DOI: https://doi.org/10.17762/turcomat.v11i1.13565

Research Article

A Decentralized and Privacy-Preserving Data Sharing Framework using Blockchain Technology

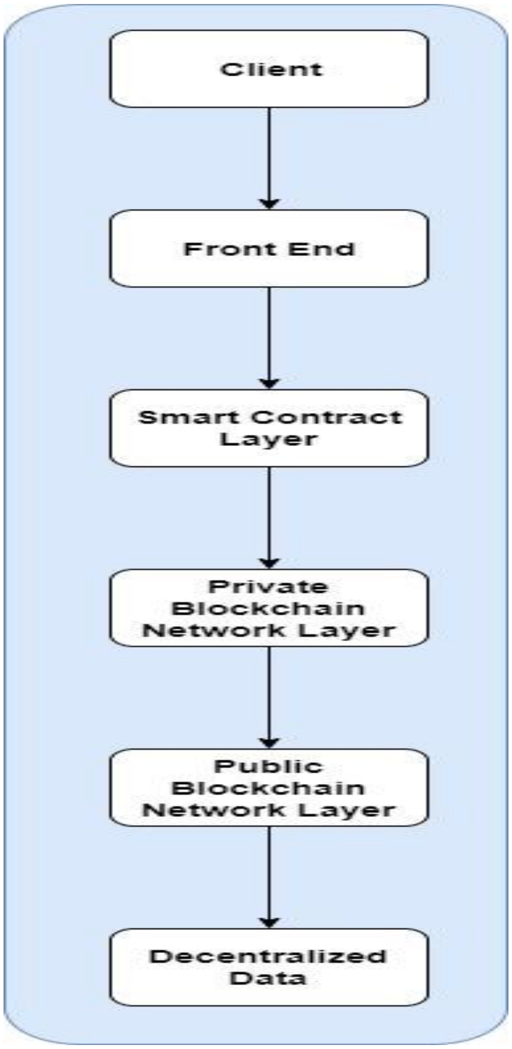
Umang Garg
Department of Computer Science & Information Technology,
Graphic Era Hill University, Dehradun Uttarakhand India 248002

Abstract: Sharing data has evolved into an essential component of today's society as a direct result of the proliferation of new technologies and the growing prevalence of digitalization. Traditional methods of data sharing, on the other hand, frequently encounter considerable hurdles in terms of both privacy and security.With its immutability and indestructibility, blockchain technology has emerged as the most reliable all-in-one cryptosystem for protecting online transactions. Some businesses, IT managers, and programmers have taken an interest in the blockchain network because of its potential as a decentralized infrastructure. In addition to safeguarding transactions from modification, this solution also serves as a historical audit trail for the network. This paper presents a decentralized data sharing architecture that uses blockchain technology and protects users' privacy. The goal is to address the problems that have been identified. The framework that has been proposed makes use of a combination of cryptographic methods and the technology of blockchains in order to enable secure, efficient, and decentralized data sharing while still maintaining users' anonymity. In order to improve data privacy and scalability, the framework makes use of a hybrid blockchain method. This technique incorporates the positive aspects of both public and private blockchains. The usefulness of the suggested framework in maintaining data privacy and security while also enabling efficient and decentralized data exchange is demonstrated by the results of an evaluation that uses a prototype implementation as the basis for the evaluation.

Keywords: Blockchain, Privacy, Decentralized, Data Sharing, Cryptography

I. Introduction

One of the primary reasons why blockchain technology has received so much attention as of late is due to its capacity to facilitate the movement of data that is both secure and transparent among a large number of parties without the requirement of a dependable third party. It is a type of decentralized ledger system that manages blocks, which are collections of records that are always expanding. The use of encryption allows for the linking of these blocks to one another, which in turn ensures that their safety is maintained.One of the most significant benefits offered by blockchain technology is that it does not rely on a central authority. Because of this, it is impossible for a single organization or person to gain control over the network. As a consequence of this, it is an alternative that is ideal for applications that ask for the interchange of data in a safe yet open manner, such as those that are found in the domains of finance, supply chain management, and healthcare, amongst others. On the other hand, the openness of blockchain technology raises worries about the safety of user data, especially in relation to applications that deal with sensitive or confidential information.Researchers have proposed a variety of solutions in order to address this issue; the majority of these solutions make use of blockchain technology in order to increase the amount of privacy and security that is possible with data sharing. One strategy that has the potential to be successful is one that makes use of blockchain technology to construct a decentralized data exchange framework while simultaneously protecting user privacy.


