Blockchain Technology in Medical Data Processing: A Study on Its Applications and Potential Benefits

Olga Siedlecka-Lamch[1][a] and Sabina Szymoniak[1][b]

[1] *Department of Computer Science, Czestochowa University of Technology, Dabrowskiego 73, 42-200 Czestochowa, Poland*

Keywords: Blockchain, Medical Data Storage, Data Modelling.

Abstract: Blockchain is a digital ledger technology that uses a decentralised, distributed database to record and validate transactions. It allows multiple parties to access the same information and make changes to it securely and transparently without the need for a central authority. The potential of blockchain technology can streamline and improve efficiency in many industries and sectors. One such application is the processing of medical data. The use of blockchain is associated with the need to meet many challenges related to the scalability of processing and storing large amounts of medical data, their security and interoperability. This article presents an original idea for storing and processing medical data by combining blockchain technology with relational databases. Such a combination will bring positive effects in terms of protecting patients' privacy, increasing trust in the system and increasing the efficiency and effectiveness of medical data management. In the proposed model, blockchain technology will ensure security, immutability and transparent medical data storage. A relational database, on the other hand, will facilitate the processing and sharing of data. The model includes patient data, their insurance, bills, healthcare workers, doctors, nurses, and data related to the treatment process: visits, referrals, releases, test results, diagnoses and medications.

1 INTRODUCTION

Blockchain is a digital ledger technology that uses a decentralised, distributed database to record and validate transactions. The underlying technology enables the creation of digital currencies such as Bitcoin, but it can also be used for a wide range of other applications. The critical feature of blockchain is that it allows multiple parties to access the same information and make changes to it securely and transparently without the need for a central authority. This makes it well-suited for use cases such as supply chain management, digital identity verification, and many more (Peck, 2017; Raikwar et al., 2020; Wang et al., 2020).

Blockchain technology has the potential to bring about significant changes in a wide range of industries and sectors. Some of the key areas where blockchain is being used or has the potential to be used include Financial Services, where it can streamline and improve the efficiency of financial transactions such as payments, remittances, and securities trading (Patel et al., 2022). In Supply Chain Management, blockchain can create a tamper-proof and transparent record of transactions across the supply chain, improving traceability and reducing fraud. Additionally, it can be used to create digital identities that are secure, private, and verifiable, which can be used to improve access to services and reduce fraud (Queiroz et al., 2019). In healthcare, it can be used to securely store and share medical data, improving patient outcomes and reducing administrative costs (Román-Belmonte et al., 2018). In the Internet of Things, it can be used to create secure, decentralized networks of connected devices, which can enable new applications and services (Miller, 2018; Wang et al., 2019). Finally, in Government and Public services, it can be used to create more transparent and efficient systems for voting, tax collection, and other public services (Hou, 2017). It should be noted that blockchain technology is still relatively new and many of the use cases are still in the development and testing phase, so the full extent of its impact is yet to be seen.

There are several reasons why blockchain technology is well-suited for use in the medical data processing. Some key considerations include security, where blockchain technology allows for secure and tamper-proof medical data storage, which is particu-

[a] https://orcid.org/0000-0001-9820-6629
[b] https://orcid.org/0000-0003-1148-5691

Siedlecka-Lamch, O. and Szymoniak, S.
Blockchain Technology in Medical Data Processing: A Study on Its Applications and Potential Benefits.
DOI: 10.5220/0011991400003464
In *Proceedings of the 18th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2023)*, pages 664-671
ISBN: 978-989-758-647-7; ISSN: 2184-4895

larly important for sensitive information such as personal health records. The following reason is interoperability, where blockchain enables the secure sharing of medical data between different systems and organizations, improving patient outcomes and reducing administrative costs. Transparency, where blockchain can give patients greater control over their medical data and who has access to it, can increase trust in the healthcare system. Auditability, where blockchain creates a transparent and audible record of all transactions, which can be used to improve trust and compliance in the medical data processing. Decentralization, where blockchain can enable the creation of decentralized networks of medical data, can reduce the dependence on centralized systems and increase system resilience.

