INTERNATIONAL JOURNAL OF AGEING, SAFETY, HEALTHCARE & SCIENCE INNOVATION (IJASHSI)
Vol. 03, Issue 1, September 2025, pp: 186 – 191

Blockchain-Oriented Consent Management for Genomic and Population Health Research: A Comprehensive Review

Akintunde Gboyega[1] Ajakaye Foluke Alao[2]
Federal University of Oye Ekiti, Ekiti State [1,2]
Bachelor of Science, Computer Science
Gboyega.Akintunde@fuoye.edu.ng [1] Ajakaye.Funke@fuoye.edu.ng [2]

ABSTRACT

The rapid expansion of genomic and population health research has created a wealth of new opportunities in precision medicine, large-scale cohort studies, and population-level interventions. However, this growing activity has also raised considerable challenges around consent management, privacy protection, and governance of sensitive health and genomic data. Current consent practices and infrastructures are often static, paper-based, and inefficient for capturing the dynamism, longevity, and interoperability needs of modern health research. Blockchain technologies, with their decentralized, immutable, and transparent properties, show significant promise in addressing these issues by creating systems that are both more participant-centric and practically aligned with the needs of precision medicine.

This review article aims to provide a comprehensive overview of the opportunities and challenges around blockchain-oriented consent management systems for genomic and population health research. It analyzes the existing evidence from peer-reviewed publications, proof-of-concept demonstrations, and pilot projects. Key themes explored include the existing consent practices and their limitations, features of blockchain and its relevance for healthcare, architectures for blockchain-based consent management systems, interoperability with federated learning and privacy-preserving technologies, ethical, legal, and social implications, as well as potential barriers to implementation. Finally, the article presents future research directions that may hold particular promise for practical deployment at scale, such as hybrid blockchain architectures, integration with artificial intelligence approaches, and policy initiatives to better enable ethically and technically sound consent management.

Keywords: blockchain, consent management, genomic research, population health, privacy, precision medicine

1. Introduction

Genomic and population health research have been rapidly maturing as core components of modern health systems, with flagship initiatives like the UK Biobank, All of Us Research Program in the United States, and national genome research projects in Asian and African countries leading the way (Nayarisseri et al., 2021). The deployment and growth of these new research platforms and datasets are critical not only for the delivery of precision medicine to patients and communities but also for addressing disease prevention, risk prediction, and other population-wide challenges. Genomic data are arguably among the most sensitive of all personal information, revealing information not only about the individual from whom they were collected but also their relatives and even their community. A major reason for this sensitivity is the higher risks of genetic discrimination, stigmatization, and privacy violations. It also has long-term implications for future generations and the use of emergent technologies for genetic modification. As such, genomic research raises complex requirements for consent and privacy which must be ethically and practically sound to ensure autonomy, trust, and compliance with evolving regulatory standards.

The long-held models of one-time and static consent are no longer fit for purpose in this context. Research often spans multiple decades, involves several institutions, and changes in focus over time (Kaye et al., 2015). As a result, participants may want to adjust their consent dynamically. At the same time, regulators demand auditability and traceability. Blockchain, a distributed ledger technology with properties like immutability, transparency, decentralization, and programmable logic in the form of smart contracts, is an especially promising technology for consent management.

This article is structured as follows. After a brief introduction to the concept of consent in the next section, it dives into blockchain in healthcare and the specific relevance of this technology for managing consent in Section 3. Section 4 then delves into the various architectures, models, and components of blockchain-oriented consent management systems before exploring ethical, legal, and social implications in Section 5. The article also highlights barriers to adoption and provides a critical discussion in Sections 6 and 7, before covering case studies and future directions in Sections 8 and 9. A conclusion is provided in Section 10.

2. Consent Management in Genomic and Population Health Research

2.1 The Importance of Consent

Consent is a legal and ethical foundation of biomedical research. It protects and respects the autonomy of research participants, ensures transparency in how data will be collected and used, and helps maintain public trust in research institutions (Grady, 2015). Consent management is a bigger issue in genomic research because of higher potential risks and adverse consequences. Genetic discrimination is a unique form of privacy violation that directly endangers people (Phillips, 2018).

