**University of Hertfordshire**

**Msc Cyber Security**

**A Systematic Literature Review: Blockchain Revolutionizing Electronic Health Record Security and Privacy: A New Era in Healthcare Data Management**

**Module Code: 7COM1085-0105-2023**

**Module Title: Research Methods**

**Group Number: Group 69**

**Date: 28 April 2024**

**Student Names: Anjali Gopinadhan Nair [21070981]**

**Akhil Kunnumpurathu Thankachan [21064307]**

**Z Jisna Mathew [21061802]**

**Mintu Murali [21071821]**

**Muhammed Kunnil Shafi [21078679]**

**TABLE OF CONTENTS**

[Chapter 1: Introduction 2](#_Toc165157806)

[Chapter 2: Background 3](#_Toc165157807)

[Chapter 3: Literature Review 4](#_Toc165157808)

[**3.1 Research Question** 4](#_Toc165157809)

[3.1.1 Research Question: 4](#_Toc165157810)

[3.1.2 Context: 4](#_Toc165157811)

[3.1.3 PICO Elements: 4](#_Toc165157812)

[**3.2 Keywords** 5](#_Toc165157813)

[**3.3 Synonyms** 6](#_Toc165157814)

[**3.4 Search String** 6](#_Toc165157815)

[**3.3 Inclusion and Exclusion Criteria** 6](#_Toc165157816)

[3.4 Number of Papers Found: 8](#_Toc165157817)

[Chapter 4: Results 10](#_Toc165157818)

[4.1 Paper Selection Process 10](#_Toc165157819)

[4.2 Data Extraction 10](#_Toc165157820)

[4.3 Data Synthesis 12](#_Toc165157821)

[Chapter 5: Conclusion 12](#_Toc165157822)

[Bibliography: 14](#_Toc165157823)

[Appendices: 16](#_Toc165157824)

# Chapter 1: Introduction

In today's world of digital healthcare, keeping your medical records safe and private is more important than ever. As hospitals and clinics switch to digital systems to improve how they care for patients, they're also facing the challenge of protecting sensitive information from hackers and unauthorized access.

Moving health records online has made things easier in many ways—it's simpler to access and manage information. But it's also raised concerns about security. With so much health data stored electronically, it's a big target for cybercriminals. The systems we use to store this data, like traditional databases, have weaknesses because they rely on centralized control, which can be risky if there's a breach.

That's where blockchain technology comes in. You might have heard of it as the tech behind Bitcoin, but it's more than just cryptocurrency. Blockchain operates on a decentralized system, which means it doesn't rely on one central authority to manage data. Instead, a network of computers (nodes) work together to validate and secure information in a way that's transparent and can't be altered.

Our research focuses on a key question: How does blockchain make electronic health records (EHRs) more secure and private compared to traditional databases used in healthcare? We're digging into this to see how blockchain can address the growing security challenges in managing healthcare data.

One of blockchain's strengths is how it ensures data integrity and security. By spreading out data across a network of computers, blockchain reduces the risk of a single point of failure or unauthorized access. Every update to the EHR is recorded in a way that can't be tampered with, which makes it easy to trace and audit without revealing private patient information.

Beyond security, blockchain empowers patients by giving them more control over their health data. With cryptographic keys, patients can decide who gets to see their records, ensuring only trusted healthcare providers have access. This approach aligns with privacy laws like GDPR and HIPAA, which emphasize patient consent and data ownership.

Moreover, blockchain technology has the potential to revolutionize healthcare beyond security and privacy. Its decentralized nature allows for increased efficiency by reducing administrative overhead and improving interoperability between different healthcare systems. This can lead to smoother data sharing among providers, ultimately improving patient care and outcomes.

As blockchain gains traction in healthcare, collaborations between healthcare providers, technology firms, and regulatory bodies become crucial. Setting standards and ensuring compliance will be key to widespread adoption and realizing the full potential of blockchain technology in transforming healthcare delivery.

Looking ahead, the integration of blockchain with emerging technologies like artificial intelligence (AI) and Internet of Medical Things (IoMT) holds tremendous promise. This combination can enable predictive analytics, personalized medicine, and real-time monitoring while maintaining the highest standards of data security and patient confidentiality.

In summary, blockchain is more than a buzzword—it's a game-changer for healthcare data management. By leveraging its decentralized architecture and cryptographic principles, we can build a more secure, efficient, and patient-centered healthcare system for the future.

