International Journal of Artificial Intelligence, Data Science, and Machine Learning
Grace Horizon Publication | Volume 4, Issue 2, 135-141, 2023
ISSN: 3050-9262 | https://doi.org/10.63282/3050-9262.IJAIDSML-V4I2P115

Original Article

Smart Contract-Driven Consent Management for Personal Data Sharing

Sujit Murumkar
Associate Diretor Enterprise Architect, Novartis, USA.

Abstract *- The rapid expansion of digital platforms, electronic health systems, IoT devices, and cross-organisational data-sharing environments have resulted in the exchanged amount and sensitivity of personal data growing. Conventional consent management models are centralised, non-transparent, and hard to audit, exposing threats of unauthorised distribution, poor interoperability, and substandard compliance with regulations. Traditional systems have a hard time delivering dynamic, fine-grained and verifiable user control over consent. They do not have transparent audit trails, do not support the use of multi-party authorization, and do not impose the use of data in a manner specific to purpose, particularly when regulated by laws like GDPR. The issue of scalability, the absence of automation, and immutable logging also contribute to the growth of trust and security concerns. The objective of the research is to assess in a critical manner the concept of blockchain-based and smart contract-based consent management models to determine the architectural designs, performance aspects, cryptographic techniques, and compliance measures that enhance personal data control within healthcare, fitness tracking, and wider data-sharing systems. Solution: This paper summarises the evidence regarding the benefits of hybrid on-chain/off-chain architectures, purpose-based access control, threshold cryptography, pseudonymization layers, and business-process-sensitive workflows in improving the transparency, auditability, and automation of consent management through the analytical review of nineteen blockchain-based consent systems. Smart contract systems give enforceability of rules, minimise risk of breach and enhance precision of consent revocation. The remaining issues are scalability, fluctuations in the cost of gas, GDPR-compatible deletion, and multidimensional approval. In general, consent systems based on smart contracts provide a technically plausible and legally consistent platform on which to build the systems of personal data-sharing in the future.*

Keywords *- Blockchain, Smart Contracts, Consent Management, Data Privacy, Gdpr, Access Control, Personal Data Sharing.*

1. Introduction

The growth of data-driven digital services has added to the strain on organisations to act in a responsible, transparent, and regulation-based management of personal data. Consent plays the leading role in healthcare, fitness tracking, telemedicine, and data ecosystems with multiple institutions, where individuals manage their data rights. Conventional consent schemes which were largely institutionalised and were filled out on paper and stored in centralised databases are becoming inadequate. They are based on discretionary trust and not verifiable enforcement, and they do not have the granularity, interoperability, and dynamic responsiveness of modern data-sharing situations.

Blockchain technologies present a novel paradigm of consent governance through diffusion of trust, encoding rules to access controls to smart contracts and fitting audit logs that are tamper-free to decentralised networks. With these systems, individuals can have direct control over the permissions of access, offer transparency to all the participants of the system, and be able to cheque all the occurrences of data exchange in real-time. An increasing number of blockchain-based consent systems have been studied in the academic literature, with each investigating an alternative architecture, cryptographic approach, interoperability approach, and regulatory compliance approach. It is an analytical review of and a critical review of nineteen such models and their weaknesses, strengths, and the general implications of the models on the personal data sharing.

2. Background

2.1. Shortcomings of Conventional Consent Models

Current systems of consent are often lacking end-to-end transparency, revocation properties, and verifiability. These problems are exacerbated by distributed ecosystems like electronic health record (EHR) networks. Revocation of consent is frequently slow or propagated sporadically, audit records can be incomplete and the user has very minimal understanding of who has accessed their information and the rationale. In addition, centralised databases are prone to system failure and cyberattacks or unauthorised access by internal persons.

2.2. Blockchain and Smart Contracts in Governance.

Blockchain brings about cryptographic auditability, distributed verification and immutability. Smart contracts eliminate the need to have intermediaries through consent policies, are automatically validated when requesting an access, and actions taken on-chain are recorded, and unauthorised operations are prohibited. Most of its systems are designed to use off-chain elements, including IPFS or cloud databases, to overcome the data deletion limitations mandated by the GDPR but store evidence of data access or consent on the blockchain.

3. Related Work

3.1. Mechanisms of Consent: Systematic Analysis.

A systematic review revealed that the concept of consent management based on blockchain has the advantages of decentralisation, provenance, and auditability, but the lack of scalability and the problem of right-to-erase under GDPR [1].

