IJSRA

International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

Int. J. Sci. Res. Arch.
IJSRA
International Journal of Science and Research Archive
Research Journal Archive, INDIA

(Review Article)

Check for updates

Conceptualising a blockchain-based framework for interoperable health data sharing between state-level public health systems

David Kajovo *

Independent Researcher.

International Journal of Science and Research Archive, 2025, 16(02), 035-039

Publication history: Received on 23 June 2025; revised on 29 July 2025; accepted on 01 August 2025

Article DOI: https://doi.org/10.30574/ijsra.2025.16.2.2276

Abstract

Health data sharing remains a critical yet underdeveloped component of many state-level public health systems, often hindered by fragmented infrastructures, poor interoperability, and limited trust among stakeholders. This study develop a conceptual framework to support secure, interoperable state-boundary health data exchange based on blockchain. Based on a desk-based, thematic synthesis approach informed by the Socio-Technical Systems (STS) Theory, the paper incorporates technology, organisation, and governance aspects in one standard model. It comprises the following major elements: data layers, a permissioned blockchain structure, interoperability (e.g., HL7, FHIR) rules, role-based access control measures and participation of state-level players, e.g., Ministries of Health and state-run hospitals. The model focuses on applying smart contracts to control the process of managing consent, validating transactions with data integrity, and compliance with privacy regulations. The suggested system has several advantages: allowing access to the data in real-time across health institutions, ensuring the higher accuracy of the data, better fraud detection in health financing, and a stronger epidemic tracking and surveillance capacity. Along with its promise, the study also singles out significant implementation barriers such as legal uncertainty, deficiencies in the levels of trust, technology illiteracy, infrastructure investment, and legacy system integration challenges. It has been recommended that enabling regulatory frameworks be developed, capacity building, adoption of international data standards, and pilot in controlled environments. This conceptual approach adds to the discussion of the digital health revolution, introducing a large and safe framework suitable for decentralised health governance. It underlines the possibility of blockchain technology to eliminate ineffectiveness in protecting patient data and enhance inter-state cooperation. The research results provide strategic advice to policy-makers, health administrators, and technology developers who want to modernise the public health information system with innovative/sustainable digital infrastructure.

Keywords: Blockchain; Health Data Sharing; Interoperability; Public Health Systems; Socio-Technical Systems Theory; Smart Contracts; Data integrity

1. Introduction

The growing complexity in the provision of medical services within the system of state-level public health requires effective channels of sharing health information. Such systems tend to work as isolated systems, whereas they have fragmented databases and technologies, which cannot facilitate good interoperability, continuity of care, and successful surveillance (Shull, 2019; Adler-Milstein & Jha, 2011). Sharing health data is important with regard to enhancing patient outcomes, evidence-based policymaking, and coping with a health crisis (World Health Organization [WHO], 2021). Nevertheless, the current structures are pained by matters of security, transparency, and trust, especially in cases where health data need to be shared across state lines on a federated healthcare setting (McGhin et al., 2019; Esmaeilzadeh, 2020). Blockchain technology has a potential solution to such issues. The use of blockchain with its decentralised

* Corresponding author: David Kajovo

structure and the immutability and cryptographic security capabilities have the ability to transform the health information exchange process by offering secure, verifiability, and unmanipulability of transactions (Khezr et al., 2019; Agbo et al., 2019). It is also able to support trust among the stakeholders by creating a consensus interaction and smart contracts which can automate and force the responses of access, consent, and compliance with data-sharing controls (Zhang et al., 2020; Griggs et al., 2022). This paper attempts to conceptualise a blockchain-based platform of interoperable sharing of health data among state-based public health systems. In particular, it aims to define important elements, technologies and governance models required to design such system, and discuss practical issues, like scalability, privacy, and fulfilling regulation. The purpose then will be to suggest a theoretical model that would be in the future applied and empirically tested.

At the current stage of integration of blockchain into the infrastructure of the field of public health, primarily in low-and middle-income countries, conceptual framework is needed as a first step. It offers an orderly comprehension over how blockchain can adequately be commingled together with public health information systems and enlightens consequent fly-on-the-wall endeavors, policy, and academic investigation. This review-based approach synthesises existing literature on health interoperability and blockchain applications to propose an innovative, scalable, and secure model tailored to the needs of decentralised public health governance.

