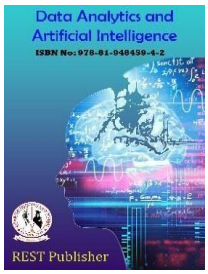
**Data Analytics and Artificial Intelligence**

**Vol: 5(1), 2025**

**REST Publisher; ISBN: 978-81-948459-4-2**

**Website: http://restpublisher.com/book-series/daai/**

**DOI: https://doi.org/10.46632/daai/5/1/14**




# Enhancing Patient-Controlled Health Data Management through Blockchain Integration: A Prototype Approach

**Prachi Patel**

*Harrisburg University of Science and Technology, United States*

Corresponding author email: prachi25898@gmail.com

***Abstract:*** *The traditional approach to managing personal health information (PHI) often suffers from issues of centralization, limited patient control, and vulnerability to data breaches. With the rapid advancement of blockchain technology, a new paradigm for secure and decentralized health data management emerges, offering patients increased autonomy and privacy over their health records. This paper proposes the design and implementation of a blockchain-based prototype for public health record (PHR) management, emphasizing decentralized storage, encryption standards, and secure data sharing. Our prototype system utilizes asymmetric encryption (RSA) to protect sensitive health data while ensuring that only authorized individuals can access the records. The blockchain structure, comprising individual blocks representing unique patient visits, fosters an immutable record of patient-provider interactions. Despite promising features, several challenges, such as network scalability, encryption robustness, and regulatory compliance, must be addressed to fully realize the potential of blockchain for healthcare data management. This work offers a pathway toward more secure, transparent, and patient-centric health data system while highlighting the obstacles to broader industry adoption.*

## 1. INTRODUCTION

Managing health records is a critical aspect of the health care industry. Traditional methods of health record manage ment are limited by factors such as centralized control, limited patient autonomy, and security risks. The growth of blockchain technology has provided a promising alternative to these chal lenges by introducing a decentralized, secure, and transparent method of health record management. This work aims to ex plore the potential of using a blockchain-based public health record system (PHR). We present a prototype implementation of a blockchain-based PHR system and discuss the challenges and limitations of our implementation that need to be addressed for practical use cases. Additionally, we focus on analyzing the benefits and drawbacks of using blockchain technology for PHR implementations, the nature of decentralization in PHRs, the use of encryption standards like RSA to safeguard patient privacy and networking infrastructure.

## 2. IMPLEMENTATION

Our implementation of a PHR system included designing and producing a prototype with much of the core functionality com pleted. Our prototype allows for the generation of encryption key pairs (private and public keys), the addition of records en crypted using the previously mentioned keys, and the ability to decrypt and view records. Additionally, it features rudimen tary networking capacities to showcase how a network could be built after expanding upon it.

### 2.1. Blockchain Structure

We decided to have individual blocks represent a single health record, which is meant to represent a single visit a patient has with a health care provider.

#### *2.1.1. Block Class*

Every block on the blockchain is represented as an instance of the" Block" class which is defined with the following fields.

- doctor - the name of the patient's doctor provided in the record.
- diagnosis - the patient's diagnosis data provided in the record.
- symptoms - the patient's symptoms are listed in the provided record.

- treatment - the prescribed treatment for the patient as listed in the record.
- prescription - the drug prescription(s) provided to the patient by the doctor as listed in the record.
- uuid - a unique identifier generated before the block is added to the chain, used to identify the block after it has been added.
- transaction - a unique identifier for the transaction cre ated during mining.
- timestamp - a timestamp string generated during mining.
- index - the index of the block within the chain, it starts at zero and is incremented by one for every additional block.
- previous hash - SHA-256 hash of the previous block's fields.

Aside from the constructor, the "Block" class contains a sin gle additional function. The create hash() function returns the SHA256 hash of a string generated from the values of all of the fields listed above. Due to the nature of SHA-256, this value is unique for every block. The value returned by this func tion is used to link adjacent blocks to each other through the previous hash field, as described above.

### *2.1.2. Blockchain Class*

There exists a Blockchain class which contains a refer ence to a single block. This block is referred to as the genesis block and is the first block in the chain. It contains dummy values and can be thought of as the head of a linked list, with the linked list being the entirety of the blockchain. The first real block is linked with the genesis block, and subsequent blocks are linked to the next block adjacent to them.

