IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Application in Genomic Data Challenges and Use of Smart Contracts to Enhance Data Security: Review

Chigozie A. Nnadiekwe[1,2]MSc, BSc, Samuel C. Iwuji[1]PhD, MSc, BSc, Taofik O. Azeez[1,2]PhD, MSc, BSc, Geraldine C. Okafor[1] BSc

[1] Federal University of Technology, Owerri, Imo State Nigeria.

[2] King David University of Medical Science, Uburu, Ebonyi State, Nigeria.

Corresponding Author: cnnadiekwe01@gmail.com

Abstract

In this paper, we examine Blockchain technology's smart contracts feature as a solution to issues with bioinformatics and the difficulties of exchanging health data. Sharing genomic data sets presents significant challenges because it is different from sharing traditional medical data, it reveals information about the data owners', ancestors and relatives, and continues to carry value even after the data owner's death and these issues raise serious concerns about data security. Therefore, while working with genomic data, strict data ownership and control mechanisms are needed. Blockchain technologies present a promising alternative to conventional distribution networks in the provision of safe and accountable infrastructure. This is the rationale behind the genomics-related Blockchain infrastructure research that is on the rise. We proposed a model that would deployed a smart contracts feature of blockchain to enhance data security.

Keyword; *Blockchain, Smart contracts, Genomic data Security, Bioinformatics.*

1.0 Background

The quality and amount of genetic data are expanding quickly as a result of recent technological advancements. In order to maximize medical resource allocation, clinical decision support, medical quality monitoring, precision medicine, and disease risk assessment and prediction,

sharing and using genomic data has been crucial [1,2]. Most frequently, exposing this data exposes users to dangers related to data security and privacy concerns, data dictatorship, inadequate subject autonomy, escalating social injustice, and others [3].

1.1 Bioinformatics

The term "bioinformatics" was initially used in the early 1970s by Paulien Hogeweg and Ben Hesper, who described it as "the study of informatics processes in biotic systems"[4]. Big data analysis for biological data sets is essentially what bioinformatics is. To derive meaning from biological data, computational and statistical analysis are required. The development of methods and tools used to comprehend biological data is sometimes referred to as bioinformatics. It is an area of study that combines biology, computer science, and statistics. It's crucial to note that research into these bioinformatics helps uncover genes that are susceptible to disease. When studied appropriately, it will open up the possibility of developing tailored therapy because it will reveal the pathogenic pathways implicated in disease.

1.2 Blockchain Technology

The original Blockchain was developed to support cryptocurrencies, but it has since received much attention for its potential to revolutionize a wide range of industries. Decentralization, autonomy, reliability, and transparency of data are also made possible through blockchain. Satoshi Nakamoto initially created the Blockchain for the cryptocurrency Bitcoin. Blockchain has been adapted as a decentralized append-only ledger for a variety of data management applications, including streamlining remittances, improving food traceability, protecting electronic health records, guaranteeing the privacy of genomic data, developing artificial intelligence, bolstering cyber security, combating climate change, etc. and assisting with clinical studies [5-10]. Blockchain technology's append-only architecture can ensure a comprehensive, traceable, and essentially tamper-proof record. The Blockchain's technology allows for the recording of transactions, continuously keeping them unchanged while providing constant updates [11]. The Blockchain is made up of a linked series of blocks containing transactions with timestamps that are protected by cryptography. As a result, the database, development platform, and virtual network intermediate all play a part in providing the Blockchain [11].

Medical professionals will be able to safely and confidentially create patient health records using Blockchain technology, as well as choose the best therapeutic interventions and forecast the course of disease.

1.2.1 Any Blockchain has the following primary characteristics:

i) Decentralized structure of data storage; a dispersed end-to-end network structure rather than a centralized management organization which governs the entire network's data storage [12-15]. Example: Preservation and authorization of health data.

ii) Maximum system transparency for users; the supply chain, clinical trials, and biomedical research network all have open and transparent transaction records, eliminating information asymmetry [13-19]. Examples include clinical trials, supply chains, and biomedical research.

iii) The inability to alter previously recorded data. Transaction data is encrypted using asymmetric cryptography, and with the aid of a workload proof method, it is ensured that the data are practically impossible to alter [13-15,18].

iv) Autonomy; [12,13,15,17&18] used consensus-based specifications and protocols to enable autonomous data sharing between all nodes in a decentralized setting. For instance, health status surveillance and monitoring under medical insurance.

