Mathematical Statistician and Engineering Applications
ISSN: 2094-0343
2326-9865

A study on effective mechanisms for secret sharing in Distributed Blockchain Systems

Chintham Nithisha [1*], A Supriya [2], P Sri Vyshnavi [3]

Computer Science and Engineering, Sri Padmavathi Mahila Visvavdhyalayam, Tirupati, India[1,2,3]*

e-mail: Chintham.Nithisha@gmail.com , supriyaaddanki@gmail.com , vyshu.sri@gmail.com

**Corresponding Author: Chintham.Nithisha@gmail.com*

Article Info
Page Number: 1968-1983
Publication Issue:
Vol. 72 No. 1 (2023)

Abstract:
The primary goal of the paper is to study the mechanisms incorporated for secret sharing by maintaining the costs incurred in distributed blockchain systems. A conventional ledger is maintained in one location with just one copy and the data is validated by a central authority. But the data can be modified and in case of any misfortune happens, the data is not recoverable. In distributed ledger, the copy of ledger is shared amongst multiple nodes. The data is immutable and validated by the participants in the network. If a data segment is lost, then the actual data is unrecoverable. Blockchain is a type of distributed ledger technology, where the transactional data is stored in the form of chain of block. Each block generates a hash code (Unique for each block) that can be used for proof of validation. Each node holds an entire ledger copy, which incurs hefty storage costs. Distributed Storage Blockchain includes private key encryption scheme, information dispersal algorithm(IDA) scheme, and shamir's secret sharing scheme as well. This reduces storage cost but incurs high communication cost and also it requires additional storage to store hash code & distribute sections of it to each node. A unique DSB approach with Local Secret Sharing scheme has been put forth, to lower the storage and recovery communication costs. This paper studies about the different techniques that are used in distributed blockchain systems for efficient secret sharing. Also, increasing system security is vital for preparing for any future scenarios. As steganography (using image processing) does not require scrambled data or secret keys to conceal the sensitive information, the idea is to integrate the DSB technique with LSS and steganography.

Article History
Article Received: 15 April 2023
Revised: 24 May 2023
Accepted: 18 June 2023
Publication: 06 July 2023

Keywords: Blockchain System, Distributed Blockchain System, Secret Sharing, and Steganography

1. Introduction

Numerous technologies are now included into many of the applications that are in use in the modern world. Users prioritize confidentiality, security, authentication, and data integrity before using any program. Users must take into account a few additional variables before continuing to utilize an application. Dependability, robustness, and many more concepts serve as examples. The transaction information that is kept in blockchain architecture as a distributed ledger is identically duplicated by each peer. Similar to repetition codes, which have a high storage cost, blockchain structures are also decentralized. It has been suggested that distributed storage blockchain (DSB) structures, which combine information dissemination, private key encryption, and secret sharing algorithms, can increase storage

efficiency. When peer catastrophes occur as a result of denial of carrier attacks, the DSB results in significant conversation costs. A new DSB strategy has recently been developed that employs an LSS mechanism and a hierarchical secret construct. The DSB procedure with LSS brings down the costs for storing and also for recovery communication. Here the idea is to integrate this innovative DSB technique with LSS and steganography using image processing to boost resilience,security, and storage and transmission costs.

This paper mainly studies what are the techniques and mechanisms that are used by the researchers so far in distributed blockchain systems and few other methods that could be integrated with blockchain technology.

'Literature Survey' is described in Section II, Section III contains the 'Survey Analysis', Section IV contains the 'Related work', Section V contains the 'Conclusion', and Section VI contains the 'References'.

2. Literature Survey

A. DYNAMIC DISTRIBUTED STORAGE FOR BLOCKCHAINS

A distributed ledger with a current replica of the prior transactions (ledger) kept in each system node as a hash chain is the foundation of the blockchain technology. Keeping the complete ledger comes at a hefty cost that unnecessarily increases as networks and transaction speeds increase. This work, established a coding technique that reduces storage costs to a minuscule portion of the original by having each node only keep a portion of each transaction. This has been accomplished by utilizing distributed storage, secret key sharing, and private key encryption. Also, showed how applying a dynamic zone allocation coding strategy can also improve data integrity [1].

B. HOW TO SHARE A SECRET

This work presents the way to partition data (say, D) into some portions (Say, n) in a way that makes it simple to reconstruct D from any k pieces, yet even knowing every single detail about the k - 1 segments does not give any knowledge about the data. This strategy allows for the creation of key management methods for cryptosystems that can be used reliably & securely even if unexpected events destroy 50% of the pieces and privacy violations reveals all except one of the remaining components [2].