Additionally, the blockchain class contains various aspects relating to networking. Further discussion of this can be found in Section 2.3.

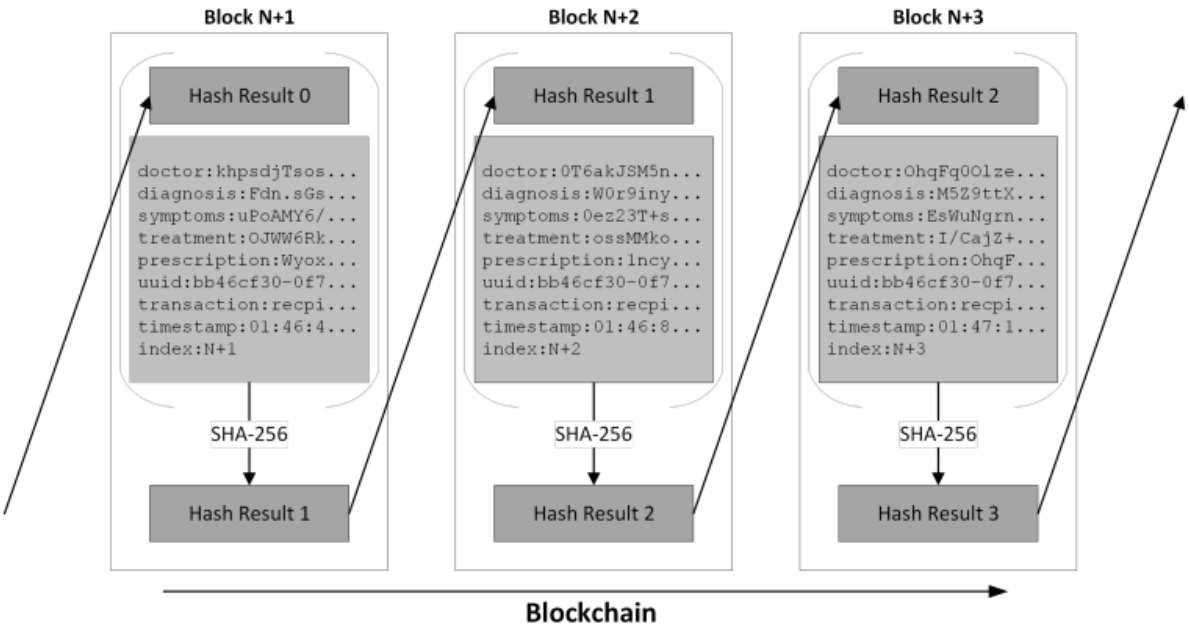



**FIGURE 1.** This diagram shows the structure of our public health record blockchain. Each block contains a single record made up of multiple fields, in cluding encrypted strings of information inputted by doctors. These encrypted strings are only readable with the correct public key. The hash of the string data is used as a pointer to the next block.

## 2.2. Encryption

Patient privacy is a critical aspect of a functional PHR imple mentation. To preserve patients' dignity and privacy, it is vital that their data is never provided to anyone else without their explicit consent. This poses a challenge to our decentralized blockchain implementation, where anyone can host a copy of all of the data contained on the blockchain. This also applies to healthcare providers—we decided that patients should be able to control what, if any, providers have access to their data.

The solution that we arrived at for this problem was to use a form of asymmetric encryption to encrypt all sensitive fields before they are added to the blockchain. We decided to use RSA for our prototype due to simplicity Menezes et al. (2001). However, there are potentially more suitable encryption stan dards that should be used for a production use case as discussed in 2.5.3.

When a patient's record is added to the blockchain, we re quire the public encryption key associated with that patient to be provided. The plain text provided for the record is then encrypted using the provided public key, and unreadable cipher text is added to the blockchain.

The cipher text that is then stored in the block can only be decrypted using the private key that is associated with the public key used to initially encrypt it. This makes it so that the data on the blockchain is only available to those with the corresponding private key.

