Bournemouth University

A Blockchain-Based Approach for Enhancing Digital Identity Security and Privacy in Healthcare

Blockchain and Digital Futures
Yasemin Karaca
s5619032

ABSTRACT

This paper proposes a blockchain solution to enhance digital identity and consent management in NHS. Blockchain technologies like cryptography, smart contracts, and self-sovereign identity are used to distribute patient data securely across nodes instead of centralised databases. Smart contracts enable consent-based sharing of records with detailed access controls. Self-sovereign identity gives patients control over medical credentials. Multilayered security is provided by additional methods. The use of blockchain technology, as opposed to traditional systems, seeks to enhance security, guarantee that audit trails are not tampered with, decrease the probability of identity theft, and simplify the process of sharing data across multiple providers.

KEYWORDS

blockchain, digital identity, self-sovereign identity, healthcare, smart contract

INDEX

LIST OF FIGURES

LIST OF TABLES

1. INTRODUCTION

1.1. Definition of Blockchain Technology

Blockchain is a distributed digital ledger that records encrypted data transparently and securely without a central authority. Every block has information specifying the date and time of recording along with the data that needs to be entered into the registry. Anyone can read and verify the data that is recorded, and anyone can obtain a copy of the registry.

According to Yaga et al. (2018), distributed digital ledgers, which include cryptographically signed transactions organised into blocks, are called blockchains. After validation and going through the approval process, every block is cryptographically connected to the one before it, making tamper apparent.

Simanta Shekhar Sarmah (2018) state that blockchain prevents a single central organisation from managing the network through permitting everyone on the network to view each other's entries. Every time a transaction is made, it is sent to the network, where computer algorithms assess its reliability. Following verification, the transaction is linked to the previous transaction to create a chain of transactions. This chain is referred as the blockchain.

1.2. Definition of Digital Identity

Digital identities, a concept that appeared with the digital age, empower individuals to authenticate their identity across various online platforms. This electronic method of verification eliminates the need for physical visits to institutions, enabling smoother transactions and optimised convenience. Digital identity has gained attraction across diverse industries, including healthcare. However, the rise of online fraud and money laundering requires robust security measures, emphasising the importance of implementing strict digital identity verification processes.

Verifying digital identities includes matching the provided information against gathered records to authenticate the claimed individual. As technology progresses, advanced identity verification algorithms have been developed, enabling the accurate assessment of document authenticity. By implementing these methods, the creation of fake identities and unauthorised transactions can be effectively prevented.

According to Zhao et al. (2021), digital identity generally refers to the digital representation of network entities. Users can verify the validity of their identity declarations within the network by using the digital information that has been generated as an authentication. Users typically have unique digital identities for application services, which enables them to prove their identities across many platforms in a unique way applying different digital IDs.

2. LITERATURE REVIEW

2.1. Blockchain Structure

Blockchain technology lacks a central structure, allowing data to be accessed from any computer. It's transparently possible to find out who owns the transactions and when they were made in addition to accessing information. Since transactions in this technology cannot be changed, any necessary corrections are made by adding a new record to the system. In this way, all information is kept safe.

In Blockchain, encryption is implemented with various mathematical algorithms called "hash." Hash enables blocks to be differentiated from one another and ensures that they are placed in the right blockchain. Each block is independent and contains the hash code of the previous block, allowing the following blocks to be linked. The consistency and non-changeability of information on blocks prove the reliability of the data recording system.

