



Design and Implementation of a Blockchain-Based Privacy Control System for Social Media Users

David Worusen Philip¹, Siman Emmanuel^{2*}, Gani Timothy Abe³

¹²³Kwararafa University Wukari, Nigeria

²Federal University Wukari, Nigeria.

*Corresponding Author

Siman Emmanuel

Federal University Wukari,
Nigeria.

Article History

Received: 12.08.2025

Accepted: 04.10.2025

Published: 20.11.2025

Abstract: Social media platforms rely heavily on centralized data storage and opaque data-sharing practices, exposing users to privacy breaches and unauthorized profiling. This paper presents a blockchain-based privacy control system that enables social media users to define, monitor, and revoke consent for data access and advertisement targeting. The system employs smart contracts deployed on the Ethereum blockchain to store user consent, manage third-party authorization, and maintain immutable access logs. A Design Science Research and Object-Oriented Analysis and Design approach guide the development of the system architecture, including user interface, smart contract layer, blockchain network, and audit dashboard. The implemented prototype is evaluated using gas usage and execution time for core operations set Consent, set Authorization, and request Access. Results show that all operations complete within milliseconds with moderate gas consumption, indicating that on-chain consent management is feasible for interactive social media scenarios. The findings suggest that blockchain can enhance transparency, user autonomy, and accountability in social media privacy management, although scalability and regulatory integration remain important directions for future work.

Keywords: Blockchain; social media; Privacy; Smart contract; Access control; Consent management.

Cite this article:

Philip, D. W., Emmanuel, S., Abe, G. T., (2025). Design and Implementation of a Blockchain-Based Privacy Control System for Social Media Users. *ISAR Journal of Science and Technology*, 3(11), 46-51.

1. Introduction

Social media platforms such as Facebook, Twitter, and Instagram have transformed communication but rely on centralized architectures that aggregate and monetize user data with limited transparency. High-profile incidents have exposed users to identity theft, profiling, and unauthorized surveillance. Existing privacy settings are complex, provider-controlled, and often insufficient to prevent data misuse. Blockchain provides decentralization, immutability, and transparent logging, making it a strong candidate for privacy-preserving consent management. However, most existing works remain conceptual or platform-specific and do not offer a practical, end-to-end framework for user-controlled data access on mainstream social networks. This paper aims to design and implement a blockchain-based privacy control system that allows social media users to set, monitor, and revoke consent for

data access and advertisement targeting, and to empirically evaluate its performance on an Ethereum test network. Figure 1 depicts the Design Science Research process followed in constructing the blockchain-based privacy control system for social media users: the study first identifies privacy and consent-management weaknesses in centralized social media and formulates clear design objectives for user-controlled data access; based on these objectives, the core artifacts—smart-contract box, access-request logic, user interface, and audit-trail components—are designed and implemented on Ethereum; the prototype is then demonstrated by handling user consent, processing third-party access requests, and logging all actions immutably; finally, its performance is evaluated using gas usage and execution time, and the insights obtained are used to refine both the artifact and the underlying design guidelines for privacy-preserving consent management.



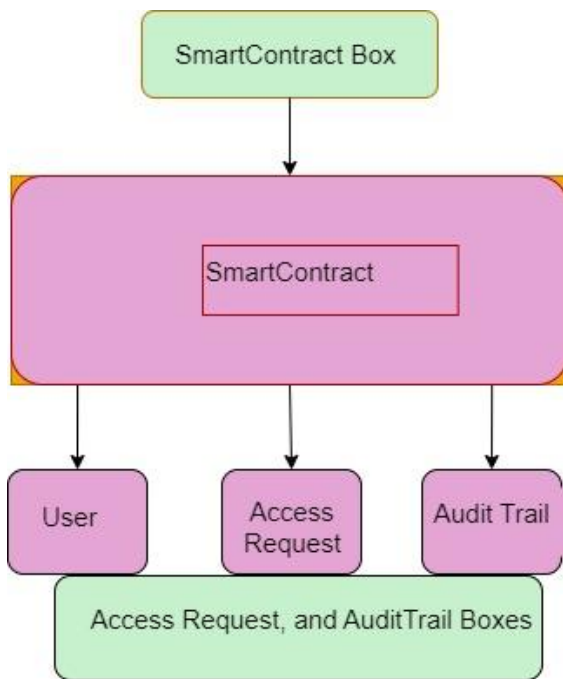


Figure 1: Design Science Research process applied to the development of the blockchain-based privacy control system.

