International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 03 | March - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

# Cross-Chain Ethereum Architecture for Secure and Dynamic Access Management

**Sreedevi Kadiyala[1], Toyakant Chaudhary[2], Suraj Ranjan[3], Shiva Kumar Chaudhary[4]**

[1]Associate Professor, Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad.
[2,3,4]Department of CSE, Guru Nanak Institutions Technical Campus, Hyderabad.

***Abstract:*** This paper introduces an innovative access control architecture based on a dual-blockchain framework that distinctly separates access management from data storage to enhance system security, scalability, and privacy. Architecture employs a primary blockchain to manage user authentication and enforce dynamic, fine-grained permissions through smart contracts. In parallel, a secondary, isolated blockchain is used exclusively for storing sensitive data, which can only be accessed following successful authorization on the primary chain. To ensure data integrity and tamper resistance, the system utilizes the SHA-256 cryptographic hash function for securing access logs and verifying data authenticity across both blockchains. The two chains are securely interconnected using Hyperledger YUI, which facilitates reliable inter-chain communication while maintaining a decentralized structure. A proof-of-concept implementation using Ethereum-based blockchains demonstrates the system's capability to enforce secure, dynamic access controls across chains. Overall, the proposed architecture overcomes key limitations of conventional blockchain systems by enhancing modularity, strengthening governance, and providing a robust, adaptable framework suitable for data-sensitive applications requiring strict regulatory compliance.

## I. INTRODUCTION

Beyond its seminal use in cryptocurrencies, blockchain technology has evolved to address a myriad of challenges across various industries. In the financial sector, blockchain is revolutionizing the way transactions are conducted, reducing the need for intermediaries [3] and enabling faster, more secure, and cost-effective cross-border payments and international trade. Supply chain management is another area where blockchain is making significant contributions. By providing an immutable record of the journey of goods from origin to consumer, blockchain enhances transparency, reduces fraud, and improves efficiency. This traceability is particularly valuable in industries such as food and pharmaceuticals where the authenticity and safety of products are paramount. In healthcare [11], blockchain is being used to secure patient data, ensuring privacy and compliance [12] with regulations such as European Union's General Data Protection Regulation (GDPR) [13]. It also facilitates the sharing of medical records [14] across different healthcare providers, improving patient care and reducing administrative burdens [15]. Moreover, blockchain's potential extends document certification and notarization, where it can provide a transparent and tamper-proof method of recording ownership [16] and origin, even for academic certifications [17], [18] and other educational applications [19] thereby enhancing the integrity of any document-driven process in the digital age [20]. Intellectual property management, digital identity verification, and even the energy sector [21] is also exploring blockchain solutions to address their unique challenges [22]. From the computer scientist's perspective, blockchain is a decentralized information repository that is replicated and distributed among computing nodes in a peer-to-peer network. The repository is implemented as a set of blocks, which are linked together and secured using cryptographic techniques. Each block may contain any kind of information depending on the type of blockchain and application field. From this perspective, each block contains a collection of information records (i.e., transactions in blockchain lingo) and a reference pointing to the hash summary of the previous block, forming a chain of blocks (block-chain). This structure allows information, once recorded, to be persistently available to users who wish to verify it. Furthermore, thanks to cryptography, information is immutable and secure, without the need for a centralized supervisor or controller. There are three broad types of blockchains, each of them with their specific characteristics. Public blockchains are fully

