Whistleblowers' Protection with XRP Ledger

Pavel PANTIUKHOV*, Dmitrii KORIAKOV†, Antonio Ken IANNILLO‡, and Radu STATE§
SEDAN research group, Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg
{pavel.pantiukhov, dmitrii.koriakov, antonioken.iannillo, radu.state}@uni.lu

2024 6th International Conference on Blockchain Computing and Applications (BCCA) | 979-8-3503-5153-8/24/$31.00 ©2024 IEEE | DOI: 10.1109/BCCA62388.2024.10844385

***Abstract*—In the wake of the European Union's directive 2019/1937, aimed at safeguarding whistleblowers reporting breaches of Union law, this paper proposes a novel solution leveraging blockchain technology, specifically the XRP Ledger (XRPL), to establish secure and anonymous communication channels. The proposed architecture integrates XRPL's inherent features, including robust security protocols, anonymization mechanisms, and low transaction costs, to facilitate seamless whistleblower reporting while ensuring data integrity, confidentiality, and immutability. Through a comprehensive design encompassing web application integration, Xaman Wallet functionality, XRPL transaction execution, and secure storage management, the system provides a user-centric and regulatory-compliant platform for whistleblowers to submit reports securely. Furthermore, the paper discusses the proposed solution's feasibility, scalability, security, privacy, and ethical implications, emphasizing its potential to reshape organizational governance, accountability frameworks, and societal trust. This research advances transparency, accountability, and integrity in organizational practices by addressing the imperative need for efficient whistleblower communication channels, fostering a culture of ethical conduct and social responsibility.**

***Index Terms*—whistleblower, XRP Ledger, security, privacy**

I. Introduction

In an era where digital integrity and transparency are paramount, the European Union's directive 2019/1937 [1] represents a significant stride towards safeguarding whistleblowers who report breaches of Union law. This directive, the majority of EU member states have transposed into national law at the time of writing [2], underscores the necessity for robust reporting channels that protect the anonymity and security of individuals who courageously come forward with critical information. In line with this transformative momentum, the European Union (EU) directive 2019/1937 underscores the imperative of safeguarding individuals who report breaches of Union law, thereby necessitating the establishment of robust communication channels for whistleblowers. Despite the legislative mandate and subsequent national implementations across EU member states, a notable gap persists, especially among Small and Medium-sized Enterprises (SMEs) and small governmental bodies, wherein efficient whistleblower communication channels are either lacking or markedly inefficient. This discrepancy underscores a pressing need to explore novel, cost-effective solutions that adhere to regulatory directives and prioritize security, anonymity, and efficacy. Against this backdrop, this research endeavors to address the lacuna in whistleblower communication channels by leveraging the transformative potential of blockchain technology, specifically focusing on the XRP Ledger (XRPL) [3].

The primary objective is to present a use case wherein public blockchain infrastructure, exemplified by XRPL, serves as the cornerstone for implementing secure, anonymous, and cost-effective reporting platforms mandated by EU directive 2019/1937. By harnessing XRPL's inherent features, the proposed architecture aims to facilitate seamless communication channels for whistleblowers while ensuring data integrity, confidentiality, and immutability.

Additionally, the study aims to propose a novel application of blockchain technology, specifically the XRP Ledger, as a solution to this pressing issue. The inherent features of XRPL, including security, anonymity, and low costs, position it as an ideal platform for developing a whistleblower reporting system.

II. Background and Related Work

Blockchain technology has sparked a paradigm shift across various sectors, catalyzing innovation [4], [5], enhancing security [6]–[10], and fostering transparency [11]. In particular, industrial applications have witnessed a surge in blockchain utilization [10], [12]–[15], heralding a new era of decentralized, secure, and intelligent interconnectivity. This technology amalgamates decentralized systems, decentralized applications, and robust authentication mechanisms to foster transparent, secure, and intelligent inter-connectivity within diverse industrial domains. It is characterized by its decentralized nature, eliminating the need for central authorities, thereby reducing bottlenecks and enhancing efficiency. The technology's ability to provide transparent, immutable, and secure transaction records makes it ideal for various industrial sectors, including manufacturing [16], agriculture [17], and transportation [18]. Integrating blockchain technology with industrial processes promises to enhance efficiency, transparency, and accountability. By leveraging distributed ledger systems and smart contracts, industries can streamline operations, automate transactions, and mitigate risks associated with centralized intermediaries. The advent of public blockchains presents a revolutionary frontier in financial technology and regulatory compliance [19]. They offer a compelling