Table 1 summarises how privacy and security risks on centralized social media platforms have evolved from broad, conventional threats to more sophisticated and targeted attacks. Conventional threats such as spam, malware, phishing, and identity theft exploit large user bases with generic, often automated campaigns that aim to steal credentials or compromise devices. Modern threats, including profile cloning, click-jacking, de-anonymisation, and account hijacking, leverage platform-specific features and rich metadata to manipulate interfaces, strip away pseudonymity, or take over accounts, thereby amplifying privacy loss. Targeted threats such as cyber-bullying, cyber-grooming, and cyber-stalking focus on individual users, using harvested personal information and persistent contact to cause psychological harm, coercion, or harassment, and thus represent a severe form of privacy violation in online social networks.

Table 1: Key privacy and security challenges in centralized social media platforms.(Jain et al., 2021)

Threats on Online Social Networks			
Conventional threats		Modern threats	Targeted threats
1	Spam	Profile cloning	Cyber-bullying
2	Malware	Click-jacking	Cyber grooming
3	Phishing	De-Anonymization	Cyber-stalking
4	Identity theft	Hijacking	

2. Related Work and Background

This section reviews blockchain fundamentals, privacy and security challenges in social media, and prior blockchain-based solutions for online social networks. The decentralization, consensus mechanisms were summarized, and smart contracts, then discuss privacy risks including unauthorized third-party access and limited user control over data flows. Representative works on was reviewed blockchain for social media privacy, decentralized identity, and access control, highlighting their strengths and limitations and identifying gaps in practical, user-facing consent management.

Figure 2: Conceptual comparison between centralized social media architecture and blockchain-based consent management.

Feature	Centralized Social Media Architecture	Blockchain-based Consent Management
Data Storage	Centralized Servers(owned by a corporation)	Distributed ledger (across a peer-to-peer network)
Control & Ownership	Corporation has ultimate control over data use.	User maintains verifiable control and ownership of their consent their consent records.
Transparency	Opaque (requires trust in the company).	Transparent & auditable (verifiable via the ledger).
Consent Model	Implicit, “all-or-nothing” privacy policies.	Explicit, granular and user-manged permissions.

Figure 2 contrasts conventional centralized social media with a blockchain-based consent management model by aligning four key features side by side: in the centralized architecture, user data are stored on corporation-owned servers, giving the platform ultimate control over data use and enforcing opaque, “all-or-nothing” privacy policies that users must accept to participate; in the blockchain-based model, the same functions are re-imagined on a distributed ledger, where consent records are stored across a peer-to-peer network, users retain cryptographically verifiable control over how their data may be accessed, all operations are transparent and auditable on the ledger, and privacy is enforced through explicit, fine-grained, user-managed permissions rather than blanket terms and conditions.

Table 3: Summary of representative blockchain-based privacy solutions for social media and related domains.

