IDENTITY BASED ENCRYPTION:A KEY TO DATA PRIVACY IN PERMISSIONED BLOCKCHAIN

S. Reshma[1,a)], N.Ramadevi1 [1,b)],S.Saliya[1], B.Sravani[1] , S.Asifa[1], U.Vaishnavi[1] and T.Sharada[1]

[1] Dept of Computer Science and Engineering (Data Science),

Santhiram Engineering College, Nandyal,

518501, India.

[a)] Corresponding Author:

reshma.cse@srecnandyal.edu.in

[b)]ramadevi.cse@srecnandyal.edu.in

Abstract: The emergence of blockchain technology has garnered significant attention due to its decentralized architecture and distributed public ledger, notably underlying Bitcoin. Governments, financial institutions, and high-tech enterprises are exploring its potential to enhance efficiency, reduce costs, and bolster data security. However, serious privacy concerns persist, potentially impeding widespread adoption. In this paper, we introduce a practical solution leveraging Identity-Based Encryption (IBE) to address these privacy issues in non-transactional applications. Our proposed scheme effectively enhances data privacy, offering protection against disguise and passive attacks. Through rigorous analysis, we demonstrate the high-security level of our proposal, showcasing its functionality, effectiveness, and practicality across various non-transactional scenarios.

Index Terms—Permissioned Blockchain, Privacy Protection, Bilinear Map, Identity-Based Encryption

1. INTRODUCTION

In today's interconnected digital landscape, ensuring data privacy has become a paramount concern for organizations across various sectors. With the proliferation of centralized systems and reliance on conventional verification methods, such as SMS or email, traditional approaches to safeguarding data have proven inadequate in addressing the evolving threats to privacy and security. As a result, there is a pressing need for innovative solutions that not only enhance data privacy but also ensure secure data sharing among authorized users, while maintaining data integrity and confidentiality. Blockchain technology has emerged as a promising solution to these challenges, offering a decentralized and transparent framework for securely recording and sharing data. Initially introduced as the underlying technology for Bitcoin, blockchain has garnered widespread attention from governments, financial institutions, and high-tech enterprises due to its potential to revolutionize various industries through enhanced efficiency, reduced costs, and improved data security [1]. Unlike traditional centralized systems, where data is stored in a single vulnerable location, blockchain distributes data across multiple computers (nodes), making it significantly more difficult for malicious actors to tamper with or compromise the system [2].

The blockchain operates as a digital ledger that records transactions in a secure and transparent manner. Each transaction is encapsulated in a block of data, which is linked to the previous block through a unique cryptographic hash, forming a chain of blocks [3]. This decentralized architecture not only enhances security but also promotes transparency, as all transactions are recorded and visible to authorized users in real-time. Furthermore, blockchain ensures data immutability, meaning once a transaction is recorded in the blockchain, it cannot be altered or deleted [4]. These inherent properties of blockchain make it an attractive solution for addressing privacy concerns and ensuring data integrity in various applications.

However, despite its potential benefits, blockchain technology is not without its challenges, particularly concerning data privacy. In permissioned blockchains, where access to data is restricted to authorized users, ensuring privacy while maintaining data integrity is crucial. Traditional encryption methods, such as public-key cryptography, can provide a level of data security but may introduce complexities in key management and access control [5]. Moreover, relying solely on encryption may not be sufficient to address privacy concerns in permissioned blockchains, where the identities of users need to be securely managed and authenticated.

To address these privacy challenges effectively, we propose the incorporation of Identity-Based Encryption (IBE) into permissioned blockchains. IBE is a cryptographic scheme that simplifies key management by using unique identifiers, such as email addresses or user names, as public keys [6]. By integrating IBE into permissioned blockchains, we aim to enhance data privacy while ensuring secure data sharing among authorized users. IBE enables administrators to have precise control over data access, allowing them to specify which users can access particular data based on their identities. This granular access control mechanism not only enhances privacy but also simplifies key management and authentication in permissioned blockchains.