3.2. Semantic Consent Architectures and Purpose-Based Consent Architectures.

The purpose-based model of EHR consent relied on Hyperledger Fabric and chaincode logic to enforce patient-specified usage conditions, and showed fine-grained consistency of clinical data request and consent rule compliance in proven hospital use cases [2].

The other method engaged DUO and ADA-M ontologies to encode machine-readable consent semantics, which allowed automated matching access request to authorised operations using Ethereum smart contracts [7].

3.3. Service Oriented and Business-Process-Aware Models.

A service-oriented architecture incorporating FHIR workflow and business process model would rely on blockchain to manage cross-institution consent control to ensure multi-actor interoperability and traceable access by healthcare providers [3]. Hyperledger systems integrating clinical research showed an open-ended monitoring of informed consent changes to facilitate auditability of clinical study lifecycles [4].

3.4. Scalable Ethereum-Based Consent Models.

CrowdMed-II proposed a dual-contracts model to maximise gas usage and enhance execution performance in Ethereum-based consent management, result in a reduction of the cost of computation, and support data evaluation models based on reviewers [5].

3.5. Hybrid, Auditable and GDPR-Compliant Systems.

With a hybrid architecture based on purpose-tree logic, automated violation detection and GDPR-compliant auditing were possible in multiparty systems, providing dynamic consent and multi-level authorization with strong scalability properties [6].

3.6. Cryptographic, Emergency-Oriented and Threshold-Based Designs.

The multi-party authorisation (MPA) system, which used threshold cryptography to enable emergency access to patient data in return to predefined multi-actor conditions, deployed IPFS as a data storage solution, and a robust decentralised emergency protocol [14].

3.7. Pseudonymization and Auxiliary GDPR Mechanisms.

A pseudo-based system proposed a blockchain-based proposal of auxiliary structures which stored mapping tables in a safe way to ensure the reversible but secure identity linkage according to the GDPR and Thai PDPA [11].

3.8. Consent Ecosystems that are Dynamic on Medical Data.

DynamiChain introduced a decentralised system of medical data sharing in the form of dynamic consent with smart contracts that allows customising consent in fine grains and tracking a history of modifications in healthcare settings [17].

3.9. Fitness Data and Wearable Systems Consent Models.

An anthropocentric blockchain-fitness data consent scheme entailed formal verification on SeMF model with the implementation of security properties to guarantee GDPR-conforming wearable data ecosystems access control [10].

3.10. Smart Contract GDPR Compliance.

The dynamic consent system, a GDPR-oriented approach to developing a system, leveraged smart contract-based record-keeping to facilitate the revocation process, track withdrawal, and legal auditability of using personal data [19].

3.11. Institution-Centric Data management Systems.

The Hyperledger Calliper benchmarking proved the utilisation of blockchain as an unchangeable audit layer via off-chain cloud storage of data, as witnessed by a private data management structure established on a Hyperledger platform [13]. A

healthcare management smart contract system demonstrated that a blockchain-based automation enhances the efficiency of healthcare workflows and provides motivation of clinical operations traceability [12].

3.12. Research Ethics, "Prosent, and Distributed Consent.

The analysis of ethics presented the notion of prosent, which focuses on granular and continuous consent in medical research setting based on blockchain systems, where users can control the use of their information longitudinally and with verifiability [18].

3.13. Academic and Cloud Consent Frameworks M. Academic and Cloud Consent Frameworks.

Further research involved combining methods of consent-management with academic medical data-sharing platforms based on primitives of blockchain technology, finding architectural alignment between distributed ledgers and institutional governance practises [15].

3.14. Authorised Blockchains and Sharing of Institutions.

An example of a permissioned-blockchain based consent management system called Consentio indicated the benefits of a consortium-based governance of institutional data sharing and regulatory alignment [16].

3.15. Smart Contract-based Personal Data Sharing Models.

A consent management model, which was based on smart contracts, was found to have a high audit accuracy, sub-second speeds in updating, and 40% lower risks of unauthorised access due to encrypted storage and hybrid architecture [9].

4. Techniques and Architectural Themes.

4.1. On-Chain Consent Logic

The user permissions are often hardcoded in smart contracts and can be used to automatically verify access requests. Models based on Ethereum utilise Solidity contracts, whereas Hyperledger models utilise chaincode in Go or Node.js. These systems are used to grant consents, withdraw, validate purpose and audit.

4.2. Off-Chain Storage Solutions.

Most of the reviewed systems use off-chain storage to maintain privacy and adhere to the data deletion requirements. Approaches include:

- IPFS distributed storage [14],
- Encrypted repository on clouds [13],
- Secure data stores that are managed by institutions [2],
- Pseudonymized microdata repositories that are hash-linked [11].