Theoretical Framework	Methodology	Findings	Limitations	Authors and Years
Blockchain Technology	Quantitative analysis (content analysis and sentiment analysis)	Communicating responsible management and the role of blockchain technology: social media analytics for the luxury fashion supply chain	Reliance on publicly available data from social media, comprising corporate statements emanating from managers is a major limitation in this study.	Oguntegbe <i>et al.</i> , (2023)
Blockchain, crowdfunding, cryptocurrencies, initial coin offerings (ICOs), social media analytics (SMA)	Blockchain Technology	Tracking the Digital Evolution of Entrepreneurial Finance: The Interplay Between Crowdfunding, Blockchain Technologies, Cryptocurrencies, and Initial Coin Offerings	The study is limited to the interplay among English speaking users of social media	Bogusz <i>et al.</i> , (2020)
Decentralized Digital Technology	Blockchain Technology	Decentralized Governance of Digital Platforms	One dimension of strategic leadership, the study examines a key aspect of governance	Chen <i>et al.</i> , (2021)
Steem Blockchain	Blockchain Technology	Steem Blockchain: Mining the Inner Structure of the Graph	Focused only on analyzing the Steem blockchain's transaction graph.	Guidi <i>et al.</i> , (2020)
Steemit Blockchain-based	User Activity Analysis and Time-Series Correlation AnalysisS	The role of cryptocurrency in the dynamics of blockchain-based social networks:	This work does consider only one platform and the analysis of rewards focuses on the hubs,	Ba <i>et al.</i> , (2022)

3. Methodology and System Model

3.1 Research Design

The study follows a Design Science Research Methodology combined with Object-Oriented Analysis and Design. The core artifact is a set of Ethereum smart contracts that implement consent storage, authorization management, and access logging.

3.2 System Architecture

The proposed architecture comprises a user interface layer, smart contract layer, blockchain network, storage, and an audit/analytics dashboard. Users set or revoke consent via the interface; transactions are sent to the smart contract, which enforces access rules and writes events to the blockchain. Figure 2 presents the proposed system architecture, in which users specify their consent preferences through a user interface that writes to a smart contract responsible for storing consent settings and logging all data-access events; when a third party issues a data request, the request is routed via the blockchain network to the access control and verification component, which checks the on-chain consent rules and returns a grant-or-deny decision to the smart contract and the data access API, where the decision is enforced; all access events are continuously forwarded as logs to an audit and analytics dashboard for transparency and compliance monitoring, while an

optimisation engine analyses these logs to tune system parameters and improve both performance and resource efficiency of the privacy control system.

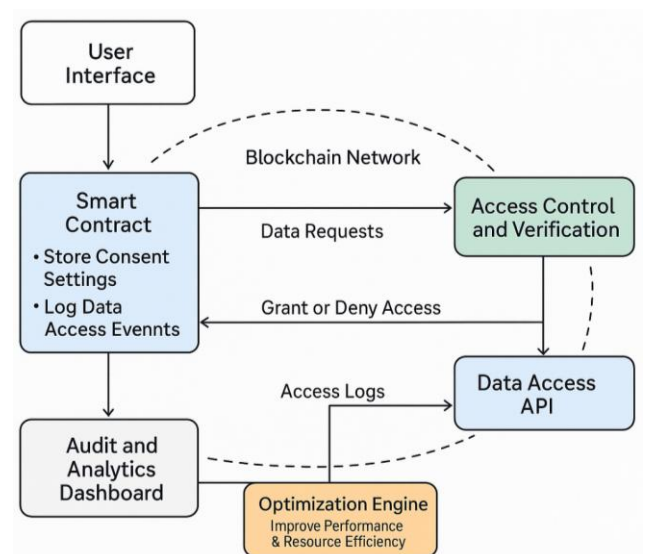


Figure 2: Proposed system architecture of the blockchain-based privacy control system.

3.3 High-Level Workflow and Data Flow

When a user specifies data-sharing and advertising preferences, the UI formats the request as a transaction. The smart contract validates the request, updates consent records, and logs the event. Third-party requests are checked against stored consent and authorization mappings. Figure 4 illustrates the consent lifecycle: the process begins with the user, who either accepts the social-media platform’s (e.g., Facebook’s) terms and conditions or exits the process if consent is denied; once consent is granted, the user’s profile data and advertising preferences are shared with online advertisers, while a parallel check assesses whether the supplied data appear fake or misleading—suspicious patterns are routed to an optimisation engine that adjusts system parameters to improve detection performance and resource use; for legitimate data, the advertiser attempts to open a blockchain block, and when this succeeds the user information is stored as “clean data,” meaning that the consented, verified attributes are immutably recorded for compliant, privacy-aware advertising use.