In addition to IBE, our project leverages the Ethereumblockchain for its advanced smart contract capabilities, which enable secure, transparent, and programmable data storage and management [7]. Ethereum's support for smart contracts allows us to implement complex access control policies and data management workflows, further enhancing the privacy and security of the system. Furthermore, to handle file storage efficiently, we integrate the InterPlanetary File System (IPFS) into our project. IPFS provides a distributed and efficient file storage solution, allowing us to store and retrieve files securely and reliably [8].

Overall, our project aims to address the pressing need for enhanced data privacy in permissioned blockchains by leveraging the combined capabilities of blockchain technology, Identity-Based Encryption, Ethereum smart contracts, and IPFS file storage. By integrating these technologies, we seek to provide a secure, efficient, and privacy-preserving solution for securely sharing data in permissioned blockchains, while ensuring data integrity and confidentiality.

2. LITERATURE SURVEY

Blockchain technology has witnessed widespread adoption and exploration across various sectors due to its potential to revolutionize data management, security, and transparency. As organizations strive to harness the benefits of blockchain while addressing privacy concerns, researchers have proposed innovative solutions and frameworks. In this literature survey, we delve into seminal works and recent advancements in blockchain technology, smart contracts, and identity-based encryption (IBE) to provide insights into the evolving landscape of data privacy and security in permissioned blockchains.

The Linux Foundation has played a pivotal role in fostering the growth of open-source blockchain ecosystems through initiatives like Hyperledger [1]. Hyperledger Fabric, one of the prominent blockchain frameworks under the Hyperledger umbrella, provides a modular and scalable platform for building permissioned blockchain networks. By leveraging Hyperledger Fabric, organizations can design customized blockchain solutions tailored to their specific requirements, including data privacy and security.

Omohundro (2014) explores the intersection of cryptocurrencies, smart contracts, and artificial intelligence (AI), highlighting the transformative potential of blockchain technology [2]. Smart contracts, programmable self-executing contracts deployed on blockchain networks like Ethereum, enable automated and transparent execution of predefined terms and conditions. Integrating AI with blockchain can further enhance the capabilities of smart contracts, enabling advanced functionalities such as predictive analytics and automated decision-making.

Detwiler (2018) discusses the application of blockchain technology in enhancing food safety and traceability [3]. By leveraging blockchain's immutable ledger, organizations can track and trace the journey of food products from farm to fork, ensuring transparency and accountability throughout the supply chain. This use case underscores the importance of data integrity and privacy in blockchain-based solutions, particularly in sensitive domains like food safety and supply chain management.

In the realm of cryptography, Shamir (1985) introduces identity-based cryptosystems and signature schemes, laying the foundation for Identity-Based Encryption (IBE) [4]. Unlike traditional public-key cryptography, IBE simplifies key management by using unique identifiers, such as email addresses or user names, as public keys. Boneh and Franklin (2001) further elaborate on IBE schemes based on the Weil pairing, offering efficient and secure solutions for data encryption and key distribution [5]. Building upon this work, Boneh and Boyen (2004) propose efficient selective-ID secure IBE schemes without relying on random oracles, addressing practical limitations and enhancing the scalability of IBE systems [6]. Subsequently, Boneh and Boyen (2004) present secure IBE schemes without random oracles, advancing the state-of-the-art in identity-based encryption [7].

Integrating IBE into permissioned blockchains presents a promising approach to enhancing data privacy and access control. By combining the security benefits of blockchain with the simplicity and efficiency of IBE, organizations can establish fine-grained access policies and securely share sensitive data among authorized users. This integrated approach aligns with the overarching goal of ensuring data privacy and confidentiality in permissioned blockchain networks.

In conclusion, the literature survey highlights the diverse applications and advancements in blockchain technology, smart contracts, and identity-based encryption. From Hyperledger frameworks to innovative cryptographic schemes, researchers and practitioners continue to explore novel approaches to address privacy concerns and enhance data security in permissioned blockchains. By leveraging these insights and advancements, organizations can develop robust and privacy-preserving blockchain solutions tailored to their specific use cases and requirements.