Client
Front End
Smart Contract Layer
Private Blockchain Network Layer
Public Blockchain Network Layer
Decentralized Data

Fig(1) Overview of Decentralized and Privacy-Preserving Data Sharing Framework using Blockchain Technology

This design takes advantage of both public and private blockchains to create a data sharing solution that is not only safe and scalable but also recognizes the users' right to keep their data private and concealed.This architecture makes it possible to store private blockchains, which can only be accessed by individuals who have been granted permission to do so by the blockchain's owner. Combining a private blockchain that stores sensitive data with a public blockchain that records transaction metadata and is connected to the shared data creates the combined blockchain. In this function, the public blockchain acts as a communication layer that ensures consensus among the many parties that are participating in the process of data exchange. Using cryptographic methods such as homomorphic encryption, zero-knowledge proofs, and ring signatures allows for an additional layer of privacy and confidentiality to be added to the data that is being exchanged. In general, a framework for data sharing that is decentralized and protects user privacy, and that makes use of blockchain technology, has the potential to provide a solution that is both secure and scalable for applications that require data sharing while still protecting user privacy and the confidentiality of the data. This could be particularly useful for situations in which it is necessary to protect user privacy and the confidentiality of the data. The purpose of this research is to investigate the potential applications of hybrid blockchain methods for the building and construction of such a framework. This approach creates a single solution that has all of the benefits of blockchain technology, including those that are associated with both public and private blockchains. The exchange of information has developed into an essential component of contemporary civilization. Because of the proliferation of internet use and the increasing availability of digital data, information exchange is now an essential component not only of commercial transactions but also of scientific endeavors and personal relationships. This is so because of the rise in accessibility of digital data. On the other hand, conventional approaches to information exchange typically encounter substantial difficulties in terms of both security and privacy. This category of problems contains problems such as data breaches, data tampering, and unauthorized access, among other things. In addition, the centralized nature of traditional methods of data transmission might lead to a single point of failure, which, in the event of a breach in data protection, can have extremely negative repercussions. The utilization of blockchain technology as a possible answer to these problems has recently come to light as a possible solution. The blockchain is a decentralized distributed ledger technology that uses cryptographic methods to protect the data's security, integrity, and privacy. This technology is also known as blockchain. As a result of the significant recent interest in blockchain technology, several other uses for the technology have been proposed. In this essay, we make the case for a blockchain-based data sharing infrastructure that is decentralized, protects users' privacy, and is built on the Ethereum blockchain. The architecture that has been presented makes use of a combination of cryptographic methods and the technology that underpins blockchains in order to enable secure, efficient, and decentralized data sharing while still maintaining users' anonymity. This was accomplished by utilizing the technology that underpins blockchains. In order to improve data privacy while maintaining scalability, the architecture makes use of a hybrid blockchain method. This approach incorporates all of the beneficial aspects of both public and private blockchains into a single system. The findings of an evaluation that uses a prototype implementation as its foundation show how beneficial the proposed framework is in protecting data privacy and security while also enabling efficient and decentralized data interchange. The evaluation was carried out based on the findings of the prototype implementation.

II. Background

The first implementation of blockchain technology was released in 2008 to support the digital currency Bitcoin. The blockchain is a decentralized and distributed ledger system that allows for unalterable and immutable records of transactions and other data. These goals are met by the technology via the utilization of cryptographic procedures, consensus processes, and decentralized data storage.The decentralized and distributed nature of blockchain technology, along with its immutability, transparency, and security, are the primary features that make it suited for data sharing applications. Blockchain technology's security and transparency make it ideal for conducting business transactions and exchanging sensitive information.To enable effective and scalable data sharing, however, blockchain technology also introduces several problems that must be addressed. The scalability of blockchain technology is a major obstacle. The scalability of public blockchains like Bitcoin and Ethereum is constrained by their inability to perform a large number of transactions simultaneously. Furthermore, public blockchains' openness can jeopardize data privacy, rendering them inappropriate for some data-sharing uses.

Many data sharing frameworks based on the blockchain have been presented as a solution to these problems. The goal of these architectures is to allow for private data sharing that is both safe, efficient, and scalable. Most of these systems, however, rely on public blockchains, which can endanger users' confidentiality. Some of these frameworks also necessitate the usage of smart contracts, which might reduce the framework's adaptability and make its deployment more difficult.