2.2 Traditional Consent Models

Traditional consent forms, usually static and paper-based, remain the dominant form of data access request in health and genomic research. However, this consent is typically non-longitudinal, cannot easily be adjusted or withdrawn, and is often provided once for broad “blanket” consent rather than specific uses. This consent cannot be relied upon ethically to cover the types of longitudinal, broad-scope research being increasingly deployed (Kaye et al., 2015). Dynamic consent has emerged as a more nuanced model, where participants can adjust their consent via digital platforms (Kaye et al., 2015). While this consent may be stored in a centralized database, concerns remain over trust, data integrity, and interoperability.

2.3 Challenges in Current Consent Systems

The primary challenges include the following.

- Data fragmentation: Consent preferences are siloed within individual institutions.
- Auditability: Consent changes are hard to track and verify.
- Scalability: How to provide consent services to potentially millions of participants?
- Lack of trust: Participants may not trust central repositories of their data.

3. Blockchain in Healthcare: Principles and Relevance

3.1 Blockchain Fundamentals

Blockchain is a distributed ledger that records information in a way that is cryptographically verifiable and cannot be altered without consensus of multiple parties. Key features of blockchain that are of interest for healthcare applications include:

- Immutability: Once data are recorded on a blockchain, they cannot be tampered with.
- Transparency: Transactions can be visible to authorized participants.
- Decentralization: Allows all participants to verify records without a central authority.
- Smart contracts: Self-executing code that automates the execution of a contract (Swan, 2015).

3.2 Blockchain in Healthcare

Blockchain in healthcare includes secure electronic health records, drug supply chains, clinical trial management, and credential management, among others (Agbo et al., 2019). For consent management, the key elements include an immutable audit trail, secure and direct engagement of participants, and decentralized trust.

3.3 Why Blockchain for Consent?

Consent is a permission record which by its very nature should be append-only, auditable, and under the control of the individual it concerns. These properties are natural for blockchain with its immutable, append-only ledgers. Additionally, smart contracts can be used to enforce conditions and rules granularly in the form of “only share my genomic data with research into cancer.”

4. Blockchain-Oriented Consent Management: Architectures and Models

4.1 Permissioned vs Permissionless Blockchains

The main variants of blockchain are permissionless (public) blockchains, like Bitcoin and Ethereum, and permissioned (private) blockchains like Hyperledger Fabric and Corda, where only approved entities can participate (Azaria et al., 2016). The former offer full decentralization, but with significant scalability and privacy concerns. The latter, with stricter access and permission controls, are more appropriate for healthcare data.

4.2 Consent as a Smart Contract

Consent preferences can be encoded as smart contracts that contain the rules for who can access what data and under what conditions (Dagher et al., 2018). These can be updated dynamically by the participant, and conditions for access can be automatically verified and enforced via smart contracts. For example, a smart contract could be set to only release access to a genomic dataset to researchers who can demonstrate ethical approval from a recognized board.

4.3 Interoperability with Federated Systems

Blockchain can serve as a sort of governance layer for consent, with the data itself remaining in off-chain databases or federated learning systems. Blockchain will then store cryptographic hashes and metadata of datasets to verify data integrity and versioning (Ezeogu & Osigwe, 2025). Smart contracts also execute the business logic of consent by enforcing conditions and rules.

4.4 Use Cases

Blockchain-oriented consent management use cases in genomics include:

- Dynamic consent management platforms that let participants easily update preferences.
- Cross-institutional genomic data sharing, where institutions can verify consent via blockchain without central authorities.
- Consent withdrawal, where immutable logs of consent revocation requests are guaranteed to be respected.

5. Ethical, Legal, and Social Implications

5.1 Autonomy and Empowerment

Blockchain consent management models are able to enhance participant autonomy, according to evidence from a range of proof-of-concept deployments (Kaye et al., 2015).

5.2 Privacy Issues

Although blockchain data are immutable, genomic data can never be truly anonymized. A hybrid model of off-chain storage of sensitive data with on-chain hashes allows addressing the re-identification risk (Shabani & Marelli, 2019).

5.3 Alignment with Regulations

GDPR, HIPAA, and other data privacy regulations and guidelines recognize the “right to be forgotten” which is in principle incompatible with blockchain immutability. Hybrid approaches and encryption-based consent revocation are potential solutions being explored (Roehrs et al., 2019).

