Efficient Local Secret Sharing for Distributed Blockchain Systems

K.Lohith Raj
Department of Computer Science and Engineering, Narayana Engineering College, Gudur
lohithrajkonduru99@gmail.com

P.K. Venkateswar Lal
Asso.Professor, Department of Computer Science and Engineering, Narayana Engineering College, Gudur
venkateswarlal@gmail.com

M.Dinakar
Department of Computer Science and Engineering, Narayana Engineering College, Gudur
mdinakar225@gmail.com

N.Amrutha Krishna
Department of Computer Science and Engineering, Narayana Engineering College, Gudur
amruthlucky1@gmail.com

ABSTRACT:

Blockchain systems store transaction data in the form of a distributed ledger where each peer is to maintain an identical copy. Blockchain systems looks like the codes that are repeated, in experiencing high storage cost. Now a days, distributed storage blockchain (DSB) systems have been introduced to improve storage capacity by incorporating secret sharing, private key encryption, and information dispersal algorithms. However, the DSB results in significant communication cost when individual failures occur due to denial of service attacks. In this letter, we propose a new DSB approach based on a local secret sharing (LSS) scheme with a hierarchical secret structure of one global secret and several local secrets. The proposed DSB approach with LSS improves the storage and recovery costs.

Key Words: Blockchain, secret sharing, distributed storage, security.

1.Introduction

Block chain systems establish a cryptographically secure data structure to store transaction data in the form of a hash chain. Their distributed and shared records of transactions reduce the friction in financial networks from various intermediaries using different technology infrastructures, and even reduce need for intermediaries to validate financial transactions. Blockchain systems have created a new environment of business transactions and self-regulated cryptocurrencies [1] .However, blockchain works on the premise that every peer stores the entire ledger of transactions in the form of hash chain, even though they are meaningless to each individuals that are not ready to transaction. Repeatedly individual nodes incur a significant ever-increasing storage cost [1]-[3].

To lower this storage cost of blockchain systems, a distributed storage blockchain (DSB) scheme has been introduced [2]. Inspired by [4] , the DSB combines Shamir's secret sharing scheme , private key encryption, and information dispersal algorithm . The DSB reduces the storage to a fraction of the original blockchain's load.In this letter, we propose local secret sharing (LSS) and incorporate it into the DSB to improve the storage and communication costs [5]. The proposed LSS has a level by level secrecy structure of one global secret and several local secrets. As in locally recoverable codes (LRCs) , each subset of peers can tolerate single peer failure. So, single individual failure can recover locally, which reduces the recovery communication cost compared to the DSB [6]. Further, the proposed LSS can even improve the storage cost of the DSB.In original DSB, the private keys acts because the local secrets for subsets of individuals and therefore hashes are the global secrets. These both local and global secrets are stored by using two independent secret sharing schemes. On other side, the LSS efficiently incorporates local secrets and global secrets into a hierarchical secret sharing scheme. Hence, the DSB with new LSS can reduce the storage overhead for hash values and private keys by half. We show that this results in storage efficiency leads to lower recovery Communication cost.

We characterize trade-offs between storage and communication costs of traditional blockchains, the original DSB, and the proposed DSB with LSS. These explicitly show how the proposed approach improves the storage and recover the communication costs.

2. Literature Survey

In the present modren Era, every one using the elctronic computing devices. In this situation lack of privacy and 3^{rd} person involvement is also occurred regularly when the data is transfering between source and destination.our concept is to share the data from soure to destination in a secured way and there is no chance of involving the un-authorized sources [7]. When we start exploring about these topic we found some resources about it and and choose the BlockChain Technolgy as our platform.

, Here we get the information about the utlities and uses of Blockchain Technology [8]. It helps us to find the multidisplinary nature of the block chain technology.

R. K. Raman and L. R. Varshney, “Distributed storage meets secret sharing on the blockchain,” in Proc. Inf. Theory App workshop program. The algorithms and the usage metrics of the block chain methodology and need of secret sharing among multiple devices. the private keys act as the local secrets for subsets of individuals and hashes are global secrets [8]. So both these local and global secrets are stored by using two independent secret sharing schemes. On other side, the LSS efficiently incorporates local secrets and global secrets into hierarchical secret sharing scheme.

3. BACKGROUND WORK

Distributed Storage Blockchain (DSB)

Blockchain systems like bitcoin store transaction data as a distributed records wherein each node within the network stores a present copy of the sequence of transactions (ledger) as hashchain [9] . Let $B^{(t)}$ be the tth data block and $H^{(t)} = h_1(W^{(t)})$be the hash value stored with the (t + 1)th transaction, where $W^{(t)} = (H^{(t-1)}, h_2(B^{(t)}))$ is that the concatenation of the previous hash value and a hash value of the present data block where $h_1(\ )$ and $h_2()$ are two hash functions [5].