solution for addressing regulatory compliance mandates; however, integrating blockchain technology into existing regulatory frameworks presents several challenges and opportunities. On the one hand, blockchains can simplify regulatory reporting by providing regulators with real-time access to verified data. They can enhance compliance processes by enabling better tracking of steps required by complex regulations. On the other hand, most public blockchains have high transaction fees, which can make this application unaffordable.

EU Directive 2019/1937 emphasizes the need for **secure, anonymous communication channels to protect whistleblowers**, i.e., individuals reporting breaches of European Union law. It mandates establishing such channels to ensure anonymity and protection against retaliatory measures. However, their practical implementation, particularly among SMEs and small governmental bodies, remains a significant challenge, necessitating innovative solutions to bridge the regulatory-implementation gap.

The XRP Ledger (XRPL) is a beacon of innovation and reliability in blockchain technology. As an open-source, permissionless, and decentralized platform, it has seamlessly operated for over a decade, underpinning a myriad of real-world solutions and value-creation endeavors. At the heart of XRPL lies a vibrant global community comprising businesses and developers. Their collaborative efforts not only address tangible challenges but also foster an environment of inclusivity. With an open invitation extended to all, XRPL epitomizes true decentralization, ensuring accessibility and participation for anyone keen on contributing or building upon its foundation. XRPL boasts an impressive track record, having processed over 63 million ledgers without any significant issues. Its transaction settlement speed, a mere 3-5 seconds, outshines many other platforms in the blockchain landscape. Moreover, its streamlined development process empowers creators to bring their ideas to life efficiently, fostering innovation. Fueling the XRPL ecosystem is XRP, its native digital asset, utilized as a transaction cost. Remarkably economical, at the time of writing, any transaction on XRPL costs 0.00001 XRP, the equivalent of about 0.50 USD. This affordability broadens the spectrum of blockchain applications and accommodates a diverse array of use cases, ranging from micropayments to large-scale financial transactions. Security is a top priority in XRPL's framework, bolstered by robust protocols designed to fend off spam and denial-of-service attacks. Each transaction requires a small amount of XRP, a mechanism that adjusts dynamically to mitigate network overload risks. XRPL also demonstrates forward-thinking by embracing post-quantum cryptography, strengthening its defenses against potential threats from quantum computing. Embracing regulatory compliance, XRPL seamlessly integrates with mandates such as EU directive 2019/1937. Its suite of security features, anonymization mechanisms, and minimal transaction costs render it an optimal choice for implementing communication channels. Specifically, it provides a cost-effective avenue for facilitating whistleblower reporting while upholding data integrity, confidentiality, and immutability.

XAMAN [20], formerly known as Xumm, stands as a prominent non-custodial wallet tailored specifically for the XRP Ledger, affording users complete autonomy over their assets. Unlike traditional custodial solutions, no third party retains control over user keys, ensuring heightened security and trust. Through passcodes or biometric authentication (fingerprint or face ID), users seamlessly access their XRP holdings directly, fostering a personalized and secure user experience. One of XAMAN's paramount functionalities is its seamless interaction with the XRP Ledger. Whether users send or receive XRP, manage accounts, or explore ledgers, XAMAN facilitates a user-friendly interface, eliminating barriers and simplifying asset management. It also facilitates the generation of new XRP Ledger accounts within its interface or the importation of existing ones, ensuring flexibility and convenience for users. Managing multiple accounts is streamlined, ensuring optimal utilization of the XRP Ledger without compromising on security protocols. Security remains at the forefront of XAMAN's priorities, underscored by rigorous auditing processes to fortify its protective measures. Furthermore, integrating XAMAN Tangem cards merges usability with Tangem NFC hardware wallet support, augmenting user security provisions. For developers, XAMAN serves as a fertile ground for exploration and innovation. The platform empowers developers to create their own applications, unleashing the full potential of XAMAN for both developers and end-users.