C. SECRET SHARING MADE SHORT

Secret sharing agreements are designed with the idea that shares must be at least as long as the secret itself. However, the idea of information theoretic secrecy is used in the verification of this lower bound. If the attacker has limited resources and the idea of secrecy is computational, it is sense to ask whether it is possible to communicate secrets more effectively. This work demonstrated how the computational model can be greatly enhanced. This work introduced an m-threshold scheme where shares size is of $|S|/m$, S is the secret + short piece of data whose length is mainly determined by the security parameter instead of the secret size, and m shares gets the secret but m-1 shares provide absolutely no information on S. As a result, the space and transmission savings compared to traditional approaches are

astounding for reasonably important secrets. The strategy is pretty simple and smoothly combines information dissemination, encryption, and traditional secret sharing mechanisms. It is demonstrably secure when used with secure encryption functions [3].

D. DISTRIBUTED STORAGE MEETS SECRET SHARING ON THE BLOCKCHAIN

As a means of data storage, blockchain technologies produce a cryptographically secure hash chain. This work dissem- inates transaction data with minimal loss to data integrity by combining distributed storage, Shamir's technique, and private key encryption. And also enhance integrity by implementing hashes and dynamic zone allocation using Shamir's top-secret sharing method. Also, showed how the cost of storage and the risk of data loss can be traded off using various zone size options and also consider the trade-off between the expense of recovery and the protection against malicious corruption when using a variety of recovery solutions. Then structured code design as an int program taking into account the chances of data retrieval and specifically aimed corruption. By understanding the expenses related to the service provider, for example in blockchain-based cloud storage systems, and also provided a method to guarantee data based on its worth [4].

E. EFFICIENT LOCAL SECRET SHARING FOR DISTRIBUTED BLOCKCHAIN SYSTEMS

The distributed ledger used by blockchain systems to record transactions is kept in sync by each peer. Repetition codes both have high storage costs like blockchain systems. Distributed storage blockchain (DSB) systems with secret sharing, information dispersal algorithms, and private key encryption are recent suggestions to improve storage efficiency. But when attempts at denial of service lead to peer failures, the DSB must pay a hefty price for communication. This work, provided a novel DSB technique based on a hierarchical local secret sharing scheme with only a single global secret and several local secrets. Costs associated with communication and storage are reduced by the DSB approach with LSS [6].

F. A STUDY ON CRYPTOGRAPHY AND STEGANOGRAPHY

In order to boost the level of security, it is preferred to go with a combination of quite well information security methods cryptography and steganography rather than either cryptography or steganography individually. This paper examined various combinations of cryptography and steganography methods and concluded that Discrete Wavelet Transformation based steganography with AES encryption provides better security because it preserves image quality. As in image-based steganography, the task is to reduce image quality degradation in order to improve security[7].

3. Survey Analysis

TITLE	AUTHOR(S)	MECHANISMS	FOCUSED ON	DESCRIPTION

Dynamic distributed storage for blockchains	Ravi Kiran Raman and Lav R. Varshney	➢ Coding scheme for data block ➢ Recovery scheme ➢ Feasible encryption scheme ➢ Individual block corruption	➢ Dynamic Zone Allocation, ➢ Data recovery and repair.	Rather than storing the entire transaction details in each node, the work presented here simply keeps a portion of each transaction, minimizing storage costs to a fairly minimal fraction of the original proportion.
How to share a secret	Adi Shamir	➢ (K,N)-Threshold scheme	➢ Secret sharing for recovery of data from few shares rather than from all.	This paper presents a (k,n)-threshold approach. The actual secret can be obtained even if k-1 = n/2 out of the n parts are lost by employing a (k, n) threshold technique with n = 2k-1; however, our adversaries cannot do so even if security flaws expose k-1 which is equivalent to n/2 of the remaining k pieces.
Secret sharing made short	Hugo Krawczyk	➢ M-Threshold scheme ➢ Information Dispersal Scheme ➢ Secure encryption scheme ➢ Perfect secret sharing scheme (Shamir's)	➢ Space efficient secret sharing.	This paper describes an m-threshold system in where m shares are required to retrieve S but m - 1 shares cannot. Shares size corresponding to a secret must be | S |/ m + some extra information.
Distributed storage	Ravi Kiran Raman and Lav R.	➢ Coding scheme for data	➢ Categorize the	This work distributes transaction data while maintaining data integrity by utilizing distributed