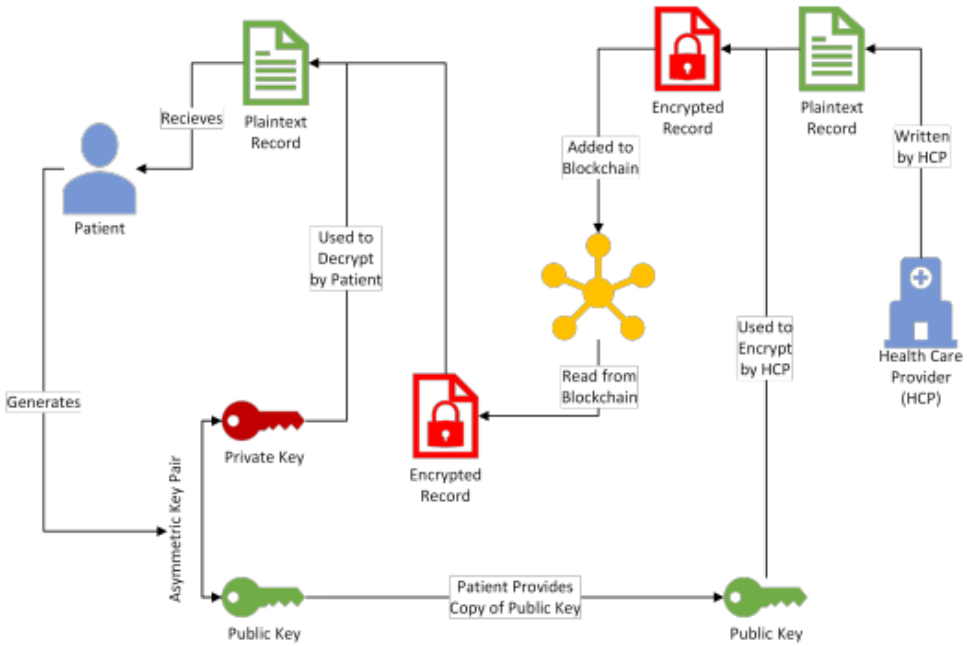



**FIGURE 2**. A visual explanation of how public key cryptography is used to en crypt and decrypt records.

### 2.3. Networking

Our networking prototype involves two nodes: a doctor and a patient. The doctor must first request access to the patient's medical record. The doctor then signs the transaction with their private key and sends it to the patient.

To decrypt the transaction, the patient must use the doctor's public key. The patient has an authorized list of doctors with their corresponding public keys, which allows them to decrypt the signatures of the doctor(s) they have authorized to view their records. If the patient cannot verify the signature, the transac tion is closed, and no data is sent to the doctor. However, if the patient can verify the signature, they can then decrypt the data the doctor requested using their private key.

Once the data has been decrypted, it can be encrypted with the doctor's public key and sent back to the doctor, ensuring that any data sent between nodes is protected against anyone who intercepts the communications. Once the doctor receives the data that is now encrypted using their public key, they can decrypt it using their private key.

Due to the limited nature of our networking implementation, there is further discussion of points where it can be expanded upon in Section 2.5.7.

### 2.4. Frontend

We created a basic application that can be accessed through a web browser. It splits functionality relevant to the two ma

jor user categories in a PHR system. For the purposes of our prototype, there is no authentication; however, in a production implementation, it would be important to strictly control who can access each side.