The proposed whistleblower protection system has been validated through a proof-of-concept implementation tailored for industrial environments. This pilot study involved collaboration with stakeholders, including legal experts from big companies, SMEs, and regulatory bodies, demonstrating the systemś efficacy in ensuring secure and anonymous whistleblower reporting.

III. Design and Architecture

The architectural design presented here aims to provide a robust and secure platform for whistleblowers to report breaches of European Union law in compliance with EU directive 2019/1937. The system utilizes the XRP Ledger (XRPL) as the underlying blockchain infrastructure. At its core, the system comprises interconnected components, including a web application, Xaman Wallet integration, XRPL, and secure storage, each fulfilling distinct roles within the ecosystem. The architecture provides a user-centric, regulatory-compliant whistleblower reporting and management

platform through seamless integration and orchestrated functionality.

The **Web Application** serves as the primary interface through which users interact with the reporting system. It facilitates user authentication, anonymous wallet management, report submission, and access to encrypted reports. Additionally, the web application orchestrates communication with other system components, including Xaman Wallet integration for wallet creation and XRPL for transaction execution.

The **Xaman Wallet integration** plays a pivotal role in enabling seamless wallet creation and management within the system. Leveraging Xaman Wallet's capabilities, the web application interfaces with the Xaman Wallet platform to securely generate new anonymous wallets for authenticated users. This integration ensures adherence to anonymity requirements while providing users a seamless experience.

The **XRP Ledger** is the foundational infrastructure for facilitating secure and immutable transactions within the whistleblowers' protection system. Leveraging XRPL's robust security protocols and low transaction costs, the system executes transactions related to report submission (NFT minting and NFT offer management). XRPL's decentralized architecture ensures resilience against attacks and guarantees the integrity of transactional data. Industrial environments often require the handling of large volumes of data and transactions.

The **Secure Storage** forms the system's data management strategy's backbone, ensuring encrypted reports' confidentiality and integrity. Reports submitted by whistleblowers are encrypted and securely stored locally, on cloud infrastructure, or utilizing InterPlanetary File System (IPFS) technology. Each report is linked to a corresponding non-fungible token (NFT) via a cryptographic hash, facilitating traceability and auditability.

A. Authentication to the Web Application

Users authenticate to the web application using secure authentication mechanisms, such as username/password credentials or multi-factor authentication (MFA). Authentication ensures the integrity of user identities and restricts access to authorized individuals.

B. Management of Anonymous Wallets

Upon authentication, the web application allows users to generate new anonymous wallets, leveraging Xaman Wallet integration. Each user can create unique anonymous wallets, ensuring anonymity throughout the reporting process while maintaining traceability for auditing purposes.

C. Report Submission

Whistleblowers can submit reports securely through the web application, initiating a multi-step process. The report submission process involves creating a message, encrypting it using robust cryptographic algorithms, uploading it to the secure storage, minting an NFT containing a reference to the report, and making an offer to the organization to acquire ownership of the NFT. Figure 1 shows the interactions among the components to report a submission.

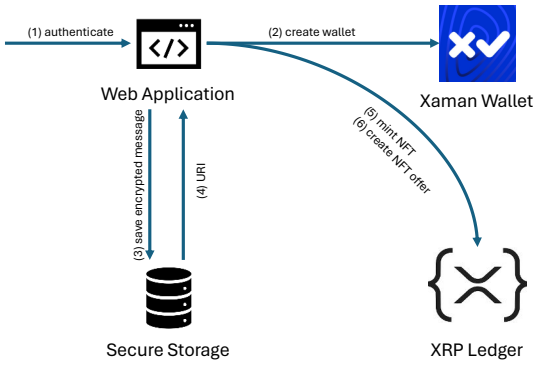

Fig. 1. Architectural Components for the Establishment of Reporting Channels.