Several challenges must be considered when using blockchain technology for medical data processing. Some of the key challenges include scalability, where processing and storing large amounts of medical data on a blockchain can be challenging due to current technology limitations. Privacy and regulatory compliance, where ensuring that medical data is stored and processed in a way that complies with privacy and regulatory requirements can be complex. Interoperability, where ensuring that different blockchain systems can work together and share data can be challenging. Standardization, where ensuring that medical data is stored and processed in a way that is consistent across different systems and organizations can be difficult. Adoption, where getting healthcare providers and patients to adopt blockchain-based solutions can be a challenge. Cybersecurity, where blockchain technology is not immune to cyber attacks, and some of the vulnerabilities that are specific to blockchain technology can be exploited by attackers. Integration with existing systems, where integrating blockchain-based solutions with existing systems and processes in the healthcare industry can be a complex task. It is important to note that these challenges are not unique to blockchain, and similar issues are faced when implementing new technologies in the healthcare sector. Additionally, ongoing research and development efforts are being made to address these challenges and make blockchain more suitable for healthcare.

Our study presents an original idea for storing and processing medical data by combining blockchain technology with relational databases. Combining these two technologies can positively impact patient privacy protection, increasing trust in the system and increasing the effectiveness and efficiency of managing medical data. Blockchain can provide secure, immutable and transparent medical data storage, while a relational database can facilitate data processing and sharing.

The rest of this paper is organized as follows. Section 1.1 presents the related works. In Section 2, we provide theoretical fundaments that are base of our work. In Section 3, we propose a model for medical data processing including conceptual and logical models. Section 4 provides an implementation of our model. In the last section, we present the conclusions of the entire article, and findings from the research.

1.1 Related Work

There are many articles and publications on blockchain technology, and new research is being published regularly. Some of the most important and influential articles and publications include:

- ”Bitcoin: A Peer-to-Peer Electronic Cash System” by Satoshi Nakamoto - This is the original white paper that introduced the concept of Bitcoin and blockchain technology (Nakamoto and Bitcoin, 2008).
- ”The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology” by William Mougayar - This book provides a comprehensive overview of the business potential of blockchain technology (Mougayar, 2016).
- ”Blockchain Basics: A Non-Technical Introduction in 25 Steps” by Daniel Drescher - This book provides a clear and concise introduction to the key concepts of blockchain technology (Drescher, 2020).
- ”A Next-Generation Smart Contract and Decentralized Application Platform” by Ethereum Foundation - This white paper introduces the Ethereum blockchain platform and its smart contract functionality (Buterin et al., 2014).
- ”Blockchain: Blueprint for a New Economy” by Melanie Swan - This book provides an overview of the potential of blockchain technology to disrupt a wide range of industries and sectors (Swan, 2015).
- ”Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World” by Don Tapscott and Alex Tapscott - This book provides a detailed look at the potential of blockchain technology to disrupt a wide range of industries and sectors (Tapscott and Tapscott, 2016).

These are just a few examples, and many other articles and publications provide valuable insights into the technology and its potential applications. It is essential to remember that blockchain technology is still relatively new and continuously evolving, so new research and publications are coming out regularly.

Many articles and publications focus on using blockchain technology in the healthcare industry. Some of the most important and influential articles and publications include:

- ”A Survey of Blockchain-Based Strategies for Healthcare” by De Aguiar et al. - This article reviews concepts of blockchain in the medical area including the management of information, drug tracking, and data security and privacy (De Aguiar et al., 2020).
- ”Blockchain-Based Electronic Health Record Systems: A Review of the Current Landscape” by K. K. Chan, J. Y. Lee, and B. K. Ng - This article reviews current efforts to use blockchain for electronic health record systems.
- ”Blockchain in Healthcare: The Future is Here” by P. J. Neuman - This article provides an overview of the potential benefits of blockchain in healthcare and potential use cases.
- ”Blockchain Technology in the Pharmaceutical Industry: The Future of Traceability and Supply Chain Management” by N. Kshetri - This article explores the potential of blockchain in the pharmaceutical industry, specifically in traceability and supply chain management.
- ”Blockchain in Healthcare: How Blockchain Technology Can Improve the Health Care System” by R. Kshetri - This article provides a detailed overview of the potential benefits of blockchain technology in healthcare, including improved data security and interoperability.
- ”Blockchain platform for industrial healthcare: Vision and future opportunities” by Farouk, Alahmadi, Ghose, and Mashatan - This paper provides an overview of the blockchain and IoT technologies usage in healthcare (Farouk et al., 2020).
- ”Blockchain for Health Data and Its Potential Use in Health IT and Health Care Related Research” by Linn et al. - This article provides an overview of the potential of blockchain for storing and sharing health data (Linn et al., 2016).
- ”Blockchain for healthcare data management: opportunities, challenges, and future recommendations” by Yaqoob et al. - This article demonstrates the practicality of blockchain technology for healthcare applications (Yaqoob et al., 2022).
- ”Blockchain-enabled supply chain: analysis, challenges, and future directions” by Jabbar et al. - This article provides an overview of challenges and future directions in pharmaceutical supply chain intervention (Jabbar et al., 2021).

