 10.31838/ecb/2023.12.s3.335

1. INTRODUCTION

Cryptographically safe hash chains are used by blockchain systems to log transactions. Their centralized and cooperative transaction records decrease the need for intermediates to authenticate financial transactions and the friction that arises when many intermediaries with varying technological infrastructures interact with one another. As a result of blockchain technology, a new ecosystem for commerce and decentralized cryptocurrency regulation has emerged. Yet, blockchain relies on the fact that each peer retains the whole transactions record in the shape of a hash chain, despite the fact that these hashes have no significance to peers that were not involved in the transaction in question. Thus, the cost of storage for individual nodes is increasing rapidly. Distributed storage blockchain (DSB) schemes have been developed to address the high storage costs of block chain infrastructure. The DSB incorporates, private key encryption, Shamir's secret sharing method and information dispersion algorithm (IDA).

Using the DSB, you just need to save a small percentage of the original block chain's data. In the event of peer failures brought on by DoS assaults, the DSB has a substantially greater recovery communication cost. All nodes in the original block chain have a copy of the ledger, so if one goes down, the network as a whole may continue operating normally. Nevertheless, the transmission cost is much higher than in conventional block chain systems since the loss of a single peer effectively wipes out the data of a portion of the peers because they no longer have access to their private encryption key.

In the paper, we suggest local secret sharing (LSS) method and explain how to implement it in the DSB to reduce the overall cost of storing and sending data. In the proposed LSS, there is a single global secret and many local secrets that are organized hierarchically. Similar to locally recovered codes, each group of peers may survive the loss of a single member. As a result, recovery from a single peer failure may be accomplished locally, saving money on transmission price related to the DSB. The suggested LSS may help reduce the DSB's storage expenditures. In the first DSB, hashes were the global secrets and private keys were used as local secrets for groups of peers. To safely keep these secrets hidden both locally and globally, we use two different secret-sharing protocols. Instead, the LSS uses a hierarchical structure to effectively merge local and global secrets. In this way, the proposed LSS may cut in half the DSB's storage requirements for hashes and private keys. We demonstrate that the reduced cost of recovery communications is a direct result of the improved storage efficiency. We describe the storage and transmission cost trade offs of the DSB and the DSB with LSS that we propose as an alternative to conventional blockchains. The suggested method improves storage and recovery communication costs, as shown by these trade-offs.

2. RELATED WORK

“Scaling Distributed Ledger Technology”

As blockchain-based cryptocurrencies are becoming more popular, scalability has become a top priority. We examine the Bitcoin protocol's basic and contextual limitations, which prevent the present peer-to-peer overlay network from supporting much larger throughputs and reduced latencies. Our findings imply that fundamentally rethinking technological methodologies is also necessary for important advancements beyond just reparametrizing block size and intervals to achieve next-generation, high-load blockchain systems. We provide a logical overview of the possibilities for such methods' layout. In this context, we provide a list of recently suggested protocol innovations, examine them

briefly, and propose numerous further concepts and open challenges.

“In a paper titled "Distributed Storage Meets Secret Sharing on the Blockchain"

The hash chain established by blockchain systems is a cryptographically sound data structure. To spread transaction data without considerable loss in data integrity, we use a new mix of distributed, secret key encryption, and Shamir's secret sharing technique. The hashes and variable zone allocation are further secured by using Shamir's secret sharing mechanism. We emphasize the trade-off between storage cost and the likelihood of data loss while making decisions about zone size. Moreover, we investigate the balance among achieve a sustainable and security against hostile corruption using a variety of recovery strategies. Finally, we cast the problem of designing a code to prevent corruption while yet allowing for the possibility of data recovery as an integer programming problem. By knowing the expenses incurred by the service provider, we use the coding scheme to develop a method to ensure data based on the worth of the data, as is done in bitcoin cloud storage systems.

"Distributed storage with dynamic updates for blockchains"

Blockchain is based on the concept of a distributed ledger, where each node on the network holds a hash chain that represents the most up-to-date version of the ledger's recorded transaction history. With high transaction volumes and extensive networks, the storage cost associated with storing the complete ledger becomes prohibitive. In this paper, we employ distributed storage, private key cryptography, and secret key sharing to devise a coding system in which each node records just a subset of each transaction. We further demonstrate that the coding method is effective when dynamic zone allocation is used to boost data security.

