Safeguarding user Data: Blockchain as an Enabler of Advanced Consent Management Systems

Siva Sai Teja Bodineni[1*], [2]Sai Lokesh Boddu,[3] Dr.D. Geethanjali

[1,2,3]Sathyabama Institute Of Science And Technology, Chennai,India

[*1]sivasaitejabodineni143@gmail.com,
[2]sailokeshboddu12@gmail.com,
[3]geethanjali.d.cse@sathyabama.ac.in

Abstract. Introducing the concept of leveraging blockchain technology for advanced con-sent management systems, this work underscores the critical need for safeguard-ing user data in today's digital landscape. By exploring the decentralized and immutable nature of blockchain, the abstract posits it as a robust platform for ensuring the secure handling of consent. Emphasizing the transparency and cryp-tographic features inherent in blockchain, the document outlines how these as-pects can elevate consent mechanisms and foster trust between users and service providers. Furthermore, the abstract discusses the potential of smart contracts to automate consent management processes, ensuring efficient and reliable execu-tion. The proposed system seeks to redefine user data protection, establishing a secure and trustworthy digital environment.

Keywords: Blockchain, consent management, user data security, privacy, digital trust, decentralized systems, cryptographic features, smart contracts, automated processes, data protection, advanced consent mechanisms, trustworthiness, transparency, digital era, secure platforms, immutable records, efficient execution, service providers.

1 Introduction

As technology rapidly advances, the need for safeguarding user data has become more critical than ever. With the advent of the internet and digital services, individuals are constantly sharing their personal information, sometimes unknowingly, with various organizations and platforms. This has raised concerns about privacy and the misuse of personal data. To address these concerns, advanced consent management systems have emerged as an effective solution, and blockchain technology has emerged as an enabler of such systems. Blockchain, the technology behind cryptocurrencies like Bitcoin, is a decentralized and distributed ledger system that ensures transparency, security, and immutability. These characteristics make it a reliable tool for managing and securing

K. R. Madhavi et al. (eds.), *Proceedings of the International Conference on Computational Innovations and Emerging Trends (ICCIET 2024)*, Advances in Computer Science Research 112,
https://doi.org/10.2991/978-94-6463-471-6_52

sensitive information, including user consent. Consent management systems built on blockchain can provide individuals with more control over their personal data and how it is used.

One of the key features of blockchain-based consent management systems is the ability to provide users with granular control over their data. With traditional consent management systems, users often have limited options for managing their consent settings. They either have to agree to a blanket consent or opt out of using the service altogether. In contrast, blockchain-based systems allow users to specify their consent preferences for each data type and even for different purposes. This ensures that users have complete control over who can access and use their data, eliminating unnecessary data sharing and potential misuse.

Furthermore, blockchain technology ensures the integrity and security of user consent. The distributed nature of the blockchain network means that data is stored and verified across multiple nodes, making it nearly impossible for any single entity to tamper with or manipulate the consent data. Additionally, the use of cryptographic techniques ensures that user consent remains confidential, with only authorized parties having access to the encrypted data. This not only protects user privacy but also builds trust between users and organizations.

Another advantage of blockchain-based consent management systems is the increased transparency they provide. Traditional consent management systems are often opaque, with users having little insight into how their data is being used. Blockchain technology, on the other hand, allows for a transparent and auditable record of consent. Every transaction and update to the consent settings is recorded on the blockchain, providing users with a clear view of who has accessed their data and for what purpose. This transparency promotes accountability and ensures that organizations are held responsible for their data practices.

In conclusion, the growing concerns over user data protection have necessitated the development of advanced consent management systems. Blockchain technology offers an ideal solution for building these systems, as it ensures data integrity, user control, and transparency. By leveraging blockchain, organizations can establish a secure and user-centric approach to managing consent, empowering individuals to protect their personal information and have greater confidence in sharing it with trusted entities.

2 Related Works

[1] Huang and Lv (2023), which focuses on the technological and engineering innovations it provides to electronic bill systems. The report emphasizes how blockchain technology has the ability to protect user data and improve consent management methods. It also improves data security and privacy in bill transfers. [2] Miltiadou, et al. (2022), proposed how a blockchain technology enhance customization and trust in digital banking. It improves the administration of clients' consent and provides guarantee of secure data sharing. [3] Rana, and et al., (2022), examines the blending of blockchain technology and artificial intelligence to create a decentralized access control paradigm for the healthcare industry. It also enables the secure interoperability and strengthening the security of healthcare data with efficient management of the user consent. [4] Goint, and et al., (2023) investigates how blockchain technology protecting the user data, accessing control privileges of the data through off-chain storage system. [5] Selvarajan, and et al., (2023), describes a blockchain cybersecurity model for healthcare systems that is built on quantum trust and consultative transactions. This work also suggests a consultative transaction-based method to guarantee safe and clear transactions, boosting user consent management and data protection in healthcare systems.