# Chapter 2: Background

The adoption of Electronic Health Records (EHRs) has revolutionized how healthcare is delivered, putting patients at the center of care while improving efficiency. However, this shift to digital records has also raised significant concerns about protecting the privacy and security of sensitive medical information.

Recent research by Argaw et al. (2019) and others highlights a troubling trend of increasing cyberattacks targeting healthcare providers. These incidents underscore the urgent need for stronger security measures within EHR systems to prevent data breaches and unauthorized access. Traditional centralized EHR systems, as noted by Spatar et al. (2019), are especially vulnerable to exploitation, potentially compromising the confidentiality and accuracy of patient records stored within these systems.

In response to these challenges, blockchain technology has emerged as a promising solution. By using decentralized ledger technology and cryptographic algorithms, blockchain offers a new approach to ensuring the security and integrity of EHRs. Decentralizing data storage and implementing consensus protocols can greatly reduce the risk of single points of failure and unauthorized tampering.

The motivation for this research comes from the critical need to address the vulnerabilities of Electronic Health Records (EHRs) in traditional database systems. Centralized databases often struggle to keep patient data confidential and secure against sophisticated cyber threats, emphasizing the necessity for innovative and resilient solutions like blockchain.

Scholars such as Gordon and Catalini (2018) have emphasized blockchain's potential to strengthen data protection and enhance patient privacy. Their research highlights blockchain as a transformative technology in healthcare data management, aligning with evolving regulatory frameworks and patient privacy rights.

This study aims to critically evaluate and compare how blockchain technology (intervention) versus traditional database systems (comparison) can enhance the security and privacy of Electronic Health Records (EHRs) (population). By conducting a detailed analysis of these technologies, the research aims to develop a comprehensive security and privacy framework tailored to the unique demands of healthcare settings.

The anticipated outcomes of this research include actionable insights and practical recommendations for integrating blockchain solutions into existing healthcare infrastructure. By enhancing stakeholders' understanding of blockchain's capabilities and potential applications, this study aims to promote innovation and best practices in healthcare cybersecurity.

Through this research, healthcare professionals, policymakers, and technology experts will gain valuable insights into leveraging blockchain technology to strengthen EHR security. Ultimately, this research aims to advance the mission of safeguarding sensitive medical information and upholding the highest standards of patient confidentiality in an increasingly digitized healthcare landscape. The study also seeks to contribute to the broader discourse on cybersecurity in healthcare, driving initiatives that prioritize patient privacy and data protection as fundamental elements of modern healthcare systems.

# Chapter 3: Literature Review

## **3.1 Research Question**

### 3.1.1 Research Question:

How does blockchain technology fortify the security and privacy of electronic health records (EHRs) compared to traditional database systems in healthcare settings?

### 3.1.2 Context:

The context of this research question lies within the healthcare sector, specifically focusing on the management and security of electronic health records (EHRs).

### 3.1.3 PICO Elements:

Population: Electronic Health Records (EHRs)

Intervention: Implementation of blockchain technology for securing EHRs.

Comparison: Blockchain-based security measures vs Traditional database security measures

Outcome: Identification of the effectiveness of blockchain technology in improving EHRs security and privacy.

**Table 1: PROTOCOL Part 1: RESEARCH QUESTION with PICO ELEMENTS**

|  |  |
| --- | --- |
| **Protocol Details** | **Research Protocol Details** |
| Topic: | Blockchain Revolutionizing Electronic Health Record Security and Privacy: A New Era in Healthcare Data Management |
| Research Question: | How does blockchain technology fortify the security and privacy of electronic health records (EHRs) compared to traditional database systems in healthcare settings? |
| Context: | Healthcare data security and privacy |
| Population: | Electronic Health Records (EHRs) |
| Intervention: | Implementation of blockchain technology for securing EHRs. |
| Comparison: | Blockchain-based security measures vs Traditional database security measures |
| Outcome: | Identification of the effectiveness of blockchain technology in improving EHRs security and privacy |

## **3.2 Keywords**

To conduct our systematic literature review (SLR), we identified the following keywords relevant to our research question:

* Blockchain
* Electronic health records (EHRs)
* Security
* Privacy
* Traditional database systems
* Healthcare

## **3.3 Synonyms**

In addition to the keywords, we also considered synonyms and related terms to ensure a comprehensive search:

* Distributed ledger technology
* Medical records
* Confidentiality
* Data protection
* Relational databases
* Healthcare information systems