2 THEORETICAL FUNDAMENTS

Blockchain is a technology used in many application domains. It is defined as a registry of decentralised data that is securely shared. Thanks to this technology, a group of participants can share data and input it into the network simultaneously. Additionally, blockchain enables accessible collection, integration and sharing of transactional data from many sources. Blockchain ensures data integrity by eliminating duplication and ensuring security. The data, in turn, is divided into shared datasets made up of blocks and a chain of data packets. Each block includes multiple transactions or entities and metadata. In addition, each block contains a timestamp, the previous block’s hash value, and a nonce, a random number to verify the hash. Blockchain can be extended with additional blocks, thanks to which the blockchain contains a complete history of transactions (Rajasekaran et al., 2022; Bashir, 2018).

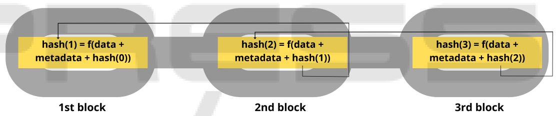

Figure 1: Hash calculation sequence.

Blockchain is an electronic list of data blocks. Integrity constraints exist between these blocks. Also, each block stores the cryptographic hash of the previous block. The data stored in the block is used to calculate the hash using appropriate hashing methods. The hash is the equivalent of a checksum. If later there are changes in a given block, the hash can be used to verify whether there has been an error or an attempted forgery. Each subsequent block uses its data and the previous block’s hash function to compute the result of the hash function. This action creates integrity constraints between the blocks. Thus, any interference with the block results in both its hash and each subsequent block’s hash is incorrect. Figure 1 shows the idea of the mentioned hash calculation sequence (Bodkhe et al., 2020).

The functions used to generate the hash should primarily be one-way and collision-resistant. If the function is one-way, finding an argument to perform the reverse operation will be impossible. An additional advantage of one-way hash functions is to increase the level of data security because one-way makes it much more challenging to try forgery. Collision resistance means generating two arbitrary inputs with the same hash is not practical. The hash function makes it much more difficult to interfere with already created blocks, but it does not prevent it. If the block is modified, the result of the hash function no longer matches. Therefore, it is necessary to calculate its new value and repeat the same operation in each subsequent block (Sheik and Muniyandi, 2023).

We can divide blockchains into public and private chains due to their availability. Private chains are only open to the group, which means that the users of such chains are known, and there is usually no need to implement additional security measures. On the other hand, public chains usually provide free network access for all internet users. The use of public chains increases the risk of abuse and contributes to the need for additional blockchain security measures, e.g., implementing a consensus algorithm. Reaching a consensus in the network is a critical situation because the blockchain is usually uniform, which means that there is one global instance of the blockchain. The occurrence of branches is undesirable, meaning that not all nodes make the same decision (Zheng and Lu, 2022).

We can indicate several methods of reaching consensus, i.e. situations in which nodes in the network agree to accept a new block consisting of a specific list of entities or transactions. The consensus mechanism should guarantee data integrity between nodes and reduce the risk of errors and illegal transactions. One of the most popular mechanisms for reaching consensus is Proof of Work. This mechanism requires proof that adequate computational resources were used to generate the new block, and the PoW algorithm characterises by the high computing power necessary to generate subsequent blocks. Another consensus-building algorithm is Proof of Stake. In this case, the algorithm selects the person who can create the next block based on certain factors. For example, the criterion for selecting a person may be the number of tokens held and their age [21]. Thus, a new block can be created by a person with such a large amount of assets that prohibited activities are unprofitable for him, as they carry the risk of losing the funds collected so far. Proof of Stake consumes less power than the Proof of Work algorithm. Proof of Importance uses information about the user's activity on the network to assess the level of trust of a given person user. On the other hand, Proof of Activity combines the features of Proof of Stake and Proof of Work. Thanks to this, it maintains an appropriate level of security while reducing the required computing power (Ferdous et al., 2021).