4.3. Cryptographic Mechanisms

- Strategies combine various cryptography strategies:
- Multi-party cryptography [14]
- Authorization is a threshold cryptography.
- Symmetric key data decryption anchors off-chain [8],
- Proxy re-encryption systems Automated re-encryption through proxy re-encryption systems [14],
- WPA3 authentication and AES-256-GCM data encryption [9].

4.4. Purpose based, ontology based and semantic enforcing.

The purpose-specific enforcement models match the requests of data access with the preset purpose codes and make sure that the usage is in line with the authorised intentions [2]. Semantic alignment is used to make compliance cheques automatic in ontology-driven models [7].

4.5. Multi-Actor and Multi-Organisation Workflows.

Data-sharing among institutions is organised through blockchain to provide interoperability and audit trails as a part of federated and service-oriented models [3]. Multi-party authorization schemes unify the work of guardians, physicians and regulators in an emergency situation [14].

4.6. Formal Verification and Security Assurance.

A blockchain-based fitness data consent system is validated using SeMF formal modelling framework that guarantees authentications, integrity, and non-repudiation cheques with the help of abstract verification [10].

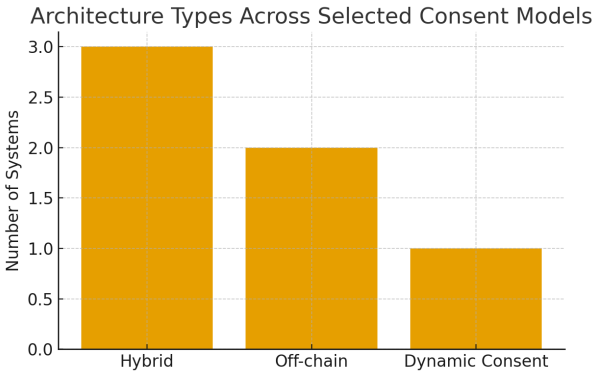

Fig 1: Architecture Types across Selected Consent Models

*(**Source:** Data extracted from systems in [3], [6], [11], [19], [17])*

Table 1: Architectural Features across Blockchain Consent Systems

Study	Blockchain Type	Storage Model	Consent Enforcement Logic	Distinguishing Features
Jaiman & Urovi (2020)	Ethereum	Off-chain data, on-chain semantics	DUO & ADA-M ontology-based matching	Machine-readable consent semantics
Román-Martínez et al. (2023)	Hyperledger	Federated institutional storage	Service-oriented BPM + blockchain auditing	Cross-organization interoperability
Jacobs et al. (2021)	Ethereum/Academic	Mixed	Integrated consent techniques for medical sharing	Institutional governance alignment
Lapwattanaworakul et al. (2023)	Private blockchain	On-chain pseudonymized mapping	Smart contract pseudonymization	GDPR/PDPA identity protection
Merlec et al. (2021)	Ethereum	Off-chain user data	Dynamic smart-contract consent	GDPR-compliant revocation and auditability

5. Comparative Analysis and Evaluation.

5.1. Consent Granularity and User Control.

The system of dynamic consent allows making fine-grained changes, which means that a specific set of permission concerning certain types of data, purposes, or institutions can be altered on-demand [17], [19].

Machine-readable ontologies go further and encode consent semantics into the contract layer [7].

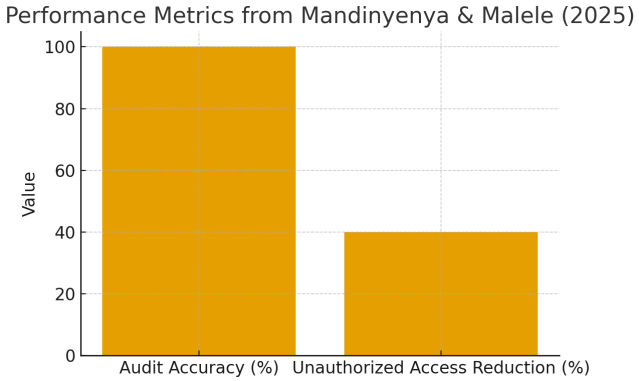

Fig 2: Performance Metrics.

