IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Efficient Certificate Storage and Compression: Optimizing Memory Utilization for Identity Management Using Blockchain

Manasa C.K
Dept of CSE.
East West Institute of Technology,VTU
Bengaluru, India

Usha M.
Assistant professor,Dept of CSE.
East West Institute of Technology,VTU
Bengaluru, India

Dhanraj S
Assistant Professor,Dept of CSE. –CY.
RNS institute of Technology,VTU
Bengaluru, India

Abstract— Utilising cryptographic principles, blockchain is a type of distributed record-keeping system that runs point-to-point. The combination of the publicly accessible blockchain ledger with statistical methods such as data mining as well as demographic mining, however, poses a major danger to users' privacy. As a result, contemporary blockchain technology development has turned its attention to privacy protection. In the realm of privacy protection, ring signatures technology is a frequently utilised encryption technique. Thus, this research develops a blockchain framework for protecting privacy based on ring signatures. This technique developed a privacy information retention system based on an ellipse curve that ensures data security & user identity confidentiality in blockchain applications by using the complete anonymity of the ring signature. A safety proof investigation and an analysis of the proposed scheme's accuracy were conducted. Implementing ring signature approaches with blockchain technology is a practical approach to optimise memory consumption, reduce storage requirements, enhance privacy, and expand the scalability of applications powered by blockchain.

Keywords— Ring signature, blockchain, and privacy protection

I. INTRODUCTION

In 2009, In his Bitcoin white paper, Satoshi Nakamoto originally introduced the idea of blockchain [1]. It is a completely new technical system based on the principles of Bitcoin. Essentially, the blockchain functions as a public, decentralised database that is immune to tampering. A chain structure that organises data blocks chronologically is the foundation of the blockchain. Technologies such as encryption ensure the security of every system link. The key technology in front of digital currencies like Bitcoin and Ethereum is now the blockchain, which has characteristics like decentralisation, resistance to manipulation, anonymity, and public verifiability. Point-to-point transactions can be conducted by nodes in the system via peer-to-peer networks, distributed acceptance, incentive mechanisms, data security, and timing throughout the stamping process. This fixes the problems with the highly trusted centralised system's inefficiencies and dangerous data storage [2]. Alongside the currency's widespread use, blockchain development and usage have increased explosively. Blockchain is the underlying technology underpinning bitcoin. It is seen as the sixth disruptive breakthrough in the computing paradigm, after mainframes, personal computers, and the internet [3]. Better technological properties of the blockchain allow it to be widely used outside of the virtual currency space. Central banks in a number of countries place a high emphasis on blockchain technology inside the financial sector. Inefficient cross-border settlement, drawn-out validation and processing cycles, and expensive central ledger data maintenance are among the issues it addresses in conventional financial systems. Every central bank develops its own digital currency based on research or practical applications.

The advanced verification and point-to-point transaction capabilities of blockchain technology are used to carry out a variety of Internet of Things device transactions [4]. IBM intends to create a "decentralised intelligent IoT" by fusing blockchain technology alongside Internet of Things applications. The anti-tampering, time stamping, and anti-forgery capabilities of blockchain technology have been utilised by intellectual property scholars to accomplish data storage, intellectual property safeguarding, and professional identification. In addition, the legal system, information confirmation, supply chain, and other sectors are gradually implementing blockchain technology to solve contemporary industrial problems [5].

The blockchain has shown to have a long life as research continues, but security issues have also begun to emerge. As there is no central organisation to manage and store data, every activity in a network built on blockchain remain transparent and available to everybody, allowing each node to quickly reach a consensus. Thus, it brings up the subject of data privacy breaches. The simplest form of pseudo-anonymity protects the user's confidential attributes on the blockchain by preventing the exchanged entity's network protocol address from being discovered, despite the fact the client's physical address is identified by the encrypted version of the public key they are using for encryption. It is possible for an attacker to ascertain the true identity of a user by employing techniques such as statistical clustering, large-scale data evaluation, and specific network attack strategies [6].

Summary: With its decentralized, impenetrable database, the blockchain—which was first unveiled by Satoshi Nakamoto in 2009—revolutionized online shopping. The technology that underpins it eliminates the inefficiencies of centralized systems by enabling peer-to-peer transactions and ensuring security via encryption. Blockchain is not just for cryptocurrencies; it is also used in supply chains, banking, and intellectual property protection, among other industries. Encryption and privacy-focused techniques are necessary, nevertheless, as recent events such as privacy breaches draw attention to security problems. Anonymity and privacy in blockchain transactions are guaranteed using a method called ring signature technology. Strong security measures are required to protect user data on blockchain due to privacy issues, even with its transparency.These components, incorporating the applicable criteria that follow.