1.2.2 Data Security

A database controlled by a single party makes data manipulation much simpler and information less secure. In contrast, Blockchain is based on a decentralized approach in which all data is spread over the network and encrypted. This guarantees that all data is extremely safe and cannot be used against it. The well-known cryptocurrency bitcoin (BTC) is built on this similar type of data storage [20]. Blockchain has limited security advantages over conventional network structures since it runs on a peer-to-peer network of nodes (tiny computers that function as servers). Each block of data must be verified by consensus of the data within the chain in addition to being decentralized across nodes in order to be included in the chain. The Blockchain's immutability (which keeps track of all data changes) and the requirement for consensus go hand in hand with the necessity for security [21]. Companies like Genobank.io, which only do genetic testing, save the genetic data of their clients in the blockchain and give them the key so that they

are the only ones with access (GenoBank.io: offering a private and safe means to store DNA data). This type of data control significantly reduces the possibility of information theft and guarantees that a record will exist in the event that a copy is made.

1.4 Current Concerns Regarding the Security and Exchange of Genomic Data

In recent years, the fast growing utility of bioinformatics has exposed hitherto unheard-of security vulnerabilities. For instance, there have apparently been a lot of instances in the US when patient genomic data has been misused and disseminated. Insurance firms and the FBI were given access to consumers' genealogy information without their knowledge [22]. In order to gain knowledge on the patient's health, bioinformatics was used. Compute-intensive data processing, as well as data storage and sharing with consideration for privacy, are additional bioinformatics concerns associated with genomics or any other omic topic.

1.4 Some Common Obstacles to Sharing Genomic Data Using Blockchain Technology

The following is a summary of the existing issues and restrictions with using Blockchain in genomics, according to [23].

i) Barriers to acceptance: Blockchain platforms are dynamic and necessitate specialist knowledge for adoption. Its use is restricted to tech-savvy individuals due to instability and poor user interfaces, which are major obstacles to widespread adoption.

ii) Interoperability: Businesses must connect and integrate blockchain systems with currently used non-Blockchain technologies. This problem is made worse by the large variety of Blockchain implementations available today, many of which are incompatible with one another. The reliance on a single Blockchain platform is decreased via interoperability between Blockchains. Most genomics-related solutions currently being proposed rely on a particular Blockchain platform. Better scalability and elimination of security threats related to the deployed platform would come from a multi-Blockchain approach that is independent of any one Blockchain platform. However, the current implementation of this strategy requires difficult cross-chain communication. Future multi-Blockchain strategies may be possible as Blockchain interoperability research continues to advance [24]

iii) Smart Contract Security: In the subsection that follows, we'll go into further detail on smart contracts. Here, the Blockchain needs to address rich applications that go beyond financial transactions. Additionally, smart contracts' expanded capability exposes the system to more potential threats [25]. According to [26], there are more smart contracts vulnerabilities being found. Additionally, they are expensive in terms of monetary loss or loss of data privacy. The security risk involved with using such smart contracts to manage genuine patient data is one of the difficulties. Research on the security of smart contracts is still ongoing, but best practices and security audits could help to lower this risk [26].

iv) Data Privacy: Because users are anonymous, it was necessary to look at several aspects of privacy and re-identification using correlation attacks. Re-identification may occasionally be necessary in research settings, but it is crucial to avoid disclosing patient information for any other reason. Re-identification is necessary, for instance, when further information about the case or supplementary materials are requested. Re-identification to reveal patients' personal information, however, needs to be prevented. The following are some privacy issues with genomic Blockchains:

(a) Identity and transaction privacy: This calls for the maintenance of the user's private identity and dissociation from the transaction. Further study is needed to address the privacy issue of correlation attacks, in which a person's genuine identity may be revealed. In a perfect world, it shouldn't be able to identify a user based on certain interactions with companies. Zero-knowledge proofs (ZKPs) have been the subject of ongoing research [27], which has shown that it is possible to do this in financial applications.