5.4 Equity and Inclusion

Access to the blockchain-based platform must not worsen digital divides, particularly in low- and middle-income countries (LMICs) (Phillips, 2018).

6. Barriers to Adoption

6.1 Technical

- Scalability: Need for high throughput for large cohorts.
- Interoperability: Integration with existing health IT systems.
- Energy consumption: Carbon footprint of public blockchains in particular.

6.2 Governance

- Who administers a given blockchain network?
- How are disputes resolved?

6.3 Ethical and Social

- Understanding: Will study participants understand a blockchain-based consent system?
- Potential misuse of consent records.

7. Integrating Blockchain with Emerging Technologies

7.1 Blockchain + Federated Learning

Federated learning is an emerging AI approach for training models on distributed data sources while preserving data locality. Blockchain can provide consent and audit records while federated learning preserves data privacy (Ezeogu & Emmanuel, 2025).

7.2 Blockchain + Homomorphic Encryption

Homomorphic encryption is a cryptographic technique that allows processing of encrypted data without revealing the data (Ezeogu, 2025a). Combining this approach with blockchain can also create trust in genomic research.

7.3 Blockchain + Synthetic Data

Synthetic data generation is a risk-mitigating alternative to using real data while preserving statistical utility (Ezeogu, 2025b). Blockchain can govern access to synthetic data and datasets and provide validation.

8. Case Studies and Pilot Projects

Several pilot projects and case studies in this space, including:
- MedRec (MIT): A blockchain-based medical record and consent management system (Azaria et al., 2016).
- MyConsent (EU funded projects): A project exploring the use of dynamic consent with blockchain support.
- Genomic Data Commons pilots: Proof-of-concept demonstrations of blockchain-enabled data sharing with auditability.

The projects to date show feasibility of key approaches, but scalability and governance issues remain significant.

9. Discussion

Blockchain-oriented consent management approaches have the potential to address some of the most pressing challenges in genomic and population health research. They can improve trust, provide tamper-proof audit trails, enable greater interoperability and data reuse, and allow more participant-centric consent approaches. At the same time, however, blockchain is not a silver bullet and is associated with its own risks, challenges, and limitations. Blockchain-based systems will not be universally applicable in practice and often have regulatory conflicts, scalability issues, and public awareness or understanding barriers. A potentially pragmatic approach may involve hybrid architectures that use permissioned blockchains as a governance layer, keep the sensitive data off-chain or in federated AI learning frameworks, and otherwise provide strong guarantees of privacy and utility. Policies and regulations should also better support blockchain systems, and regulators need to more clearly articulate how this technology can be aligned with privacy rights and human subject protections while incentivizing innovations in this space. Ethical oversight of blockchain-based research is also critical to ensure transparency and inclusion.

10. Conclusion

Blockchain-oriented consent management in genomic and population health research presents tremendous opportunity and challenge. This technology can in principle address long-standing issues of trust, transparency, and scalability of consent processes while creating more participant-centric approaches. However, to realize this potential will require work on multiple levels. Technical barriers, legal and ethical issues, and public education and awareness will all need to be addressed. Future blockchain-based systems are also likely to be hybrid, combining blockchain with emerging technologies such as federated AI, homomorphic encryption, and synthetic data to strike a better balance between utility and privacy. Ultimately, blockchain-based consent systems have the potential to underpin a new era of ethically responsible, global, and interoperable genomic and population health research, but only if the right technical and governance architectures are chosen and if they are paired with an enabling environment for policy and regulation as well as ethical guidance.

REFERENCES

1. Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences*, *9*(9), 1736. https://doi.org/10.3390/app9091736

2. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. *Proceedings of the 2nd International Conference on Open and Big Data (OBD)*, 25–30. https://doi.org/10.1109/OBD.2016.11

3. Adekunle, K. A. (2025). Operational Efficiency Meets Safety: Leveraging Industrial Management Principles to Strengthen EHS Performance. *Multidisciplinary Journal of Healthcare (MJH)*, *2*(1), 114-144.

4. Adekunle, K. (2024). Empowering Communities for a Greener Future: The Role of Public Awareness and Engagement in Sustainable Waste Management.