II. LITERATURE SURVEY

The literature survey conducted for this study is summarized in a tabular format, providing a comprehensive overview of relevant research works. The table encompasses crucial details such as the name of the study, author(s), publication year, research objectives, and key advantages and disadvantages identified in each work.

Title	Authors	Year	Objectives	Advantages	Disadvantages
A distributed biometric authentication scheme based on blockchain	Toutara and Spathoulas, , Bálint, Kumar and Mehta et al.	2020	All computer systems are connected by a common file system. Contents are stored worldwide. Index of content is transaction data.	Mutual trust is not required to protect users data	Failure to provide data protection, that is strong enough
Modern, decentralized blockchain-based solutions for saving video footage	Bálint	2020	Based on IPFS protocol, storage miners lease out storage. Retrieval miners Slicing of data to segments and separated into stripes which are grouped into new erasure codes then uploaded. Uses asymmetric encryption Larger block size creation achieved through testing only.	Secure storage with endpoint encryption.pass clients data to the storage miners. Miners are renumerated with crypto coins. Data is secured by private keys. Can store video footage. Block size of 5Gb is available	High cost of transaction. Cost of 1GB is 0.01 dollars/month which is comparatively high. Not widely implemented
A distributed blockchain-based video sharing system with copyright, integrity, and immutability	Esmaili and Javidan	2020	Peer to peer storage service. A torrent like service, incentive drive and coupled with Ethereum network.	It has zero downtime and DDoS resistant. Appropriate for IoT networks. Its fault tolerant and censorship resistant.	Coupled with only Ethereum.
An encryption approach using information fusion techniques involving prime numbers and face biometrics	Mudliar et al., Iovane et al.,	2018	Utilize a fusion of prime number sequences and facial biometrics descriptors for encryption. Prime numbers serve as key components, while facial features provide additional authentication layers. Combine the unique characteristics of both domains to enhance security and resist cryptographic attacks. This hybrid approach ensures robust encryption by leveraging diverse information sources.	Transparent Decentralized storage and processing, Fault tolerant and has its own coupled storage (swarm).	Has cost called ether/gas. Has limit for scalability, Vulnerabilities in smart contract,
A distributed blockchain-based video sharing system with copyright, integrity, and immutability	Esmaili and Javidan, and Zerka et al.	2020	Employ a distributed blockchain network to facilitate video sharing while ensuring copyright protection, data integrity, and immutability. Smart contracts can enforce ownership rights and regulate access, while cryptographic hashing ensures content integrity. Immutable records on the blockchain guarantee tamper-proof storage and transparent transaction history.	Single validator, Uses smart contract, Privacy protected	Can risk centralization
Permission blockchain based smart contract utilizing biometric authentication as a service: A future trend	Sawant and Bharadi	2020	Future trends foresee blockchain-based smart contracts integrating biometric authentication as a service to enhance permission control. Biometric data offers secure and immutable identity verification, strengthening trust in decentralized systems. These contracts enforce access rights based on unique physiological traits, reducing reliance on traditional credentials.	Controlled by a consortium, User access programmed by chaincode, Has an orderer peer and endorser peer, There is control with decentralization, secure and private	Prone to network attacks, Not post quantum secure
Assuring the integrity of videos from wireless-based IoT devices using blockchain	Danko et al.	(2019)	Leverage blockchain technology to ensure the integrity of videos captured by wireless IoT devices. Each video is hashed and timestamped on the blockchain, creating an immutable record of its content. Smart contracts can enforce validation rules, preventing tampering or unauthorized modifications. This approach guarantees the authenticity and reliability of video data in IoT ecosystems.	Transparent, Available, Secure, Decentralized storage and processing	Prone to rewritten chain and is costly

III. SYSTEM MODEL

In some situations, ring signature methods combined with blockchain technology can be very effective way in order to

maximise memory use. How it would operate: Blockchain Data structure: A batch of transactionis contained in each block of distributed and decentralized ledger structure used by blockchain. Each of these block has an association to the hash of the block before it, joining them in a blockchain. The security and immutability of the data recorded on the blockchain is guaranteed by this data structure. Signatures for Privacy: Within a group of users, ring signatures provide anonymous and unlinkable signatures. Ring signatures can be used in the framework of blockchain transactions to protect the anonymity of the participants in the transaction while maintaining the transaction's legitimacy.