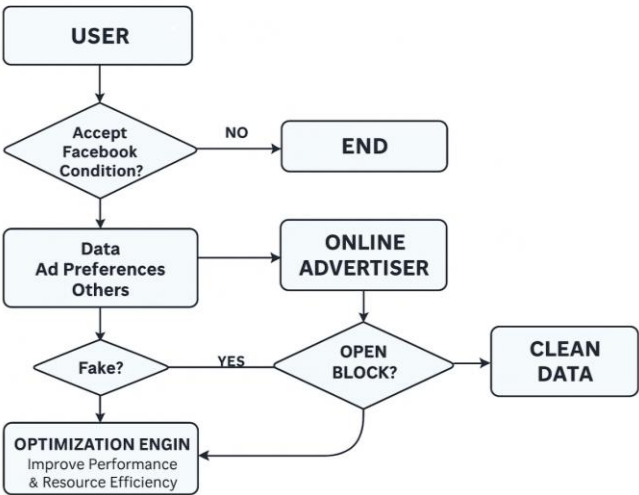


Figure 4: Consent lifecycle data flow diagram.

3.4 Implementation Environment

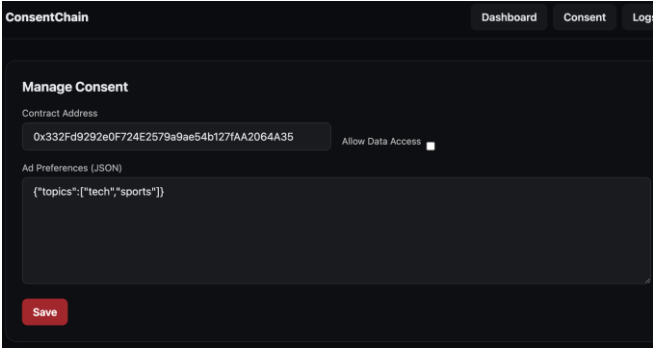
The prototype is implemented using Solidity smart contracts deployed with Hardhat on a local Ethereum test network. Node.js and TypeScript provide the backend, with Web3.js/Ethers.js handling on-chain interactions. MetaMask is used for wallet management and transaction approval.

Table 3. Tools and technologies used in system implementation.

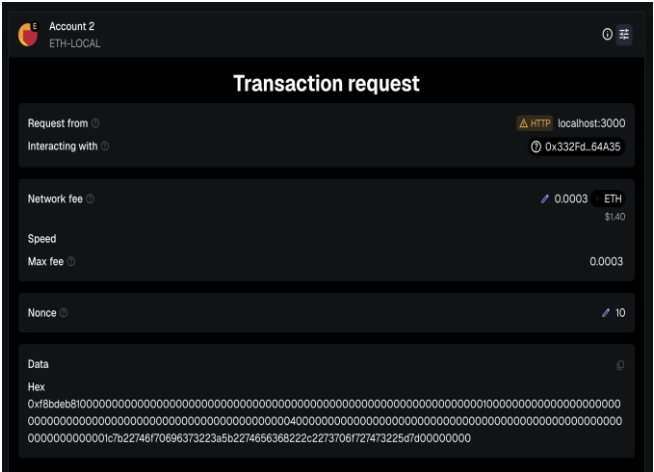
4. Results

4.1 Input and Output Interfaces

The input interface lets users define consent and authorization using structured forms. When preferences are submitted, MetaMask prompts the user to sign and broadcast the transaction. After confirmation, an access log interface displays on-chain events.