Every individual in blockchain systems stores the entire ledger of transactions. Such data replication creates significant storage cost. Assuming that $B^{(t)}$ F_η (a finite field of order η) and $W^{(t)}$ F_q, the blockchain’s storage cost per transaction per peer is $S_B = \log_2 \eta + \log_2 q$. A drawback of the DSB is that it incurs much higher *recovery communication cost* when peer failures occur due to denial of service (DoS) attacks. When a single individual failure occurs, the original blockchain systems can recover this failure.

Locally Recoverable Codes

An (n, k, r) LRC may be a code of length n with information (message) length k, minimum distance d, and recovery local- ity r. The relation between d and r is given by Global secret s. data block $B^{(t)}$ and the hash value $W^{(t)} = (H^{(t-1)}, h_2(B^{(t)}))$ are stored according to Al0g. 1. Note that Φ is an encryption scheme with a random private key $K^{(t)}$ [7]. In this scheme, the private key $K^{(t)}$ and the hash value $W^{(t)}$ are stored by using Shamir’s $(r+1, r+1)$ secret sharing scheme.

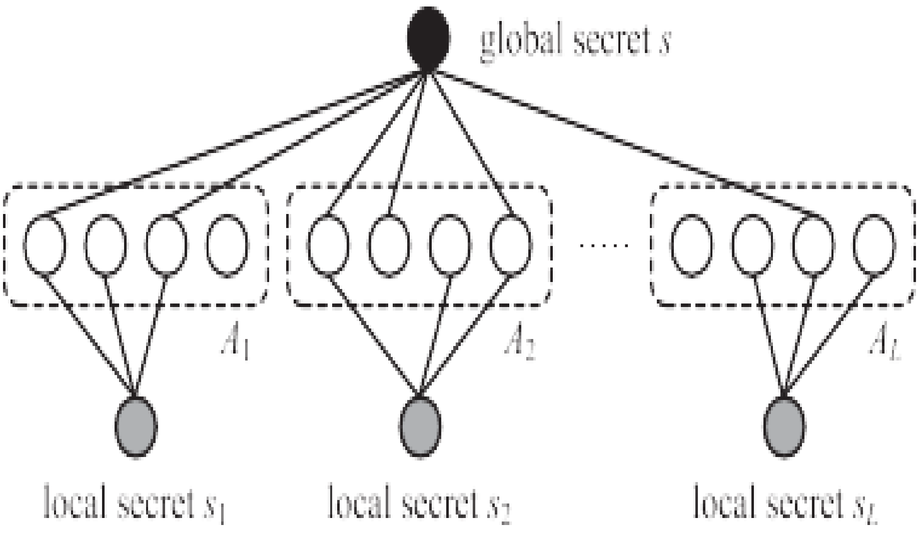

Fig 1: connection of local and global secret sharing system.

4.LOCAL SECRET SHARING

We propose an LSS scheme, which shares a global secret across all peers and the local secrets among peers in subsets as shown in Fig. 1. The more important secret is set as the global secret, which can be accessed by any k^J peers and the less important secrets are reconstructed by r peers of the corresponding subset [4]-[6].