3 MODEL FOR THE MEDICAL DATA PROCESSING

In this section, we will present a model that combines the advantages of a relational model and blockchain technology. For personal data of patients, doctors, and healthcare workers, as well as descriptions of insurance and payments, we will use relationships. On the other hand, we will utilise blockchain for diagnostic information such as test results, diagnoses, and prescribed medications.

3.1 Conceptual Model

A conceptual model was built in the first step of database modelling, resulting in an entity relationship diagram (Figure 2). For the article, we limited the visibility of each entity's properties to the basic ones due to the size of the entire diagram. It should also be noted that the most important entities for analysing the problem have been shown.

In the project, we distinguished entities closely related to patient data: patient, insurance, and bill, where we describe information about the patient, what their insurance covers, and information about their payments related to treatment. The subsequent entities relate to medical staff: doctor, nurse, and healthcare worker, where information about the listed employees and their specialisations will appear. The next group of entities describes the treatment process, so we have a visit that is first reserved and then takes place. Finally, we have referrals for procedures, to other specialists, or for tests. There will also be an entity regarding medical leave and completed tests. The last group of entities is significant for the treatment process, including test results, diagnosis, and prescription. Here we will describe the patient's health status at a given time, the diagnosis made, and the prescribed drugs with the dosing instructions. These data are complex and will require nesting, and collections, in short, complex structures. In Figure 2, we have marked them with the term: Data.

Most of the relationships we identified between entities are simple one-to-one or one-to-many relationships. However, attention should be paid to relationships that occur in three entities describing the treatment process. We wanted to emphasise the causal relationship and the sequence of subsequent tests, diagnoses, and medications. Therefore, each entity instance should refer to its predecessor in time. This requirement is shown in the form of relationships between entities with themselves. Importantly, in medical history, there will always be the first and last test