meets secret sharing on the blockchain	Varshney	block ➢ Recovery scheme ➢ Security based scheme selection ➢ Data insurance	probability of data loss and targeted corruption by budget-limited DOS and active adversaries, ➢ Enabling the client or service provider to choose the coding requirements based on the required data and security guarantees.	storage, private key encryption, and Shamir's secret sharing method.
Efficient local secret sharing for distributed blockchain systems	Yongjune Kim, Ravi Kiran Raman, Young-Sik Kim, Lav R. Varshney, and Naresh R. Shanbhag	➢ DSB systems ➢ Shamir's secret sharing scheme ➢ LRC ➢ LSS scheme ➢ LSS scheme with DSB systems	➢ Storage Cost, ➢ Communication cost, & ➢ Robustness to peer failures.	This study proposed an unique DSB method based on a hierarchical LSS scheme with one secret as global and numerous secrets as local. As a result, both recovery and communication costs are reduced.
A study on cryptography and steganography	Vishnu S Babu, Prof. Helen K J	➢ A Simple combination ➢ DES with LSB Steganography ➢ AES with LSB Steganography ➢ AES with DCT-	➢ Combinations of the Cryptographic and Steganographic techniques.	Rather than using Cryptography and steganography individually, it is preferred to use the combination of both for better security.

		Steganography ➢ AES-DCT-Steganography with cipher text splitting ➢ AES with DWT-steganography		

General details on the methods focused in the survey

TECHNIQUE	INTRODUCED IN	INTRODUCED/ PROPOSED BY	PROS	CONS
Blockchain System	2008	Satoshi Nakamoto – Pseudonym for the group of people who developed the first bitcoin software and introduced the concept of cryptocurrency	• Immutability • Decentralized • Free from Censorship • Easy Tracing of changes on the network	• High storage cost • High communication cost • Considerably slower as it needs to validate new data everytime • High implementation cost (Costlier) • Doesn't allow easy modification
Distributed Storage Blockchain (DSB) Systems	2018	Ravi Kiran Raman and Lav R. Varshney	• Reduces the storage cost	• Incurs much recovery communication costs
Local Secret Sharing (LSS) Scheme	2019	Yongjune Kim, Ravi Kiran Raman, Young-Sik Kim, Lav R. Varshney, and Naresh R. Shanbhag	• Implements a hierarchy structure for hashes and keys maintenance that reduces the overhead of the system	• By attempting to further lower the costs associated with storage and recovery communication, a
Distributed Blockchain	2019		• Improves both storage and recovery	

Systems with Local Secret Sharing Scheme			communication costs • Cuts about half the amount of space needed to store hashes and private keys	system with high security might be anticipated for future scenarios.
Information Dispersal Algorithm	1989	Michael Rabin	• Redundancy safeguards data in the case of a location interruption	• Unauthorised access at any single location does not yield information that is useful
Shamir's Secret Sharing Scheme (k,n)-Threshold Scheme	1979	Blakley & Adi Shamir - renowned Israeli cryptographer.	• Unless the attacker has stolen the quorum number of shares, it is impossible for them to recreate the secret.	• Single points of failure • Share revocation • Implementation complexity • Share integrity
m-Threshold Scheme	1998	Hugo Krawczyk	• Utilising this strategy, the total amount of info in the system has increased by 66% over the size of the data base, compared to a 400% rise utilising the conventional schemes • Minimises the difficulty of computing, sending, and storing these shares.	• Here, Information dispersal approaches avoid dealing with malicious parties or information confidentiality.
Cryptography	Around 1900 BC	An inscription etched into the main chamber of the Egyptian nobleman Khnumhotep II's	• Secret writing • Confidentiality • Authentication • Data Integrity • Non-repudiation	• Access could be hard even for authorised users • Significant budget is needed because public key

		tomb was the first piece of evidence ever discovered.	• Makes the message readable to only the intended receiver	infrastructure must be set up and maintained in order to employ public key cryptography • Exclusively utilized on text files • Relies on the keys
Hash Functions	1940s	Hans Peter Luhn	• Best method since even if the server is compromised, the passwords are still protected	• It is not possible to recover a password; you can only reset your password
Symmetric Key Cryptography: Data Encryption Standard (DES)	1976	IBM	• 2^56 possibilities of keys means brute force attack will never have any impact • Convenient for software & hardware requirement	• DES is weak. Note that 3-DES is more secure than DES • Capable of encrypting 64 bits of plain text • Slower than AES
Symmetric Key Cryptography: Advanced Encryption Standard (AES)	1999	Vincent Rijmen and Joan Daemen	• More secure than DES • Can encrypt 128 bits of plain text. • No known attacks • Faster than DES	• Every block is always encrypted in the same way • Hard to implement with software
Asymmetric Key Cryptography: RSA algorithm	1973	Discovered by Clifford Cocks	• Very secure method • Widely used • Relatively fast and efficient	• Complex mathematical method • Requires large prime numbers • Also increases the key size and processing time. • Can be slower
Asymmetric				