## **3.4 Search String**

("blockchain technology" OR "distributed ledger technology") AND ("electronic health records" OR "EHR" OR "EMR") AND (security OR privacy OR confidentiality) AND (improve\* OR enhanc\*) AND ("healthcare data" OR "patient information" OR "electronic medical records")

Number Of papers Returned (All Results): 200

## **3.3 Inclusion and Exclusion Criteria**

**Inclusion criteria:**

* Papers discussing the technical aspects, challenges, or benefits of implementing blockchain for EHRs.
* Peer-reviewed academic papers focusing on blockchain technology applications in electronic health records (EHRs), including comprehensive literature reviews.
* Research articles comparing blockchain architectures with traditional database systems for managing EHRs.
* Studies evaluating the effectiveness of blockchain in enhancing the security and privacy of EHRs.
* Scholarly works discussing the technical aspects, challenges, or potential benefits of implementing blockchain technology in the context of EHR management.

**Exclusion criteria:**

* Non-complete works, such as book chapters, PowerPoint presentations, or incomplete manuscripts.
* Non-peer-reviewed publications, such as magazine articles, blogs, or general interest pieces.
* Non-academic sources, including opinion pieces or secondary studies lacking primary investigation.
* Duplicate publications, with preference given to the most comprehensive version in cases where authors publish both conference and journal papers.

**Table 2: PROTOCOL Part 2 – SEARCH STRINGS and INCLUSION/EXCLUSION CRITERIA**

|  |  |
| --- | --- |
| Criteria Type | Description |
| Search string | ("blockchain technology" OR "distributed ledger technology") AND ("electronic health records" OR "EHR" OR "EMR") AND (security OR privacy OR confidentiality) AND (improve\* OR enhanc\*) AND ("healthcare data" OR "patient information" OR "electronic medical records") |
| No. of papers | 200 |
| Inclusion Criteria | Papers focused on blockchain technology for electronic health records (EHRs) or electronics medical records (EMRs). |
|  | Papers comparing blockchain architectures to traditional database systems for EHRs. |
|  | Papers evaluating blockchain for improving EHR security and privacy. |
|  | Papers discussing the technical aspects, challenges, or benefits of implementing blockchain for EHRs. |
| Exclusion Criteria | Non-complete works, such as book chapters, PowerPoint presentations, or incomplete manuscripts. |
|  | Non-peer-reviewed publications, such as magazine articles, blogs, or general interest pieces. |
|  | Non-academic sources, including opinion pieces or secondary studies lacking primary investigation. |
|  | Duplicate publications, with preference given to the most comprehensive version in cases where authors publish both conference and journal papers. |

## 3.4 Number of Papers Found:

Screenshot 1: All Results

A screenshot of a computer

Description automatically generated

Screenshot 2: Total Number of papers returned after applying the filter inclusion criteria: 88

Filter Applied:

* Abstract contain: security or privacy
* Document title contain: health\* and Document title contain: blockchain

A screenshot of a table

Description automatically generated

Screenshot 3: Filter applied to exclude the records as per the exclusion criteria:

Filter Applied:

* Document Identifier Does Not contain Magazines
* Document Identifier Does Not equal to Magazines

Number of papers returned after applying the filter: 87.

A screenshot of a computer

Description automatically generated

# Chapter 4: Results

The results of the search are:

1. 200 articles were found by our search string in the initial search.
2. 88 papers successfully completed the inclusion phase.
3. There were 87 papers that made it through the “exclude” phase.
4. 17 papers were found by “RQ answer= Yes” phase.

## 4.1 Paper Selection Process

|  |  |
| --- | --- |
| **Table 1: Paper selection process** | |
| **Selection Stage** | **Number of Papers** |
| Papers downloaded from implementing the Boolean search in IEEE Xplore | 200 |
| Papers that pass your inclusion criteria by checking the title: “include title” column in your papers.csv file | 99 |
| Papers that pass your inclusion criteria by reading the abstract “include abstract” column in your papers.csv file | 88 |
| Papers that remain after you apply the exclusion criteria | 87 |
| Papers that clearly meet all your criteria, and answer your research question: | 17 |