"Confidentiality reduced in length"

In the philosophy of secret sharing, it is often accepted that the duration of a share must be at least as long as the secret being shared. This lower limit is proved, however, with the help of statistical significance secrecy. The topic of whether or not a computational definition of secrecy, in particular against resource-bounded adversaries, is superior for secret sharing is an obvious (and extremely practical) one. In this note, we discuss how the computational model might be significantly improved upon. Shares matching to a secrets S are of size |S|/m plus a small piece of information for whom the length does not rely on the secret size but only on the security parameter. In this scheme, m shares retrieve the secret. If you need to retrieve the secret from m shares, the limit of |S|/m is certainly the best choice. Hence, the savings in storage and transmission compared to conventional systems is substantial for relatively big secrets (a private file, a lengthy letter, a sizable data base). The concept is straightforward and elegant in its integration of cryptography and information dissemination. With a safe encryption function (such as a private key), its security may be shown.

“Methods for Confidentiality”

In this study, we illustrate how to make n subsets of data D that can be pieced back together with relative ease from any k components, yet knowing all but one of those pieces still tells you nothing about D.

This method may be used to build cryptographic systems with safe and reliable key management techniques, even if half of the pieces are lost or stolen, or if a security breach exposes all but a single of the remaining parts.

2. METHODOLOGY

Data is protected by blockchain technology because it is transformed into a

series of transactions, and a verification hash code is created for each one. When a new transaction is uploaded to the blockchain, the hash code of the previous transaction is checked to make sure it has not been tampered with. Due to data verification, blockchain maintains all data in all nodes, which necessitates a lot of storage space but provides the additional benefit of retrieving data from those other node whenever one node loses data or is compromised via assault.

For the sake of compactness, instead of each node keeping the complete blockchain's worth of data or keys locally, a new distributed storage protocol called SHAMIR SECRET KEY allows for just a subset to be stored locally.

If the private key data in a Blockchain has to be stored as 527166, for instance, the distributed blockchain will split the data into block such as 52,71,66, apply a polynomial on the above block to acquire a share, and then transfer each share to a number of nodes. Blockchain collects all share from all nodes during the reconstruction of original data, and then uses the reverse polynomial to recover the original/private key data. Each node in the original blockchain stored the whole data set (5271366), but in a distributed blockchain, each node would only keep its own portion of the data set (52 in one node, 71 in another, and 66 in a third). This secret sharing mechanism helps save store space, but it might be prohibitively expensive to communicate between nodes in order to determine which ones have these shares so that the original data can be reconstructed. The fact that each node in a distributed blockchain has to keep its own copy of the hash code and its portion of the data is an additional drawback.

This study proposes a solution to this issue by introducing Local Secret Sharing (LSS), in which hash codes are stored on a network's global peers rather than individually on each node. As private keys are considered to be non-essential shared information, they will be stored on local peers rather than centrally. If a node goes down or is hacked, the data may be recovered by connecting to other nodes in the area. To further minimize storage costs, the proposed approach distributes hash codes and private keys throughout a network of nodes, some of which are geographically close to one another.

Traditional Bitcoin storage, distributed storage, and Consolidated Bitcoin Local Secrets Sharing have all been tested by the LSS.

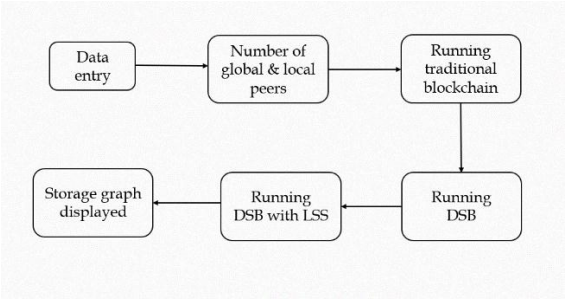

Figure 1 System Architecture

3. RESULTS

By transforming data into transactions and using hash codes for verification, blockchain technology ensures the safety of the data. Blockchain will first check the hash code of the previous transaction before adding the new one, and only the new transaction records will be added if the previous one was successfully verified. Blockchain keeps shares of the same data at various nodes and in case of any loss of data, it retrieves the data using local recoverable codes resulting in less recovery communication cost.