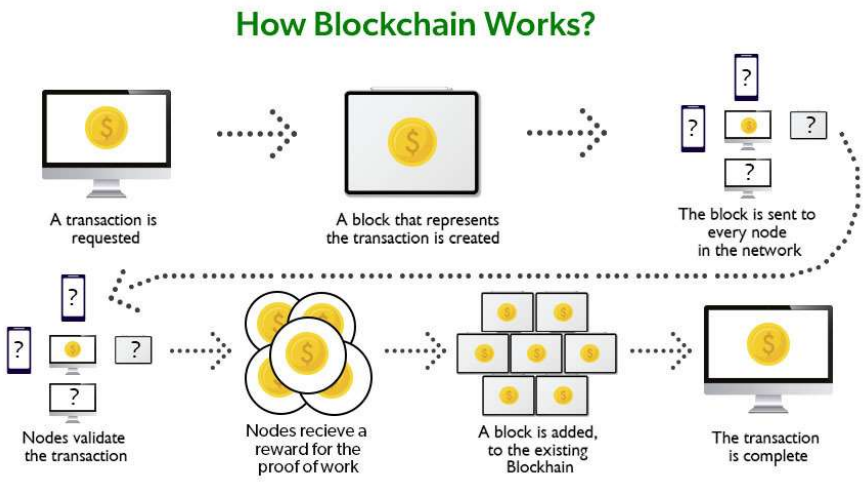

Figure 1. Blockchain Structure. Source: (Ujjawal, 2018)

2.2. Digital Identity and Blockchain

In today's digital world, where sensitive information is shared online, the need for a strong and secure identity authentication system is more important than ever. Typical methods of identity management, such as usernames and passwords, are disposed to hacking and fraud, therefore, they are not enough to provide the required level of security to protect people's data. Blockchain technology provides a potential solution to this problem.

Ahmed et al. (2022) state that by utilising blockchain for digital identity, individuals can have ownership and control over their identities. Digital identity plays a crucial role in various aspects of our lives, from accessing online services to receiving government benefits (Singla et al., 2022).

3. PROBLEM STATEMENT

3.1. Use Case Scenario

Alice is a dedicated healthcare professional working within a prominent department of the UK's National Health Service (NHS). After a consultation with a patient, Alice recommends a medical procedure to address a health issue. To proceed with the treatment, Alice needs the patient to provide sensitive personal information, traditionally processed through conventional channels. Trusting the system's security measures, the patient promptly provides the required personal information, including personal identification, social security number, medical history, contact details, and financial information.

This data is associated with a digital identity, accessible through a username and password, within the NHS's centralised system. However, despite the system's convenience for processing, it has become a security vulnerability due to the sensitive nature of the stored information, exposing it to potential hacking and unauthorised access. In an era of increasing cyber threats, organisations like the NHS, which store vast amounts of sensitive patient data centrally, become attractive targets for hackers.

If the NHS falls victim to a data breach, all patient records, including personal identification, medical history, contact details, and financial information, could be exposed, making both patients and the institution vulnerable. This situation could lead to identity theft, fraudulent medical claims, and unauthorised access to confidential health information.

Recognising the security risks associated with centralised systems, the NHS's cybersecurity team is actively seeking an innovative and comprehensive solution to secure the patient information collection process. Their goal is to protect both the institution and patients from potential identity theft and fraud in the face of increasing cyber threats. The challenge lies in finding a secure method to manage and store large amounts of sensitive patient data while mitigating the risks associated with centralised systems.