Key Cryptography: RSA algorithm	1977 (General Version)	MIT colleagues Ron Rivest, Adi Shamir, and Leonard Adleman		than other encryption methods • Vulnerability to Quantum Computing • Key management is challenging
Diffie Hellman Key Exchange algorithm	1976	Whitfield Diffie, Martin Hellman, Ralph Merkle	• There is no requirement for prior acquaintance between the sender and the recipient • The sharing of the secret key is safe	• Vulnerable to man-in-the-middle attacks • Limited key size • Requires a secure communication channel • Not suitable for digital signature • Data transmission via an unsafe connection is possible after the keys have been exchanged
Steganography	1499	Johannes Trithemius (First recorded use of the term)	• Covered writing • Confidentiality • Authentication • Both secure & undetected • Can be utilized on any medium (text files, audio-video) • Doesn't rely on any parameter • No key required	• No specific algorithms • Can be crackable if once identified • Needs a lot of overhead to hide associatively few bits of information

Least Significant Bit Steganography	3 Different approaches in Steganography	• Easiest way of hiding the information	• Decreases its quality • A hacker has the ability to alter the least important bit among all the image pixels
Discrete Cosine Transform Stegaography		• Robustness to noise • High compression efficiency • Fast and efficient computation • Compatible with mist image formats	• More complex • Lossy compression • To decide on the values in each DCT block and provide output with integer values, a quantization step is required
Discrete Wavelet Transformation		• Far better at high Compression levels • High flexibility • Without distorting the cover image, DWT can store more data	• Only spatial correlation of the pixels inside the single 2D block is considered and from the neighbouring blocks are neglected
Simple Combination of Cryptography and Steganography		• Takes the advantages of both Cryptography and Steganography	• At the same time, it takes the disadvantages of both Cryptography and Steganography
DES with LSB [8]		• Fixed size of key • Very hard to	• Since, In LSB method the information is gone if

	All possible combinations of Cryptography & Steganography [Two-level Security]	attack	the hacker changes the LSB of every image pixel. Noise and image compression cannot be tolerated by this technology.
AES with LSB [9]		• Key length used in AES can be increased • More Robust • Error between Original image and encrypted image is less • Quality of reconstructed image is better	• Performs better when compared to DES-LSB but AES with DCT/DWT would work much better
AES with DCT		• Key length used in AES can be increased	• Image quality declines as data volume rises
AES with DCT – with cipher text splitting		• Key length used in AES can be increased	• Key exchange should be costly since it needs two additional keys that are quite large relative to the amount of data included in the cover image
AES with DWT		• Because this approach can maintain image quality, it offers improved security • Key length used in AES can be increased	• Capacity and Security levels could be enhanced better

4. Related Work

4.1 Traditional Blockchain

Given data, D:
1: A transaction is requested.
2: Block creation, representing the transaction.
3: Latestly created block is sent to every node in the network.
4: The existing nodes in the network validate the new block.
5: Nodes receive reward for the PoW (Proof of Work), if validation is successful. Otherwise, discard the block.
6: After successful validation, the block is added to the existing blockchain.
7: Done with transaction.
$H(t) = h(H(t-1), h(B(t)))$
A block's hash value is created by concatenating the hashes of the preceding and current data blocks.
That is how a blockchain network is created. In a typical blockchain system, each node (peer) with in system holds the complete transactional ledger. Costs incurred for storage as a result are high.