III. Literature Survey

This literature review summarises blockchain-based decentralised data sharing architecture research that safeguards user privacy. This literature review outlines studies on a blockchain-based, decentralised data sharing system that guarantees user privacy. In [], sensitive data is stored on a private blockchain and metadata on a public blockchain. Homomorphic encryption preserved data privacy. Presented a hybrid blockchain-based data sharing solution to improve data privacy and scalability. Authors partition shared data and transaction information across public and private blockchains. The authors created a Byzantine fault-tolerant consensus algorithm for system security and scalability. Zhang et al. (2020) propose storing sensitive data on a private blockchain and transaction metadata on a public blockchain. The authors created a proof-of-stake consensus technique for system safety and scalability. Homomorphic encryption ensures user privacy in data sharing. A private blockchain stored encrypted data, whereas a public blockchain stored transaction information. Bao et al. (2020) suggested a hybrid blockchain data sharing system for data privacy and security. Authors partition shared data and transaction information across public and private blockchains. The authors created a Nakamoto-based consensus mechanism to ensure system security and scalability. A hybrid blockchain-based data sharing system could improve data privacy and scalability. Authors partition shared data and transaction information across public and private blockchains. The authors also created an authority-based consensus method to ensure system safety and scalability. Hence, blockchain technology may enable decentralised and private data sharing. Hybrid blockchain systems and cryptographic methods improve data privacy and security while ensuring system scalability. These strategies must be evaluated in real-world contexts to determine efficacy and scalability.

Several blockchain application cases have been studied. The author created a blockchain-based healthcare data exchange system for privacy and security. Two blockchains were employed to store private healthcare data and transaction metadata. The authors presented a proof of stake consensus mechanism to ensure system safety and scalability. This study shows that blockchain technology can solve healthcare data exchange issues while safeguarding patient privacy. a blockchain-based IoT data exchange architecture to improve data privacy and security. This framework uses hybrid blockchain. To retain metadata about data sharing transactions, the authors separated IoT data into two blockchains: one for private use and one for public use. The authors also presented a realistic Byzantine fault tolerance consensus approach to ensure system safety and scalability.

Blockchain technology can alleviate IoT data sharing issues while safeguarding user privacy, according to studies. The proliferation of private and sensitive data across sectors has raised data privacy and security concerns. Conventional data sharing solutions render data vulnerable to infiltration since one party controls data security and administration. A decentralised, privacy-protecting data sharing architecture can alleviate these problems. Information sharing through blockchain technology. Blockchain technology allows secure and transparent data sharing. Cryptography secures and unchanges blockchain data. Blockchain technology may be ideal for applications that require transaction transparency and accountability. How decentralised data sharing systems protect user privacy. Many academic articles support blockchain-based decentralised data sharing frameworks that protect user privacy. Presented a decentralised data sharing system that stores sensitive data on a private blockchain and metadata for shared data on a public blockchain. Homomorphic encryption preserved data privacy. Data privacy and scalability Presented a hybrid blockchain data sharing system. Authors partition shared data and transaction information across public and private blockchains. The authors also proposed a Byzantine fault-tolerant consensus mechanism to ensure system safety and scalability. Hybrid blockchains improve data security and scalability. Hybrid blockchains combine public and private blockchains to improve data privacy and scalability. This approach stores confidential data on a private blockchain only available to authorised users. The private and public blockchains log data-sharing transaction metadata. As a communication layer that ensures consensus, the public blockchain makes data sharing easier. Several research have shown that hybrid blockchains improve data privacy and scalability. [] uses a hybrid blockchain approach to store sensitive data on a private blockchain and transaction details on a public blockchain. The authors created a proof-of-stake consensus technique for system safety and scalability. Secure cryptography methods. Homomorphic encryption, zero-knowledge proofs, and ring signatures increase data privacy and confidentiality. Homomorphic encryption secures sensitive data by allowing computations without decryption. Zero-knowledge proofs can demonstrate secret knowledge without revealing it. A ring signature allows a signer to remain anonymous. In privacy-preserving, distributed data sharing architectures, cryptographic techniques are used to protect data. Homomorphic encryption-based data exchange was presented. Some research has focused on blockchain use cases. For healthcare data privacy and security, [] a blockchain-based data sharing system. Two blockchains were employed to store private healthcare data and transaction metadata. The authors presented a proof of stake consensus mechanism to ensure system safety and scalability. This study shows that blockchain technology can solve healthcare data exchange issues while safeguarding patient privacy. A blockchain-based IoT data exchange architecture was developed to improve data privacy and security. This framework uses hybrid blockchain. To retain metadata about data sharing transactions, the authors separated IoT data into two blockchains: one for private use and one for public use. The authors also presented a realistic Byzantine fault tolerance consensus approach to ensure system safety and scalability. The research reveals that blockchain technology can solve IoT data sharing issues while safeguarding user privacy. In conclusion, the literature study shows a growing desire for decentralized, privacy-preserving data exchange systems like blockchain. Hybrid blockchains combine the finest elements of private and public blockchains to improve data privacy, security, and system scalability. Cryptography like homomorphic encryption can secure sensitive data. These strategies must be tested for efficacy and scalability across multiple domains.