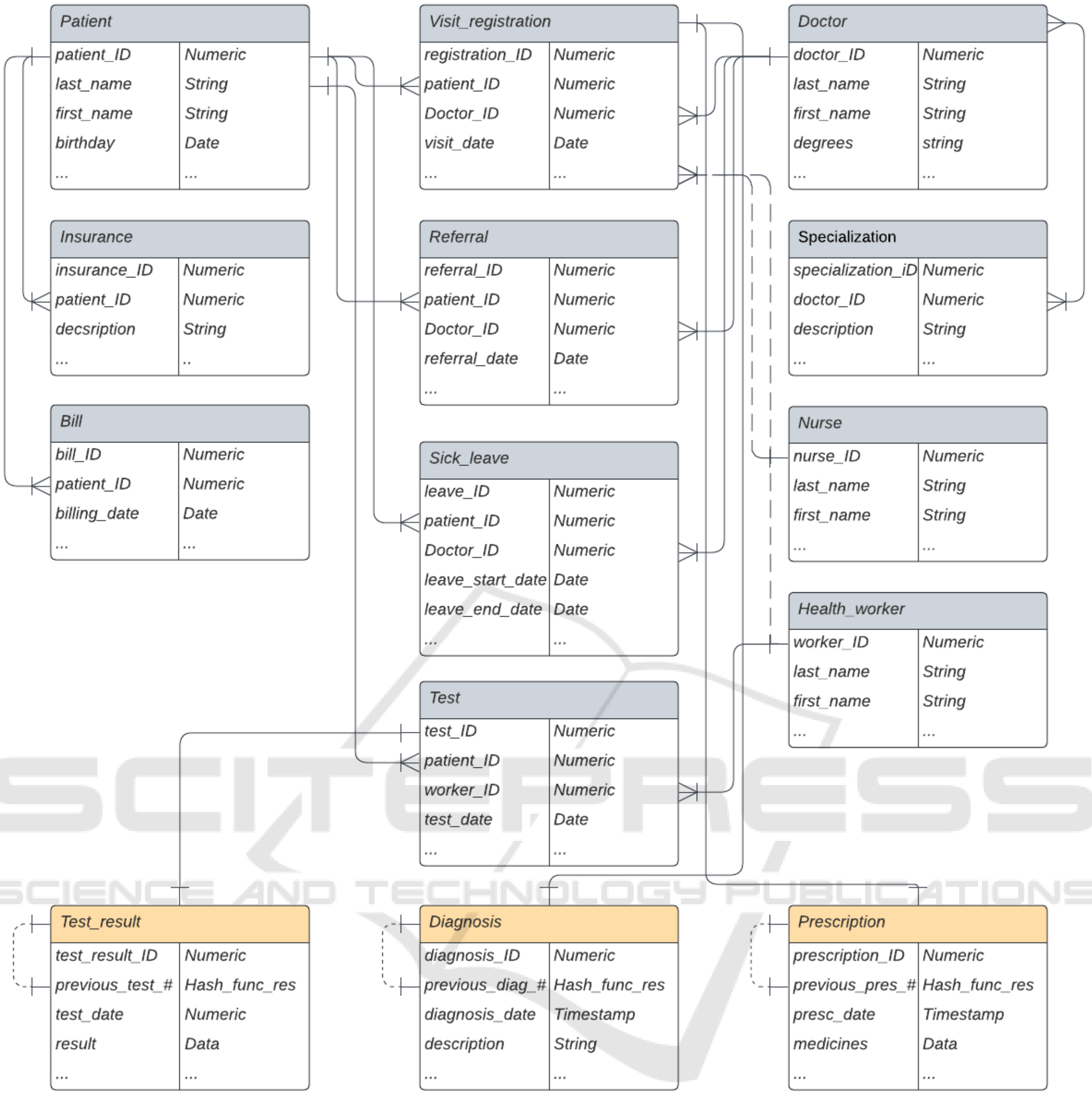

Figure 2: Conceptual model of healthcare data.

or the first and last diagnosis; hence, the relationships are bidirectionally optional.

3.2 Logical Model

After the first design phase, entities can be identified as possible to implement in a relational (optionally relational-object) form. In Figure 2, we have highlighted them with a blue background in the header. We would particularly like to secure three entities, which are sensitive data important in terms of the order of occurrence, time, and immutability. Therefore, we have highlighted them with an orange background.

In the case of diagnostics, the system beneficiaries: doctors, staff, and patients themselves, will have access to an immutable history of diagnoses, prescriptions, and test results. Each of the mentioned entities contains a record of the key to the previous one (the result of the hash function), a precise timestamp, metadata, and the actual data related to the diagnosis.

As we mentioned, the data related to these entities are complex. We will not be able to use regular relationships. We propose a hybrid model that will use blockchain technology to secure the order and data and protect them from changes after approval. In addition to blockchain, we will use a relational-object model that will allow us to store both atomic data (patient number, doctor, date) and complex data (test result, prescribed drugs with dosing) that can take the form of a collection in rows.

4 IMPLEMENTATION

The designed database can be implemented using Oracle 19i or a newer server. In the above distribution, we can use the existing solution - Oracle Blockchain Platform. This platform provides blockchain tables. Access to them is assigned in the form of individual permissions. Hence, all blockchain technology in Oracle is a permissioned blockchain.

Relational tables are implemented traditionally with a standard set of types. However, in the case of patient or visit data, it is necessary to consider using partitioning, as these may be large data sets. All of these tables will be able to undergo insertion, modification, and deletion of data according to the actual state. Authorised healthcare workers will make changes.

Blockchain tables designated for data insertion only will be used for test results, diagnoses, and prescriptions. These tables organise rows into a certain number of chains. Each row in the chain, except for the first, is linked to the previous row in the chain using a cryptographic hash (Figure 3).

An interesting feature of blockchain tables is the ability to add certificates used to sign rows. Signing a row makes it clear who inserted the row. The signature is optional and provides additional security against manipulation. Another important aspect is the ability to set the expiration time of the data. The total inability to delete outdated data could be too restrictive. Therefore, a storage period can be set during the table creation.