3. METHODOLOGY

a) Proposed Work:

The proposed system aims to address the limitations of the existing encryption methods by leveraging Identity-Based Encryption (IBE) to enhance data privacy in permissioned blockchain networks. In this system, each participant's unique identity, such as an email address or username, serves as their public key, eliminating the need for complex key management infrastructure.

Instead of traditional public keys derived from cryptographic key pairs, the proposed system uses user identities directly as public keys in the encryption process.

Unlike centralized key management systems, the proposed system utilizes decentralized key generation mechanisms to ensure the security and integrity of cryptographic keys.

By leveraging IBE, the proposed system enhances user privacy by preventing unauthorized parties from linking users' public keys to their real-world identities. This mitigates the risk of identity theft and unauthorized surveillance while preserving the anonymity of participants within the blockchain network.

The proposed system offers a comprehensive solution for enhancing data privacy in permissioned blockchain networks through the adoption of Identity-Based Encryption. By addressing the limitations of existing encryption methods and leveraging the benefits of IBE, the proposed system provides a secure, scalable, and privacy-preserving framework for data sharing and transaction processing within permissioned blockchain ecosystems.

b) System Architecture:

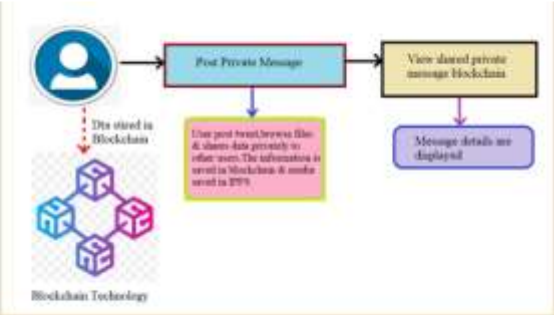

Post Private Message
View shared private message blockchain
Dta stored in Blockchain
User post tweet,browse files & shares data privately to other users.The information is saved in blockchain & media saved in IPFS
Message details are displayed
Blockchain Technology

Fig1 Proposed Architecture

The system architecture for managing private messages using blockchain technology comprises several key components. Firstly, a user interface facilitates interaction with the system, enabling users to compose, send, and view private messages securely. Upon composing a message, it undergoes encryption using Identity-Based Encryption (IBE) for enhanced security and privacy. The encrypted message, along with metadata such as sender, recipient, and timestamp, is then packaged into a transaction. These transactions are validated and added to a block by network participants, leveraging consensus mechanisms like proof of work or proof of stake. Once added to the blockchain, the block becomes an immutable record, ensuring data integrity and preventing tampering. Users can retrieve and view shared private messages by querying the blockchain using appropriate cryptographic keys. Overall, this architecture leverages blockchain's decentralized, transparent, and tamper-resistant nature to provide a secure and efficient platform for managing private messages while preserving user privacy.

c) New User Signup

This module enables secure user registration within the application. Users input unique credentials like username, email, and password, which undergo validation and are securely stored on the blockchain, ensuring data integrity. Moreover, the module generates individual identity-based encryption key pairs for users, bolstering the security of their interactions within the system.

d) User Login

This module facilitates secure user authentication for registered accounts. Users input their unique credentials, usually comprising a username and password, to access their accounts. These credentials undergo authentication to verify the user's identity, ensuring only authorized individuals gain entry to the application. By implementing robust authentication mechanisms, the module enhances the security of user logins and protects against unauthorized access.

e) Post Private Messages

This module enables authenticated users to compose and share private messages securely. Users input message content and recipient details, triggering the generation of encrypted messages using Identity-Based Encryption (IBE) for confidentiality. The module securely stores these encrypted messages and associated data on the blockchain, ensuring the integrity and privacy of shared information. By leveraging IBE and blockchain technology, the module facilitates secure communication while maintaining data confidentiality.

f) View Shared Private Message

This module enables message owners and authorized users to safely read shared private messages. It presents a list of shared messages and employs the recipient's private key to decrypt and reveal the content. By utilizing the recipient's private key, the module ensures that only authorized users can access and comprehend the messages, preserving the privacy and confidentiality of the information exchanged within the system.

g) Blockchain Integration

Ethereum'sblockchain serves as a secure repository for various types of data, including user signup information and private messages.