## 4.2 Data Extraction

|  |  |  |
| --- | --- | --- |
| **Table 2. Data Extraction** | | |
| **RQ answer** | **Reference** | **Code** |
| “BigchainDB is a blockchain database that supports decentralized storage, scalability, and security..”[p.3] | Baldi et al., 2022 | data security |
| “Having a standardized ontology can help to ensure consistency and interoperability across..”[p.3] | Li, Pandey and Rasha Hendawi, 2023 | Interoperability |
| “The system should hash the patients’ personal and medical data to maintain..”[p.4] | El Sayed et al., 2020 | data privacy |
| **RQ answer** | **Reference** | **Code** |
| “Due to the sensitivity of the data contained inside an EHR, it is necessary to come up with good..”[p.2] | Ramachandran et al., 2020 | data security |
| “Henceforth, recent cryptographic approaches use the blocks across..”[p.3] | Chandini and Basarkod, 2022 | cryptographic |
| “Blockchain technology with IoT devices, serving as a..”[p.2] | T Sivashankari et al., 2024 | data privacy |
| “Blockchain has become an indispensable technology in the healthcare industry..”[p.1] | Mukta Mithra Raj et al., 2023 | data security |
| “Using the key characteristics of blockchain, decentralization..”[p.6] | Ansari et al., 2023 | decentralization |
| “This paper proposes a blockchain-based design for e-wellbeing..”[p.2] | S. Joseph Gabriel and P. Sengottuvelan, 2021 | access control |
| “Additionally, the framework allows for Interoperability and handles scalability..”[p.1] | Sandeepkumar and Suresh, 2023 | scalability |
| “However, the security challenges associated with patient data storage in IT..”[p.1] | Marry et al., 2023 | data storage |
| “We maintain a hash of each blockchain-based record to prevent manipulation..”[p.2] | Asan et al., 2023 | data authorization |
| “The fundamental goal of an access control system is to keep system resources safe agains..”[p.2] | Jayasinghe et al., 2022 | access control |
| “The necessary information would then be applied to the consensus chain..”[p.3] | Mohammad Tabrez Quasim et al., 2023 | consensus |
| “The main goal of developing such a system is to focus on providing a smooth experience..”[p.2] | Mudaliar et al., 2022 | data security |
| “The existing system focused only on role assignment and access rules for the users, and data transaction performance..”[p.2] | Kalaipriya et al., 2020 | data transfer |
| “The privacy and confidentiality of important medical data used by patients and licensors will be highly..”[p.1] | Wang and He, 2021 | data privacy |

## 4.3 Data Synthesis

|  |  |  |
| --- | --- | --- |
| **Table 3. Data Synthesis** | | |
| **Code** | **Theme** | **References** |
| data security | **Blockchain's Core** | [Baldi et al., 2022], [ Ramachandran et al., 2020], [ Mukta Mithra Raj et al., 2023], [Mudaliar et al., 2022] |
| data transfer | **Blockchain's Core** | [Kalaipriya et al., 2020] |
| Consensus | **Access Control and Privacy** | [Mohammad Tabrez Quasim et al., 2023] |
| data privacy | **Access Control and Privacy** | [Wang and He, 2021], [T Sivashankari et al., 2024], [El Sayed et al., 2020] |
| decentralization | **Blockchain's Core** | [Ansari et al., 2023] |
| access control | **Access Control and Privacy** | [Jayasinghe et al., 2022], [S. Joseph Gabriel and P. Sengottuvelan, 2021], |
| data authorization | **Blockchain's Core** | [Asan et al., 2023] |
| Scalability | **System performance** | [Sandeepkumar and Suresh, 2023] |
| data storage | **System performance** | [Marry et al., 2023] |
| interoperability | **Advanced Blockchain** | [Li, Pandey and Rasha Hendawi, 2023] |
| cryptographic | **Blockchain Mechanism** | [Chandini and Basarkod, 2022] |

# Chapter 5: Conclusion

The traditional methods of electronic health record (EHR) management face significant challenges related to security and privacy, which are increasingly critical in today's digital healthcare landscape. Traditional database systems, characterized by centralized architectures, are susceptible to various cybersecurity threats and privacy breaches. These vulnerabilities include unauthorized access, data tampering, and a lack of transparency in data sharing practices.

One of the primary issues with traditional EHR systems is their centralized nature, which presents a single point of failure and increases the risk of data breaches. Additionally, the reliance on a trusted intermediary for data management raises concerns about data integrity and transparency. Privacy breaches and unauthorized access to sensitive medical information continue to be pressing issues in healthcare settings.