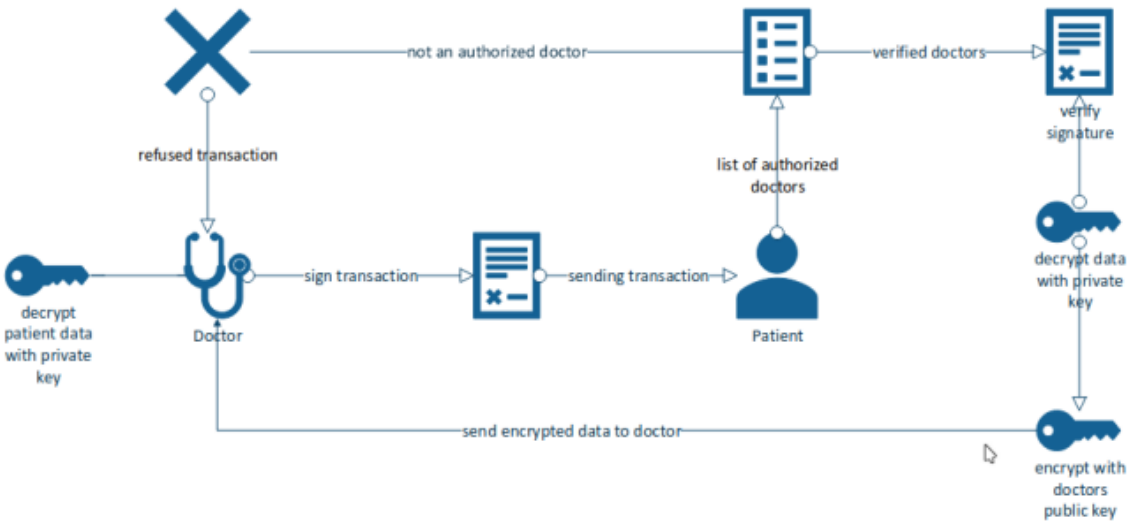



**FIGURE 3.** Diagram showcasing our network's peer-to-peer connection

### *2.4.1. Provider Use Case*

Health care providers (HCPs) are able to use the app to add records (in the form of a block) to the blockchain, provided they are given the public key corresponding to a specific pa tient. A patient would need to send their public key to their HCP, which will be used to encrypt every field in the record before it is added to the blockchain. A transaction ID (in the form of a UUID) is then given to the doctor and will be used to identify the block where the encrypted cipher text will be stored. The HCP will need to give the transaction ID to the pa tient, preferably sending them back the public key file, which has a section that stores a transaction log.

### *2.4.2. Patient Use Case*

The app allows patients to generate key pairs and view their health records. To view their data, they need a public key file and a private key file. The public key file must also contain a list of transaction IDs. The transactions are then decrypted and shown to the user in a table that allows them to filter and search data.

## 2.5. Limitations and Considerations

There are several aspects to consider regarding the limitations of our PHR system. Some of these limitations are due to choices we make, whereas others are unavoidable consequences of blockchain technology.

### *2.5.1. Scalability*

Scalability refers to a blockchain's ability to handle increasing transaction volume and data storage as the blockchain grows. Scalability has been a significant challenge in the adoption of blockchain technology, as it can limit the number of transactions the network can process and increase the time required to validate new transactions.

Some aspects of our implementation are not very scalable. As more blocks are added to the blockchain, the time it takes to validate it will increase. The time it takes to traverse the blockchain will also increase, which will affect users by increasing the time it takes to locate all of their records.

Because the chain is immutable, the disk space required to host a node will only increase as more blocks are added. Due to file size constraints, it could possibly become infeasible to host a copy on readily available hardware.

As the number of users rises, the number of transactions per second will also rise. Alongside this, the amount of data need ing to be stored and processed at any given moment will in crease, which could cause delays in transaction processing and validation, leading to slower network performance. Similarly, as the number of nodes rises, there is the potential for

network congestion, which could possibly result in longer confirmation times and a decrease in network performance. Further discussion of scalability and potential solutions can be found in 3.1

#### *2.5.2. Mutability*

Our implementation features an intentionally immutable blockchain. We designed it this way to ensure the authenticity and integrity of the records. Once records have been added to the blockchain, they cannot be forged or altered, thus reducing the chances of fraud and deception.

However, this implementation is not fool proof. There are valid reasons why mutability is desirable in a PHR system.

- Correcting mistakes in place is not possible. The only thing that can be done is create a new record with the fixes stored in it, however this will take up additional storage space on the blockchain.
- If a patient's private key is compromised, there is no way to protect their data from being accessed and read. If someone publicly releases a patient's private key, the entirety of their medical records will be publicly accessible for perpetuity.
- An immutable blockchain makes it so that the fields and data types are unchanging. We will be unable to introduce new fields that may eventually become necessary in the medical field.

#### *2.5.3. Encryption*

We have chosen to use RSA-4096 to encrypt patient records for reasons of convenience, but our implementation can be easily adapted to other encryption standards. However, there are some downsides to our current approach, which we outline be low.

- RSA encryption is vulnerable to attacks using quantum computers. If quantum computing technology advances to the point where it can readily crack RSA-4096, then our records may be compromised. This could be particularly problematic since blockchain records are immutable and cannot be changed retroactively. The details of how quantum computing might be able to do this are beyond the scope of this paper.
- RSA is relatively slow in some cases compared to the encryption and decryption speeds of other algorithms, such as elliptic curve cryptography (ECC).
- The size of our keys has to be large, which results in larger key file sizes and higher encryption and decryption times.