Smart contracts on the Ethereumblockchain enforce predefined rules, improving security and transparency. They validate user actions, ensure data integrity, and enable secure sharing.

Ethereum'sblockchain verifies and records all user interactions and transactions, forming a transparent and tamper-proof record. This enables users to easily verify and trace their actions, fostering transparency and accountability across the platform.

Blockchain's decentralization removes the need for a central authority, boosting security. Data isn't vulnerable to a single point of failure, reducing risks and ensuring data resilience.

And Data integrity is maintained in the system through the utilization of the SHA-256 algorithm (Secure Hash Algorithm 256-bit). Each block in a blockchain is linked with a unique Hashcode. These blocks are maintained across multiple nodes or servers. Before storing new records, blockchain verifies the Hashcode of each block. If any block data is modified, it results in a different Hashcode, triggering security alarms and ensuring the integrity and immutability of the data.

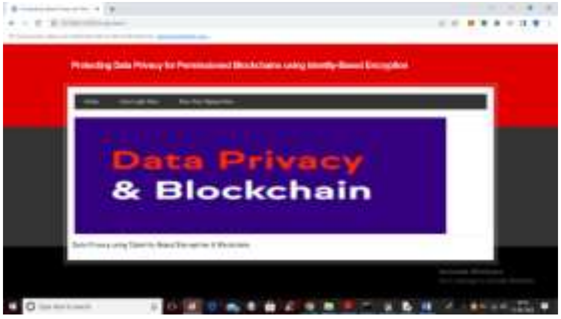
IPFS (InterPlanetary File System) is used for efficient and distributed file storage. Rather than storing bulky files directly on the blockchain, which could be slow and resource-intensive, IPFS is employed. IPFS assigns a unique hash code to each stored file. Importantly, these hash codes are recorded on the blockchain, ensuring that files can be efficiently retrieved while benefiting from the data integrity and security offered by the blockchain.

4. EXPERIMENTAL RESULTS

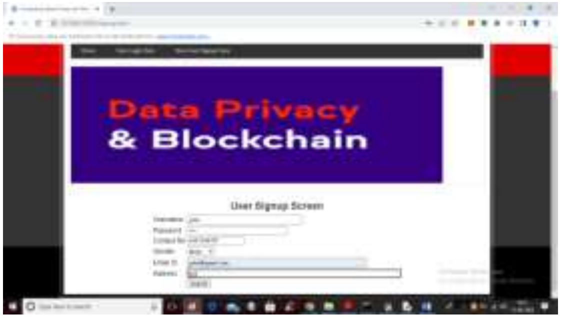
To run project first double click on 'Start_IPFS.bat' to start IPFS file server and get below output

In above screen IPFS server started and it running and now double click on 'runServer.bat' file to start python DJANGO server and get below screen

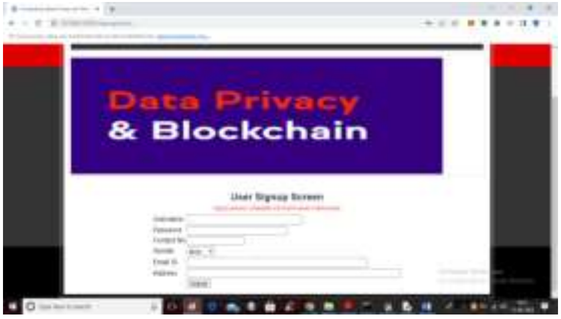
In above screen python server started and now open browser and enter URL as 'http://127.0.0.1:8000/index.html' and press enter key to get below home page


Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption
Data Privacy
& Blockchain