decentralized and open, which allows any individual to participate in them, send transactions, and even create new blocks. Prominent examples are Bitcoin [1] and Ethereum [23]. Although they provide great transparency and security, data cannot be modified, and the blockchain lacks scalability as the whole chain is replicated in all nodes participating in the peer-to-peer network. Besides, the performance of transaction validation is limited. Additionally, information confidentiality is non-existent, as all parties can access all the data stored in the chain, as it is fundamentally public. It is possible to store encrypted data, but as a public blockchain is an immutable storage medium, the encryption algorithm used now may be broken in the future (e.g., because flaws or backdoors are discovered, or because presently emerging technologies like quantum computing eventually make it obsolete). These blockchains are also known as permissionless blockchains. Private blockchains are those created, maintained and controlled by an organization in such a way that, to join them, it is necessary to obtain permission from the deploying entity. Therefore, the organization that governs it decides who can or cannot participate in the network. An outstanding example of this type of blockchains are the ones constructed on the Linux Foundation's Hyperledger framework [24] or Hyperledger Besu. In this case, as the nodes that form part of the network are known, less rigorous control mechanisms can be employed than in public blockchains, which allows for better scalability and speed when recording transactions and creating new blocks. As a drawback, decentralization is lost at a varying degree, and therefore private blockchains are conceptually centralized system independently of the underlying decentralized technology. Data confidentiality can be seen as a positive aspect, as not everyone can access the information managed, but those nodes that were granted permission to participate in the network. These chains are also known as permissioned blockchains. Federated or consortium blockchains are those in which several organizations collectively control the blockchain. Each organization is allowed to deploy its own nodes, but joining the federated network still requires the corresponding permission. Certain information may be shared with any user across the consortium (i.e., beyond the organization owning that information), which differentiates these blockchains from private blockchains. Although they are permissioned blockchains, they can be seen as a hybrid of public and private blockchains, with their own set of advantages and disadvantages. Another concept that gained relevance in recent years is that of smart contracts, originally proposed by Nick Szabo [25]. These are computer programs run on a virtual machine hosted by blockchain nodes that are automatically executed when certain predefined conditions are met. While they are not unique to blockchains, their features are greatly enhanced in combination with blockchain technology. These programs are stored and executed on the blockchain, guaranteeing immutability, tamper-resistance and autonomous execution without human intermediaries. Ethereum is a blockchain platform launched in July 2015 that gained considerable recognition for its capacity to deploy and execute smart contracts.

## II. RELATED WORK

Several researchers have investigated how blockchain technology can be used to provide secure and privacy-preserving access control in distributed systems. One of the early approaches was introduced by Zyskind and Nathan, who proposed a hybrid architecture that separates data storage from access management. In their model, sensitive user data is stored outside the blockchain in a distributed hash table (DHT), while the blockchain is used to manage access permissions and ownership records. This design improves data privacy by ensuring that only the data owner has full control over the information. However, the system does not provide flexible mechanisms for sharing data with multiple users, which limits its usefulness in collaborative environments.

Another approach was developed by Xu et al., who designed a blockchain-based access control system that integrates Hyperledger Fabric with ring signature techniques. Their system uses distributed storage such as the Hadoop Distributed File System (HDFS) to store data outside the blockchain, while access policies are maintained within the blockchain network. The use of ring signatures helps protect user identity during authentication. Although this framework improves privacy and security, it relies on predefined communication channels, which can reduce flexibility when scaling the system or integrating multiple blockchain environments.

The Chain Anchor system proposed by researchers at the MIT Media Lab introduces another privacy-focused solution. It uses zero-knowledge proofs to allow users to prove that they belong to a blockchain network without revealing their actual identity. This method enhances authentication and privacy in permissioned blockchain systems. Despite its advantages, the approach requires major modifications to existing blockchain infrastructures, which makes practical implementation more challenging.

Other studies have focused on combining blockchain with encryption-based access control methods. For example, some frameworks use attribute-based encryption (ABE) to protect sensitive information stored in cloud environments. In these systems, the actual data is stored outside the blockchain, while the blockchain maintains metadata, hash values, and access control policies. This combination allows secure data sharing while maintaining data integrity and transparency. However, these solutions can introduce additional complexity in managing encryption keys and maintaining system scalability.

Researchers have also explored blockchain-based data sharing systems using platforms such as Multichain combined with Ciphertext Policy Attribute-Based Encryption (CP-ABE). These approaches aim to enable secure collaboration between multiple users while maintaining strong confidentiality and integrity guarantees. Although these systems improve decentralized data sharing, challenges remain in terms of interoperability and efficient enforcement of access control policies across different blockchain platforms.

Recent research further investigates improving blockchain security by introducing additional control layers. One such example is the Blockchain Application Firewall (BAF), which acts as a monitoring layer between users and blockchain services. This firewall evaluates incoming and outgoing requests based on predefined access policies and blocks unauthorized actions. Such mechanisms help improve security and privacy in blockchain-based systems while enabling more controlled interaction with blockchain networks.

## III. LITERATURE SURVEY

One of the earliest blockchain-based access control models was proposed by Zyskind and Nathan [44], who introduced a hybrid privacy-preserving architecture where access policies are enforced on-chain while encrypted personal data is stored off-chain in a Distributed Hash Table (DHT). This design ensures that only the data owner can access or modify their information, thereby improving data privacy and security. However, the proposed model does not support selective data sharing among multiple users, which limits its applicability in collaborative environments requiring controlled access mechanisms.