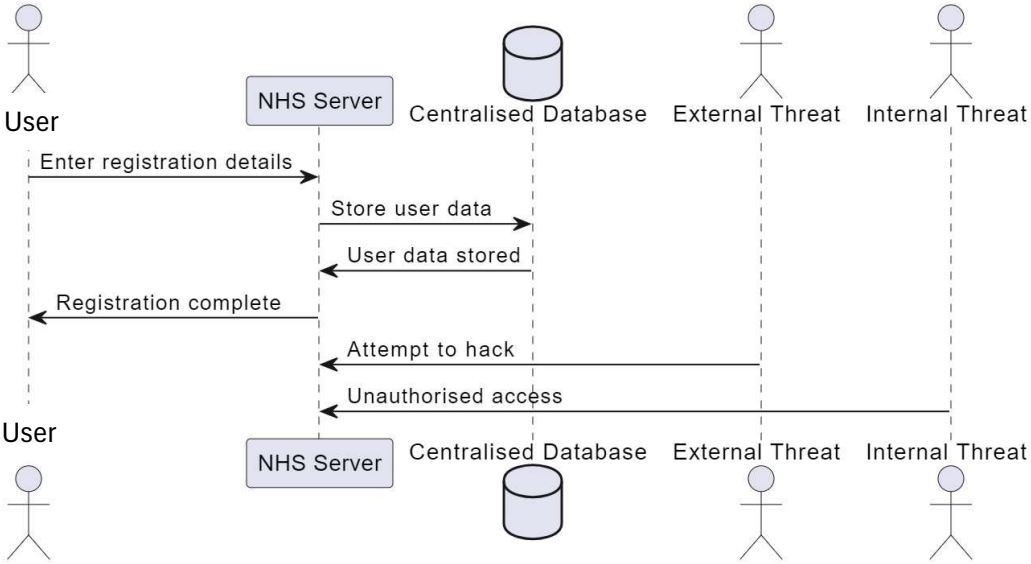

Figure 2. Threat Modelling Diagram

Table 1 – Risks of using Centralised Database

Risk Type	Description
Unauthorised Access	Unauthorised individuals gaining access to the centralised database.
Data Breach	Leakage of private and confidential patient information due to a security breach in the centralised system.
Single point of failure	The reliance on a single patient database can result in data loss or service disruption.
Insider Threats	Internal staff can be a threat to data security through intentional or inadvertent actions.
Data Consistency	Managing data integrity and maintaining data consistency across a centralised database can be a demanding struggle

As shown in table 1, using centralised database led to facing numerous data security challenges. These challenges can have serious consequences for both the institution and individuals. Institutions may face reputational damage and legal consequences, while individuals may experience privacy concerns, identity theft and financial losses. To effectively mitigate these risks, healthcare institutions should implement blockchain technology. The reliability of hospital IT systems and management is lacking, potentially compromising patient care and legal processes (Thimbleby, 2018).

4. BACKGROUND AND RELATED WORK

4.1. Previous Case Study and Existing Solution

4.1.1. Case Study

The study by Song & Yu (2022) discusses the problem of existing challenges and weaknesses in digital identity management systems. These challenges include difficulty in cross-domain authentication and interoperation, lack of credibility in identity authentication, and weak security of identity data.

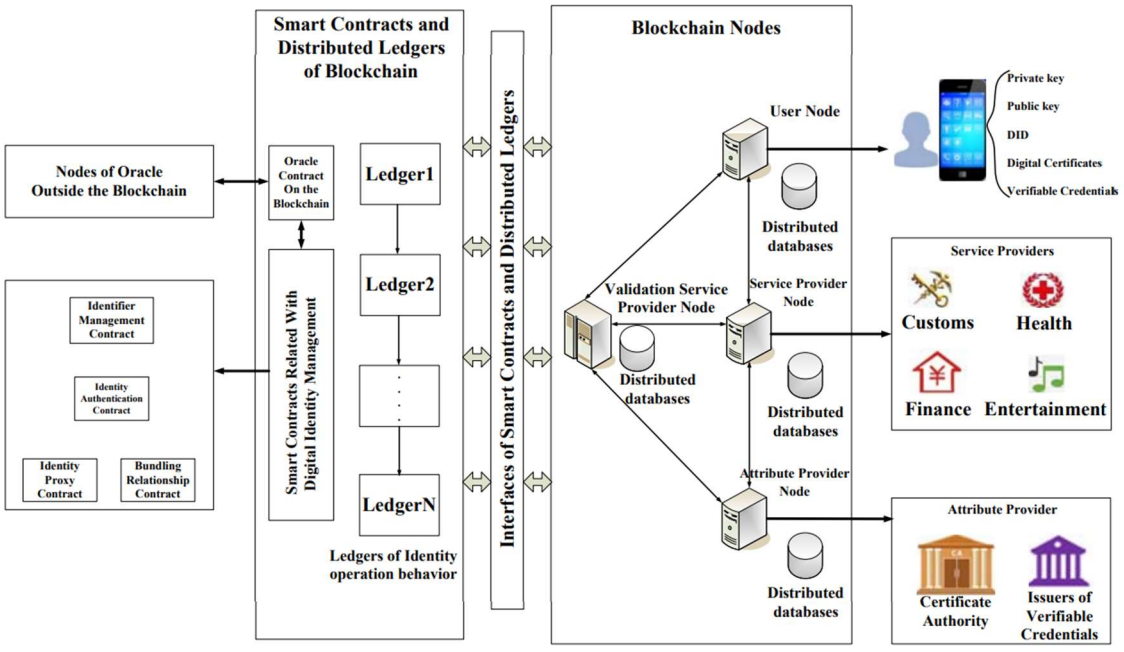

Figure 3. The architecture of the proposed system model (Song & Yu, 2022)