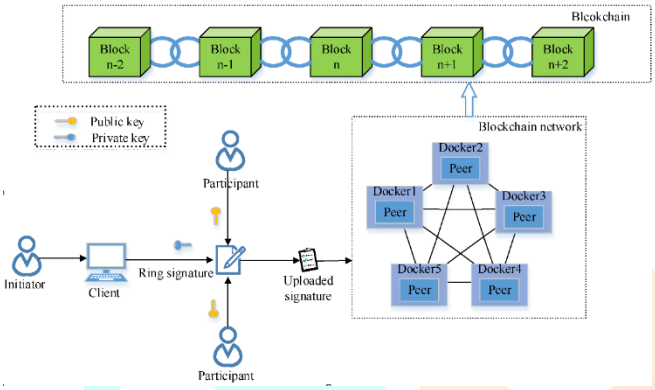

Fig 1: Architecture of Proposed system

Combining these two approaches results in number of advantages for memory optimization. First ,Decreased storage requirements is one where conventional blockchain systems require a large amount of storage, particularly when the blockchain expands over time, because every transaction is stored in full on each node. Nonetheless, it is feasible to combine several transactions into an individual ring-signed transaction by using ring signatures. This aggregation combines several transactions under a single data entry hence decreasing the blockchains total size. Second, Improved privacy with lower overhead: Ring signatures enable transactions to be conducted in a private manner without the need for extra protection-focused layers or protocols. In the process, the expense of deploying sophisticated privacy solutions is decreased, while the blockchain network's anonymity and secrecy are preserved.

Third, increased Scalability: Blockchain networks can increase scalability by lowering the size of distinct transactions by aggregation with ring signatures. Smaller transaction sizes contribute to improved performance and scalability in the long run by accelerating network propagation times, lowering bandwidth needs, and expediting network node validation. Fourth, Efficient Resource Utilisation: Blockchain nodes may function more effectively and use less computational and storage power when memory utilisation is optimised. This may result in less hardware needed by participating nodes, increasing the accessibility and lowering the operating costs of blockchain networks. All things considered, the combination of blockchain technology with ring signature methods presents a viable way to maximise memory use, minimise storage needs, boost privacy, and increase the scalability of blockchain-based systems. This might have a big impact on a lot of different applications, such as supply chain administration, identity verification, cryptocurrency, and more.

IV. ALGORITHM

Blockchain technology has enormous promise for protecting privacy in a variety of industries. Strong safeguards for confidential data are provided by its decentralized design and cryptographic underpinnings.

Blockchain technology has several aspects that make it useful for protecting privacy, including Immutable Ledger: An immutable block chain is created when all activities are recorded chronologically on an electronic ledger. Since each block is connected to the one before it by a cryptographic hash, it is almost impossible to secretly alter previous data. Immutability is the inability to change or manipulate sensitive data without authorization, which ensures data integrity and protects privacy.

A. Decentralization and Distribution

Because data is stored in a single location in traditional centralised systems, they are vulnerable to security breaches and unauthorized access. Blockchain, on the other hand, is a decentralised network of nodes in which every node keeps a copy of the whole blockchain. By spreading the data over several nodes, this improves resilience against assaults and lowers the possibility of only one point of failure. Furthermore, consumers gain control over their data thanks to decentralisation because they are no longer dependent on reliable middlemen to handle and secure their data.Consensus mechanisms are used by blockchain networks to verify and reach an agreement on the current state of the ledger. Blockchain keeps the system reliable and secure by ensuring that only legitimate transactions are entered to the ledger through the establishment of a consensus of network members. Proof of Works (PoW), on the other hand, are two examples of consensus techniques that encourage moral behaviour and deter dishonest people from exploiting the ledger for their personal benefit.

B. Cryptography techniques

Blockchain transactions are protected to ensure validity, secrecy, and integrity by use of cryptographic algorithms. A set of cryptographic keys, which consists of a common key for encryption & an encrypted private key for decryption, may be created by users using public-key cryptography. This asymmetric encryption improves privacy and secrecy by guaranteeing that only the intended receiver can decode or gain access to the data. Blockchain ensures that only valid transactions are added to the ledger, ensuring the security and dependability of the system by fostering consensus among network users. A pair of consensus strategies that promote moral conduct and discourage dishonest persons from influencing the information within it for their own gain are proof of work.