Xu et al. [45] proposed a blockchain-based access control framework that utilizes ring signatures to enhance anonymity and data protection. Their system integrates Hyperledger Fabric for blockchain management and Hadoop Distributed File System (HDFS) for off-chain storage of encrypted data. Ring signatures provide anonymous authentication while maintaining system security. However, the approach relies heavily on predefined communication channels within Hyperledger Fabric, which restricts flexibility in environments requiring dynamic access control across multiple blockchain platforms.

The ChainAnchor framework, proposed by the MIT Media Lab [46], introduces an access control model based on zero-knowledge proofs to enable anonymous yet verifiable identities in permissioned blockchain networks. In this approach, access control is enforced at the consensus layer, reducing reliance on external authentication services. Despite its theoretical advantages, ChainAnchor remains largely conceptual, as the implementation requires significant architectural modifications to existing blockchain infrastructures, making practical deployment challenging.

Another approach combines Hyperledger blockchain technology with Attribute-Based Encryption (ABE) to provide secure access control for cloud-stored data [48]. In this system, encrypted data is stored in the cloud, while a hash digest of the data is maintained on the blockchain to ensure integrity. Access control policies are implemented through chaincode, enabling secure data retrieval. However, storing hash digests on the blockchain may still raise privacy concerns in some applications.

| S.No | Author & Year | Technique / Method | Key Contribution | Limitations |
|---|---|---|---|---|
| 1 | Zyskind & Nathan [44] | Blockchain + Distributed Hash Table | Hybrid on-chain/off-chain privacy model | No selective access sharing |
| 2 | Xu et al. [45] | Ring Signatures + Hyperledger Fabric | Anonymous blockchain access control | Limited flexibility due to predefined channels |
| 3 | MIT Media Lab [46] | ChainAnchor with Zero-Knowledge Proofs | Anonymous identity verification on blockchain | Conceptual, lacks practical deployment |
| 4 | Hyperledger + ABE [48] | Blockchain + Attribute-Based Encryption | Secure cloud data access control | Privacy concerns with blockchain hash storage |
| 5 | Jemel & Serhrouchni [51] | Multichain + CP-ABE | Fine-grained distributed data access control | Implementation complexity |
| 6 | Delgado-Von-Eitzen (2025) | Blockchain Application Firewall | Improves privacy and access control for Ethereum | Adds architectural complexity |
| 7 | Delgado-Von-Eitzen (2024) | Inter-blockchain communication | Improves interoperability between blockchain systems | Still developing standards |
| 8 | Falazi et al. (2024) | Cross-chain smart contract framework | Classification of cross-chain approaches | Reliance on trusted third parties |
| 9 | Fernández-Iglesias (2024) | Smart contract traceability system | Improves supply chain transparency | Dependence on off-chain storage |
| 10 | Abdallah & Nizamuddin (2023) | Ethereum smart contract supply chain | Secure pharma product distribution | Requires blockchain infrastructure |

Jemel and Serhrouchni [51] proposed a blockchain-based shared data access control mechanism implemented using the Multichain platform and the Ciphertext-Policy Attribute-Based Encryption (CP-ABE) scheme. This system enables fine-grained access control for shared data in distributed environments, allowing authorized users to access encrypted information while maintaining confidentiality and data integrity.

Recent studies have also explored improvements in blockchain infrastructure. Delgado-Von-Eitzen et al. (2025) proposed the concept of a Blockchain Application Firewall (BAF) to enhance privacy and access control in Ethereum-based platforms. The firewall operates as an intermediary layer between users and blockchain services, monitoring incoming and outgoing requests based on predefined access policies. A proof-of-concept implementation using the Besu platform demonstrates that BAF can significantly improve security and enable new blockchain use cases involving private transactions.

Another important research direction focuses on blockchain interoperability. Delgado-Von-Eitzen et al. (2024) investigated methods for enabling seamless interoperability between Ethereum-based blockchain networks using inter-blockchain communication protocols. Blockchain networks are typically isolated systems, which limits data exchange and collaboration across platforms. The study highlights how smart contracts can facilitate cross-chain interactions and support decentralized applications operating across multiple blockchain ecosystems.