4.2 Distributed Storage Blockchain (DSB)

To reduce the storage cost incurred by traditional blockchain system, DSB came into existence.
Given data, D:

1: A transaction is requested.
Given data is partitioned as $D = \{D1,...,Dn/r+1\}$:
// Assuming $L = n/r+1$ where n = no. of peers, L = no. of subsets, r+ 1 is the size of each subset.
1: for $l = 1$ to $n/r+1$ do // every transaction is encrypted with a unique set of private keys.
2: Generate an arbitrary private key $Kl(t) \in Fq$.
3: Perform encryption of B(t) with K (t):
$m(t) = \Phi(B(t) ; K(t))$
//Note: Φ = encryption scheme & Kl(t) = random private key.
4: Distribute and store ml(t) among r + 1 peers in Dl.
// The peers of the subset use a secure sharing protocol to store the hashes & private keys.
5: Store K (t) and [H(t-1), h(B(t))] by Shamir's (r + 1, r + 1) sharing scheme.
6: end for
Instead of distributing & storing D1, D2,..,Dl, Distribute & store m1, m2,.., ml. As the size of encrypted data would be much smaller than the actual data, storage cost reduces gradually. Also, the distribution will be made for r+1 peers instead of the entire network. Store (K1,H1), (K2,H2),……,(Kl,Hl) by shamir's secret sharing scheme.

4.3 Shamir's secret sharing scheme [2],[6]

It is refered as (n, k) secret sharing or (k, n) threshold scheme.
Reason:

Let shares be the representation of secret S (the key) as n different values. S can be rebuilt iff at least k out of n shares is known. No information on s is revealed by (k) shares or less.

1: Let's us consider 'S' is the secret that needs to be encoded.

2: Divide 'S' into n parts. (Say S1, S2… Sn)

3: A random number is chosen (say 'k' shares) by the user to decrypt the parts and find out the actual 'S' later.

Rules:

• It must be chosen in such a way that if one know less than k parts, then one will not be able to find the 'S'.

• Only those who know at least k shares can create "S." After then, reconstructing "S" is simple.

4: Finding a polynomial equation with degree (k-1) while preserving the secret code as a constant term and the other values at random is the goal here.

Note: Any k points out of n points created from this polynomial using "Lagrange's Basis Polynomial" can be used to find the constant term.

4.4 Locally Recoverable Codes (LRC)

A (n, k, r) LRC has length (say n), information length (say k), minimum distance (say d), and recovery locality (say r). Only r additional symbols may be accessed to restore a symbol's value if it is lost in LRC-coded data because of a single peer breakdown [5], [6].

4.5 Local Secret Sharing (LSS) scheme

(i) A global secret is shared by all peers in the LSS scheme's hierarchical structure, and local secrets are shared by peers in subsets. The most essential secret is considered as the global secret which is possible to access by any k peers. The corresponding subset's r peers reconstruct the less crucial secrets [6].

(ii) The employment of two classes of secret sharing techniques is a simple LSS strategy.

• An (n, k) sharing technique shares the global secret, and

• An (r + 1, r) sharing technique is to distribute the local secret sl for a subset Al, where |Al| = r + 1.

To put it simply, each node keeps 2 shares, f(xi) is for s and f(l)(xi) is for sl. As a result, there are n total shares. The LSS scheme only has n shares, not 2n, because each peer keeps only one share of fa() for A.

Note: f(l)(xi) represents an encoding polynomial for a subset Al, s is the global secret, & sl is the local secret.

Note: Maximum distance separable codes serve as the foundation for Shamir's secret sharing., the LSS system operates using LRCs [6].

Given g(x) which is a polynomial and A = {A1,...,A n/r+1 }:

1: Build a random vector a = (ai,j) ∈ Fqk and set s = a0,0 where i ∈ [0, r − 1] and j ∈ [0, k r − 1].

2: for loop l = 1 to n/r+1 do

3: Define a local secret

sl = f0(β) = k/r −1 j=0 a0,jg(β)j for β ∈ Al.

4: end for

5: Evaluate (fa(α) : α ∈ A) by (4) and share them among n peers.

4.6 Distributed Storage Blockchain with LSS

When compared to conventional blockchain systems, the distributed storage blockchain technology considerably reduces the cost of storage. There is a flaw in the DSB system. A single peer failure in fact causes the failure of r + 1 peers since it is impossible to retrieve the private key and related subset hashes. In order to resolve this problem, distributed storage blockchain should make contact with r+1 peers in a different subset, incurring communication overhead [6].

Considering A = {A1,...,A n/r+1 }:

1: Define hashes (H(t-1), h(B(t))) as global secret

2: Generate an arbitrary vector.

3: Evaluate local secrets sl (t) for l ∈ [1, n/r+1] and (fa(t) (αi)) for i ∈ [1, n].

4: Distribute and store (fa(t) (αi)) to all the n peers.

5: for loop l = 1 to n/r+1 do

6: Encryption: ml(t) = Φ(B(t); sl(t)).

7: Encode ml(t) to cl(t) using (r + 1, r) scheme.