Additionally, the use of public key cryptography has down sides. Users must be careful not to publicize their private keys and must actively protect them from theft or unauthorized ac cess. If a malicious third party acquires their private key, all of their records will be made available to that third party. Since the blockchain is immutable, nothing can be done to revoke their access to the patient's data.

#### *2.5.4. Usability and Security*

A blockchain based PHR system has many privacy, security, and patient autonomy benefits, however the level of knowledge and experience required to use our blockchain system is higher than what is ideal. In many jurisdictions, patients are not accustomed to having any sort of digital health records, let alone blockchain-based technology. It will be difficult to ease the transition into this sort of system for those who are older and less technologically savvy. We attempted to make our simple mentation as user-friendly as possible and added clear instructions, but there may be gaps in our implementation. In order to seriously assess the feasibility of a given implementation, extensive quality assurance testing must be completed by a wide array of individuals to reduce the chances of patients being left out and unable to use the system.

This is also a security concern, as uncertain users might be more likely to take security risks, such as exposing their private key information to unauthorized or malicious actors. According to the Anti-Phishing Work Group, the third quarter of 2022 set the highest record for the number of recorded phishing attacks www (2022). They note that the number of phishing attacks has been rising. Our PHR system is reliant on public key cryptography where the user must keep their key private at all costs. If it is seen by a phisher, the entirety of a patient's medical records could be accessed and read. There would be no way to recover from this aside from generating a new key pair for use in new records (all previous records would be permanently accessible to anyone with the original private key).

We are also limited by internet connectivity. Patients who are unable to gain access to the internet would be unable to view their medical records. As global internet connectivity is still less than 70% (itu (2022)) of the global population, it

is important to note that it will be impossible to implement such a system globally until global factors such as internet connectivity and political instability are addressed.

Another factor to consider is the format of our front end. We designed it with desktop computer sensibilities in mind. However, a large subset of users only uses mobile platforms, which is not something our design was intended for. Therefore, to provide a more seamless experience, we would need to design our systems to support as many platforms as possible.

### *2.5.5. Node Host Incentives*

A major limitation of our PHR system is the lack of incentive for individuals or organizations to host additional nodes. Without a sufficiently distributed network, the blockchain becomes vulnerable to centralization and may compromise the integrity of the system.

Hosting a node may require significant resources such as pro cessing power and storage, resulting in high operating costs. The benefits of hosting a node are not always readily apparent to users, so they may not understand how vital it is for the blockchain's security and reliability to have many hosts. Additionally, an absence of financial or other incentives can make it difficult to attract and retain node hosts.

Potential solutions to this issue include providing financial incentives to hosts. If governments subsidize a PHR, they could provide minor tax benefits to node hosts proportional to the computational resources they provide. Alternatively, node hosts could receive compensation in the form of tokens or other cryptocurrencies. A downside of financial incentives is that they may attract nodes primarily motivated by profit and not interested in the system's interests.

Another approach is to offer non-financial incentives to node hosts. For example, node hosts could be given a greater say in the governance of the PHR system, including voting rights and a voice in the decision-making process. However, this would have to be considered very carefully so as not to silence the needs of those who cannot afford to contribute to the network.

Overall, creating incentives for individuals and organizations to host nodes is critical for the integrity and security of a pro duction PHR. By implementing a compelling incentive scheme, we can attract a wide range of participants to create a distributed network that is resilient against centralization and other security threats.

### *2.5.6. Legal Considerations*

In addition to the security and privacy concerns discussed previously, it should also be noted that there is an ethical and legal dimension to the issue as well. Due to the immutable na ture of the blockchain, it is impossible for data to be removed from it. This may have legal consequences in locations such as the European Union (EU) where they have the General Data Protection Regulation (GDPR) which requires services oper ating in the EU to give users the ability to have all of their data deleted European Parliament and Council of the European Union (2016). This is not possible to implement in a decen tralized blockchain, which may make it impossible to legally deploy this technology in the EU Fang et al. (2021).

### *2.5.7. Networking Implementation*

As discussed previously, our prototype's networking imple mentation is very limited. In this section, we will describe how networking could be expanded in a future iteration of our pro totype.