Proposed Solution: Song & Yu, 2022 offers a solution by presenting a model that integrates self-sovereign identity, oracle, and blockchain technologies. The system model includes five node types, including blockchain nodes, smart contracts, and distributed ledgers, with the user node functioning as the intelligent mobile terminal for users. Individuals can maintain their digital identity components such as private keys, public keys, decentralised identifiers (DIDs), verifiable credentials (VCs), and digital certificates through this node. In addition, the proposed framework emphasises the importance of increasing the reliability of identity authentication. Unlike many traditional systems that rely on external authentication, which may lack transparency and provide a fraud risk, this model tries to mitigate these problems while improving the overall reliability and security of identity identification processes.

4.2. Analysis of the Previous Proposed Blockchain Approaches

The proposed solution integrates blockchain technology to improves the reliability of identity authentication. Unlike traditional systems that relies on external authentication, the authors proposed a decentralised system to identity management, enhancing security and providing users more control over their digital identity data.

However, it's important to note that the lack of a mentioned consensus mechanism in the proposed blockchain implementation raises concerns about the system's ability to ensure agreement and consistency among nodes in the network. A consensus mechanism is crucial for validating transactions and maintaining the integrity of the blockchain, and its absence may impact the overall effectiveness of the system.

5. PROPOSED BLOCKCHAIN SOLUTION

5.1. Overview of the Solution

The use of blockchain technology can potentially provide a strong and safe method for the NHS to handle confidential patient data. Blockchain offers features such as distributed ledger, decentralised storage, authentication, security, and traceability, which can help secure sensitive patient data and overcome issues with centralised data management systems (Saragih et al., 2022).

1. **Decentralisation**

Unlike traditional centralised systems, which have a single point of vulnerability, blockchain operates on a decentralised network of interconnected computers, known as nodes. This distributed architecture makes it more resistant to cyberattacks, as hackers would need to breach all nodes at once to compromise the entire system. Each patient would have a unique digital identity stored on the blockchain, eliminating the need for a centralised database vulnerable to large-scale breaches.

2. **Immutable Records**

Blockchain technology's fundamental feature provides a stronghold for identity data, protecting it from getting harmed and unauthorised modifications. With blockchain technology, patient records will be stored in a tamper-proof manner. Once information is recorded, it becomes a permanent part of the chain, it cannot be altered or deleted, providing a reliable and secure historical record of patient information, and preserving the integrity of identity information for life, which makes it difficult for malicious actors to forge or manipulate the documents.

3. **Smart Contracts for Consent and Access Control**

To manage patient consent and access control, smart contracts can be utilised on blockchain. These contracts are irreversible and allow the realisation of transactions

between signatories depending on predefined conditions. Patients can explicitly specify requirements and grant permission for NHS workers to access specific parts of their medical data, ensuring that their medical records are only accessible to authorised healthcare professionals.

4. **Consensus Algorithm**

The consensus algorithm can offer all nodes in the network agree on the validity of transactions. This feature prevents unauthorised changes to the data and ensures that any changes to patient records are legal and agreed upon by the network.

5. **Self-Sovereign Identity (SSI)**

Patients would be able to securely share their medical records with healthcare providers while keeping control over who can access them and for what purposes by using SSI, which would give patients authority over their own digital identities.

6. **Enhanced Security through Cryptography and Digital Signatures**

Blockchain utilises cryptographic techniques to protect identity information. This multilayered defence system integrates encryption and decryption protocols, ensuring that only authorised users with the corresponding cryptographic keys can access and verify identity data. Digital signatures add an extra layer of security. When data is shared, the sender can sign it with their private key. The receiver can then verify the sender's identity using the sender's public key. This process ensures data integrity and non-repudiation.

5.2. System Architecture of the Solution

The system architecture of the solution is illustrated in figure 4.