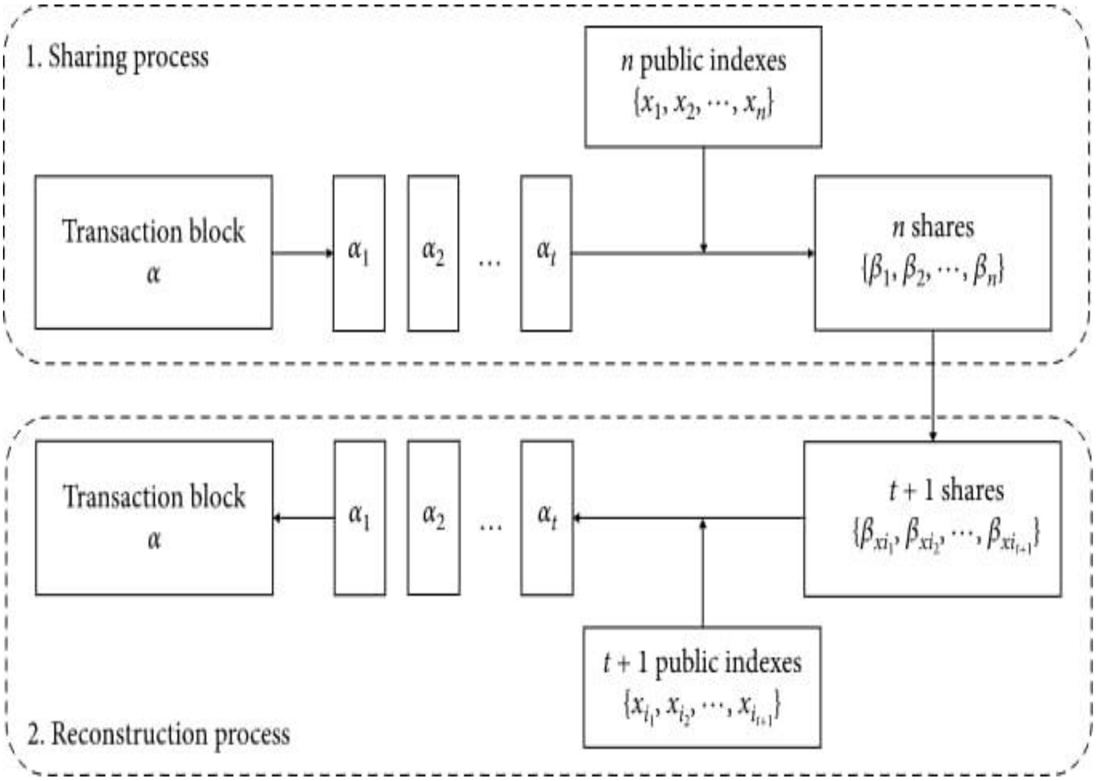

Fig. 2 LSS Scheme

A naive LSS approach in fig 2 is to use two classes| of secret sharing schemes. The global secret is shared by an (n, k^{j}) secret sharing scheme and the local secret s_l for a subset A_l is distributed by an (r + 1, r) secret sharing scheme where A_l = r + 1. In this approach, each individual stores two shares: f (x_i) for the global secret s and $f^{(l)}(x_i)$ for local secret s_l where $f^{(l)}(x)$ denotes an encoding polynomial for a subset A_l. Hence, the total number of shares is 2n [8].

In the proposed LSS scheme, each and every individual stores only one share $f_a(\alpha)$ for α A in (3) thereby having n shares instead of 2n. As Shamir's secret sharing is based on the max distance separable (MDS) codes, the proposed LSS scheme isrepresented by using LRCs [3]

	Traditional Blockchain	Original DSB (Algorithm 1)	DSB with LSS (Algorithm 3)
S	$\log_2 \eta + \log_2 q$	$\frac{\log_2 \eta}{r+1} + 2\log_2 q$	$\frac{\log_2 \eta}{r} + \log_2 q$
$C^{(r)}$	$\log_2 \eta + \log_2 q$	$\log_2 \eta + 2(r+1)\log_2 q + \rho$	$\log_2 \eta + r\log_2 q$
$v^{\dagger}$	$n-1$	$\frac{n}{r+1} - 1$	$2 \cdot \frac{n}{r+1} - 1$

Table 1:Recovery of transaction is guaranteed up to an v peers failure

5.Communication Costs

There are two kinds of communication cost: Cost to store new transactions (transaction communication cost) and cost to recover peer failures (recovery communication cost) [2]. Since each peer should receive the amount of S for a new transaction, the transaction communication cost per peer $C^{(n)}$ is proportional to the storage cost per peer per transaction S (i.e., $C^{(n)}$ S).

The more interesting cost is recovery communication cost $C^{(r)}$. An individual under DoS attacks cannot respond to a request and its data is not available. This failure can be modeled as an erasure channel [8]. As distributed storage codes such as

regenerating codes focus on the communication cost to recover a single node failure, we aim to reduce the communication cost to recover a single peer failure, which is the most common scenario. Since every individual stores the entire records of transactions in blockchains, the single peer failure can be recovered by receiving the stored ledger of any other peers. Hence, the recovery communication cost of traditional blockchain

$$C_B^{(r)} \propto \log_2 \eta + \log_2 q$$

which is the smallest possible, as repetition codes incur the least communication cost in distributed storage systems.In the original DSB [2], [3], a single peer failure disables the corresponding subset due to private key loss. In order to recover this subset, we should access *r* +1 peers of another subset. The recovery communication cost is

$$C_{DSB}^{(r)} \propto \{(r+1)S_{DSB} + \rho\} \\ = \log_2 \eta + 2(r+1)\log_2 q + \rho$$

where *ρ resembles* the additional cost to access another subset [6]. In the LSS, the data block of each subset can be recovered locally by accessing *r* peers in the same subset. Hence, the recovery communication cost is given by