Similarly, Falazi et al. (2024) conducted a systematic literature review on Cross-Chain Smart Contract Invocations (CCSCIs). The authors analyzed several academic and industry studies to classify different cross-chain communication

approaches. Their analysis revealed that most existing solutions face challenges such as protocol heterogeneity, dependency on trusted intermediaries, and difficulties in achieving reliable transaction processing across multiple blockchains.

Blockchain technology has also been widely explored in supply chain applications. Fernández-Iglesias et al. (2024) proposed a blockchain-based traceability framework using smart contracts to enhance transparency and reliability in supply chain management. The study compares two approaches: storing complete data on-chain and storing only cryptographic hash references on-chain while keeping detailed data off-chain. The hybrid approach significantly improves scalability and reduces storage costs while preserving data integrity and privacy.

In the pharmaceutical sector, Abdallah and Nizamuddin (2023) proposed a decentralized blockchain framework for pharmaceutical supply chain management. Their system utilizes Ethereum smart contracts to manage interactions between manufacturers, suppliers, and consumers. Smart contracts automatically record transactions, monitor IoT-enabled containers carrying pharmaceuticals, and manage refund policies in case of delivery issues. This approach improves transparency, trust, and security in pharmaceutical product distribution.

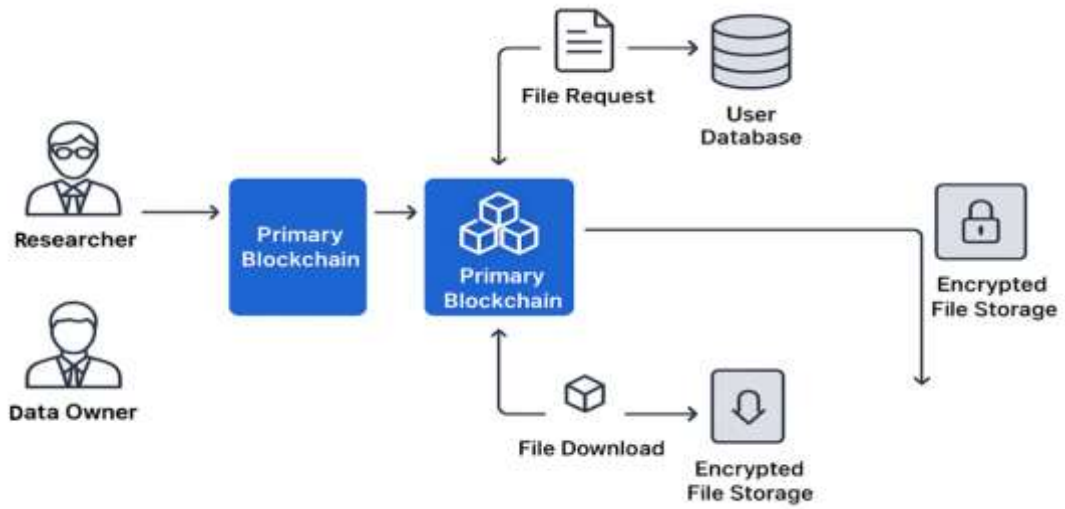
## IV. PROPOSED WORK

The proposed system addresses the inherent contradiction between the public blockchain principle of full data transparency and the need for privacy and controlled access in sensitive applications. While traditional public blockchains like Bitcoin prioritize decentralization and transparency—often relying on anonymity rather than access control—this architecture introduces a dual-blockchain model specifically designed to support confidential data handling through robust access control mechanisms. Recognizing that not all blockchain applications benefit from unrestricted data exposure, the system separates access management and data storage across two interconnected blockchains. The primary blockchain manages authentication and permission verification via smart contracts, while the secondary, isolated blockchain stores sensitive data that can only be accessed following validated authorization. This approach ensures that privacy-sensitive information, such as account balances or medical records, remains protected while still benefiting from blockchain's immutability and decentralization. By doing so, the system resolves the tension between transparency and confidentiality, offering a flexible, blockchain-based access control framework suited for real-world scenarios where data privacy is essential.

PROPOSED SYSTEM ADVANTAGE

- Separation of concerns: Access control and data storage are handled independently.
- Improved security: Sensitive data is stored in an isolated blockchain, not directly accessible.
- Fine-grained access control using smart contracts on the primary blockchain.
- Reduced risk of data leakage due to strict permission checks.
- Better scalability: Each blockchain can scale independently.
- Enables secure inter-chain communication via Hyperledger YUI.