Blockchain technology emerges as a transformative solution to fortify the security and privacy of EHRs by leveraging decentralized ledger technology and cryptographic algorithms. Blockchain overcomes the limitations of traditional methods in several ways:

1. Decentralization: Blockchain eliminates the need for a central authority, distributing data across a network of nodes. This decentralized approach enhances security by reducing the risk of a single point of failure.

2. Data Integrity and Transparency: Blockchain's immutable ledger ensures data integrity, making it tamper-proof and auditable. Each transaction is cryptographically linked, providing a transparent and traceable record of data access and modifications.

3. Enhanced Security Features: Cryptographic techniques, such as hashing and digital signatures, ensure data confidentiality and authentication, mitigating the risk of unauthorized access and data tampering.

4. Patient Empowerment: Blockchain empowers patients to have more control over their medical data, enabling secure data sharing while maintaining privacy preferences through smart contracts.

5. Interoperability and Data Sharing: Blockchain facilitates secure and efficient data sharing among healthcare providers, promoting interoperability without compromising privacy or security.

By implementing blockchain technology, healthcare institutions can establish a robust framework for managing EHRs that prioritizes security, privacy, and data integrity. The adoption of blockchain has the potential to revolutionize healthcare data management, addressing the evolving challenges of cybersecurity and privacy in electronic health records.

In conclusion, blockchain technology represents a paradigm shift in healthcare data management, offering innovative solutions to fortify the security and privacy of electronic health records compared to traditional database systems. However, further research and real-world implementations are necessary to fully realize the potential benefits of blockchain in transforming healthcare data security and privacy.

# Bibliography:

Ansari, M.F., Dash, B., Swayamsiddha, S. and Panda, G. (2023). *Use of Blockchain Technology to Protect Privacy in Electronic Health Records- A Review*. [online] IEEE Xplore. doi:https://doi.org/10.1109/IDCIoT56793.2023.10053417.

Argaw, S.T., Bempong, N.-E., Eshaya-Chauvin, B. and Flahault, A. (2019). The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Medical Informatics and Decision Making, 19(1). doi:<https://doi.org/10.1186/s12911-018-0724-5>.

Asan, M., Kiran Shrinivaas S, R U and V. Vanitha (2023). Blockchain In Healthcare Data. doi:https://doi.org/10.1109/icaeca56562.2023.10199723.

Baldi, A.M., Celestrini, J.R., Andreao, R.V., Mota, S. and Santos (2022). A Blockchain Approach for eHealth Situation-Aware Data Processing. *2022 International Wireless Communications and Mobile Computing (IWCMC)*. doi:https://doi.org/10.1109/iwcmc55113.2022.9824729.

Chandini, A.G. and Basarkod, P.I. (2022). A Robust Blockchain Architecture for Electronic Health Data using Efficient Lightweight Encryption Model with Re-Encryption Scheme. *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*. doi:https://doi.org/10.1109/icdsis55133.2022.9915902.

El Sayed, A.I., Abdelaziz, M., Megahed, M.H. and Azeem, M.H.A. (2020). A New Supervision Strategy based on Blockchain for Electronic Health Records. *2020 12th International Conference on Electrical Engineering (ICEENG)*. doi:https://doi.org/10.1109/iceeng45378.2020.9171765.

Gordon, W.J. and Catalini, C. (2018). Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability. Computational and Structural Biotechnology Journal, [online] 16, pp.224–230. doi:<https://doi.org/10.1016/j.csbj.2018.06.003>.

Jayasinghe, A., K. G. S. Shiranthaka, T. Kavith, Jayasinghe, V., Kavinga Yapa Abeywardena and Kanishka Yapa (2022). Blockchain-based Secure Environment for Electronic Health Records. *2022 13th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. doi:https://doi.org/10.1109/icccnt54827.2022.9984371.

Kalaipriya, R., Devadharshini, S., Rajmohan, R., Pavithra, M. and Ananthkumar, T. (2020). *Certain Investigations on Leveraging Blockchain Technology for Developing Electronic Health Records*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICSCAN49426.2020.9262391.

Li, J., Pandey, V. and Rasha Hendawi (2023). A Blockchain-Based Personal Health Knowledge Graph for Secure Integrated Health Data Management. doi:https://doi.org/10.1109/iscc58397.2023.10218032.

Marry, P., Koteswar Yenumula, Alekhya Katakam, Akshitha Bollepally and Alekhya Athaluri (2023). Blockchain based Smart Healthcare System. doi:https://doi.org/10.1109/icscss57650.2023.10169704.