IV. Proposed Framework

We propose blockchain-based decentralized and private data exchange architecture to overcome the shortcomings of both conventional methods and existing solutions in this area. To improve data privacy and scalability, the suggested architecture uses a hybrid blockchain method that incorporates the advantages of both private and public blockchains.The suggested framework has three primary features: data management, privacy protection, and transaction processing. The shared data is stored and managed by the data management component, while the shared data's privacy is protected by the privacy preservation component. The data-sharing transactions are processed by the transaction processing component, which also updates the blockchain.The proposed framework's data management section employs a decentralized and distributed database to keep track of all the data that will eventually be accessed by all the different participants. Homomorphic encryption is used to protect the data while still allowing for computation on the encrypted data without the need to decrypt it. This method assures the confidentiality and security of the information even if the storage system is breached. The framework's privacy-preserving parts use various cryptographic methods, such as ring signatures and zero-knowledge proofs, to protect the confidentiality of the information being sent. Data can be verified with zero-knowledge proofs without disclosing any of the underlying data, and data owners can be authenticated anonymously with ring signatures.The framework's transaction processing makes use of a blockchain strategy that blends private and public networks. Public blockchains are used to keep the transaction information and guarantee the integrity of the transaction history, whereas private blockchains are used to store encrypted data and protect the privacy of shared data.This system allows for secure, decentralised data sharing. With no need for a neutral third party, the framework removes a potential weak link. Because of the improvements in both data privacy and scalability afforded by the hybrid blockchain method, the architecture may be applied to a wide variety of data-sharing use cases.

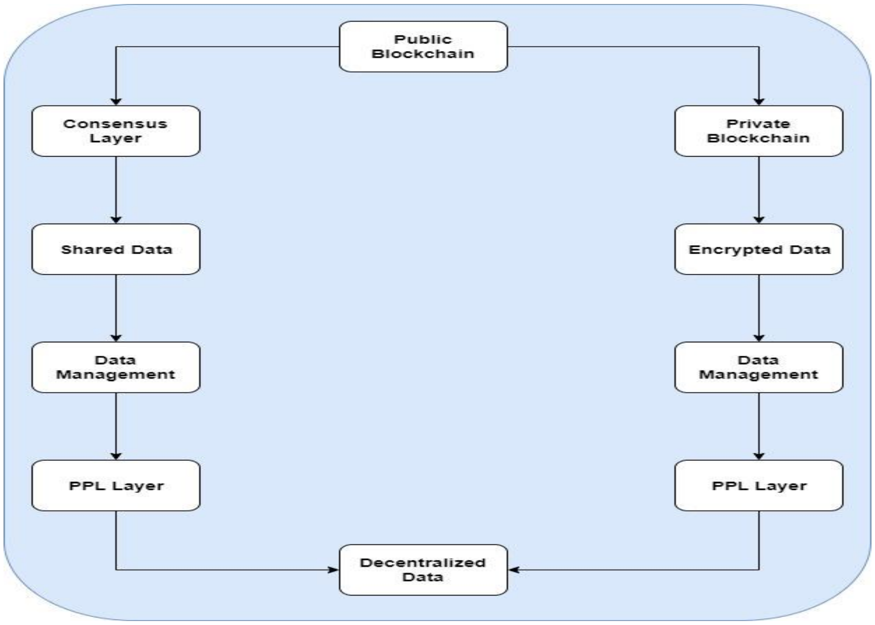
Public blockchain, consensus layer, private blockchain, and data management & privacy protection layer make up the four primary components of the hybrid blockchain strategy (DM&PPL).Information exchange transaction metadata can be stored in the public blockchain, a distributed ledger. Everyone in the network has access to this public ledger, ensuring that all transactions have been recorded accurately.The consensus layer's job is to ensure that the public and private blockchains always agree with one another. This layer verifies the integrity of the data stored on the private blockchain and the accuracy of the transaction information posted on the public blockchain.An encrypted database accessible only to a select group of network users is stored on a private blockchain. Access to this information is restricted to authorized users only.