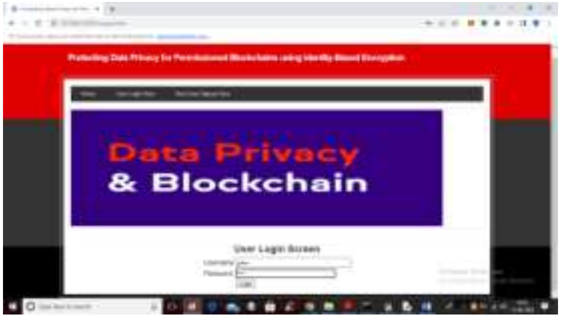
In above screen click on ‘New User Signup Here’ link to signup user



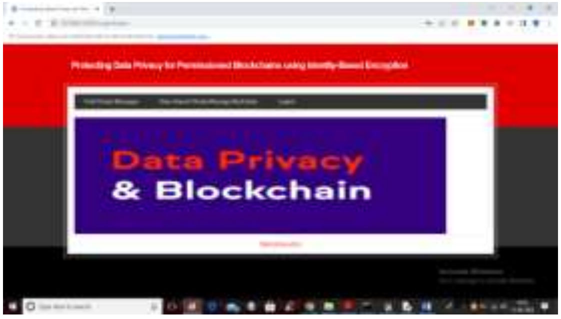
In above screen user is entering signup details and press submit button to store details in Blockchain and get below output



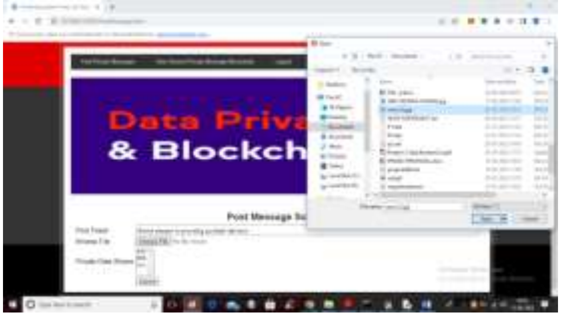
In above screen user signup completed and details saved in Blockchain and now click on ‘User Login’ link to get below screen


Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption
Data Privacy
& Blockchain
User Login Screen

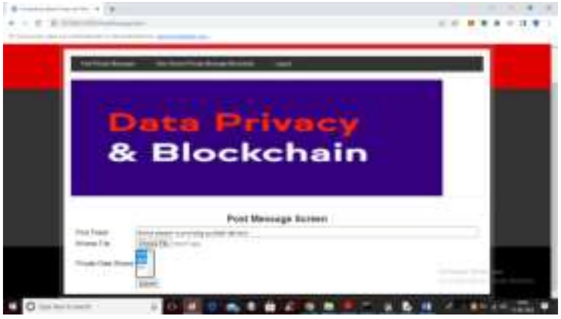
In above screen user is login and after login will get below screen


Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption
Data Privacy
& Blockchain

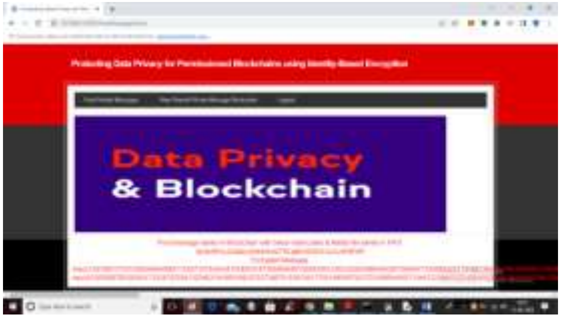
In above screen user can click on ‘Post Private Messages’ link to upload message



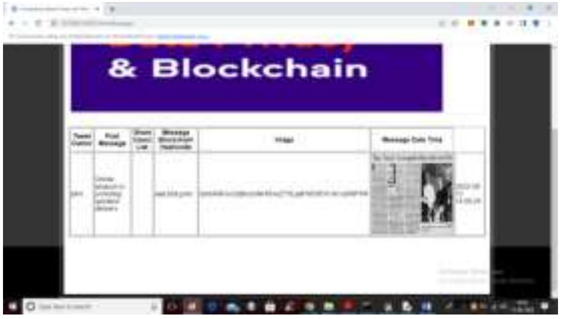
In above screen user type some message and then uploading image and then select list of users to share with and you can select multiple users by holding CTRL key like below screen