Our blockchain-based PHR system is decentralized which means that there is no central node/network that users will con nect to. Instead, users become nodes themselves by hosting a copy of the blockchain and connecting to other nodes. Nodes would usually mine or listen in on other nodes. Mining is the process of adding a new block to the blockchain by perform ing computational work, in our case, proof of work, to vali date transactions and create new blocks. When a node makes a request to add a block, all the active nodes will do proof of work on that block (mining), and whoever finishes first would ideally be rewarded with some cryptocurrency or other incen tives as discussed in Section 2.5.5. This mining process helps strengthen the integrity and security of the network by ensuring only valid transactions are added to the blockchain.

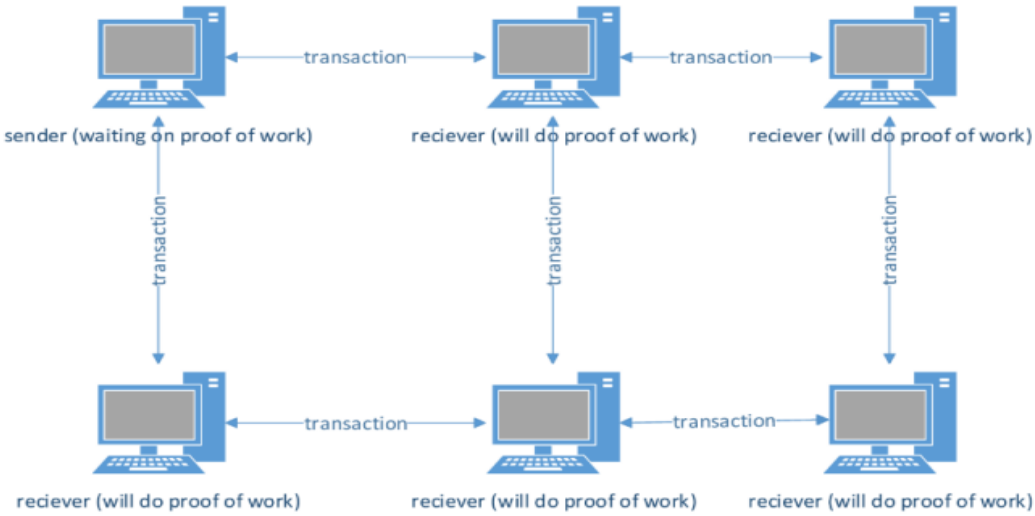



**FIGURE 4**. This diagram presents a visual representation of how our decentralized PHR blockchain network would operate.

### *2.6. Intended Use Case*

Based on our analysis of our system's functionality and limitations, we believe it is best used alongside a traditional health record database. Blockchain-specific benefits, like patient autonomy over their own records, will be limited. However, as discussed in the previous section, we do not currently have solutions in place to overcome our system's major limitations.

Having a blockchain-based" mirror" (new records would be inserted into the regular database as well as automatically encrypted and then added to the blockchain) of medical health records that is opt-in would overcome many of the limitations discussed in the previous section. The opt-in nature of it might make it so that less technically savvy individuals are less likely to use the system, thus reducing the chances of user error. A smaller network would also mean fewer concerns relating to scalability, and fewer compute resources would be required to keep the blockchain operational. An opt-in system might also help build trust in the blockchain-based PHR system for pa tients who might end up being interested in using it but would not be satisfied if they were forced into using it.

Having the blockchain system implemented in parallel will still bring many benefits, including giving patients the ability to be certain that their data is stored in a location that is immutable. While the database has the potential to be altered, a patient who is unsure of the validity of their medical records in the database can always check with the data on the blockchain to ensure that their records have been unaltered from the moment they were posted.

There are still potential downsides to this approach, the great est of which is cost. It will cost a lot more to run two redundant systems than it would to just run one. This approach should be considered for implementation in stable environments with the financial capacity to support two systems in parallel. Ad ditionally, patients would also still have to make sure that their key is kept hidden from outsiders, otherwise their data will be permanently compromised as described previously.

## 3. INDUSTRY ANALYSIS

Blockchain-based PHR systems are a rapidly evolving area of research that has gained popularity due to their potential to address several long-standing issues in healthcare data management.