Unfortunately, in the case of an Oracle server, blockchain tables also have significant limitations regarding the allowable types of rows. They only allow for simple types and do not permit object or collection types. As a result, assumptions made during conceptual and logical modelling must be altered. For example, the results of tests that may involve multiple factors being studied must be broken down into individual key-value entries, where the key is the name of the factor being studied and the value is the obtained result. The same approach should be taken in the case of a diagnosis. If more than one illness is detected during a visit, each illness will be allocated a separate row. Similarly, in the case of medications, individual rows will describe individual drugs and their dosage.

In Figure 3, among the data, metadata inserted into each row in the chain is highlighted. These metadata will include database instance identifiers, row identifiers, consecutive row numbers, data insertion timestamp, user number who inserted the data, row hash value, signatures, and certificates.

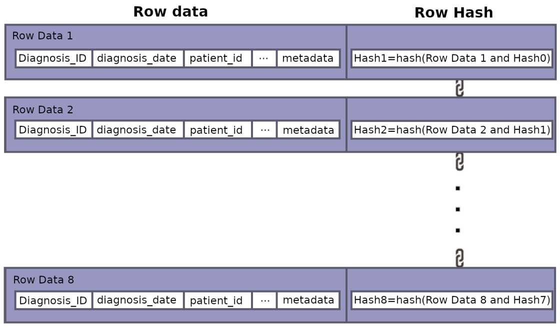

Figure 3: Blockchain model of diagnosis table.

We must add many constraints to our blockchain tables to facilitate their management and security. The first step will be establishing a period for storing rows in the table. In the case of medical data, it can be set for a period of several years, after which older data is archived. In the next step, because we will be breaking down the results of tests and prescribed medications so much, the tables will quickly grow in size. Finally, to optimise and avoid full table scans, we must implement a data partitioning mechanism during the implementation stage.

We want each entry to have a specified and signed author, so we must also add certificates to the tables during the implementation stage. We will use the DBMS_USER_CERTS.ADD_CERTIFICATE procedure for this purpose.

After the database structure implementation phase, it is necessary to implement supporting database triggers, stored procedures and functions, additional indexes on large tables and their most important columns in the case of data search. These are essential steps from the view of application optimisation rather than from the point of view of the blockchain model. What will also be necessary is the selection of users and their privileges.

Among users, we will distinguish those who have access to traditional tables; these will be healthcare professionals who can enter patient, visit, and procedure data. Laboratory technicians will have certificates and can sign off on test results recorded in the blockchain table. There will be doctors who have access to patients, visits, procedures, and referral data but also can sign off on entries related to diagnosis and prescribed medications using a certificate. Finally, there will be patients without modification rights but only with the ability to read their own data.

Of course, throughout the entire implementation phase, we have only described the database side here. Simultaneously it is necessary to add an API allowing easy database handling by individual users.

5 CONCLUSIONS

In our article, we have outlined the ideas behind blockchain technology and subsequently developed and demonstrated a data model for the patient treatment process. The model includes patient data, their insurance, bills, healthcare workers, doctors, nurses, and data related to the treatment process: visits, referrals, releases, test results, diagnoses and medications. The last three are designed using blockchain technology, guaranteeing data integrity and maintaining a precise entry sequence. Additionally, each entry is accompanied by a certified signature. Overall, our article illustrates how blockchain technology can bring security and transparency to the healthcare industry by allowing tamper-proof records of sensitive patient data and medical procedures.

Blockchain technology, in the case of medical data, offers certain benefits, including:

- High level of security;
- Reduced reliance on external intermediaries;
- Real-time record allowing detection of manipulation that can be shared with all interested parties;
- Facilitation of authenticity and integrity of entries throughout the treatment process;
- Building trust between patients and healthcare providers by offering credible, shared data;
- It enables seamless tracking of the treatment process.

When implementing a hybrid data model for medical data using blockchain technology, we may encounter challenges such as complexity in implementation, scalability issues, data standardisation needs, difficulties in integrating with existing systems, and regulatory compliance. These challenges vary depending on the specific use case and the current infrastructure in place. Therefore, it is essential to consider these potential challenges and have a plan to address them to ensure a successful implementation of the hybrid data model.

ACKNOWLEDGEMENTS

The project financed under the program of the Polish Minister of Science and Higher Education under the name "Regional Initiative of Excellence" in the years 2019–2023 project number 020/RID/2018/19 the amount of financing PLN 12,000,000.