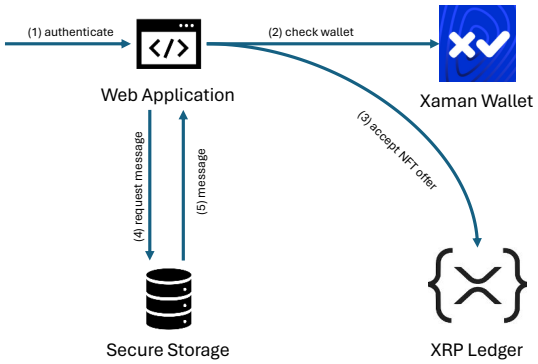

Fig. 2. Architectural Components for the Establishment of Reporting Channels.

D. Access Report

Authorized individuals can access encrypted reports in secure storage. Access to reports is facilitated through the web application, which decrypts and presents the reports to authorized users while ensuring confidentiality and integrity.

Figure 2 shows the interactions among the components for a whistleblower to report a submission.

E. Exchange Messages

In addition to whistleblower submissions, the system facilitates communication for organizations to respond to reported incidents or initiate dialogues with whistleblowers. While the organization replies to the report, the web application performs the same operations of report submission (cfr. subsection III-C) to transfer the message. From the other side, the whistleblower can access the reply in the same way organizations access report (crf. subsection III-D) and, eventually, keep the conversation with a new message.

This two-way communication framework enables organizations to address concerns, provide clarifications, or collaborate with whistleblowers in resolving issues related to regulatory compliance.

F. Security Measures

The architectural design outlined above incorporates a multifaceted approach to security, addressing various aspects of confidentiality, integrity, authentication, and resilience against cyber threats. Below, we delve into the security measures implemented across different system architecture components. However, before discussing the specific security measures, conducting a comprehensive threat modeling exercise is crucial to identifying potential threats and vulnerabilities inherent in the system. Threat modeling allows for a proactive approach to security by anticipating potential attack vectors and designing mitigating controls accordingly. In the context of this whistleblowers' protection system, threat modeling would involve considering threats such as:

- unauthorized access to sensitive reports,
- tampering with transactional data on the XRPL, and
- exploitation of vulnerabilities in the web application or wallet integration.

Data confidentiality is paramount in a system designed to handle sensitive information submitted by whistleblowers. To ensure confidentiality, robust encryption standards are employed throughout the system. Reports submitted by whistleblowers are encrypted before being stored in secure storage. Additionally, the web application facilitates access to encrypted reports, decrypting the data only for authorized users. Advanced encryption techniques, such as asymmetric encryption for key exchange and symmetric encryption for data transmission, are utilized to safeguard the confidentiality of sensitive information.

Access control mechanisms are crucial for enforcing the principle of least privilege and preventing unauthorized access to system resources. In the web application, user authentication uses secure mechanisms such as username/password credentials and multi-factor authentication (MFA). This ensures that only authenticated and authorized users can access the system functionalities. Furthermore, access to encrypted reports stored in secure storage is restricted to authorized individuals, preventing unauthorized disclosure of sensitive information.

Effective key management is essential for maintaining the integrity and confidentiality of encrypted data. The system employs robust key management practices to generate, store, and exchange cryptographic keys securely. During report submission, the organization's public key is used to encrypt the report so that only the organization itself can read it. Eventually, the whistleblower's public key is used to encrypt the messages sent by the organization. Key rotation and revocation mechanisms are also implemented to mitigate the risk of key compromise and unauthorized decryption. The system architecture leverages decentralized and resilient technologies (i.e., XRPL) to enhance resilience against cyber threats. XRPL's decentralized architecture ensures that no single point of failure exists, reducing the risk of data manipulation or unauthorized access. By leveraging XRPL's inherent security features, the system enhances resilience against attacks and guarantees the integrity of transactional data.