Consent Configuration



Transaction Confirmation

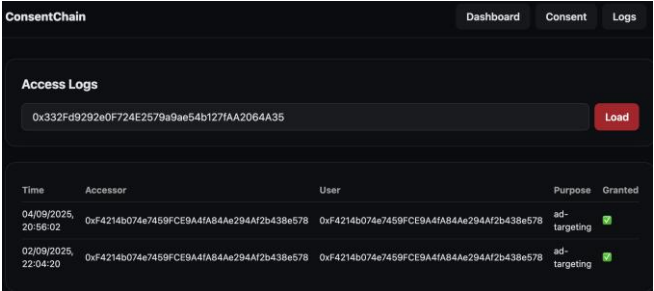


Figure 5: User interfaces for consent configuration, transaction confirmation, and access log dashboard.

Figure 5 presents the key user interfaces that support the privacy control workflow: the consent-configuration screen allows users to specify which categories of personal data may be shared with third-party applications and under what conditions; the transaction-confirmation interface prompts users to review and authorize individual access or policy-update transactions before they are committed to the blockchain, thereby enforcing explicit, fine-grained consent; finally, the access-log dashboard visualizes on-chain records of who accessed which data, when, and under which consent rule, providing users and auditors with transparent monitoring, anomaly detection, and compliance reporting capabilities.

4.2 Performance Evaluation

Three core smart contract functions are evaluated: set Consent, set Authorization, and request Access. For each, gas usage and execution time are measured on the Ethereum test network, Figure 4.

Table 4: Smart contract performance metrics for core operations.

	Elapsed (ms)	Gas Used
Set consent	295544	0.0003
Set Authorization	154201	0.0034
Request Access	2983	0.001

Figure 6 compares the gas consumption and execution time of three core smart-contract operations in the privacy control system:

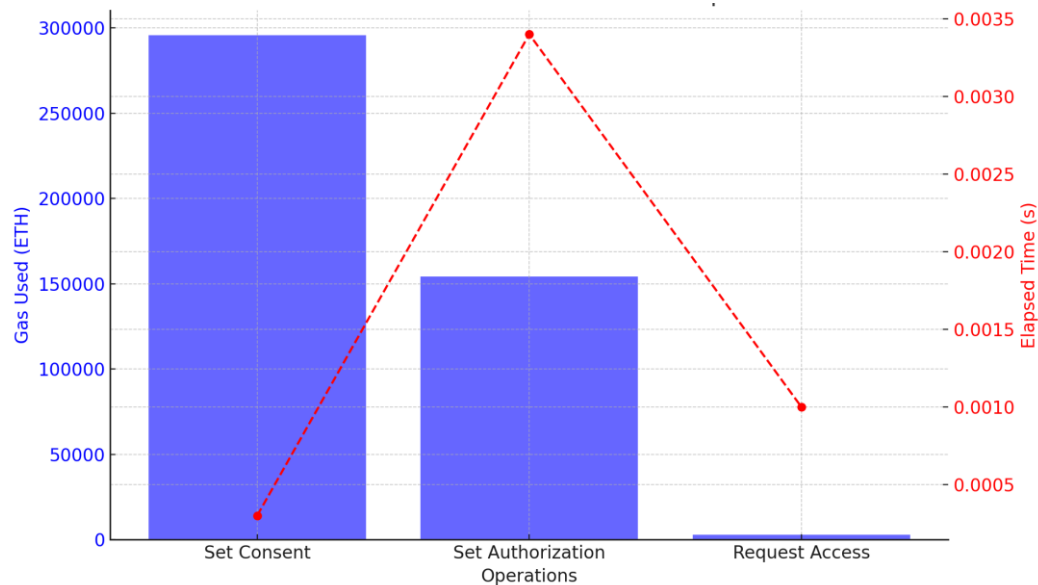


Figure 6: Bar charts of gas usage and execution time per operation.

5. Discussion

The results show that the proposed Ethereum smart contracts can enforce consent and access control with millisecond-scale latency and moderate gas usage, where `setConsent` and `setAuthorization` incur higher costs due to state updates, while `requestAccess` remains lightweight for frequent querying. Overall, this indicates that on-chain consent management is technically viable for interactive social media workloads, particularly if combined with standard gas-optimization techniques and migration to Layer-2 networks to improve scalability. Beyond performance, the design contributes explicit, auditable consent records and access logs directly at the blockchain layer, addressing the opacity of traditional social media privacy settings and strengthening accountability for third-party data use. At the same time, the prototype is limited to a test-network deployment and a simplified workload, so future work should examine usability, large-scale stress behaviour, integration with off-chain storage, and alignment with emerging data-protection regulations.