[6] Peyrone and et al., (2023), presented a novel method for managing and protecting user data through blockchain-based solutions in an effort to address the growing concerns over data privacy and user consent in the digital era through cutting-edge security and privacy features. [7] Mukkala, A. and et al., (2022), investigates how blockchain technology, utilizing artificial intelligence (AI) for improved privacy and data control, can provide safe and transparent consent management. This research shows how blockchain technology and AI can work together to alleviate privacy issues and offer cutting-edge safeguards for user data. [8] Barbaria et al. (2022) examines the significance of blockchain technology in providing sophisticated permission management systems for protecting user data in the healthcare systems. For ease of access, the patient data has been shared in the decentralized network through the secure and reliable channels. This system also improves the ability of consent management, guarantee of data integrity and privacy in the health care environment. [9] Roosan et al. (2022) suggests a framework that integrates blockchain technology with artificial intelligence. This framework makes use of cutting-edge permission management tools to improve data security and privacy. According to the report, consumers can exert more control over their data and uphold transparency in the usage and access of their personal health information by utilizing blockchain. [10] Kareem and et al., (2023) describes the development of a decentralized personal identifiable information (PII) management system that makes use of the blockchain dBFT consensus algorithm. The authors investigate how, in circumstances pertaining to higher education, this approach might enhance consent management and protect user data.

[11] Merlec and et al., (2021), proposed a smart contract-based dynamic consent management system for personal data usage under the General Data Protection Regulation (GDPR). The system revolves around the concept of dynamic consent, where users can grant or revoke their consent for the usage of their personal data. By leveraging smart contracts, the system provides a transparent and auditable way of managing data access

and usage permissions. [12] Keshk and et al., (2021) presented a privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems. The authors focus on the challenges arising from the integration of various data sources, including sensor data, social media data, and other forms of data generated in cyber-physical systems. The proposed schemes aim to ensure the privacy and security of data while enabling effective data analysis and decision-making. [13] Karisma and et al., (2023) proposed a data protection governance framework as a solution for blockchain-enabled applications. The authors highlight the need for a comprehensive framework that addresses privacy and security concerns in blockchain systems. The framework includes privacy enhancement techniques, such as pseudonymization, encryption, and access control mechanisms, to ensure the protection of user data throughout the blockchain applications. [14] Mahesh and et al., (2022), presented a trustworthy platform for safeguarding and validating educational credentials using blockchain technology. The authors highlight the importance of secure and tamper-proof verification of educational credentials, particularly in the context of online education and remote learning. The proposed platform utilizes blockchain to establish trust and transparency in the validation process, ensuring that educational credentials are reliable and immutable. [15] Islam and et al., (2022), discussed the integration of blockchain into supply chain management, specifically safeguarded by physically unclonable function (PUF)-enabled RFID technology. The authors address the challenges of supply chain security, including counterfeit products, unauthorized access, and data tampering. By combining blockchain and PUF-enabled RFID, the proposed solution enhances the traceability and integrity of supply chain data, ensuring the authenticity of products and mitigating potential risks.

3 Existing System

The existing system for safeguarding user data is plagued with numerous disadvantages. One of the major drawbacks is the lack of user control and consent management. Users often have little control over their personal data once it is collected by companies or institutions. This lack of control leads to a disproportionate power dynamic, where users have no say in how their data is used, shared, or monetized.

The current system's centralization is an additional drawback. Since most user data is handled and kept in centralized systems, hacking and data breaches are a possibility. Serious repercussions from these hacks may include identity theft, monetary loss, and harm to one's reputation. Furthermore, governments and other organizations can more easily access and exploit user data for surveillance or other purposes due to the centralized nature of data storage.

Moreover, there is a lack of accountability and transparency in the current system. Frequently, users are unaware of who is accessing or how their data is being utilized. Users find it challenging to make educated judgments regarding their security and privacy as a result of this lack of openness. A further common issue is the absence of accountability for organizations and businesses that abuse or improperly manage user data. The loop of data breaches and privacy violations is sustained by this lack of accountability.

Finally, the current system is expensive and ineffective. Companies and organizations may suffer large financial losses as a result of security events and data breaches. There are significant expenses related to protecting and handling user data. An additional layer of complication and expense is added by the fact that the current system manages user data through intermediaries and other organizations.