C. Ring signature

Ring signature architecture is a cryptographic approach designed to provide online anonymity for transactions and chats. Ring signatures allow a group member to sign a communication or transaction anonymously while yet ensuring authenticity verification. They were developed by Tauman ,shamir and Rivest. When using a standard digital signature technique, a signer generates a signature using their personal key, which anybody with the matching public key may verify. This method establishes a clear connection between the signature and the signer's identity. On the other hand, ring signatures work differently.

Key Generation: A set of public keys and private keys is generated by each group member.

Signature creation: To generate a signature, a member chooses a set of group public keys, together with their personal key, resulting in a "ring." Next, using their own private key as well as the chosen public keys, the signer creates a signature.

Crucially, the signature conceals the precise key that was used to sign it.

Verification: The legitimacy of the signature may be confirmed by anybody with access to those public key contained in the ring. The verification method preserves the signer's anonymity by confirming that the verification is authentic for at least every one of the publicly accessible keys for the ring without disclosing which particular key has been utilized for signing.

There are several benefits of using ring signatures to protect privacy

Anonymity: Signers remain anonymous within the group, as the signature does not reveal their identity.

Unlinkability: It is difficult to link a specific signer to their signature, as multiple public keys are included in the ring.

Decentralization: Ring signatures can be employed in decentralized systems, where there is no central authority controlling the signing process.

Ring signature architecture finds applications in various privacy-sensitive domains such as

Cryptocurrencies: To mask transaction data and provide users more privacy, ring signatures are employed in secrecy-focused cryptocurrencies like Monero.

Anonymous Messaging: Users can send messages without disclosing their identities by using ring signatures in anonymous messaging platform.

Voting Systems: To ensure the secrecy and reliability of the voting process, ring signatures provide an anonymous voting method.The ring signature architecture, which offers anonymity business unlinkability while retaining authenticity and security, is an effective technique for protecting confidentiality in digital transactions as well as communications overall.

CONCLUSION

In summary, ring signature methods combined with blockchain technology offer a strong way to maximise memory use in decentralised applications. Storage needs can be significantly reduced by using ring signatures to combine multiple actions into only one private object. By decreasing the size of each transaction transactions, this not only increases scalability and efficiency inside the network of blockchain connections but also improves the security and privacy within it. Blockchain networks may function more efficiently and sustainably with lower resource consumption because to these memory optimisation advantages. Ring signature schemes are a viable way to improve the usefulness and sustainability of decentralised systems as blockchain technology develops and finds applications in a variety of sectors.

REFERENCES

[1] BitLaunder. The "major exchanges" mixer and BitLaunder's mixer

[2] Bitcoin Mist. Using the bitcoin fog [EB/OL]

[3] Blockchain. EB/OL Wallet.

[4] BONNEAU, A. MI LLER, A. NARAYANAN, et al. Mixcoin: responsible mixes combined with bitcoin anonymity[C]//World Congress on Data Security and Financial Cryptography. Berlin, Heidelberg: Springer, 2014: 486–5004.

[5] International Conference on Financial Cryptography and Data Security; VALENTA L, ROWAN B. Blindcoin: blinded, responsible mixes for bitcoin[C]

[6] CHAUM D. Blind signatures for untraceable payments[C]//Advances in Cryptology. Boston, MA's Springer

[7] [7] A distributed biometric authentication scheme based on blockchain, Toutara and Spathoulas, 2020, Bálint, 2020, Kumar et al., 2021

[8] Modern, decentralized blockchain-based solutions for saving video footage, Bálint (2020)

[9] A distributed blockchain-based video sharing system with copyright, integrity, and immutability, Esmaili and Javidan (2020

[10] An encryption approach using information fusion techniques involving prime numbers and face biometrics, Mudliar et al., Iovane et al.,2018

[11] A distributed blockchain-based video sharing system with copyright, integrity, and immutability, Esmaili and Javidan, and 2020

[12] Permission blockchain based smart contract utilizing biometric authentication as a service: A future trend, Sawant and Bharadi 2020

[13] Assuring the integrity of videos from wireless-based IoT devices using blockchain, Danko et al. 2019

[14] Gregory Maxwell. CoinJoin: real-world bitcoin privacy

[15] DUFFIELD E, DIAZ D. Dash: a cryptocurrency focused on privacy[J].

[16] CoinShuffle: a workable decentralised coin mixing system for Bitcoin[C]//European Symposium on Research in Computer Security RUFFING T, MORENO-SANCHEZ P, KATE A. 345–364, Springer, Cham, 2014[20] MIERS I, GREEN M, GARMAN C, and others. Zerocoin is a bitcoin-based anonymous electronic currency.IEEE Security and Privacy Symposium (SP).