2. Literature Review

Health data interoperability is the capacity in different health information systems, applications, or instruments to gain access to, exchange, and utilise data in a harmonised method (Shull, 2019). It helps to have successful health information exchange (HIE), and it works at three levels; technical, semantic, and organisational (European Commission, 2021). Technical interoperability provides a physical ability of systems to exchange data via such standards as APIs and transport protocols (HIMSS, 2020). The semantic interoperability concentrates on the maintenance of the meaning of data across systems via the usage of terminologies like SNOMED CT or LOINC (Benson & Grieve, 2021). Organisational interoperability deals with policy, legal and governance structures that facilitate harmonised inter-institutional use of data (WHO, 2021). Interoperability, although of high priority, is lacking in numerous systems of public health (Adler-Milstein & Jha, 2011). Scattered infrastructures, inadequate data compatibility and the overall regulatory inconsistency withhold a smooth way of sharing data between state-level institutions (Esmaeilzadeh, 2020). Examples of such models include the US National Health Information Network (NHIN), NHS Spine (United Kingdom), or Health Information Exchanges (HIEs), which are advancing but have already encountered the problem of data silo, lack of scalability, and trust (McGhin et al., 2019). These issues prompted the increasing interest in blockchain as a possible innovator in the secure and combined planned data exchange (Khezr et al., 2019).

Blockchain is a decentralised ledger technology that cannot be changed and that stores an ever-increasing chain of records (blocks) chained together with cryptography (Zhang et al., 2020). It is appealing to sensitive industries such as healthcare because of its major characteristics which include immutability, decentralisation, agreement methods, and smart contracts (Agbo et al., 2019). Immutability makes information stored immutable, so after it is written, it can no longer be changed without a record of such an operation, which guarantees data integrity (Griggs et al., 2022). Decentralisation eliminates the differentiation towards a central authority, increasing the resilience of the system and trustworthiness (Kshetri, 2022). The transactions made are confirmed by a kind of consensus mechanism, i.e. Proof of Work (PoW) or Proof of Authority (PoA) and ensure stability of the network (Mettler, 2016). They have automated rules and permissions so that the sharing of data becomes dynamic and more like, in access control and managing consent (Rahman et al., 2021). Examples of blockchain are public, private, and consortium (ledger) networks (Yli-Huumo et al., 2016). Although the public blockchains ensure complete transparency, it is inappropriate in the healthcare setting because of the privacy and speed limits (Kuo et al., 2017). More suitable in the context of the application in the sphere of public health are permissioned blockchains, where participating entities are only allowed to take part in them after verification, meaning that they are more scalable, maintain confidentiality, and easier to regulate (Vazirani et al., 2022).

One of the areas where Blockchain has gained popularity in the healthcare sector is in a number of areas (Angraal et al., 2020). It enables longitudinal and patient-centrist data exchange across institutions in a secure way in electronic health records (EHRs) (Zhang et al., 2020). This makes record keeping correct and helps with auditing, as well as improving compliance (Dubovitskaya et al., 2020). Blockchain can help to counterfeit drugs in the pharmaceutical supply chain as the system is traceable (Mackey & Nayyar, 2017). Smart contracts are used in health insurance to make the process of claims and handling much easier by automating verifications and rendering payments, thus minimizing fraud (Rahman et al., 2021).   Blockchain is increasingly becoming viable, as reflected in real-life applications (Kshetri, 2022). The blockchain is used in the e-health system of Estonia where they guarantee the security of the national scheme of access to health data system (Holtbl et al., 2018). It is possible to take control of the patients record across providers using MedRec, which is developed at MIT (Azaria et al., 2016). Guardtime is a cybersecurity company that uses blockchain technology to protect health documentation and identify breaches with help of national agencies (Taylor et al., 2020). These are just a few instances of real life practicality of applying blockchain in healthcare, especially where secure, auditable and connected data systems are a must (Griggs et al., 2022).

Blockchain has limited application in the public health system, although it presents overwhelming benefits because there are technical, legal, and organisational problems associated with the implementation of blockchain (McGhin et al., 2019). One of the concerns would be scalability, because the majority of blockchain platforms fail to support a significant number of transactions per second and record large amounts of data in real-time (Vazirani et al., 2022). Those rules, including the NDPR, GDPR and HIPAA, are especially difficult to deal with when it comes to privacy and information protection (Esmaeilzadeh, 2020). The immutability of blockchain can clash with such provisions as the right to be forgotten, which makes it necessary to find architectural solutions to ensure compliance using creative methods of off-chain storage and strong encryption (Griggs et al., 2022). Limited resources and infrastructure also limit the uptake particularly in resource-limited environments (Agbo et al., 2019). Its implementation requires investing in hardware, technical knowledge, and integration with the already existing legacy systems (Kshetri, 2022). No standardised blockchain protocols make interoperability and system design even more complicated (Zhang et al., 2020). Lastly, it has problems with regard to policy and governance (WHO, 2021). Concerns pertaining to the right to own data, liability when breaches occur, and harmonisation of regulatory regimes in different jurisdictions reduce the level of confidence that stakeholders might have and hinder the mass adoption (Rahman et al., 2021).