Blockchain technology has promise in mitigating these drawbacks and facilitating sophisticated consent management frameworks. Users may choose who has access to their data and exert more control over it by taking use of the decentralized nature of blockchain technology. Additionally, blockchain offers immutability and transparency, enabling users to monitor and confirm the usage of their data. Furthermore, using smart contracts can guarantee that data is only used for the objectives that have been agreed upon and help with the automatic enforcement of consent. All things considered, blockchain has the power to completely transform the current system and give users greater security, control, and visibility over their personal information.

4 Proposed System

Leveraging the decentralized and immutable characteristics of blockchain technology to improve the privacy and security of user data is the suggested effort for protecting user data through the usage of blockchain as an enabler of advanced consent management systems. Blockchain shows enormous promise in resolving the growing concerns about data privacy and the growing need for user consent management.

First off, consent management systems can be made decentralized by using blockchain technology, doing away with the requirement for a middleman or central authority to handle user data. This guarantees that user permission and data are securely managed and kept across a network of nodes, thereby lowering the danger of a single point of failure. The blockchain can be used to record each user's consent, resulting in an audit trail that is transparent, unchangeable, and simple to authenticate.

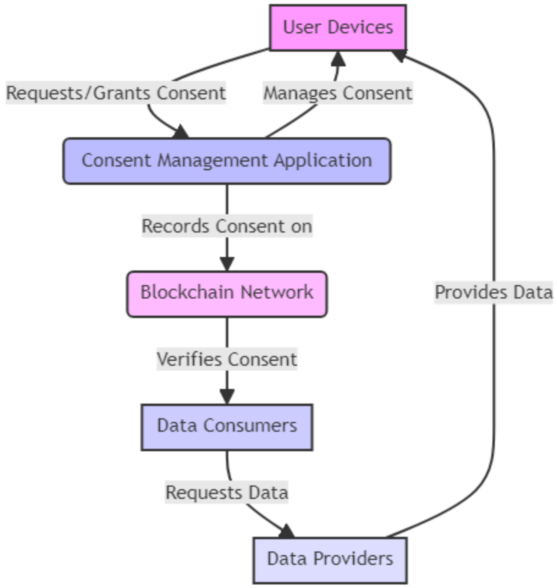


Fig. 1 System architecture of the proposed system

Moreover, smart contracts which may automate and enforce consent agreements between consumers and service providers can be used with blockchain technology. These smart contracts can manage consent preferences more easily, provide consumers with explicit terms and conditions, and describe data usage regulations. Furthermore, predetermined restrictions for data access and usage can be coded into smart contracts, guaranteeing that data is only accessed and used with the authorization of the user.

Giving people more control over their data is another benefit of employing blockchain for consent management. Users can choose which companies have access to their data and securely manage their consent preferences with blockchain technology. Additionally, they can simply withdraw their agreement at any moment, instantly changing the blockchain to reflect their new choices. Because of the increased accountability and openness, people are more confident in how their data is handled.

The proposed system provides a lot of advantages to the suggested approach for protecting user data by utilizing blockchain technology to support sophisticated consent management systems. It makes use of blockchain's decentralized and unchangeable features to improve user control, security, and privacy of data. Blockchain can give users more transparent consent agreements, automate consent management procedures, and boost user confidence in the management of their data by leveraging smart contracts and producing an open audit trail.

5 Methodology

1. Contract Deployment and Initialization:

The system initiates by deploying the smart contract defined in the Consent.sol file onto the Ethereum blockchain. Using Hardhat, the contract's bytecode and ABI (Application Binary Interface) are compiled, and a contract factory is created.The Ethereum provider and wallet are initialized to interact with the blockchain, and the contract factory deploys the contract. Upon deployment, the contract address and the owner's address are logged for reference. If the /src directory exists, the artifacts and contract configurations are copied into it for frontend integration.