(b) Re-identification risks: According to [23], [28], the process of anonymizing and obtaining consent for genomic data is time-consuming and necessitates an honest third party in the scenario where Blockchain serves as open access to genomic data for research purposes. Scaling this up is challenging when there are many patients. However, as demonstrated in [29], the dangers of re-identification linked to open data sharing persist even after the whole re-identification procedure. There is still a chance that more sophisticated re-identification attacks could appear in the future, even though this procedure may adhere to best practices for anonymizing the data [23].

v) Validity and reproducibility: duplicable research is very vital since data in a decentralized network live in many storage places, this issue must be addressed when Blockchain promotes data exchange for scientific studies [23].This issue arises more frequently in off-chain storage-based systems.

vi) Verifiability: One of the problems with disclosing data to unknown people is confirming the correctness of the results. Outsourcing the same analysis task to numerous analysis nodes, where the findings may then be compared to guarantee accuracy, is one potential option [23]. However, this strategy can be expensive, especially if the same task is divided among many analysis nodes. Therefore, there is still a need for further research into a workable and scalable verification approach to confirm that outsourced computation/analysis is truly successfully computed by untrusted nodes in a Blockchain network. Verifiable computation has undergone major breakthroughs [30], which can be investigated in a Blockchain environment. Verifiable findings can be maintained using cryptographic methods such homomorphic encryption [31] and zero-knowledge proofs [32]. The constraints of the current work in genomic Blockchains may be overcome by using these strategies.

vii) Key management: It might be difficult to make sure that patients (data owners) can securely maintain their keys and identities, especially when dealing with information on a person's personal health [23]. In order to give patients useful knowledge about best data management practices, education methods must be put in place once they have complete authority over their data [23]. Also necessary are ways for "break glass" access to genomic/healthcare data in emergency situations, as well as appropriate key management strategies.

viii) Ethical Issues: According to Alghazwi et al. [33,34], the growth of genomic marketplaces presents some ethical issues. Informed permission, according to the authors, is dubious when a financial incentive is involved and can result in unthinking data sharing. Although it is still unknown if these financial incentives will truly succeed in encouraging more people to give their private data for research reasons, it may be worthwhile to investigate non-financial alternatives. For instance, [35] demonstrated how the usage of digital collectibles might encourage people to take part in animal conservation. The writers and CryptoKitties have collaborated to produce a non-fungible coin (NFT) and a CryptoKitty with a turtle theme. Then, they offered it for sale on

the Blockchain, raising $25,000 for wildlife preservation. The purchaser has an unchangeable, one-of-a-kind digital item that symbolizes their support for wildlife. Therefore, more investigation into non-financial incentives that promote involvement in genetic research with the goal of promoting medical research may prove fruitful.

2.0 Biological Boolean Logic Gates and Smart Contracts

When computer engineer Wei Dei posted about anonymous credits in the 1990s, [36] later suggested the potential use of smart contracts and the use of cryptographic procedures to increase security. From there, the history of smart contracts was established. It would enable the user to define who can query and publish data to his Blockchain, as well as when and what data was viewed. The user could also provide a set of access rights. In this scenario, only the user would be able to modify the access control regulations, which would also be safely kept on a Blockchain. This will provide a transparent environment and give the user complete control over what information is gathered and how it can be shared.

Blockchain has become a desirable platform for encoding Boolean logic gates for biological systems because to the implementation of Smart contracts characteristics. Smart contracts protocols are implemented automatically thanks to this, which was first proposed by Nick Szabo and then merged with the Ethereum Blockchain by Vitalik Buterin [37]. The protocols for smart contracts automatically execute when specific requirements are met and benefit from all the key characteristics of the Blockchain, including decentralization, immutability, and validity. For instance, smart contracts on a Blockchain can automatically handle the sale of property through an agreement that cannot be lost or fraudulently changed, replacing the need for a real estate broker [37]. The fundamentals of conditionality are shared by Boolean logic gates and smart contracts. Boolean logic utilizes binary values (true (1) and false (0)) and logic operators like conjunction (AND gate), disjunction (OR gate), negation (NOT gate), and exclusivity (XOR gate). Smart contracts are created using the procedural programming language Solidity. Declarative languages specify the desired outcome, whereas procedural languages describe how a procedure is carried out step-by-step. There have been significant efforts to move toward declarative programming in order to develop logic-based smart contracts that are less prone to mistakes and ambiguity than conventional smart contracts [38,39]

2.1 The Benefits of Smart Contracts

The capacity to prevent single points of failure and maintain an immutable record of data are two characteristics that smart contracts inherit from the underlying Blockchains. Contractual processes can be automated, reducing the need for parties to engage and cutting down on administrative costs.