3. Theoretical Framework

In the quest to conceptualise a blockchain framework of interoperable sharing of health data among state-level public health systems, it must be ensured that the process begins with a strong theoretical model on which it can base the analysis (Bostrom & Heinen, 1977). A much apt theory to be used as basis in that regard is the Socio-Technical Systems (STS) Theory (Baxter & Sommerville, 2011). The STS theory was initially created to investigate the relationship between human and technology within the working place (Mumford, 2006) and it is based in the idea that organisations are formed as a combination of social systems i.e. people, processes and culture and the technical systems i.e. tools, technologies and structure and both systems need to be integrated in order to implement innovations successfully (Berg, 1999). The introduction of blockchain into the public health data system means not only the change of technology but the change of the management, sharing, and governance of sensitive information within institutions (Kshetri, 2022). Thus, the STS theory allows one to get a complex picture of how blockchain can be introduced into the current socio-political and institutional context of public health (Coiera, 2015). Not only does the theory allow investigating the technical characteristics of blockchain (i.e., not only decentralisation, consent and immutability) (Zhang et al., 2020), but also the social and organisational aspects, including user acceptance, institutional readiness, policy alignment and governance (McGhin et al., 2019).

Making use of the concept of the STS to blockchain settings means determining the manner in which technological variables namely permissioned ledgers, smart contracts, and interoperability protocols (Griggs et al., 2022) interseed with social elements that include data ownership, trustworthiness between institutions, and regulatory adherence (Esmaeilzadeh, 2020). To provide an example, smart contracts can manage access controls through predetermined patient consent policies, yet their effective implementation is possible due not only to the authenticity bestowed upon them by institutional players and citizens but also to their legitimate status (Rahman et al., 2021). mimically, the operation of decentralised data governance structures is possible only when state health agencies consent to a unified data format and shared oversight arrangements (Adler-Milstein & Jha, 2011). Possible mismatches of technological and organisational abilities are also identifiable across the spectrum of the STS approach (Shull, 2019). An otherwise technically viable blockchain solution can turn out a failure because medical employees are not digitally literate enough to work with it or because proper legal framework fails to support it (WHO, 2021). This framework can therefore be used as a diagnostic framework in the prediction of challenges as well as a design framework to create a system which is technically viable as well as socially acceptable (Baxter & Sommerville, 2011).

3.1. Proposed Blockchain-Based Conceptual Framework

The specified conceptual framework suggests the introduction of the blockchain technology into the public health systems operating at a state level to allow the safe and interoperable sharing of health data. It has five fundamental parts: Data layers, blockchain level, interoperability protocols, access control and governance and state-level actors. A combination of these aspects creates a decentralised, secure, and scalable model of health information exchange. At the data level, the data sets are standardised and may contain patient identifiers, clinical encounters, laboratory findings and immunisation records. The latter are stored on-chain using cryptographic hash and metadata as an immutable trail of accountability and authenticity, whereas secure databases are used off-chain to optimise scaling. Specifically the blockchain layer has been implemented on a permissioned blockchain which enables decentralised control by verified stakeholders. Such consensus algorithms as Proof of Authority (PoA) or Practical Byzantine Fault Tolerance (PBFT) confirm transactions effectively. The data sharing, enforcing of the rights to access, and patient consent are all automated via smart contracts at this layer. Protocols for interoperability allow the technical and semantics consistency of shared information as HL7 and FHIR, which facilitate the compatibility with the current health systems. The process of access control is coordinated by smart contracts and role-based mechanisms limiting the access to the data to the authorised users like clinicians and health administrators. Lastly, state-level players, such as the Ministries of Health, health hospitals, and health research institutes serve as validator nodes and regulators of the governance policies. Their participation also guarantees compliance, accountability and sustainability of the system. The framework therefore provides a unified approach to sharing health data in real time, secure, standards-based across the lines of states.