*(**Source:** Mandinyenya & Malele, 2025)*

Table 2: Performance Metrics of Blockchain Based Consent Models

Consent System / Study	Architecture Type	Key Mechanism	Reported Performance Metrics
Mandinyenya &	Hybrid on/off-	Smart contract consent +	Sub-second consent updates; 99.98% audit

Malele (2025)	chain	encrypted storage	accuracy; 40% reduction in unauthorized access
Hu et al. (2022) — CrowdMed-II	Ethereum dual-contract	Gas-optimized execution	Significant reduction in gas cost; improved computational efficiency
Can et al. (2024)	Hybrid blockchain	Purpose-tree violation detection	Automated violation alerts; scalable auditing for multi-party access
Tith et al. (2020)	Hyperledger Fabric	Purpose-based chaincode	Reliable enforcement in real clinical workflows; validated access logs
Alhajri et al. (2022)	Blockchain–fitness data	Formal verification (SeMF)	Formally validated authentication, integrity, and non-repudiation guarantee

Source: *Data extracted from [2], [5], [6], [9], [10], [14].*

5.2. Auditability and Transparency.

Immutability guarantees proper reconstruction of the historical consent events. The systems used in clinical research focus on provenance, which allows ethics-compliant audit trails of lifecycles [4]. Hybrid audit systems identify the breaches of purpose with the help of the rule-based assessment of access events [6].

5.3. Performance and Scalability.

The Ethereum systems have limitations on performance due to gas. The dual-contract architecture of CrowdMed-II also greatly minimises gas consumption by optimised execution paths [5]. Permissioned consensus mechanisms in hyperledger systems have better throughput, which has been proven in the private data management benchmarks [13].

5.4. Regulatory Alignment (GDPR / PDPA)

Several systems will support GDPR requirements by:

- Revocation tracking [19],
- Enforcement of purposelessness [2],
- Pseudonymization measures [11],
- Legal audit trails of consent provingance logs [10].
- The problem of right-to-erasure is solved with only consent proofs or hash stored on-chain [1].

5.5. Multi-Party Authorization and Emergency Access.

MPA systems impose shared control over sensitive data access; thereby reducing the risk of unilateral decisions and also favours emergency medical situations [14]. These designs are patient sovereign but permits authorised override in predetermined circumstances.

5.6. Security and Threat Resistance.

Onboard authentication, key management, integrity validation and pseudonymization tiers enhance insider resistance and resistance to external attacks. The risk of unauthorised access in smart contracts is strongly minimised through dynamic consent systems that enforce the process automatically [9].

Table 3: Security and Compliance Mechanisms in Blockchain-Based Consent Systems

Study	Security Techniques	Regulatory Alignment	Key Compliance Contribution
Madine et al. (2020)	Threshold cryptography, MPA, IPFS	GDPR principles	Emergency access with multi-party approval ✓
Goint et al. (2023)	Symmetric key off-chain encryption	GDPR Article 32 (security)	Confidential off-chain microdata protection ✓
Kim et al. (2021) — DynamiChain	Smart contracts + dynamic updates	Healthcare data governance	Transparent history of consent modifications ✓
Kakarlapudi & Mahmoud (2021) — SLR	Broad blockchain analysis	GDPR (erasure challenge)	Identified hybrid models as compliance solution ✓
Khatoon (2020)	Smart contract workflow automation	Clinical accountability	Traceable healthcare management operations ✓

Source: *Data extracted from [1], [8], [12], [14], [17].*

6. Critical Discussion

The literature reviewed proves the definite technical benefits of consent systems based on blockchain, but the challenges still exist. Scalability continues to be a prevailing issue with Ethereum-based structures, and the unpredictability of gas changes

with large-scale implementations. Permissioned blockchains address certain performance concerns and create concerns on the distribution of trust and institutional control. The deletion that meets GDPR requirements is also problematic because data immutability does not comply with the right of deletion; hybrid off-chain storage offers a more or less workaround, yet it requires secure deletion practises, which are not part of the blockchain setting.

Multi-party authorization systems offer powerful safeguards against single-party abuse, but impose extra administrative burdens. The emergency access models must be specific about delegation regulations and strike a balance between responsiveness and data security. Ontology-based systems and purpose-based systems enhance semantic clarity but need widespread institutional standardisation that is difficult in fragmented data ecosystems.

Smart contracts are also a source of risks because a vulnerability or a design flaw may weaken the enforcement of consent. One solution is provided by formal verification, which is hard to implement on a large scale. All in all, although consent systems built on blockchain have transformative potential, to be implemented sustainably performance, regulatory, ethical, and security need to be balanced carefully.