Mohammad Tabrez Quasim, Mohammad Mufareh Mobarak, Khair Ul Nisa, Meraj, M. and Mohammad Zunnun Khan (2023). Blockchain-based Secure Health Records in the Healthcare Industry. doi:https://doi.org/10.1109/icoei56765.2023.10125802.

Mudaliar, A., More, Y., Kulkarni, A., Joshi, L. and Chaudhari, D. (2022). Blockchain-Based User-Centric Electronic Health Record Management System. doi:https://doi.org/10.1109/icbds53701.2022.9935834.

Mukta Mithra Raj, Raja Muthalagu, Pawar, P.M., Tamizharasan Periyasamy, Elakkiya R and Alavikunhu Panthakkan (2023). An Analysis of Blockchain Frameworks for Electronic Health Records Using Hyperledger. doi:https://doi.org/10.1109/icspis60075.2023.10344122.

Ramachandran, S., Obu Kiruthika, O., Ramasamy, A., Vanaja, R. and Mukherjee, S. (2020). A Review on Blockchain-Based Strategies for Management of Electronic Health Records (EHRs). *2020 International Conference on Smart Electronics and Communication (ICOSEC)*. doi:https://doi.org/10.1109/icosec49089.2020.9215322.

S. Joseph Gabriel and P. Sengottuvelan (2021). An Enhanced Blockchain Technology with AES Encryption Security System for Healthcare System. doi:https://doi.org/10.1109/icosec51865.2021.9591956.

Sandeepkumar, E.V. and Suresh, A. (2023). *Blockchain Assisted Cloud Storage For Electronic Health Records*. [online] IEEE Xplore. doi:https://doi.org/10.1109/ICCCI56745.2023.10128219.

Spatar, D., Kok, O., Basoglu, N. and Daim, T. (2019). Adoption factors of electronic health record systems. Technology in Society, 58, p.101144. doi:<https://doi.org/10.1016/j.techsoc.2019.101144>.

T Sivashankari, M Pallikonda Rajasekaran, Kottaimalai Ramaraj, T Arunprasath, Muthangi kantha Reddy and Thilagaraj M (2024). A Three-Tier Architecture Framework with Blockchain Integration to Improve the Security in Healthcare Applications. doi:https://doi.org/10.1109/confluence60223.2024.10463242.

Wang, Y. and He, M. (2021). CPDS: A Cross-Blockchain Based Privacy-Preserving Data Sharing for Electronic Health Records. doi:https://doi.org/10.1109/icccbda51879.2021.9442539.

# Appendices:

Diagram 1: Data storage workflow in healthcare without blockchain

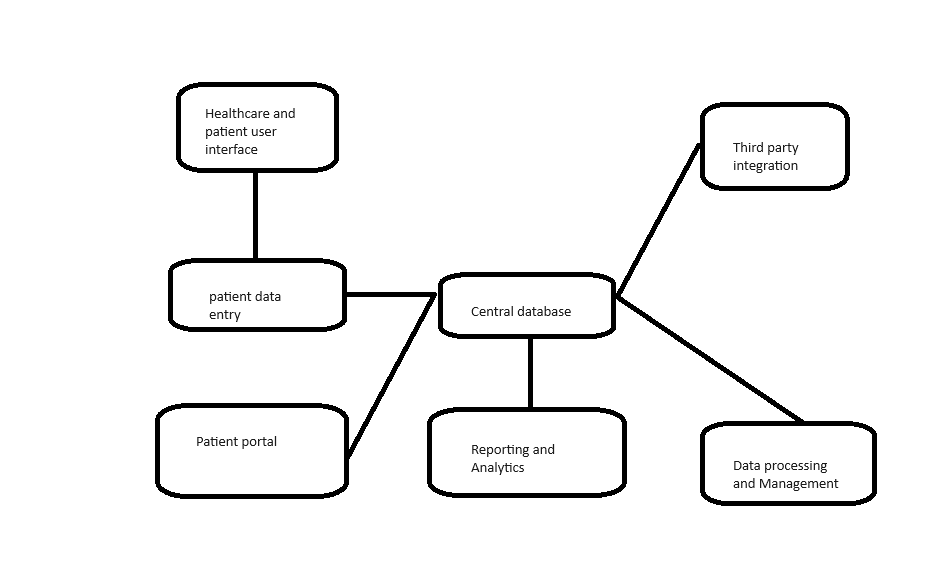


Diagram 2: Data storage workflow in healthcare with blockchain