2.User Consent Management:
The frontend components (GiveConsent, CheckConsent, RevokeConsent) allow users to manage their consent preferences.When a user interacts with these components, they connect to the Ethereum blockchain through a Web3 provider.The GiveConsent component enables users to grant consent for data sharing by invoking the giveConsent function of the deployed contract.Conversely, the RevokeConsent component allows users to revoke previously granted consent using the revokeConsent function.The CheckConsent component enables users to verify if consent records exist for specific data recipients by calling the checkConsent function.
These interactions are facilitated through Ethereum transactions, ensuring data integrity and transparency on the blockchain

.
3. Blockchain Integration and Data Security:
Ethereum's blockchain is leveraged to provide a decentralized and tamper-resistant platform for consent management.Smart contracts are utilized to enforce consent rules and record consent decisions transparently on the blockchain.User data is encrypted and securely stored off-chain, with only hashed references or identifiers stored on the blockchain to ensure privacy and compliance with GDPR regulations.Fine-grained access controls are implemented within the smart contract to restrict data access to authorized entities only, enhancing data security and privacy.Through integration with Metamask or similar Ethereum wallet providers, users can securely interact with the blockchain and manage their consent preferences in a user-friendly manner

.
4. Frontend Integration and User Experience:
The frontend components are designed to provide a seamless and intuitive user experience for managing consent preferences.Components such as input forms, dropdown menus, and buttons allow users to easily input their preferences and submit transactions to the blockchain.Feedback mechanisms, such as toast notifications, inform users of the success or failure of their consent transactions, enhancing transparency and trust in the system.Integration with React Router enables smooth navigation between different consent management functionalities, providing users with a cohesive experience.

5. Testing and Deployment:
The system undergoes thorough testing to ensure the reliability, security, and functionality of the consent management functionalities.Automated tests, such as unit tests and integration tests, are executed to validate the behavior of smart contracts and frontend components.Once testing is complete, the system is deployed to a production environment, making it accessible to users for real-world consent management scenarios.
Overall, the implemented system utilizes blockchain technology and smart contracts to provide a transparent, secure, and user-centric approach to consent management, empowering users to control their data sharing preferences while ensuring compliance with privacy regulations.

6 Results and Discussion

The comparison of security features between blockchain and other technologies reveals that blockchain's decentralized and immutable nature provides a higher level of security for consent management systems. Unlike traditional centralized databases, blockchain eliminates single points of failure and reduces the risk of unauthorized access or tampering. The transparency and auditability offered by blockchain ensure that consent procedures are enforced and monitored in a trustworthy manner, fostering greater trust between users and organizations.

Adoption rate	Resource utilization	ROI Ratio	Transaction processing time
85%	90%	3.5	<10s

Table.1. Performance metrics

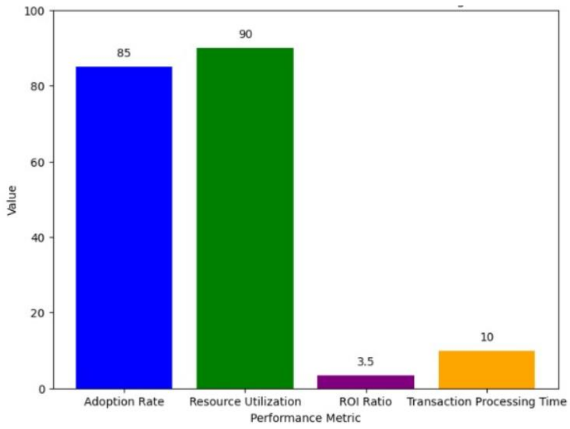
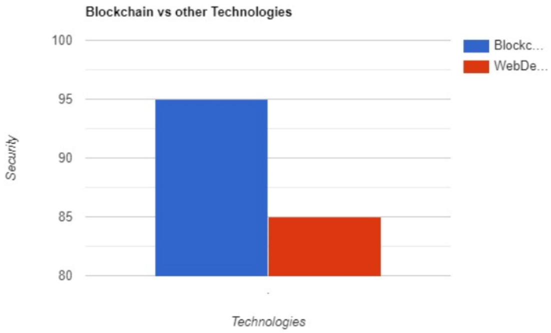


Fig.2. Performance metrics graphical representation



.

Fig.3. Comparison of security in Blockchain and other technologies

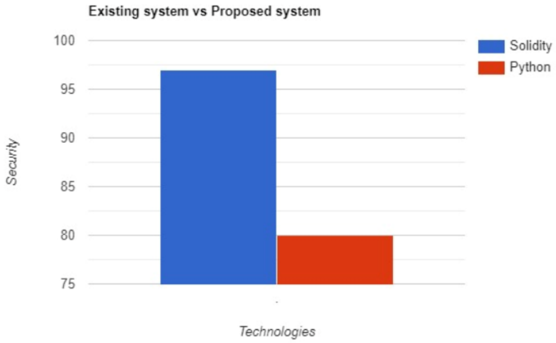


Fig.4. Existing system and proposed system security comparison

In addition, the comparison between the existing consent management system and the proposed blockchain-based solution highlights the advantages of the latter in terms of data security, user control, and transparency. The blockchain-based system enables real-time consent management, automated enforcement through smart contracts, and enhanced visibility into data handling processes. These features address the shortcomings of traditional consent management systems, especially in light of increasing data privacy incidents and regulatory scrutiny.