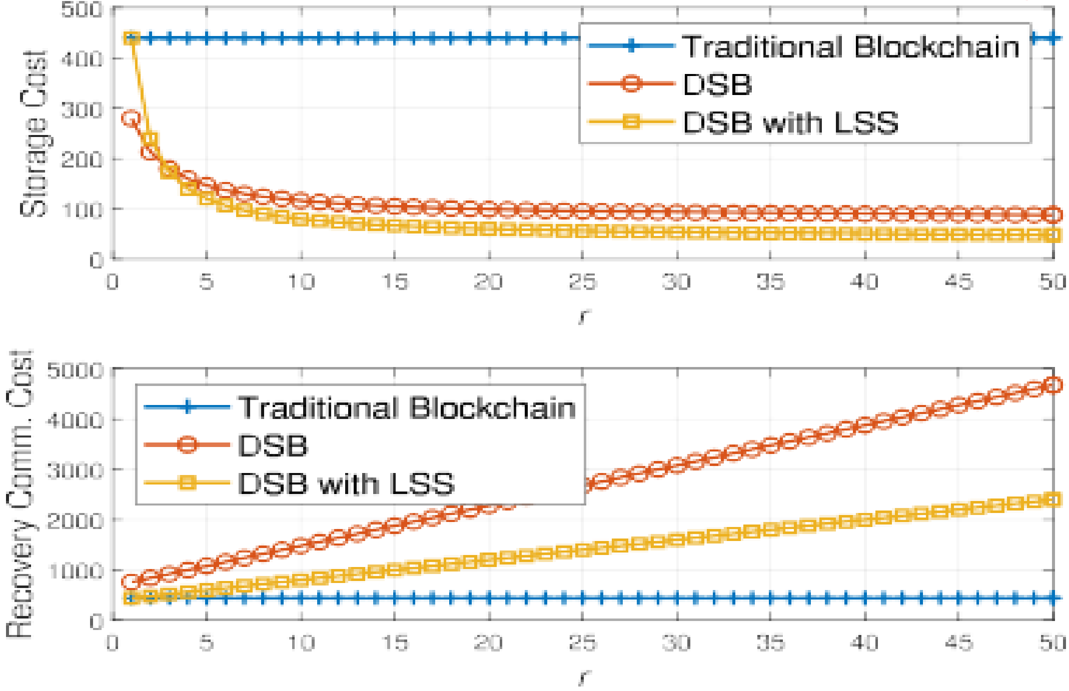

Fig: 3 Tradeoff between storage cost and recovery communication cost

Every subset undergoes failure,so Both the DSBs with the proposed LSS enhance the robustness since each subset can recover a single peer failure.Therefore the DSBs with LSS schemes guarantee transaction data recovery up to$\frac{2n}{r+1}$ 1 failures. Note that the transaction data cannot be recovered if every subset suffers from two peers failures [5].

Table I and Fig. 3 compare the storage/communication costs and robustness to peer failures. Traditional blockchains represents the best recovery communication cost and worst storage cost like repeating codes in distributed storage systems [7]. The proposed LSS improves the storage cost incorporating private key values and hash values with a coding-oretic approach. Furthermore, the LSS reduces the recovery communication cost. Note that the slope of the DSB with LSS is 1 whereas the slope of the DSB [9].

6.Conclusion

We have proposed a new DSB scheme based on LSS. The proposed scheme improves the storage and recovery communication costs. The extending of the LSS to more general frameworks could be interesting future topics.

7.References

[1] Build software better, together. (n.d.). Retrieved December 15, 2014, from https://github.com

[2] H. Li , W. Sun, F. Li, and B. Wang , "Secure and privacy-preserving data storage service in public cloud," J. Comput. Res. Develop

[3] H. T. Dinh , C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," Wireless Commun. Mobile Comput., vol. 13, no. 18, pp. 1587–1611, 2013.

[4] L. Xiao , Q. Li, and J. Liu, "Survey on secure cloud storage," J. Data Acquis. Process.

[5] J. S. Plank , "T1: Erasure codes for storage applications," in Proc. 4th USENIX Conf. File Storage Technol.

[6] P. Mell and T. Grance, "The NIST definition of cloud computing," Nat. Inst. Stand. Technol., vol. 53, no. 6, pp. 50–50 , 2009.

[7] P Penchalaiah, M Vijay Kumar *etl*, **“***A Research Threshold Efficient Hybrid Encryption Schema for Secure File System***”,** International Journal of Recent Technology and Engineering (IJRTE),ISSN: 2277-3878, **(SCOPUS)** Volume-8, Issue-2S3, Page 888 – 891,July 2019

[8] Penchalaiah P, Ramesh Reddy K, “Random Multiple Key Streams for Encryption with Added CBC Mode of Operation*”, Perspectives in Science (ISSN: 2213-0209), (***ELSEVIER**, **UGC Journal no-62532**), Volume 8, pp.57-62, April 2016.

[9] Penchalaiah P, Ramesh Reddy K, “Secure and Cost Effective Cryptosystem Design Based on Random Multiple Key Streams”, *Journal of Information Security Research,(* ISSN: 0976-4143) *DIRF Publisher,* Volume 7, Number 1, pp. 29-40, March 2016.