5. Adekunle, K. (2024). Technological Innovations in Industrial Waste Recycling. *Available at SSRN 4874176*.

6. Dagher, G. G., Mohler, J., Milojkovic, M., & Marella, P. B. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society, 39*, 283–297. https://doi.org/10.1016/j.scs.2018.02.014

7. Ezeogu, A. O. (2025). POST-QUANTUM CRYPTOGRAPHY FOR HEALTHCARE: FUTURE-PROOFING POPULATION HEALTH DATABASES AGAINST QUANTUM COMPUTING THREATS. *Research Corridor Journal of Engineering Science*, *2*(1), 29-56.

8. Ezeogu, A. O. (2025). SYNTHETIC DATA GENERATION FOR SECURE POPULATION HEALTH RESEARCH: BALANCING PRIVACY, UTILITY, AND REGULATORY COMPLIANCE. *Multidisciplinary Journal of Healthcare (MJH)*, *2*(1), 51-92.

9. Ezeogu, A. O., & Osigwe, D. F. (2025). Secure Multiparty Computation for Cross-Border Population Health Research: A Framework for International Healthcare Collaboration. *NextGen Research*, *1*(1), 14-39. https://nextgresearch.com/index.php/nextgr/article/view/16

10. Ezeogu, A. O., & Emmanuel, A. (2025). Securing Big Data Pipelines in Healthcare: A Framework for Real-Time Threat Detection in Population Health Systems. *Research Corridor Journal of Engineering Science*, *2*(1), 8-28.

11. Ezeogu, A. O. (2025). Homomorphic Encryption in Healthcare Analytics: Enabling Secure Cloud-Based Population Health Computations. *Journal of Advanced Research*, *1*(02), 42-60.

12. Ezeogu, A. O. (2023). Real-Time Survival Risk Prediction with Streaming Big Health Data: A Scalable Architecture. *Contemporary Journal of Social Science Review*, *1*(1), 50-65. https://doi.org/10.63878/cjssr.v1i1.123

13. Ezeogu, A. O. (2024). Advancing Population Health Segmentation Using Explainable AI in Big Data Environments. *Research Corridor Journal of Engineering Science*, *1*(1), 267-2883.

14. Ezeogu, A. (2025). Data Analytics Approach to Population Health Segmentation. *Multidisciplinary Journal of Healthcare (MJH)*, *2*(1), 93-113.

15. Grady, C. (2015). Enduring and emerging challenges of informed consent. *New England Journal of Medicine, 372*(9), 855–862. https://doi.org/10.1056/NEJMra1411250

16. Kaye, J., Whitley, E. A., Lund, D., Morrison, M., Teare, H., & Melham, K. (2015). Dynamic consent: A patient interface for twenty-first century research networks. *European Journal of Human Genetics, 23*(2), 141–146. https://doi.org/10.1038/ejhg.2014.71

17. M’Bachi, F. D. N. C. (2025). Diaspora and Afro-Descendants in Angola–USA Business Relations. *MULTIDISCIPLINARY JOURNAL OF INSTRUCTION (MDJI)*, *8*(1), 1-20.

18. M’Bachi, F. D. N. C. (2025). Strengthening Angola-USA Relations: A Win-Win Perspective. *Journal of Social Sciences and Community Support*, *2*(1), 57-68.

19. M’Bachi, F. D. N. C. (2025). Lobito Corridor's Impact on Angola-USA Trade Relations. *MULTIDISCIPLINARY JOURNAL*

OF INSTRUCTION (MDJI), *8*(1), 21-25.

20. Nayarisseri, A., Khandelwal, R., Tanwar, P., Sharma, A., & Malapure, S. (2021). Genomic data: The future of precision medicine. *Current Genomics*, *22*(1), 7–13. https://doi.org/10.2174/1389202921666200902100517

21. Phillips, M. (2018). Genetic data and privacy. *Nature Biotechnology*, *36*(6), 490–492. https://doi.org/10.1038/nbt.4152

22. Roehrs, A., da Costa, C. A., da Rosa Righi, R., & da Silva, V. F. (2019). Personal health records: A systematic literature review. *Journal of Medical Internet Research*, *21*(1), e9744. https://doi.org/10.2196/jmir.9744

23. Shabani, M., & Marelli, L. (2019). Re-identifiability of genomic data and the GDPR. *EMBO Reports*, *20*(6), e48316. https://doi.org/10.15252/embr.201948316

24. Swan, M. (2015). *Blockchain: Blueprint for a new economy*. O'Reilly Media.