G. Compliance of EU Directive 2019/1937

The architectural design is meticulously crafted to adhere to the requirements outlined in "Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law".

The system places utmost importance on the confidentiality and anonymity of whistleblowers throughout the reporting process. By leveraging robust encryption standards and advanced cryptographic algorithms for report encryption and storage, the system ensures that whistleblowers can submit reports securely without fear of reprisal or disclosing their identities. Moreover, the integration with Xaman Wallet enables the creation of anonymous wallets, ensuring that whistleblowers' identities remain protected while maintaining traceability for auditing purposes. The directive mandates traceability and auditability of reported breaches. To meet this requirement, the system implements robust measures that ensure accountability and transparency in the reporting process. Each report submitted by a whistleblower is linked to a corresponding non-fungible token (NFT) via a cryptographic hash, facilitating traceability and auditability. Administrators can track each report's submission and acceptance history, ensuring accountability throughout the process. Furthermore, utilizing XRPL for transaction execution enhances transactional data's integrity and immutability, further bolstering the system's traceability and auditability. Compliance with Authentication Requirements EU Directive 2019/1937 also mandates secure authentication mechanisms to ensure the integrity of user identities and restrict access to authorized individuals. The system complies with these requirements by implementing secure authentication mechanisms such as username/password credentials and multi-factor authentication (MFA). This ensures that only authenticated users can access the system functionalities, bolstering security and compliance with the directive.

IV. Discussion

A. Feasibility and Scalability

While blockchain's transformative potential is evident, widespread adoption across diverse industrial sectors necessitates meticulous planning, seamless integration, and robust infrastructure support. Utilizing

the XRP Ledger (XRPL) presents several advantages in terms of scalability and efficiency. With its low transaction costs and decentralized architecture, XRPL offers a viable solution for implementing secure and cost-effective whistleblower reporting systems, especially for small and medium-sized enterprises (SMEs) with limited resources. However, challenges may arise concerning the scalability of blockchain networks. Efforts to optimize network performance and scalability are paramount to ensuring the system's efficacy and reliability. Furthermore, the feasibility of integrating blockchain technology into existing organizational frameworks hinges on factors such as regulatory compliance, interoperability with legacy systems, and organizational readiness for technological adoption. While the proposed solution aligns closely with regulatory directives such as EU directive 2019/1937, seamless integration requires collaborative efforts between regulatory bodies, industry stakeholders, and technology providers. Scalability concerns extend beyond technical considerations. Access, affordability, and ease of implementation are essential for widespread adoption and scalability. Collaborative initiatives, knowledge-sharing platforms, and incentivization mechanisms can foster a conducive ecosystem for blockchain adoption, facilitating scalability and sustainability.

To support the feasibility of the proposed solution, a proof-of-concept implementation has been developed, showcasing the seamless integration of blockchain technology and robust security measures. Leveraging Node.js for the frontend, XRPL as the blockchain infrastructure, local storage for simplicity, and industry-leading encryption algorithms such as AES-256 for data encryption, the proof-of-concept demonstrates the system's capabilities in ensuring confidentiality, integrity, and compliance with regulatory directives. In the proof-of-concept implementation, the storage mechanism is kept local for simplicity, facilitating rapid prototyping and testing. This approach allows for quick iteration and validation of key system functionalities without the complexities associated with cloud or distributed storage solutions. However, the architecture is designed to seamlessly integrate with cloud infrastructure or decentralized storage systems such as IPFS for scalability and resilience in production environments. The proof-of-concept implementation features a user-friendly interface designed to streamline the process and enhance user experience, as presented in Figure 3. The web application interface is intuitive and accessible, guiding users through each step of the reporting process while prioritizing usability and clarity.