8: Disseminate and hold cl(t)among peers in Al.

9: end for

As each peer stores the entire record, blockchain systems can fetch the data from such a single node failure by reaching any other peer. By targeting one participant of each subgroup (i.e., n/r+1 peers), a Denial-of-Service attacker can destroy the entire ledger. But a traditional block chain technology can withstand n-1 peer failures. LSS is added to the existing DSB in this case to improve robustness and lower capacity and transmission costs [6].

Similar to Algorithm 2, private keys and hashes are retained as global and local secrets, respectively. As we've already seen, the LSS cuts the cost of maintaining private keys and hashes in half. Every subset in the LSS can withstand a single node failure, just like LRCs can.

Therefore, (r + 1, r) MDS codes are used to cipher the data block ml (t). As a result, the communication cost to rebound from a single node breakdown is decreased while DoS attack resilience is enhanced [6].

4.7 A Study on Cryptography and Steganography

The cryptography is to cipher the information and the steganography is to hide the existence of the data communication.

Cryptography techniques:

(i) The symmetric key DES algorithm is risky because it encrypts data with a 56-bit key, which is too little to be cracked by brute force.

(ii) The RSA algorithm makes the encrypted key public and the decrypted key private. It employs the factoring of two large prime numbers.

(iii) AES is a symmetric key algorithm that uses 128 bits for the data block and 128, 192, or 256 bits for the key size.

Steganography techniques:

(i) LSB - Steganography embeds the text in digital image LSBs.
(ii) (ii) DCT - Steganography on blocks of single pixels, where a coding error results in a break in the blocks, producing an obtrusive artifact.
(iii) DWT - Steganography overwhelms DCT's disadvantage by applying it to the entire image and partitioning it into sub-bands.

Combinations of the above two techniques:

(i) A simple combination: Text-> Encryption-> Cipher text-> (+) Cover image=> Stegno-image-> Cipher text-> Decryption-> Text
(ii) DES with LSB Steganography: Text-> DES Cryptography-> Cipher text->Binary cipher text replaced by LSB of cover image. The adversary can manipulate the LSB of all image pixels, but this method is not resistant to noise or image compression.
(iii) AES with LSB Steganography (24 bit cover carrier): Text-> AES Cryptography-> Cipher text ->Binary.
(iv) AES with DCT: Here, the cover image is divided into high (vulnerable), middle, and low frequency components. Data size is inversely proportional to the image quality.
(v) AES with DCT – with cipher text splitting: The cipher text is in hexadecimal format, with the numbers & alphabets separated by position as a key. However, the additional two keys can be used to maintain the cipher text, which might necessitate a costly key exchange.
(vi) AES with DWT: DWT can handle more data while preserving the cover image.

According to the comparisons made above, DWT-based steganography with AES encryption can provide greater security because it can maintain image quality.

5. Conclusion and Future Scope

Various blockchain technology research proposals have been studied and analyzed how they were enhanced upon one another. By integrating the DSB with LSS system with the well-known idea of "Steganography," which doesn't require any data scrambling or key (s) for concealing the secret data, we hope to improve the security of the system in future work.

6. References

1. R. K. Raman and L. R. Varshney, “Dynamic distributed storage for blockchains,” in Proc. IEEE Int. Symp. Inf. Theory (ISIT), Jun. 2018, pp. 2619–2623.[Online]. Available: https://arxiv.org/pdf/1711.07617.pdf
2. Shamir, “How to share a secret,” Commun. ACM, vol. 22, no. 11, pp. 612–613, Nov. 1979.
3. H. Krawczyk, “Secret sharing made short,” in Proc. Annu. Int. Cryptol. Conf., Jan. 1994, pp.136–146.
4. R. K. Raman and L. R. Varshney, “Distributed storage meets secret sharing on the blockchain,”in Proc. Inf. Theory Appl. Workshop (ITA), Feb. 2018.

5. 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.
6. Yongjune Kim, Ravi Kiran Raman, Young-Sik Kim, Lav R. Varshney, and Naresh R. Shanbhag “Efficient local secret sharing for distributed blockchain systems”, Feb 2019.
7. Vishnu S Babu, Prof. Helen K J “A Study on Combined Cryptography and Steganography”.
8. Krati Yadav, Swapnil Rajput, “Data hiding in image using LSB with DES Cryptography”, IJEAST, Vol. 1, Issue 3, ISSN No. 2455-2143, Pages 80-85
9. Priya Paresh Bandekar, Suguna G C ,“LSB based text and image steganography using AES algorithm”