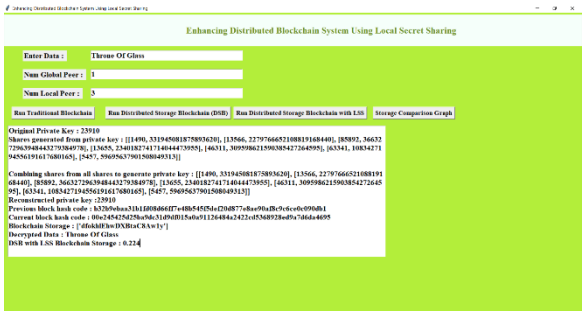

Figure 2 DSB with LSS output

In the above Figure 2, we see the hash codes of the previous and current blocks, followed by the encrypted data, then the decrypted information with the assistance of the private keys, and finally the DSB storage cost.

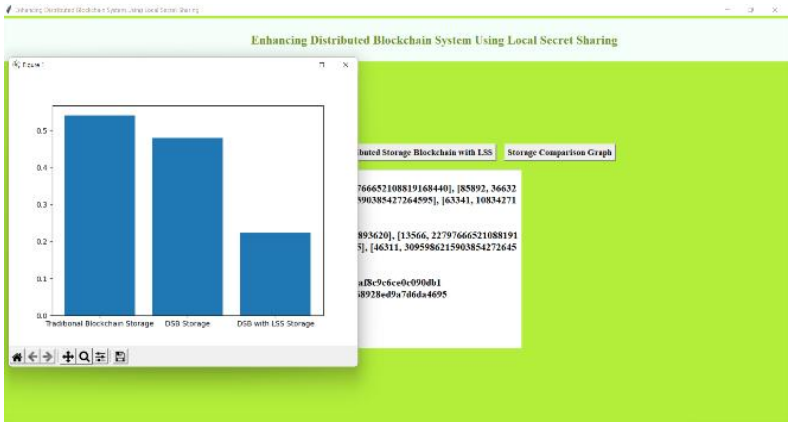

Figure 3 Communication comparison graph

The above Figure 3, shows the storage costs associated with various data storage methods, with the x-axis representing the various methods, and the y-axis indicating storage space used.

4. CONCLUSION

In this paper, we present an alternative DSB method that makes use of LSS. The suggested method reduces the amount of money spent on communication during storage and recovery. The LSS has been expanded to include future research on broad frameworks that might be quite exciting.

5. REFERENCES

K. Croman et al., "On scaling decentralized blockchains," in Proc. Financial Cryptography and Data Security, Aug. 2016, pp. 106–125.

R. K. Raman and L. R. Varshney, "Distributed storage meets secret sharing on the blockchain," in Proc. Inf. Theory Appl. Workshop (ITA), Feb. 2018.

"Dynamic distributed storage for blockchains," in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2018, pp. 2619–2623.

H. Krawczyk, "Secret sharing made short," in Proc. Annu. Int. Cryptol. Conf., Jan. 1994, pp. 136–146.

A. Shamir, "How to share a secret," Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.

M. O. Rabin, "Efficient dispersal of information for security, load Balancing, and fault tolerance," J.

ACM, vol. 36, no. 2, pp. 335–348, Apr. 1989.

I. Tamo and A. Barg, "A family of optimal locally recoverable codes," IEEE Trans. Inf. Theory, vol. 60, no. 8, pp. 4661–4676, Aug. 2014.

A. Pannetrat and R. Molva, "Efficient multicast packet authentication," in Proc. Netw. Distrib. Syst. Secur. Symp. (NDSS), Feb. 2003, pp. 251–262.

A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," IEEE Trans. Inf. Theory, vol. 56, no. 9, pp. 4539–4551, 2010