7 Conclusion

In conclusion, the research demonstrates the potential of blockchain technology to revolutionize consent management systems and enhance user data security and privacy. By leveraging blockchain's inherent characteristics of immutability, transparency, and decentralization, organizations can build sophisticated consent management systems that empower users and ensure compliance with data protection regulations. Future work should focus on further exploring blockchain integration into consent management systems, addressing technical challenges, privacy concerns, and implementation considerations to realize the full potential of blockchain in safeguarding user data.

8 References

[1] Huang, Y., & Lv, Y. (2023). Leveraging Blockchain Technology for Bill Transactions: Innovations in Blockchain-based Electronic Bill Systems in Engineering and Technology. Highlights in Science, Engineering and Technology, 56, 469-478.

[2] Miltiadou, D., Pitsios, S., Kasdaglis, S., Spyropoulos, D., Misiakoulis, G., Kossiaras, F., ... & Perakis, K. (2022). Leveraging management of customers' consent exploiting the benefits of blockchain technology towards secure data sharing. In Big Data and Artificial Intelligence in Digital Finance: Increasing Personalization and Trust in Digital Finance using Big Data and AI (pp. 127-155). Cham: Springer International Publishing.

[3] Rana, S. K., Rana, S. K., Nisar, K., Ag Ibrahim, A. A., Rana, A. K., Goyal, N., & Chawla, P. (2022). Blockchain technology and artificial intelligence based decentralized access control model to enable secure interoperability for healthcare. Sustainability, 14(15), 9471.

[4] Goint, M., Bertelle, C., & Duvallet, C. (2023). Secure Access Control to Data in Off-Chain Storage in Blockchain-Based Consent Systems. Mathematics, 11(7), 1592.

[5] Selvarajan, S., & Mouratidis, H. (2023). A quantum trust and consultative transaction-based blockchain cybersecurity model for healthcare systems. Scientific Reports, 13(1), 7107.

[6] Peyrone, N., & Wichadakul, D. (2023). A formal model for blockchain-based consent management in data sharing. Journal of Logical and Algebraic Methods in Programming, 134, 100886.

[7] Mukkala, A. R. K., Sreeja, K. R., Reddy, P. K., Reddy, B. S., & Ahmed, M. A. (2022). Protecting Information Using Ai And Blockchain. Journal of Algebraic Statistics, 13(3), 513-522.

[8] Barbaria, S., Mont, M. C., Ghadafi, E., Machraoui, H. M., & Rahmouni, H. B. (2022). Leveraging Patient Information Sharing Using Blockchain-Based Distributed Networks. IEEE Access, 10, 106334-106351.

[9] Roosan, D., Wu, Y., Tatla, V., Li, Y., Kugler, A., Chok, J., & Roosan, M. R. (2022). Framework to enable pharmacist access to health care data using Blockchain technology and artificial intelligence. Journal of the American Pharmacists Association, 62(4), 1124-1132.

[10] Kareem, Y., & Jahankhani, H. (2023). Development of a Decentralized Personal Indefinable Information (PII) Management Systems Using Blockchain dBFT Consensus Algorithm. In AI, Blockchain and Self-Sovereign Identity in Higher Education (pp. 167-191). Cham: Springer Nature Switzerland.

[11] Merlec, M. M., Lee, Y. K., Hong, S. P., & In, H. P. (2021). A smart contract-based dynamic consent management system for personal data usage under GDPR. Sensors, 21(23), 7994.

[12] Keshk, M., Turnbull, B., Sitnikova, E., Vatsalan, D., & Moustafa, N. (2021). Privacy-preserving schemes for safeguarding heterogeneous data sources in cyber-physical systems. IEEE Access, 9, 55077-55097.

[13] Karisma, K., & Tehrani, P. M. (2023). Data protection governance framework: A silver bullet for blockchain-enabled applications. Procedia Computer Science, 218, 2480-2493.

[14] Mahesh, P. S., & Muthumanickam, K. (2022). A Trustworthy Platform for Safeguarding and Validating Educational Credentials using Blockchain Technology. Periodico di Mineralogia, 91(5), 1-14.

[15] Islam, M. D., Shen, H., & Badsha, S. (2022). Integrating blockchain into supply chain safeguarded by PUF-enabled RFID. Internet of Things, 18, 100505.