[17] SIMON D R, RACKOFF C. Annual International Cryptology Conference / Non-interactive proof of lack of knowledge and selected ciphertext attack[C]. Heidelberg, Berlin: Springer,

[18] GARMAN C, SASSON E B, CHIESA A, and others. Zerocash: Anonymous payments made decentralised using bitcoin[C]//2014 IEEE Symposium on Security and Privacy (SP).

[19] WATTENHOFER R, DECKER C. Fast and scalable payment network with micropayment channels for bitcoin duplex[C]//Self-Stabilizing Systems Symposium. Cham, Springer,

[20] DRYJA T, POON J. Scalable off-chain quick payments via the bitcoin lightning network[J]. Draft Version 0.5, September 14, 2016.

[21] Sprites: payment channels that move quicker than lightning[J], Miller A, Bentov I, Kumaresan R, et al. 2017:1–23.

[22] Bolt: anonymous payment methods for decentralised currencies, Green M, and Iverson I.[C]The ACM SIGSAC Conference on Computer and Communications Security 2017 proceedings. ACM, 2017: 473–489.

[23] Monero [27]. A little comment on chain reactions in cryptoNote 2.0 [EB/OL] traceability.[10 June 2017].

[24] Boyen X. and Thomas H. (2016). VOTOR: essentially a remote voting tool to combat small-time autocrats. In Australasian Computer Science Week Multiconference Proceedings (ACSW '16). Article 32, 1–13, Association for Computing Machinery, New York, NY, USA.

[25] Zekeriya Erkin, Oguzhan Ersoy, and Mourad El Maouchi. 2019. DECOU- ł PLES: a decentralised supply chain traceability system that is unlinkable and protects privacy. In the 34th ACM/SIGAPP Symposium on Applied Computing (SAC '19) Proceedings. New York, NY, USA: Association for Computing Machinery, 364–373.

[26] The paper "An ID-based block ring signature system for secret data sharing" was presented at the 2017 International Conference on Computer Communication and Informatics (ICCCI) in Coimbatore, India. [30] Patil K and Wasnik C. T.

[27] "Effective data sharing with forward security: Identity based ring signature using different algorithms," by V. Pandey and U. Kulkarni, will be presented at the 2017 International Conference on Intelligent Computing and Control (I2C2) in Coimbatore, India, from May 1–6, 2017.

[28] Zhang X Y, Cui Y Q, Cao L, and Zeng G X. Latice-Based Ring Signature with VANET Privacy Preserving[J]. JOURNAL OF COMPUTERS IN CHINA, 2019; 42(5):980-992.

[29] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]

[30] Yuan Y, Wang F Y. Blockchain: the state of the art and future trends. Acta Automatica Sinica, 2019, 42(4): 481-4940

[31] SWAN M. Blockchain: blueprint for a new economy[M]. “O’Reilly Media, Inc.”, 2015: 212-235.

[32] ZHENG Z, XIE S, DAI H N, et al. Blockchain challenges and opportunities: a survey[J]. International Journal of Web and Grid Services, 2019: 1-19.

[33] CROSBY M, PATTANAYAK P, VERMA S, et al. Blockchain technology: beyond bitcoin [J]. Applied Innovation, 2020, 2: 6-10.

[34] Natoli C, Gramoli V. The Balance Attack Against Proof-Of-Work Blockchains: The R3 Testbed as an Example[J]. 2016.

[35] Dhillon V, Metcalf D, Hooper M. The DAO Hacked[J].2017.

[36] Rivest R L , Shamir A , Tauman Y . How to Leak a Secret[A]. Proc ASICRYPT’01[C]. Springer-Verlag, 2001.552-565.

[37] Chaum D , Heyst V E. Group Signatures[A]. Proc CROCRYP’91[C]. Springer-Verlag, 1991.257-265.

[38] Chuam D. Untraceable electronic mail, return addresses and digital pseudonyms[J]. Communications of the ACM,1981,24(2):84-90.

[39] Dilip Kr. Saikia and Surmila Thokchom. 2018. Effective plan for sharing dynamic Cloud data among static group members while maintaining privacy through auditing and traceability. Published in the Proceedings of the 18th International Conference on Internet of Things and Cloud Computing (CCIOT 2018). New York, NY, USA: Association for Computing Machinery, 25–32.