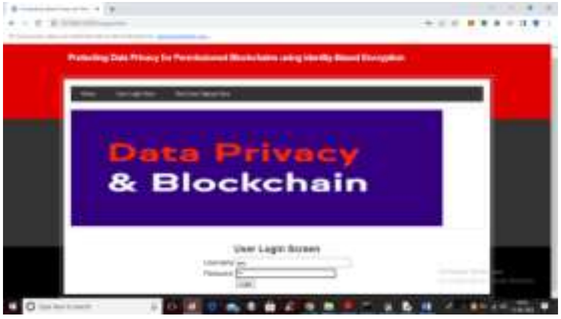
In above screen user John is uploading some post and then giving share access to user ‘aaa and bbb’ and user ‘ccc’ cannot access and now press ‘submit’ button to save post in Blockchain and get below output


Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption
Data Privacy
& Blockchain

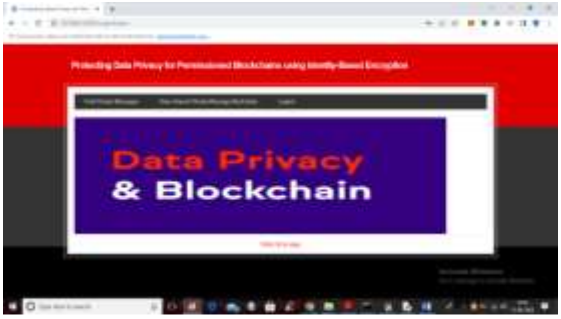
In above screen we can see message in red colour as POST MESSAGE saved in Blockchain and with Hashcode and we can see IBE encrypted message and now click on 'View Shared Private Message Blockchain' link to view message in decrypted format



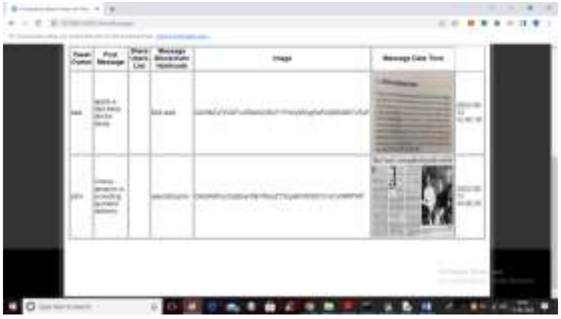
In above screen use can view decrypted message with image and hashcode and this user has shared post with user 'aaa' and now we login as 'aaa' and check message


Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption
Data Privacy
& Blockchain
User Login Screen
Username
Password
Login

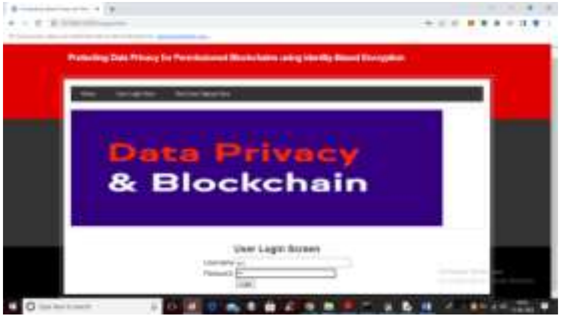
In above screen user 'aaa' is login and after login will get below screen


Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption
Data Privacy
& Blockchain

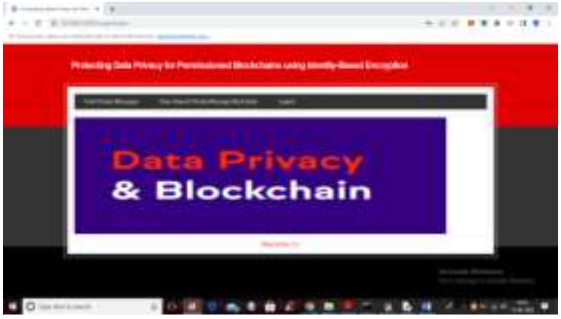
In above screen click on 'View Shared Message' link to get below output