2.1.1 Smart Contracts in Medical Studies

Here, we divide smart contracts into two categories based on the Blockchain platforms they use: public smart contracts and permissioned (private) smart contracts.

	Public Smart Contracts	Permissioned Smart Contracts
Similarities	Immutable record Proper encryption on data and pseudonymity Interoperability among different platforms Traceable modifications.	
Differences	Easy to deploy Accessible for the public	Faster settlement Lower operational cost Permissioned access

Table 1: Characteristics of public and permissioned smart contracts. [40]

2.2 Blockchain technology applications

The list of uses for Blockchain technology is not exhaustive.

Supply Chain Management, Capital Markets, Trade Finance, Regulatory Compliance and Audit, Money Laundering Protection, Insurance, Peer-to-Peer Transactions, Real Estate, Media, Energy, Record Management, Identity Management, Voting, Taxes, Non-Profit Organizations, Compliance/Regulatory Oversight, Big Data, Data Storage, and Internet of Things (IoT).

2.1.2 Healthcare

In this study, we would concentrate on discussing health statistics. Scalability, access security, and data privacy are the three main components that Blockchain for health care would need to address technologically. General information like age and gender, as well as potentially more fundamental medical history information like immunization records and vital signs, are examples of health data that are excellent candidates for Blockchain. Notably, none of the aforementioned data can be used to specifically identify any one patient, allowing it to be maintained on a

Blockchain and viewed by many people without raising any privacy issues. Many medical practitioners view smart contracts and Blockchain technology as a safe means to share and access patients' electronic medical records (EMR). Smart contracts, as mentioned in the previous article, can include multi-signature approvals between patients and providers to restrict who is allowed to view or add to a patient's record. Additionally, they facilitate interoperability through cooperative version control to keep the consistency of record. Smart contracts can be used to give researchers access to specific personal health data and make it possible for micropayments to be automatically given to patients for participation, in addition to helping patients and their healthcare providers. Blockchain for health data and its possible use in studies on health and medical treatment [41].

Conclusion

Decentralized, transparent, and secure health care service improvements are possible using Blockchain technology. Blockchain technology has the potential to provide long-term advantages in health care data management with the development of smart contracts, these technologies, and their interaction with other cutting-edge technologies. Blockchain is a potent instrument that can enable people to govern their own health data, enable a flawless health data history, and establish medical accountability in addition to being a means to safeguard electronic health information. Additionally, the use of Blockchain technology improves privacy and trust while speeding up the completion of financial transactions and medical records [42].

Future Work

Having reviewed several works on application of Blockchain in genomic data security, we would propose a model where smart contracts would be deployed to enhance genomic data protection where unauthorized identification of data owners, alteration or manipulation of data without consent and sharing of patients data without consent would be impossible. The model would provide maximum security and also aids the care giver with enough data for optimum decision making.

Ethics approval and consent to participate: There were no ethical barrier against this review.

Consent for publication: This paper is consented for publication Availability of data and material: All data and material on this paper are readily available at any giventime.

Competing interests: Authors declared no competing or conflicting interests.

Funding: There was no funding received for this review.

Authors' contributions: this review was written by all authors. They approved the final version of the paper. Nnadiekwe C.A.(Corresponding author): conceptualization, writing, editing, supervision and review. Iwuji S.C.: coordinating, writing, editing and review. Azeez T.O.: writing and editing. Okafor G.C.: writing.

Acknowledgements: The authors wish to acknowledge Dr. Saviour Igboanusi for his great contributions towards the success of this review.

References

1 TK Mackey, T Kuo, B Gummadi, KA Clauson, G Church, D Grishin, et al. 'Fit-for-purpose?' - challenges and opportunities for applications of blockchain technology in the future of healthcare. BMC Med 2019 Mar 27;17(1):68.

2 T Justinia. Blockchain technologies: opportunities for solving real-world problems in healthcare and biomedical sciences. Acta Inform Med 2019 Dec;27(4):284-291.

3 Y Xie, MD; J Zhang, MD; H Wang, MD; P Liu, MD; S Liu, et al. Applications of Blockchain in the Medical Field: Narrative Review, (J Med Internet Res 2021;23(10):e28613) doi: 10.2196/28613.

4 PLOS Computational Biology, https://journals.plos.org/ploscompbiol/article?id=10.1371/journal.pcbi.1002021, Accessed September 2022.