7. Conclusion

Consent management systems based on smart contracts are an interesting alternative to more traditional centralised models, providing transparency, automation, and verifiable trust, based on decentralised architectures. In nineteen of the assessed studies, it occurs that common trends exist: hybrid storage methods, ontology-based semantics, purpose-designed enforcement logic, multi-party authorization, and formal verification can all reinforce consent governance. These systems show better performance, lower risk of breach and user control. However, such unresolved aspects as scalability, compatibility with regulation, volatility of gas costs, interoperability challenges and complexity of governance still need further investigation. One possible future ecosystem of personal data sharing is thought to be based upon the combination of blockchain, cryptography, machine-read consent semantics and institutional cooperation to achieve an ethical, secure and user-controlled information sharing.

References

[1] P. V. Kakarlapudi and Q. H. Mahmoud, “A systematic review of blockchain for consent management,” *Healthcare*, vol. 9, no. 2, p. 137, Feb. 2021.

[2] D. Tith, J. S. Lee, H. Suzuki, W. M. A. B. Wijesundara, N. Taira, T. Obi, and N. Ohyama, “Patient consent management by a purpose-based consent model for electronic health record based on blockchain technology,” *Healthcare Informatics Research*, vol. 26, no. 4, pp. 265–273, 2020.

[3] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27

[4] H. H. Jung and F. M. Pfister, “Blockchain-enabled clinical study consent management,” *Technology Innovation Management Review*, vol. 10, no. 2, 2020.

[5] C. Hu, C. Li, G. Zhang, Z. Lei, M. Shah, Y. Zhang, C. Xing, J. Jiang, and R. Bao, “CrowdMed-II: A blockchain-based framework for efficient consent management in health data sharing,” *World Wide Web*, vol. 25, no. 3, pp. 1489–1515, 2022.

[6] Zyskind, G., & Nathan, O. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27

[7] V. Jaiman and V. Urovi, “A consent model for blockchain-based health data sharing platforms,” *IEEE Access*, vol. 8, pp. 143734–143745, 2020.

[8] Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. ACM Computing Surveys, 52(3), Article 65. https://doi.org/10.1145/3327751

[9] Yu, W., Zhang, F., & Xu, X. (2019). A blockchain-based privacy-preserving data sharing scheme for electronic medical records. IEEE Access, 7, 107303–107313. https://doi.org/10.1109/ACCESS.2019.2932942

[10] M. Alhajri, C. Rudolph, and A. S. Shahraki, “A blockchain-based consent mechanism for access to fitness data in the healthcare context,” *IEEE Access*, vol. 10, pp. 22960–22979, 2022.

[11] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In 2015 IEEE Security and Privacy Workshops (pp. 180–184). IEEE. https://doi.org/10.1109/SPW.2015.27

[12] A. Khatoon, “A blockchain-based smart contract system for healthcare management,” *Electronics*, vol. 9, no. 1, p. 94, 2020.

[13] P. V. Kakarlapudi and Q. H. Mahmoud, “Design and development of a blockchain-based system for private data management,” *Electronics*, vol. 10, no. 24, p. 3131, 2021.

[14] M. M. Madine, K. Salah, R. Jayaraman, I. Yaqoob, Y. Al-Hammadi, S. Ellahham, and P. Calyam, "Fully decentralized multi-party consent management for secure sharing of patient health records," *IEEE Access*, vol. 8, pp. 225777–225791, 2020.

[15] B. Jacobs, C. Lal, and M. Conti, "Integrating consent management techniques into blockchain-based medical data sharing," Delft University of Technology, 2021. [Online]. Available: http://resolver.tudelft.nl/uuid:b40c42e6-4369-46cf-a49a-4d50123ff505

[16] R. R. Agarwal, D. Kumar, L. Golab, and S. Keshav, "Consentio: Managing consent to data access using permissioned blockchains," in *Proc. IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–9.

[17] T. M. Kim, S. J. Lee, D. J. Chang, J. Koo, T. Kim, K. H. Yoon, and I. Y. Choi, "DynamiChain: Development of medical blockchain ecosystem based on dynamic consent system," *Applied Sciences*, vol. 11, no. 4, p. 1612, 2021.

[18] S. P. Mann, J. Savulescu, P. Ravaud, and M. Benchoufi, "Blockchain, consent and prosent for medical research," *Journal of Medical Ethics*, vol. 47, no. 4, pp. 244–250, 2021.

[19] M. M. Merlec, Y. K. Lee, S. P. Hong, and H. P. In, "A smart contract-based dynamic consent management system for personal data usage under GDPR," *Sensors*, vol. 21, no. 23, p. 7994, 2021.