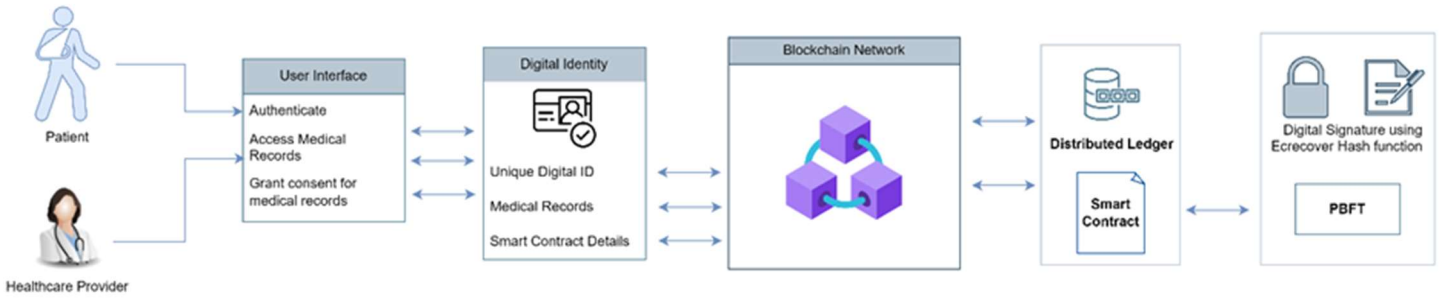

Figure 4. System Architecture of the Digital Identity Management System

In figure 5, a flowchart of immutable records is provided.

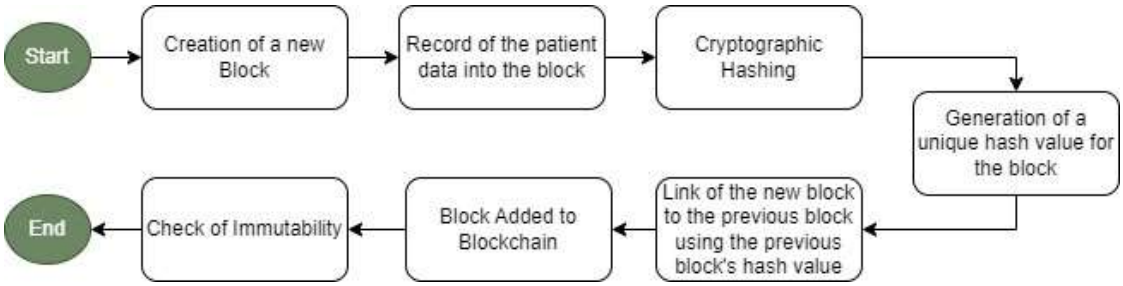

Figure 5. Data Flow Diagram for NHS's Blockchain System

The main goal in designing NHS smart contracts is to enable secure and decentralised verification of patient identities. This ensures NHS providers can reliably access accurate and current patient information. To do this requires integrating components like unique IDs for patients and providers, a verification status marker for patients, and rules specifying provider access to medical records.

The process starts with patients registering on NHS, creating a digital ID and asking to have their identity verified by submitting documents. A smart contract manages the verification, using a consensus protocol called Practical Byzantine Fault Tolerance (PBFT) across healthcare nodes to validate it in a tamper-proof way. Once PBFT says the patient is verified, they can selectively let providers access certain records by updating the contract. Providers then request access through the contract, which uses consensus to grant it and update permissions. Any changes to a patient's records get immutably logged on the blockchain.

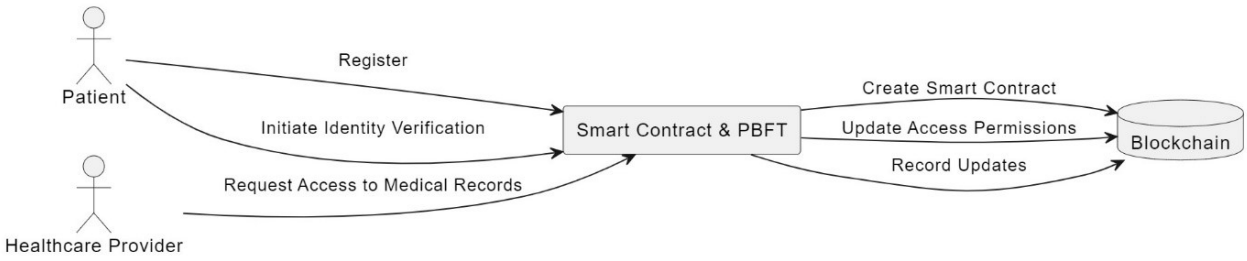

Figure 6. Use Case Diagram for NHS's Blockchain System

Li et al. (2022) state that PBFT, which stands for Practical Byzantine Fault Tolerance, serves as a consensus algorithm in alliance blockchain systems, ensuring nodes reach an agreement on transactions.