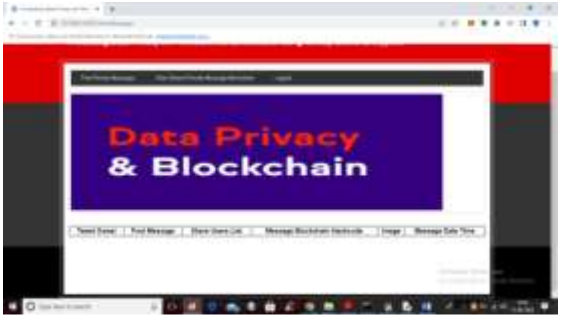
In above screen user aaa can view all his and shared messages and now we will login as user 'ccc' and check message as this user has no sharing permission


Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption
Data Privacy
& Blockchain
User Login Screen
Username
Password
Login

In above screen user 'ccc' is login and after login will get below output


Protecting Data Privacy for Permissioned Blockchains using Identity-Based Encryption
Data Privacy
& Blockchain

In above screen user can click on 'View Shared Message' link to view messages



Tweet Owner	Post Message	Share Users List	Message Blockchain Hashcode	Image	Message Date Time

In above screen we can see user CCC has no share permission so he cannot decrypt and view messages and privacy will be achieved

5. CONCLUSION

The project has significantly enhanced data privacy within permissioned blockchains by addressing security concerns associated with traditional methods, ensuring the confidentiality of sensitive information. Through the integration of Identity-Based Encryption (IBE) and blockchain technology, users can securely share data while maintaining data integrity. Leveraging the Ethereumblockchain establishes a robust and decentralized foundation for transparent data storage, enhancing trust and reliability. The IBE system enables precise control over data access, ensuring only authorized users can decrypt and view shared information. By eliminating reliance on traditional transaction methods and external verification, the project simplifies the data sharing process. Integration with IPFS further expands capabilities, enabling secure storage of various data types, including images. Designed for scalability, the project can seamlessly accommodate growing user numbers and larger data volumes while maintaining optimal performance and security standards.

6. FUTURE SCOPE

Future enhancements could involve integrating Identity-Based Encryption (IBE) with zero-knowledge proof (ZKP) techniques to further enhance privacy in permissioned blockchains. By combining IBE with ZKP, users could authenticate their identities without revealing sensitive information, ensuring confidentiality while verifying access permissions. This integration could enhance the granularity of access control, allowing for more nuanced data sharing policies within permissioned blockchains. Additionally, integrating ZKP with IBE could mitigate potential vulnerabilities associated with key management and authentication processes, further bolstering the security of the system. Moreover, exploring advancements in cryptographic primitives and consensus mechanisms could contribute to the development of more robust and scalable solutions for privacy-preserving data sharing in permissioned blockchains. Overall, integrating IBE with ZKP represents a promising avenue for future research and development, offering the potential to enhance privacy, security, and usability in permissioned blockchain applications.

REFERENCES

[1] General Data Protection Regulation (GDPR).[Online]. Available: https://gdpr-info.eu/art-5-gdpr.

[2] G. HILEMAN, M. RAUCHS, 2017 Global blockchain benchmarking study, 2017. [Online]. Available: https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/global-blockchain.

[3] DELOITTE, Breaking blockchain open - Deloitte's 2018 global blockchain survey, 2018. [Online]. Available: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf.

[4] M. EMEM, Facebook's Crypto Division Might Build a Blockchain Identity System: Mark Zuckerberg.

[Online]. Available: https://www.ccn.com/facebook-crypto-mark-zuckerberg-blockchain.

[5] Libra White Paper. [Online] Available: https://libra.org/en-US/white-paper.