### 3.1. Scalability

Scalability is a major challenge of a blockchain-based PHR system. It is a crucial factor in the context of blockchain systems as it determines the ability of a blockchain network to handle high transaction volumes and store vast amounts of data. Scalability has been a widely discussed topic among blockchain researchers, particularly with the use of decentral ized blockchains, which are immutable and lack any form of centralized control. Many of the issues discussed in Section 2.5.1 apply broadly to the industry, and many of the scalability related issues we encountered during the development of

our prototype are active areas of research that have yet to be fully solved.

#### *3.1.1. Off-Chain Storage and Processing*

Off-chain data storage is an approach that can be used to en hance a blockchain's potential for scalability. Off-chain data storage involves storing data off of the blockchain, usually in the form of an InterPlanetary File System (IPFS) or a secure database. It allows certain data or functions to be processed outside of the blockchain network, freeing up resources and al lowing for faster transaction processing. This can potentially increase the efficiency of the network and result in lower trans action fees. For example, medical images can be encrypted and stored off-chain inside an IPFS. If a healthcare provider re quests a patient's records, the blockchain would only handle the verification process through a smart contract, while the decryp tion and delivery of the data would be done off-chain. Essen tially, this approach delegates the task of storing and processing data to an off-chain system while the blockchain keeps track of who has authorization to view this data.

The use of off-chain data storage/processing also introduces potential issues that must be considered. A significant concern is the potential privacy and security risks that off-chain data storage might introduce. Since off-chain storage may not fol low the same security protocols as a blockchain, it may not be immutable in nature, and data may be deleted or edited.

Data availability is another related concern. Depending on the specific off-chain storage solution, a third-party might be introduced that would manage or maintain the infrastructure. For example, a hospital may have control over the off-chain data and could edit or remove data, which could compromise data privacy and security. While this approach has potential benefits in terms of scalability and efficiency, it may compromise data privacy, as other nodes would not be able to ensure that the data has not been tampered with.

This appears to be a common theme: to increase privacy and security, scalability must be sacrificed, and vice versa. Over all, off-chain storage provides solutions to longstanding issues with blockchain technology; however, it comes with significant compromises that need to be carefully assessed before imple mentation.

## 4. CONCLUSION

In conclusion, blockchain technology presents an exciting opportunity to revolutionize the traditional methods of data storage and management in the opportunity. Our implementa tion of a prototype for what this system could look like provides insights into the many benefits of using this technology, such as greater patient autonomy, security, transparency, and privacy, while also acknowledging the challenges and limitations that it would face if deployed in practical use cases. Our analysis of the industry shows there are some solutions to the problems our prototype faced, however it also showed us that there is a lot more research that needs to be done, specifically in terms of scalability and the lack of legal precedent for blockchain tech nology in the healthcare industry. Overall, the potential ben efits of blockchain technology in PHR management make it a promising area for future research and development.

## REFERENCES


[1]. 2022. Measuring digital development: Facts and figures 2022. URL: https://www.itu.int/en/ITU-D/Statistics/Pages/facts/default.aspx.

[2]. 2022. Summary – 3rd quarter 2022. URL: https://docs.apwg.org/ reports/apwg_trends_report_q3_2022.pdf.

[3]. European Parliament and Council of the European Union, 2016. Regulation (eu) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/ec (general data protection regulation). URL: https://gdpr-info. eu/art-17-gdpr/. article 17 GDPR.

[4]. Fang, H.S.A., Tan, T.H., Tan, Y.F.C., Tan, C.J.M., 2021. Blockchain personal health records: Systematic review. J Med Internet Res 23, e25094. URL: https://www.jmir.org/2021/4/e25094, doi:10.2196/25094.

[5]. Ghadamyari, M., Samet, S., 2020. Decentralized electronic health records (dehr): A privacy-preserving consortium blockchain model for managing electronic health records. Proceedings of the 6th International Conference on Information and Communication Technologies for Ageing Well and e Health doi:10.5220/0009398101990204.

[6]. Menezes, A.J., van Oorschot, P.C., Vanstone, S.A., 2001. Public-Key Encryp tion. 5 ed.. CRC Press. pp. 285–291.

[7]. Nakamoto, S., 2008. Bitcoin: A peer-to-peer electronic cash system. URL: https://bitcoin.org/bitcoin.pdf.

[8]. Zanbaghi, S., Samet, S., 2022. A blockchain-based privacy-preserving physical delivery system. World Academy of Science, Engineering and Technology International Journal of Information and Communication Engineering 16, 532–539.