**System Architecture**




As discussed above, blockchain technology is in constant evolution, with blockchain intercommunication being a relevant research topic. However, in the case of interconnecting blockchains with different technologies, progress is slow. In our case, to demonstrate the feasibility of the proposed blockchain based access control system,a PoC was developed using two Ethereum-based blockchains interconnected by means of Hyperledger YUI.5 Hyperledger YUI is an initiative to facilitate the inter connection of heterogeneous blockchains (permissioned blockchains only at this time) following the inter-blockchain communications protocol of the Cosmos project [55], so that communication between chains can be carried out using middleware protocols that are agnostic with respect to the interconnected chains, facilitating interoperability between different platforms. In addition, it allows atomic token exchanges and even atomic execution of arbitrary code. Currently, it provides interconnection modules for public blockchains (Ethereum,BNBSmartChain) and permissioned blockchains (Hyperledger Fabric, Hyperledger Besu, Quo rum and Corda), but the project's goal is to support a broad portfolio of heterogeneous blockchain platforms. Another relevant feature of Hyperledger YUI is cross chain authentication, which allows inter-chain communication through on-chain verification of the state of the other chain, thus ensuring security without relying on the behaviour of off-chain elements. This facilitates the transmission of messages between chains not only to trusted and privileged actors, but also to any user that meets the criteria encoded in access control lists (ACL) in the permissioned chain. This solution does not add new components to the system that could compromise security, as users only interact with their corresponding chains. Thus, for this PoC, two Ethereum blockchains were created. The first chain, called blockchain A, acts as the main access point where users request data (in this case, a user U account). A smart contract (Smart Contract A) was implemented on this chain to manage access requests and verify user permissions according to a predefined list of authorized users. The second chain, blockchain D, contains the sensitive information intended to be accessed only when appropriate permissions are held, as verified by the smart contract in blockchain A. A communication mechanism was designed between these two chains using Hyperledger YUI, ensuring that the information consulted by users remains confidential and is not directly accessible from a single source.

## V. CONCLUSION

The proposed project — Automated Security Assessment and Approval for Conveyed Registering Including Graphical Models for Security — aligns with the emerging need for controlled, decentralized, and secure data management illustrated in modern blockchain access control systems. Similar to the dual-chain architecture discussed in the referenced work, this project implements a layered security mechanism through Primary and Secondary Chains, where the Primary Chain governs access permissions, approvals, and key exchanges, while the Secondary Chain securely stores encrypted file data. By integrating smart contracts, AES-based encryption, and dynamic approval workflows, the system ensures that only authorized entities can access or decrypt sensitive information, preserving confidentiality

and integrity. This design supports adaptable access control, enabling real-time approval, revocation, and monitoring of data usage, addressing key challenges in transparency, privacy, and compliance. Beyond secure file transmission, this framework demonstrates the feasibility of applying blockchain-driven access control in domains such as healthcare, certification management, and data governance — ensuring security, trust, and auditability at every stage of data interaction. Thus, the project not only provides a technically sound proof of concept but also contributes toward building a scalable, privacy-preserving, and trustworthy model for next-generation secure information sharing.

## VI.FUTURE ENHANCEMENT

As a future line of work, we propose implementing this architecture using hardware acceleration technologies such as ASICs or FPGAs to optimize performance in high-demand environments. Integrating FPGA-based co-processors would enable the acceleration of key operations such as cryptographic verification and dynamic permission validation. Meanwhile, ASIC-based solutions could help reduce latency and increase processing capacity in large-scale enterprise deployments. These hardware enhancements would complement the proposed architecture, facilitating its adoption in industrial applications that require real-time access control and high operational efficiency. To sum up, this work contributes significantly to the field of IT security in decentralized applications by proposing an innovative solution for secure and efficient data management using blockchain technology. The combination of blockchain interconnection with smart contracts offers a robust and adaptable framework that sets the path for future standards in dynamic and flexible access control for decentralized applications.

## REFERENCE

[1] S. Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System, 2008, doi: 10.2139/ssrn.3440802.

[2] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, ‘‘A review of blockchain technology applications for financial services,’’ Bench Council Trans. Benchmarks, Standards Eval., vol. 2, no. 3, Jul. 2022, Art. no. 100073, doi: 10.1016/j.tbench.2022.100073.

[3] P. Treleaven, R. Gendal Brown, and D. Yang, ‘‘Blockchain technology in finance,’’ Computer, vol. 50, no. 9, pp. 14–17, 2017, doi: 10.1109/MC.2017.3571047.