5 G Chapron. The environment needs cryptogovernance. Nature 545, 403–405 (2017). https://doi.org/10.1038/545403a.

6 D Grishin., K Obbad, and G Church. (2019). Data privacy in the age of personal genomics. Nat. Biotechnol. 37, 1115–1117.doi: 10.1038/s41587-019-0271-3.

7 P Howson. (2019). Tackling climate change with blockchain. Nat. Clim. Chang. 9, 644–645. doi: 10.1038/s41558-019-0567-9.

8 DR Wong, S Bhattacharya, and AJ Butte, (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain. Nat. Commun. 10:917. doi: 10.1038/s41467-019-08874-y.

9 C. Krittanawong, A.J. Rogers, M. Aydar, E. Choi, K.W. Johnson, Z. Wang, et al. (2020). Integrating blockchain technology with artificial intelligence for cardiovascular medicine. Nat. Rev. Cardiol. 17, 1–3. doi: 10.1038/s41569-019-0294-y.

10 A. Reina, (2020). Robot teams stay safe with blockchains. Nat. Mach. Intell. 2, 240–241. doi: 10.1038/s42256-020-0178-1.

11 N. Rasskazova, & L. Ratushnaia, (2021). Blockchain Technology Changing Traditional Methods of Applied Research in Bioinformatics. In I. Management Association (Ed.), Research Anthology on Blockchain Technology in Business, Healthcare, Education, and Government (pp. 1813-1822). IGI Global. https://doi.org/10.4018/978-1-7998-5351-0.ch098.

12 M.S. Porsdam, J. Savulescu, P. Ravaud, M. Benchoufi. Blockchain, consent and prosent for medical research. J Med Ethics 2020 May 04:244 doi: 10.1136/medethics-2019-105963.

13 S.S. Ahmad, S. Khan, M.A. Kamal. What is blockchain technology and its significance in the current healthcare system? A brief insight. Curr Pharm Des 2019;25(12):1402-1408. doi: 10.2174/1381612825666190620150302.

14 M. Kim, S. Yu, J. Lee, Y. Park. Design of secure protocol for cloud-assisted electronic health record system using blockchain. Sensors (Basel) 2020 May 21;20(10):2913 doi: 10.3390/s20102913.

15 H. Rathore, A. Mohamed, M. Guizani. A survey of blockchain enabled cyber-physical systems. Sensors (Basel) 2020 Jan 03;20(1):282 doi: 10.3390/s20010282.

16 T. Kuo, R.H. Zavaleta, L. Ohno-Machado. Comparison of blockchain platforms: a systematic review and healthcare examples. J Am Med Inform Assoc 2019 May 01;26(5):462-478 doi: 10.1093/jamia/ocy185.

17 T. Alladi, V. Chamola, JJPC Rodrigues, S.A. Kozlov. Blockchain in smart grids: a review on different use cases. Sensors (Basel) 2019 Nov 08;19(22):4862 doi: 10.3390/s19224862.

18 I. Abu-Elezz, A. Hassan, A. Nazeemudeen, M. Househ, A. Abd-Alrazaq. The benefits and threats of blockchain technology in healthcare: A scoping review. Int J Med Inform 2020 Oct;142:104246 doi:10.1016/j.ijmedinf.2020.104246.

19 H. Shu, P. Qi, Y. Huang, F. Chen, D. Xie, L. Sun. An efficient certificateless aggregate signature scheme for blockchain-based medical cyber physical systems. Sensors (Basel) 2020 Mar 10;20(5):1521 doi: 10.3390/s20051521.

20 https://bccollective.io/what-is-blockchain-and-how-does-it-work/

21 L. Eduardo 2021-2-14 Blockchain and Bioinformatics - Converging Technologies that Strive to Improve Genetic Data Security - GeneOnline News.

22 https://www.axios.com/dna-test-results-privacy-genetic-data-sharing-4687b1a0-f527-425c-ac51-b5288b0c0293.html.

23 M. Alghazwi, F. Turkmen, J. Van Der Velde, D. Karastoyanova, Blockchain for Genomics: A Systematic Literature Review arXiv:2111.10153v1 [cs.CR] 19 Nov 2021.

24 B. Rafael, André Vasconcelos, Sérgio Guerreiro, and Miguel Correia. 2020. A survey on blockchain interoperability: Past, present, and future trends. arXiv preprint arXiv:2005.14282 (2020).