REFERENCES

Bashir, I. (2018). *Mastering blockchain*. Packt Publishing Ltd.

Bodkhe, U., Tanwar, S., Parekh, K., Khanpara, P., Tyagi, S., Kumar, N., and Alazab, M. (2020). Blockchain for industry 4.0: A comprehensive review. *IEEE Access*, 8:79764–79800.

Buterin, V. et al. (2014). A next-generation smart contract and decentralized application platform. *white paper*, 3(37):2–1.

De Aguiar, E. J., Faiçal, B. S., Krishnamachari, B., and Ueyama, J. (2020). A survey of blockchain-based strategies for healthcare. *ACM Computing Surveys (CSUR)*, 53(2):1–27.

Drescher, D. (2020). *Blockchain basics*. Ascent Audio.

Farouk, A., Alahmadi, A., Ghose, S., and Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. *Computer Communications*, 154:223–235.

Ferdous, M. S., Chowdhury, M. J. M., and Hoque, M. A. (2021). A survey of consensus algorithms in public blockchain systems for crypto-currencies. *Journal of Network and Computer Applications*, 182:103035.

Hou, H. (2017). The application of blockchain technology in e-government in china. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)*, pages 1–4. IEEE.

Jabbar, S., Lloyd, H., Hammoudeh, M., Adebisi, B., and Raza, U. (2021). Blockchain-enabled supply chain: analysis, challenges, and future directions. *Multimedia systems*, 27(4):787–806.

Linn, L. A., Koo, M. B., et al. (2016). Blockchain for health data and its potential use in health it and health care related research. In *ONC/NIST use of blockchain for healthcare and research workshop. Gaithersburg, Maryland, United States: ONC/NIST*, pages 1–10.

Miller, D. (2018). Blockchain and the internet of things in the industrial sector. *IT professional*, 20(3):15–18.

Mougayar, W. (2016). *The business blockchain: promise, practice, and application of the next Internet technology*. John Wiley & Sons.

Nakamoto, S. and Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin.–URL: https://bitcoin.org/bitcoin.pdf*, 4:2.

Patel, R., Migliavacca, M., and Oriani, M. (2022). Blockchain in banking and finance: is the best yet to come? a bibliometric review. *Research in International Business and Finance*, page 101718.

Peck, M. E. (2017). Blockchain world-do you need a blockchain? this chart will tell you if the technology can solve your problem. *IEEE Spectrum*, 54(10):38–60.

Queiroz, M., Telles, R., and Bonilla, S. (2019). Blockchain and supply chain management integration: a systematic review of the literature. *Supply Chain Management: An International Journal*, 25.

Raikwar, M., Gligoroski, D., and Velinov, G. (2020). Trends in development of databases and blockchain. In *2020*

Seventh International Conference on Software Defined Systems (SDS), pages 177–182. IEEE.

Rajasekaran, A. S., Azees, M., and Al-Turjman, F. (2022). A comprehensive survey on blockchain technology. *Sustainable Energy Technologies and Assessments*, 52:102039.

Román-Belmonte, J. M., de la Corte-Rodriguez, H., and Rodríguez-Merchán, E. C. (2018). How blockchain technology can change medicine. *Postgraduate Medicine*, 130:420 – 427.

Sheik, S. A. and Muniyandi, A. P. (2023). Secure authentication schemes in cloud computing with glimpse of artificial neural networks: A review. *Cyber Security and Applications*, 1:100002.

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

Tapscott, D. and Tapscott, A. (2016). *Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world*. Penguin.

Wang, X., Zha, X., Ni, W., Liu, R. P., Guo, Y. J., Niu, X., and Zheng, K. (2019). Survey on blockchain for internet of things. *Computer Communications*, 136:10–29.

Wang, Y., Hsieh, C.-H., and Li, C. (2020). Research and analysis on the distributed database of blockchain and non-blockchain. In *2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA)*, pages 307–313. IEEE.

Yaqoob, I., Salah, K., Jayaraman, R., and Al-Hammadi, Y. (2022). Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications*, 34(14):11475–11490.

Zheng, X. R. and Lu, Y. (2022). Blockchain technology–recent research and future trend. *Enterprise Information Systems*, 16(12):1939895.