B. Security and Privacy Implications

The proposed solution prioritizes security and privacy, leveraging advanced encryption techniques, decentralized infrastructure, and robust authentication mechanisms to safeguard sensitive information

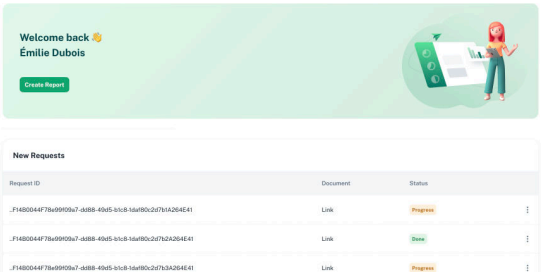

Fig. 3. Web Application UI.

and protect whistleblower identities. By harnessing XRPL's inherent security features, including robust security protocols and anonymization mechanisms, the system enhances resilience against cyber threats and guarantees data integrity, confidentiality, and immutability. However, while blockchain technology offers inherent security benefits, it also introduces unique security challenges, including smart contract vulnerabilities, consensus mechanism attacks, and privacy concerns. Mitigating these risks requires a proactive approach to security, encompassing threat modeling, vulnerability assessments, and ongoing monitoring and mitigation strategies. Additionally, compliance with data protection regulations such as GDPR (General Data Protection Regulation) is paramount to safeguarding user privacy and ensuring regulatory compliance.

Anonymity and confidentiality are central tenets of the protection mechanisms. The proposed solution ensures whistleblower anonymity through anonymous wallets and encrypted communications, bolstering trust and encouraging whistleblowers to come forward without fear of reprisal. However, maintaining a delicate balance between anonymity and accountability is essential to prevent misuse of the platform for malicious purposes. Implementing robust identity verification mechanisms and audit trails can enhance accountability while preserving whistleblower anonymity.

C. Ethical and Societal Implications

Adopting blockchain technology in whistleblower protection systems has profound ethical and societal implications, reshaping organizational governance, accountability frameworks, and societal trust. By empowering whistleblowers to report breaches of Union law anonymously and securely, the proposed solution promotes transparency, accountability, and integrity within organizations and society at large. However, the ethical implications of whistleblower protection extend beyond technological considerations to encompass broader societal values such as justice, fairness, and social responsibility. Protecting whistleblowers from retaliation, ensuring due process, and fostering a culture of ethical conduct is essential for upholding

organizational integrity and societal trust. Moreover, addressing power imbalances, promoting diversity and inclusion, and fostering ethical leadership are critical components of a holistic approach to whistleblower protection. The societal impact of whistleblower protection mechanisms extends beyond individual organizations to encompass systemic change, legislative reform, and cultural transformation. By raising awareness of ethical issues, promoting accountability, and empowering individuals to speak truth to power, whistleblower protection systems are pivotal in promoting democratic values, corporate accountability, and social justice.

V. Conclusion and Future Work

In conclusion, this research paper has presented a comprehensive architectural design leveraging blockchain technology, specifically the XRP Ledger (XRPL), to address the imperative need for secure and anonymous whistleblower communication channels mandated by EU directive 2019/1937. The proposed solution not only offers a novel approach to enhancing organizational governance, accountability frameworks, and regulatory compliance mechanisms, but also addresses a common challenge faced by Small and Medium-sized Enterprises (SMEs). The proposed solution aligns closely with the requirements outlined in EU directive 2019/1937, emphasizing key aspects such as confidentiality, anonymity, traceability, auditability, and security. This alignment is not just a mere coincidence, but a testament to our thorough understanding and compliance with the directives. It ensures regulatory bodies that the system is in full compliance with the directives, promoting transparency, accountability, and integrity within organizations, instilling a sense of confidence in the regulatory bodies. The proposed system leverages XRPL's inherent scalability features, such as low transaction costs and high transaction throughput. Additionally, strategies such as sharding and layer-two solutions are explored to further enhance scalability, accommodating the demands of large-scale industrial applications. Secondly, ongoing research is needed to address emerging security challenges associated with blockchain technology. Proactive security measures, including threat modeling, vulnerability assessments, and ongoing monitoring, safeguard sensitive information and preserve whistleblower anonymity. Additionally, future research could explore the ethical and societal implications of whistleblower protection mechanisms, particularly concerning power dynamics, social justice, and cultural transformation.