6. Conclusion and Future Work

This study has proposed and evaluated a blockchain-based privacy control system that repositions user consent as a verifiable, on-chain asset rather than an opaque checkbox controlled by centralized platforms. By combining smart contracts, a consent-aware access API, and an audit dashboard, the prototype

Set Consent and Set Authorization incur the highest gas usage, reflecting the cost of writing new consent and authorization rules to the blockchain, whereas Request Access requires only a small amount of gas because it mainly reads existing on-chain state; however, despite the higher gas usage, all operations complete within a few milliseconds, indicating that the observed latency is acceptable for interactive consent management while still highlighting that further optimization should focus on reducing the cost of write-intensive transactions.

demonstrates that fine-grained, transparent consent management can be achieved with acceptable latency and moderate gas costs, while also generating immutable logs for accountability and compliance monitoring. Therefore, the work provides both an architectural blueprint and an empirical indication that social-media consent can be enforced at infrastructure level instead of through informal policy statements. Future work will extend the prototype beyond a controlled test-network setting to more realistic workloads and multiple social-media platforms, investigate integration with off-chain storage and emerging Layer-2 scalability solutions, and explore formal verification of smart-contract logic. Further research is also required on usability, incentive design for third-party developers, and alignment with evolving data-protection regulations, so that the technical guarantees of blockchain-based consent can translate into practical, user-centred privacy in real deployments.

References

1. Anderson, K. E. (2021). Getting acquainted with social networks and apps: talking about TikTok. *Library Hi Tech News*, 38(6), 1–6. <https://doi.org/10.1108/LHTN-10-2021-0077>
2. Bernabe, J. B., Moreno, R. T., Canovas, J. L., Hernandez-Ramos, J. L., & Skarmeta, A. (2019). Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE*