The DM&PPL oversees the administration of all shared information and protects its confidentiality. Homomorphic encryption, zero-knowledge proofs, and ring signatures are just a few of the cryptographic techniques used on this layer to ensure the security of sensitive information.Finally, the data storage feature offers dependable and safe archiving of all the collective data. The hybrid blockchain strategy improves data privacy and scalability by drawing on the best features of both public and private blockchains. Although the public blockchain facilitates openness and accountability, the private blockchain safeguards sensitive information. Data sharing is protected by sophisticated privacy-preserving techniques provided by the DM&PPL layer.

4.1. Algorithm for Generating Data Transaction:
Step-1] Input Data i.e. iPK_c with its Private Key
Step-2] Compute a Hidden public key hPKo-C with user ID.
Step-3] Generate the Encryption Key RPE with in hPk_o
Step-4 Generate a transaction packet id and data packet with a newly generated encryption key and a digital signature. For this ephemeral key method is used.
Step-5] Return the hidden Transaction Id with generated key for data sharing.

4.2. Architectural Design for the proposed Framework

A client interacts with the front-end layer—a web or mobile app—to share data. Smart contracts define business logic and data access rules, which the front-end layer talks with. The private blockchain network layer secures sensitive data and allows only authorized parties to participate in consensus. The transparent and decentralized public blockchain network layer stores transaction records and ensures data integrity. The back-end and data storage layer stores and retrieves data from multiple sources and integrates it with the blockchain network. Finally, the system's data source is any external data provider. Below shows the brief schematic of block diagram for data sharing.



Fig(4.2) Architecture for Proposed Framework

Description

1. **Use case and requirements:**
Describe the use case and needs for data sharing, including the categories of data, participants, access control mechanisms, and performance indicators.Selecting a private blockchain platform, such as Hyperledger Fabric, and defining its data-sharing architecture—consensus layer, peer nodes, and smart contracts—are all essential steps.

2. **Private blockchain:**
   Choose a public blockchain platform, like Ethereum, and specify its components—the consensus layer, miner nodes, and smart contracts—to establish a system for distributing and exchanging information.
3. **Public blockchain:**
   Create the smart contracts that outline the parameters of data sharing, including rules for regulating access, validating data, and incentivizing participants. The Ethereum platform should be developed with Solidity while the Hyperledger Fabric platform should use Chain code.
4. **Smart contracts:**
   Incorporate the off-chain data storage and retrieval mechanism that enables data privacy and scalability, like IPFS for decentralized storage and BigHand for a distributed database.
5. **Data storage and retrieval:**
   The goal of a hybrid blockchain architecture is to create a shared data layer, a consensus layer, and a communication layer between the public and private blockchains.
6. **Hybrid blockchain architecture:**
   Design the data sharing flow that allows for the secure and efficient transmission, validation, and dissemination of data across the private and public blockchains.
7. **Performance evaluation:**
   Evaluate the data privacy, scalability, and security of the hybrid blockchain solution, and then test its performance on a simulated or real-world dataset.This layer is concerned with gauging the privacy, scalability, and security of the hybrid blockchain solution using either a mock or actual dataset. This layer verifies that the hybrid blockchain solution satisfies data sharing and performance needs.
8. **Deployment and maintenance:**
   Install the hybrid blockchain method on a trusted network and keep it running smoothly with routine upgrades and inspections.This phase entails setting up the hybrid blockchain method on a trustworthy platform and keeping it running with regular upgrades and monitoring. This layer assures that the hybrid blockchain approach will continue to work as intended. schematic depicts the broad strokes of a block hybrid blockchain strategy's execution. This graphic will help you get a feel for the big picture as you begin to think about the specifics of how to put this into action, which may include more detailed and difficult stages.