5.3. Smart Contract of the Solution

```solidity
// SPDX-License-Identifier: MIT
pragma solidity >=0.7.0 < 0.9.0;

contract NHSDigitalIdentityConsent {
    struct Patient {
        bool isVerified;
        mapping(address => bool) nhsProviders;
        bytes32 ssiDid;
    }
    mapping(address => Patient) public patients;

    modifier onlyVerifiedPatient() {
        require(patients[msg.sender].isVerified, "Patient is not verified");
        _;
    }

    event IdentityVerification(address indexed patient, bool isVerified, bytes32
ssiDid);
    event ConsentGranted(address indexed patient, address indexed nhsProvider);
    event ConsentRevoked(address indexed patient, address indexed nhsProvider);

    function verifyPatient(bytes32 ssiDid) external {
        patients[msg.sender].isVerified = true;
        patients[msg.sender].ssiDid = ssiDid;
        emit IdentityVerification(msg.sender, true, ssiDid);
    }

    function grantConsent(address nhsProvider) external onlyVerifiedPatient {
        patients[msg.sender].nhsProviders[nhsProvider] = true;
        emit ConsentGranted(msg.sender, nhsProvider);
    }

    function revokeConsent(address nhsProvider) external onlyVerifiedPatient {
        patients[msg.sender].nhsProviders[nhsProvider] = false;
        emit ConsentRevoked(msg.sender, nhsProvider);
    }

    function implementPBFTConsensus() external {
    }

    function verifySignature(bytes32 message) internal view returns (address) {
        address signer = ecrecover(message, 0, 0, 0);
        require(signer != address(0), "Invalid signature");
        require(signer == msg.sender, "Signature does not match sender");
        return signer;
    }
}
```

Figure 7. Smart Contract

In figure 7, this implemented Solidity smart contract, called NHSDigitalIdentityConsent, simplifies a digital identity and consent management system for patients and National Health Service (NHS) providers on the Ethereum blockchain. Patients are represented by a struct containing a verification status, a mapping of NHS providers with their consent status, and a self-sovereign identity decentralised identifier (SSI DID). The contract includes functions for patients to verify their identity, grant and revoke consent for specific NHS providers, and implement Practical Byzantine Fault Tolerance (PBFT) consensus. The contract also verifies the signature of a given message, ensuring that the sender is the legal signer by using Solidity's ecrecover function, which is a cryptographic method. The events IdentityVerification, ConsentGranted, and ConsentRevoked are emitted upon relevant

actions. The code focuses on ensuring patient consent and identity verification through the Ethereum blockchain.