25 I.M. Muhammad, L.S. Charles, G. Alana, G. Elgar, F. Gabrielle, S. Ryan, M.K. Henry, and L. Marek. 2019. Understanding a revolutionary and flawed grand experiment in blockchain: the DAO attack. Journal of Cases on Information Technology (JCIT) 21, 1 (2019), 19–32.

26 C. Huashan, P. Marcus, N. Laurent, and X. Shouhuai. 2020. A survey on ethereum systems security: Vulnerabilities, attacks, and defenses. ACM Computing Surveys (CSUR) 53, 3 (2020), 1–43.

27 P. Juha, N. Tri Hong, and S. Pirttikangas. 2020. Non-Interactive Zero-Knowledge for Blockchain: A Survey. IEEE Access 8 (2020), 227945–227961.

28 B. S. Glicksberg, B. Shohei, R. Currie, A. Griffin, Z. J. Wang, D. Haussler, T. Goldstein, and E. Collisson. 2020. Blockchain-Authenticated Sharing of Genomic and Clinical Outcomes Data of Patients With Cancer: A Prospective Cohort Study. J Med Internet Res 22, 3 (20 Mar 2020), e16810. https://doi.org/10.2196/16810.

29 L. Rocher, J. M. Hendrickx, and Y-A De Montjoye. 2019. Estimating the success of re-identifications in incomplete datasets using generative models. Nature communications 10, 1 (2019), 1–9.

30 X. Yu, Z. Yan, and A. V. Vasilakos. 2017. A survey of verifiable computation. Mobile Networks and Applications 22, 3 (2017), 438–453.

31 R. Gennaro, C. Gentry, and B. Parno. 2010. Non-interactive verifiable computing: Outsourcing computation to untrusted workers. In Annual Cryptology Conference. Springer, 465–482.

32 J. B. Almeida, E. Bangerter, M. Barbosa, S. Krenn, A-R Sadeghi, and T. Schneider. 2010. A certifying compiler for zero-knowledge proofs of knowledge based on σ-protocols. In European Symposium on Research in Computer Security. Springer, 151–167.

33 E. Ahmed and M. Shabani. 2019. DNA Data Marketplace: An analysis of the ethical concerns regarding the participation of the individuals. Frontiers in genetics 10 (2019), 1107.

34 De Francesco and A. Klevecz. 2019. Your DNA broker. Nature biotechnology 37, 8 (2019), 842.

35 N. Mofokeng and T. Fatima. 2018. Future tourism trends: Utilizing non-fungible tokens to aid wildlife conservation. African Journal of Hospitality, Tourism and Leisure 7, 4 (2018).

36 N. Szabo. Formalizing and securing relationships on public networks. First Monday, 2(9), 1997.

37 A.C. Chin (2020) Blockchain Biology. Front. Blockchain 3:606413. doi: 10.3389/fbloc.2020.606413.

38 F. Idelberger, G. Governatori, R. Riveret, and G. Sartor, (2016). "Evaluation of logic-based smart contracts for blockchain systems," in Rule technologies. Research, Tools, and Applications. RuleML 2016. Lecture Notes in Computer Science, Vol. 9718, eds J. Alferes, L. Bertossi, G. Governatori, P. Fodor, and D. Roman (Stony Brook, NY: Springer), 167–183.

39 J. Hu, and Y. Zhong, (2018). "A method of logic-based smart contracts for blockchain system," in Proceedings of the 4th International Conference on Data Processing and Applications (Guangdong: ACM), 58–61. doi: 10.1145/3224207.3224218.

40 H. Yining, L. Madhusanka, M. Ahsan, T. Kanchana, J. Guillaume, S. Aruna, Blockchain-based Smart Contracts - Applications and Challenges arXiv:1810.04699v2 [cs.CY] 8 Jun 2019.

41 https://www.healthit.gov/sites/default/files/11-74 Blockchain for health data and its potential use in health it and health care related research. a blockchain for health care .pdf. Accessed: 2022-09-29.

42 F.M. Bublitz, A. Oetomo, K.S. Sahu, A. Kuang, L.X Fadrique, P.E. Velmovitsky, et al. Disruptive technologies for environment and health research: an overview of artificial intelligence, blockchain, and Internet of Things. Int J Environ Res Public Health 2019 Oct 11;16(20):3847.