- Access, 7, 164908–164940. <https://doi.org/10.1109/ACCESS.2019.2950872>
3. Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. [Details as in your main project], 41, 1027–1038.
 4. Bogusz, C. I., Laurell, C., & Sandström, C. (2020). Tracking the Digital Evolution of Entrepreneurial Finance: The Interplay between Crowdfunding, Blockchain Technologies, Cryptocurrencies, and Initial Coin Offerings. *IEEE Transactions on Engineering Management*, 67(4), 1099–1108. <https://doi.org/10.1109/TEM.2020.2984032>
 5. Chen, Y., Pereira, I., & Patel, P. C. (2021). Decentralized Governance of Digital Platforms. *Journal of Management*, 47(5), 1305–1337. <https://doi.org/10.1177/0149206320916755>
 6. Chu, S. C., Chen, L., Kumar, S., Kumari, S., Rodrigues, J. J. P. C., & Chen, C. M. (2020). Decentralized Private Information Sharing Protocol on Social Networks. *Security and Communication Networks*, 2020. <https://doi.org/10.1155/2020/7137480>
 7. Di Pietro, R., & Cresci, S. (2021). Metaverse: Security and Privacy Issues. *2021 3rd IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, 281–288. <https://doi.org/10.1109/TPSISA52974.2021.00032>
 8. Guidi, B. (2021). An overview of blockchain online social media from the technical point of view. *Applied Sciences (Switzerland)*, 11(21). <https://doi.org/10.3390/app11219880>
 9. Guidi, B., Michienzi, A., & Ricci, L. (2020). Steem Blockchain: Mining the Inner Structure of the Graph. *IEEE Access*, 8, 210251–210266. <https://doi.org/10.1109/ACCESS.2020.3038550>
 10. Hisseine, M. A., Chen, D., & Yang, X. (2022). The Application of Blockchain in Social Media: A Systematic Literature Review. *Applied Sciences (Switzerland)*, 12(13). <https://doi.org/10.3390/app12136567>
 11. Jain, A. K., Sahoo, S. R., & Kaubiyal, J. (2021). Online social networks security and privacy: Comprehensive review and analysis. *Complex and Intelligent Systems*, 7(5), 2157–2177. <https://doi.org/10.1007/s40747-021-00409-7>
 12. Jozani, M., Ayaburi, E., Ko, M., & Choo, K. K. R. (2020). Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective. *Computers in Human Behavior*, 107. <https://doi.org/10.1016/j.chb.2020.106260>
 13. Li, C., Palanisamy, B., Xu, R., Xu, J., & Wang, J. (2021). SteemOps: Extracting and Analyzing Key Operations in Steemit Blockchain-based Social Media Platform. *CODASPY 2021 – 11th ACM Conference on Data and Application Security and Privacy*, 113–118. <https://doi.org/10.1145/3422337.3447845>
 14. Liu, X., Xie, L., Wang, Y., Zou, J., Xiong, J., Ying, Z., & Vasilakos, A. V. (2021). Privacy and Security Issues in Deep Learning: A Survey. *IEEE Access*, 9, 4566–4593. <https://doi.org/10.1109/ACCESS.2020.3045078>
 15. Masinde, N., & Graffi, K. (2020). Peer-to-Peer-Based Social Networks: A Comprehensive Survey. *SN Computer Science*, 1(5). <https://doi.org/10.1007/s42979-020-00315-8>
 16. Ogonji, M. M., Okeyo, G., & Wafula, J. M. (2020). A survey on privacy and security of Internet of Things. *Computer Science Review*, 38. <https://doi.org/10.1016/j.cosrev.2020.100312>
 17. Oguntegbe, K. F., Di Paola, N., & Vona, R. (2023). Communicating responsible management and the role of blockchain technology: Social media analytics for the luxury fashion supply chain. *TQM Journal*, 35(2), 446–469. <https://doi.org/10.1108/TQM-10-2021-0296>
 18. Oumaima, F., Karim, Z., Abdellatif, E. L. G., & Mohammed, B. (2022). A Survey on Blockchain and Artificial Intelligence Technologies for Enhancing Security and Privacy in Smart Environments. *IEEE Access*, 10, 93168–93186. <https://doi.org/10.1109/ACCESS.2022.3203568>
 19. Quach, S., Thaichon, P., Martin, K. D., Weaven, S., & Palmatier, R. W. (2022). Digital technologies: Tensions in privacy and data. *Journal of the Academy of Marketing Science*, 50(6), 1299–1323. <https://doi.org/10.1007/s11747-022-00845-y>
 20. Ramesh, R., Raman, R. S., Bernhard, M., Ongkowijaya, V., Evdokimov, L., Edmundson, A., Sprecher, S., Ikram, M., & Ensafi, R. (2020). Decentralized Control: A Case Study of Russia. *27th Annual Network and Distributed System Security Symposium (NDSS)* (2020). <https://doi.org/10.14722/ndss.2020.23098>
 21. Shahbazi, Z., & Byun, Y. C. (2021). Fake Media Detection Based on Natural Language Processing and Blockchain Approaches. *IEEE Access*, 9, 128442–128453. <https://doi.org/10.1109/ACCESS.2021.3112607>
 22. Sharkar, E., Mohammad, D., & Fariha, T. T. (2022). Enhancing Privacy on Facebook using Blockchain Technology. pp. 1–10.
 23. Shrestha, A. K., Vassileva, J., & Deters, R. (2020). A Blockchain Platform for User Data Sharing Ensuring User Control and Incentives. *Frontiers in Blockchain*, 3, 1–22. <https://doi.org/10.3389/fbloc.2020.497985>
 24. Tawalbeh, L., Muheidat, F., Tawalbeh, M., & Quwaider, M. (2020). IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, 10(12), 1–17.