Acknowledgment

We thankfully acknowledge the support from the RIPPLE University Blockchain Research Initiative (UBRI) for our research.

References

[1] E. W. Directive, "Directive (eu) 2019/1937 of the european parliament and of the council of 23 october 2019 on the protection of persons who report breaches of union law," 2019.
[2] Whistleblowing monitor. [Online]. Available: https://www.whistleblowingmonitor.eu/
[3] Ripple. (2024) XRPL: The ripple protocol consensus algorithm. [Online]. Available: https://xrpl.org/
[4] H. L. Lee, M. H. A. Au, and S.-F. Sun, "Blockchain-based trustless fair payment protocol for verifiable confidential outsourcing computation," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 221–228.
[5] W. Yao, Y. Liu, F. P. Deek, and G. Wang, "ibctrans: A practical blockchain-based framework for cellular vehicular-to-everything networks," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 239–246.
[6] C. Dong, S. Pal, Q. An, A. Yao, F. Jiang, Z. Xu, J. Li, M. Lu, Y. Song, S. Chen *et al.*, "Securing smart uav delivery systems using zero trust principle-driven blockchain architecture," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 315–322.
[7] V. Biró, W.-Y. Chiu, and W. Meng, "Securing iot firmware dispatch systems with blockchain," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 229–238.
[8] Z. Lin and S. S. Yau, "A blockchain-based approach to improving smart home security with situation-aware access control," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 340–347.
[9] X. Zhang, X. Tan, J. Xu, S. Luo, and Z. Qi, "A trusted sharing model for risk information of food full-process and all-information based on blockchain and federated learning," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 186–191.
[10] R. Huo, D. Ni, and Z. Shao, "Trusted access control mechanism for intelligent manufacturing based on decentralized identifier," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 192–197.
[11] I. Homoliak, Z. Li, and P. Szalachowski, "Bbb-voting: Self-tallying end-to-end verifiable 1-out-of-k blockchain-based boardroom voting," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 297–306.
[12] C. Chi, W. Chen, H. Liu, X. Li, and F. Meng, "The ecological system of digital asset markets: Based on the perspective of asset trading and valuation," in *2023 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2023, pp. 215–220.
[13] T. Alladi, V. Chamola, R. Parizi, and K.-K. R. Choo, "Blockchain applications for industry 4.0 and industrial iot: A review," *IEEE Access*, vol. 7, pp. 176 935–176 951, 2019.
[14] J. Al-Jaroodi and N. Mohamed, "Blockchain in industries: A survey," *IEEE Access*, vol. 7, pp. 36 500–36 515, 2019.
[15] A. Tyagi, S. Dananjayan, D. Agarwal, and H. F. T. Ahmed, "Blockchain—internet of things applications: Opportunities and challenges for industry 4.0 and society 5.0," *Sensors (Basel, Switzerland)*, vol. 23, 2023.
[16] S. R. Talpur, H. Sikandar, A. F. Abbas, and J. Ali, "Revolutionizing manufacturing with blockchain technology: Opportunities and challenges," *International Journal of Online and Biomedical Engineering (iJOE)*, 2023.
[17] J. Ordóñez, A. Alexopoulos, K. Koutras, A. P. Kalogeras, K. Stefanidis, and V. M. Martos, "Blockchain in agriculture: A pestels analysis," *IEEE Access*, vol. 11, pp. 73 647–73 679, 2023.
[18] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, and U. Biswas, "Blockchain for intelligent transportation systems: Applications, challenges, and opportunities," *IEEE Internet of Things Journal*, vol. 10, pp. 18 961–18 970, 2023.
[19] C. Baum, J. Chiang, B. David, and T. Frederiksen, "Sok: Privacy-enhancing technologies in finance," pp. 12:1–12:30, 2023.
[20] XRPL Labs, "XAMAN: A non-custodial wallet for the xrp ledger," 2024, accessed: April 2024. [Online]. Available: https://xumm.app/