[4] Q. Deng, ‘‘Application analysis on blockchain technology in cross-border payment,’’ in Proc.5thInt. Conf.FinancialInnov.Econ.Develop.(ICFIED ), 2020, pp. 287–295, doi: 10.2991/aebmr.k.200306.050.

[5] T.Qiu,R.Zhang,andY.Gao,‘‘Ripplevs.SWIFT: Transforming cross border remittance using blockchain technology,’’ Proc. Comput. Sci., vol. 147, pp. 428–434, Jan. 2019, doi: 10.1016/j.procs.2019.01.260.

[6] E. Ganne, Can Blockchain Revolutionize International Trade?. Geneva, Switzerland: World Trade Organization, 2018.

[7] M. Pournader, Y. Shi, S. Seuring, and S. C. L. Koh, ‘‘Blockchain applications in supply chains, transport and logistics: A systematic review of the literature,’’ Int. J. Prod. Res., vol. 58, no. 7, pp. 2063–2081, Apr. 2020, doi: 10.1080/00207543.2019.1650976.

[8] M. J. Fernández-Iglesias, C. Delgado von Eitzen, and L. Anido-Rifón, ‘‘Efficient traceability systems with smart contracts: Balancing on-chain and off-chain data storage for enhanced scalability and privacy,’’ Appl. Sci., vol. 14, no. 23, p. 11078, Nov. 2024, doi: 10.3390/app142311078.

[9] S. Abdallah and N. Nizamuddin, ‘‘Blockchain-based solution for pharma supply chain industry,’’ Comput. Ind.

Eng., vol. 177, Mar. 2023, Art. no. 108997, doi: 10.1016/j.cie.2023.108997.

[10] A. Ghadge, M. Bourlakis, S. Kamble, and S. Seuring, ‘‘Blockchain implementation in pharmaceutical supply chains: A review and conceptual framework,’’ Int. J. Prod. Res., vol. 61, no. 19, pp. 6633–6651, Oct. 2023, doi: 10.1080/00207543.2022.2125595.

[11] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, ‘‘Blockchain technology applications in healthcare: An overview,’’ Int. J. Intell. Netw., vol. 2, no. 2, pp. 130–139, Sep. 2021, doi: 10.1016/j.ijin.2021.09.005.

[12] A. Hasselgren, P. Kengfai Wan, M. Horn, K. Kralevska, D. Gligoroski, andA.Faxvaag,‘‘GDPRcompliancefor blockchainapplicationsinhealth care,’’ 2020, arXiv:2009.12913.

[13] P. Voigt and A. Von dem Bussche, The EU General Data Protection Regulation (GDPR). Cham, Switzerland: Springer, 2017.

[14] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, ‘‘Blockchain technology in healthcare: A comprehensive review and directions for future research,’’ Appl. Sci., vol. 9, no. 9, p. 1736, Apr. 2019, doi: 10.3390/app9091736.

[15] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, ‘‘BlocHIE: A Blockchain-based platform for healthcare information exchange,’’ in Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP), Jun. 2018, pp. 49–56, doi: 10.1109/SMARTCOMP.2018.00073.

[16] G. Ishmaev, ‘‘Blockchain technology as an institution of property,’’ Metaphilosophy, vol. 48, no. 5, pp. 666–686, Oct. 2017, doi: 10.1111/meta.12277.

[17] P. Bhaskar, C. K. Tiwari, and A. Joshi, ‘‘Blockchain in education man agement: Present and future applications,’’ Interact. Technol. Smart Educ., vol. 18, no. 1, pp. 1–17, May 2021, doi: 10.1108/itse-07-2020-0102.

[18] C. Delgado-Von-Eitzen, L. Anido-Rifón, and M. J. Fernández-Iglesias, ‘‘Application of blockchain in education: GDPR-compliant and scalable certification and verification of academic information,’’ Appl. Sci., vol. 11, no. 10, p. 4537, May 2021, doi: 10.3390/app11104537.

[19] C. Delgado-Von-Eitzen, L. E. Anido-Rifón, and M. J. Fernández Iglesias, ‘‘Blockchain applications in education: A systematic literature review,’’ Appl. Sci., vol. 11, no. 24, p. 11811, Dec. 2021, doi: 10.3390/app112411811.

[20] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalan sky, ‘‘Ensuring data integrity using blockchain technology,’’ in Proc. 20th Conf. Open Innov. Assoc. (FRUCT), Apr. 2017, pp. 534–539, doi: 10.23919/FRUCT.2017.8071359.