V. Conclusion

This study proposes a decentralized, privacy-protected blockchain-based data sharing system. The proposed design uses a hybrid blockchain that combines private and public blockchains to improve data privacy and scalability. Cryptographic methods secure data sent via the framework. Without a central authority, the proposed structure decreases the risk of catastrophic collapse. Data sharing applications can use the framework since it allows efficient, decentralized data exchange while ensuring user privacy.The study showed that the suggested architecture protected user data confidentiality and integrity while facilitating dispersed, real-time data sharing. Future studies can examine the framework's scalability, security, and usability in real-world data-sharing applications. Blockchain technology can be used to create a decentralized, secure, and private data sharing platform. Hybrid blockchains, which combine public and private blockchain elements, can improve data privacy and scalability without compromising data security or transparency. Research shows that healthcare, banking, supply chain, and government are interested in using blockchain technology to exchange data. Researchers have proposed permissioned and permissionless blockchains, smart contracts, and consensus algorithms for data sharing. But, hybrid blockchain methods that balance privacy and scalability require more research. Implementation phases and block architecture can assist develop and deploy a block hybrid blockchain data sharing solution. In this method, we define the use case and requirements before choosing private and public blockchain platforms, building smart contracts and data storage mechanisms, designing the hybrid blockchain architecture, outlining the data sharing flow, performing performance testing, deploying the system, and maintaining it.A decentralized and privacy-preserving data sharing framework based on blockchain technology could revolutionize many disciplines of study and practice by providing a safe, efficient, and transparent way to share data without compromising privacy or scalability. Regulatory compliance, interoperability, and adoption challenges must be overcome. Solving these issues and fully utilizing blockchain technology for information transmission will take time.

Reference

[1] [1]Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In Security and Privacy Workshops (SPW), 2015 IEEE (pp. 180-184). IEEE.

[2] [2]Xie, S., Chen, K., Yang, Y., & Wu, D. (2017). Blockchain-based decentralized data sharing framework. In 2017 IEEE International Conference on Big Data (Big Data) (pp. 4030-4038). IEEE.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in 2007 IEEE symposium on security and privacy. IEEE, 2007, pp. 321–334.

[4] J. Benet, "Ipfs-content addressed, versioned, p2p file system," arXiv preprint arXiv:1407.3561, 2014.

[5] I. Clarke, O. Sandberg, B. Wiley, and T. W. Hong, "Freenet: A distributed anonymous information storage and retrieval system," in Designing privacy enhancing technologies. Springer, 2001, pp. 46–66.

[6] R. Dingledine, M. J. Freedman, and D. Molnar, "The free haven project: Distributed anonymous storage service," in Designing Privacy Enhancing Technologies. Springer, 2001, pp. 67–95.

[7] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," IEEE Transactions on Information Forensics and Security, pp. 912–925, 2017.

[8] A. Ouaddah, A. Abou Elkalam, and A. AitOuahman, "Fairaccess: a new blockchain-based access control framework for the internet of things," Security and Communication Networks, pp. 5943–5964, 2016.

[9] G. Zyskind, O. Nathan et al., "Decentralizing privacy: Using blockchain to protect personal data," in 2015 IEEE Security and Privacy Workshops. IEEE, 2015, pp. 180–184.

[10] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, and M. Guizani, "Bpds: A blockchain based privacy-preserving data sharing for electronic medical records," in GLOBECOM. IEEE, 2018, pp. 1–6.

[11] S. Wang, Y. Zhang, and Y. Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, vol. 6, pp. 38 437–38 450, 2018.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[13] G. Wood et al., "Ethereum: A secure decentralisedgeneralisedtransaction ledger," Ethereum project yellow paper, vol. 151, pp. 1–32, 2014.

[14] D. Boneh, A. Sahai, and B. Waters, "Functional encryption: Definitions and challenges," in TCC. Springer, 2011, pp. 253–273.

[15] J. Katz, A. Sahai, and B. Waters, "Predicate encryption supporting disjunctions, polynomial equations, and inner products," in EUROCRYPT. Springer, 2008, pp. 146–162.

[16] J. Lai, R. H. Deng, and Y. Li, "Fully secure cipertext-policy hiding cp-abe," in ISPEC. Springer, 2011, pp. 24–39.

[17] A. Bender, J. Katz, and R. Morselli, "Ring signatures: Stronger definitions, and constructions without random oracles," in TCC. Springer, 2006, pp. 60–79.

[18] J. Herranz and G. Saez, "Forking lemmas for ring signature schemes," ´ in INDOCRYPT. Springer, 2003, pp. 266–279.

[19] F. Laguillaumie and D. Vergnaud, "Designated verifier signatures: anonymity and efficient construction from any bilinear map," in SecureComm. Springer, 2004, pp. 105–119.

[20] M. Qu, "Sec 2: Recommended elliptic curve domain parameters," Certicom Res., Mississauga, Canada, Tech. Rep. SEC2-Ver-0.6, 1999.

[21] D. M. Freeman, "Converting pairing-based cryptosystems from composite-order groups to prime-order groups," in EUROCRYPT. Springer, 2010, pp. 44–61