[6] P. DUNPHY, F. A. P. PETITCOLAS, A First Look at Identity Management Schemes on the Blockchain, IEEE Security & Privacy, 16, 4, pp. 20-29, 2018.

[7] J. ROOS, H. NIEDERMAYER, Identity Management on the Blockchain, Seminars FI / IITM SS 18, Network Architectures and Services, 2018.

[8] A. TOBIN, D. REED, The inevitable rise of self-sovereign identity. The Sovrin Foundation, 2016. [Online]. Available: https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

[9] A. MÜHLE, A. GRÜNER, T. GAYVORONSKAYA, C. MEINEL, A Survey on Essential Components of a Self-Sovereign Identity, Computer Science Review 30 (2018): 80-86.

[10] X. ZHU, Y. BADR, Identity Management Systems for the Internet of Things: A Survey TowardsBlockchain Solutions, Sensors, 18(12):4215, 2018.

[11] P. ANGIN, B. BHARGAVA, R. RANCHAL, N. SINGH, M. LINDERMAN, L.B. OTHMANE, L. LILIEN, An entity-centric approach for privacy and identity management in cloud computing. In Proceedings of the 29th IEEE Symposium on Reliable Distributed Systems (SRDS'10), New Delhi, India, pp. 177–183, 2010.

[12] D. RECORDON, D. REED, OpenID 2.0: A Platform for User-centric Identity Management. In Proceedings of the Second ACM Workshop on Digital Identity Management, Alexandria, VA, USA, 2006.

[13] L. AXON, Privacy-Awareness in Blockchain-Based PKI. Oxford University Research Archive: Oxford, UK, 2015.

[14] M. AL-BASSAM, SCPKI: A Smart Contract-based PKI and Identity System. In Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, UAE, pp. 35–40, 2017.

[15] P. DUNPHY, L. GARRATT, F. PETITCOLAS, Decentralizing Digital Identity: Open Challenges for Distributed Ledgers. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), London, pp. 75-78, 2018.

[16] D. van BOKKEM, R. HAGEMAN, G. KONING, L. NGUYEN, N. ZARIN, Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology, 2019. arXiv:1904.12816.

[17] C. ALLEN, The path to self-sovereign identity, 2016. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-toself-sovereign-identity.html.

[18] R. SOLTANI, U.T. NGUYEN, A.AN, A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger. In 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1129-1136. IEEE, 2018.

[19] T. HARDJONO, A. PENTLAND, Verifiable Anonymous Identities and Access Control in Permissioned Blockchains.[Online]. Available: https://arxiv.org/pdf/1903.04584.pdf.

[20] Y. LIU, Z. ZHAO, G. GUO, X. WANG, Z. TAN, S. WANG, An Identity Management System Based on Blockchain, 2017 15th Annual Conference on Privacy, Security and Trust (PST) Calgary, Canada, 2017.

[21] D. AUGOT, H. CHABANNE, T. CHENEVIER, W. GEORGE, L. LAMBERT, A User-Centric System for Verified Identities on the BitcoinBlockchain. In Data Privacy Management, Cryptocurrencies and Blockchain Technology, Springer: Berlin, Germany, pp. 390–407, 2017.

[22] B. FABER, G. C. MICHELET, N. WEIDMANN, R. R. MUKKAMALA, R. VATRAPU, BPDIMS: A Blockchain-based Personal Data and Identity Management System. Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019.

[23] Namecoin. [Online]. Available: https://namecoin.org.

[24] Blockstack. [Online]. Available: https://blockstack.org.

[25] uPort. [Online]. Available: https://www.uport.me.

[26] SOVRIN-FOUNDATION, A protocol and token for self-sovereign identity and decentralized trust, 2018. [Online]. Available: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf

[27] Everest [Online]. Available: https://everest.org.

[28] SelfKey. [Online] Available: https://selfkey.org.

[29] ShoCard [Online]. Available: https://shocard.com.

[30] M. TAKEMIYA, B. VANIEIEV, Sora identity: Secure, digital identity on the blockchain. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), IEEE, 2018.