[21] J. Bao, D. He, M.Luo, and K.-K.-R. Choo, ‘‘A survey of blockchain applications in the energy sector,’’ IEEE Syst. J., vol. 15, no. 3, pp. 3370–3381, Sep. 2021, doi: 10.1109/JSYST.2020.2998791.

[22] Q. Wang and M. Su, ‘‘Integrating blockchain technology into the energy sector—From theory of blockchain to research and application of energy blockchain,’’ Comput. Sci. Rev., vol. 37, Aug. 2020, Art. no. 100275, doi: 10.1016/j.cosrev.2020.100275.

[23] V. Buterin, ‘‘A next-generation smart contract and decentralized application platform,’’ White Pap., vol. 3, pp. 1–2, Jan. 2014.

[24] E. Androulaki et al., ‘‘Hyperledger fabric: A distributed operating system for permissioned blockchains,’’ in Proc. 13th EuroSys Conf., Apr. 2018, pp. 1–15, doi: 10.1145/3190508.3190538.

[25] N. Szabo, ‘‘Formalizing and securing relationships on public networks,’’ 1st Monday, vol. 2, no. 9, pp. 1–15, Sep. 1997, doi: 10.5210/fm.v2i9.548.

[26] H. Al-Breiki, M. H. U. Rehman, K. Salah, and D. Svetinovic, ‘‘Trustworthy blockchain oracles: Review, comparison, and open research challenges,’’ IEEE Access, vol. 8, pp. 85675–85685, 2020, doi: 10.1109/ACCESS.2020.2992698.

[27] A. Beniiche, ‘‘A study of blockchain oracles,’’ 2020, arXiv:2004.07140.

[28] S.Ellis, A. Juels, and S. Nazarov. (2017). Chainlink: A Decentralized Ora cle Network

[29] S.Suratkar, M.Shirole, and S.Bhirud,‘‘Cryptocurrency wallet: A review,’’ in Proc. 4th Int. Conf. Comput., Commun. Signal Process. (ICCCSP), Sep. 2020, pp. 1–7, doi: 10.1109/ICCCSP49186.2020.9315193.

[30] S. Zhang and G. Mani, ‘‘Popular cryptoassets (Bitcoin, Ethereum, and Dogecoin), gold, and their relationships: Volatility and correlation modeling,’’ Data Sci. Manage., vol. 4, pp. 30–39, Dec. 2021, doi: 10.1016/j.dsm.2021.11.001.

[31] J.Reed,Litecoin:AnIntroductionToLitecoinCryptocurrencyandLitecoin Mining. North Charleston, SC, USA: CreateSpace Independent Publishing Platform, 2017.

[32] S.AggarwalandN.Kumar,‘‘Hyperledger,’’ in The Blockchain Technology for Secure and Smart Applications Across Industry Verticals. Amsterdam, The Netherlands: Elsevier, 2020, pp. 323–343.

[33] Q. Nasir, I. A. Qasse, M. Abu Talib, and A. B. Nassif, ‘‘Performance analysis of hyperledger fabric platforms,’’ Secur. Commun. Netw., vol. 2018, pp. 1–14, Sep. 2018, doi: 10.1155/2018/3976093.

[34] ConsenSys. (Nov. 12, 2024). Tessera.

[35] ConsenSys. (2018). Quorum Whitepaper. [Online]. Available:https://github.com/Consensys/quorum-docs/blob/master/Quorum

[36] A.AlniamyandB.D.Taylor, ‘‘Attribute-based access control of data shar ing based on hyperledger blockchain,’’ in Proc. 2nd Int. Conf. Blockchain Technol., Mar. 2020, pp. 135–139, doi: 10.1145/3390566.3391688.

[37] T. Lyons, L. Courcelas, and K. Timsit, ‘‘Blockchain and the GDPR,’’ European Union Blockchain Observatory and Forum, Brussels, Belgium, Tech. Rep., 2018. [Online]. Available:https://blockchain-observatory.ec.europa.eu/publications/blockchain-and-gdpr_en#files

[38] M. Finck, ‘‘Blockchain and the general data protection regulation: Can distributed ledgers be squared with European data protection law?’’ in Proc. Eur. Parliamentary Res. Service Study, Jul. 2019, pp. 1–44, doi: 10.2861/535.