3.2. Potential Benefits, Implementation Scenarios, and Challenges

The advantage of using a blockchain-based interoperable health data sharing framework is of great value to the public health system. The very high degree of data integrity is one of its most significant advantages. Health data cannot be modified or deleted since it is stored in blockchain, which supports the former and eliminates the possibility of tampering or fraud. This increases the confidence between institutions and patients. Moreover, the framework will result in real-time access to data about patients across states and, therefore, the continuity of care, accelerated decision-making, and better patient outcomes, mainly when they are addressed in different places. In health financing, blockchain may identify fraud since all financial and service transactions are recorded in an open system; hence, claims are easily audited, and inconsistencies can be spotted. The system is also quite appropriate in crisis surveillance and pandemic tracking because it permits secure and timely communication among epidemiological data among state health departments and enhances coordination and response efforts. These advantages, however, do not come without significant hurdles. Proper legal structures and community confidence are essential, particularly in sensitive health data. Without sturdy data protection laws and open communication, people might be wary of stopping its usage. Further, health workers and administrators are usually low in technological literacy; special training and capacity building are therefore required so that implementation is successful. This can hinder the expenditure to implement the blockchain infrastructure and its upgrades, training, and future upkeep costs that can be a cost in resource settings. Planning in phases and social-private joint ventures can reduce it. Finally, legacy systems integration is technically challenging; the migration to open standards and interoperability regulations like FHIR will facilitate the process and enable the current systems to be connected to the blockchain platform effortlessly.

Recommendations

To facilitate the efficient sharing of health data using blockchain technology at the state level, Ministries of Health should develop clear regulatory frameworks to promote data privacy, governance, and interoperability. This involves a partnership between stakeholders (i.e., the participation of the public hospital, IT developers, and policymakers) to align both the technical and the institutional requirements. Digital infrastructure and workforce training should be invested to fill historical technological illiteracies. The integration into the existing systems will be ensured by adopting international standards such as FHIR and HL7. Roll-outs in a few areas can be conducted to generate findings practically before scaling up in the country. Lastly, trust in blockchain should be created to help protect health data and simultaneously improve service delivery.

4. Conclusion

This paper has conceptualised a blockchain architecture that is a transparent way of sharing health data between state-based municipal systems. Blockchain is a secure and efficient way to resolve old trust and data fragmentation issues because of decentralization, immutability, and smart contracts. The proposed model model fuses technical and governance aspects specific to the field of public health. Although considerable advantages like enhanced data integrity, real-time accessibility, and fraud detection, among others, seem to be apparent, issues concerning legal, infrastructural, and educational mismatches need to be considered. Finally, blockchain can be transformative in the case of its implementation in a phased, inclusive, and well-regulated way that corresponds to the realities of the local health system.

References

[1] Adler-Milstein, J., & Jha, A. K. (2011). Health information exchange among U.S. hospitals. Health Affairs, 41(2), 197-205.

[2] Agbo, C. C., Mahmoud, Q. H., & Eklund, J. M. (2019). Blockchain technology in healthcare: A systematic review. Healthcare, 7(2), 56.

[3] Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From design methods to systems engineering. Interacting with Computers, 23(1), 4-17.

[4] Berg, M. (1999). Patient care information systems and health care work. Social Science & Medicine, 48(6), 773-781.

[5] Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. MIS Quarterly, 1(3), 17-32.

[6] Coiera, E. (2015). Guide to health informatics (3rd ed.). CRC Press.

[7] Esmaeilzadeh, P. (2020). The impacts of interoperability and trust on health information exchange. Journal of Medical Internet Research, 22(6), e16407. Griggs, K. N., Ossipova, O.,

[8] Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2022). Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. Journal of Medical Systems, 46(3), 17.

[9] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. Applied Sciences, 9(9), 1736.

[10] Kshetri, N. (2022). Blockchain in healthcare: Opportunities and challenges. IT Professional, 24(1), 8-14.

[11] McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. Journal of Network and Computer Applications, 135, 62-75.

[12] Mumford, E. (2006). The story of socio-technical design. Journal of Information Technology, 21(4), 226-234.

[13] Rahman, M. A., et al. (2021). Secure and provenance-enhanced Internet of Health Things. IEEE Journal of Biomedical and Health Informatics, 25(3), 871-881.

[14] Shull, J. G. (2019). Digital health and the state of interoperable electronic health records. JMIR Medical Informatics, 7(4), e12712.

[15] World Health Organization. (2021). Global strategy on digital health 2020-2025. https://www.who.int/publications/i/item/9789240020924

[16] Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2020). Applying blockchain technology to improve clinical trial transparency. IEEE Transactions on Emerging Topics in Computing, 8(1), 184-195.