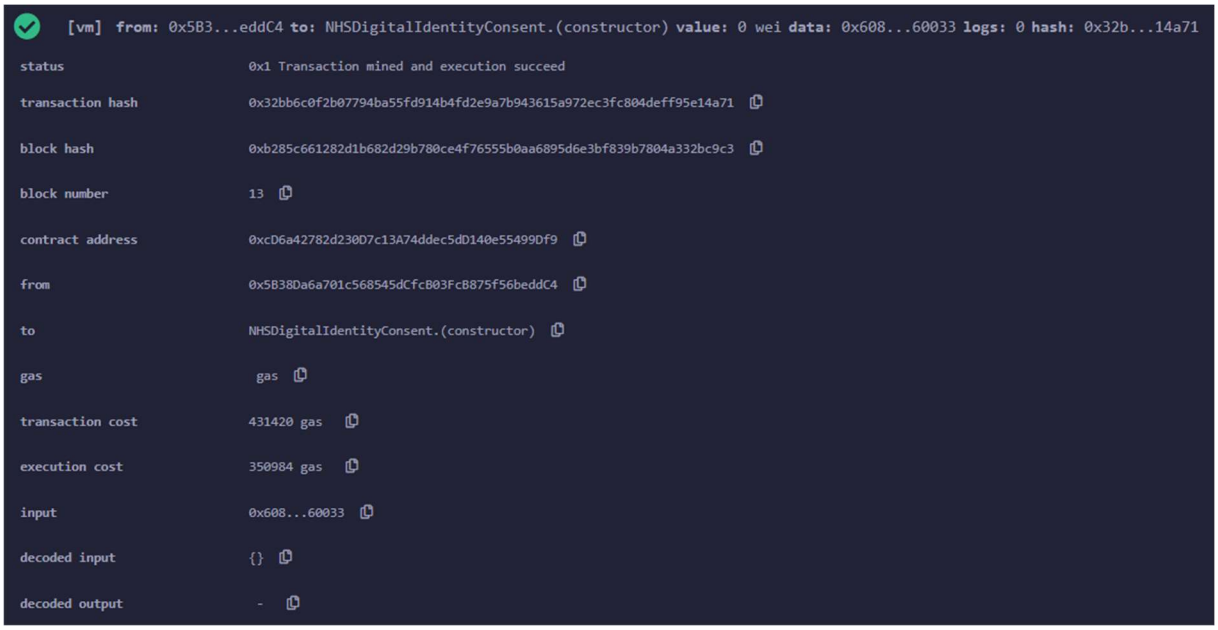

Figure 8. Deploy output of the code

The NHSDigitalIdentityConsent smart contract can be deployed by initiating an Ethereum blockchain transaction. This transaction contains the constructor arguments, the required computation gas, and the contract's compiled bytecode. The deployed smart contract receives a unique contract address from the Ethereum network. The contract address, which indicates where the contract is located on the blockchain, the transaction hash, which enables users to keep track of the transaction on blockchain users, and the gas used during deployment are often included in the deployment output. Transaction receipts may contain event logs from the deployment process, such as the IdentityVerification collecting patient verification. Rouhani and Deters (2019) state that smart contracts play a crucial role in blockchain technology, enhancing security, performance, and applications across various industries.

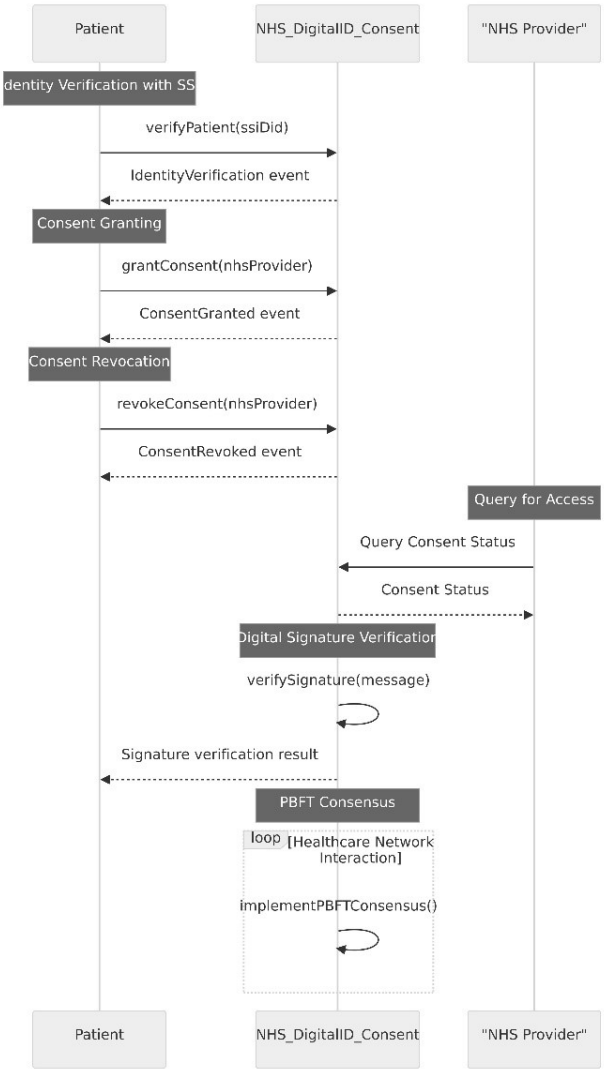

Figure 9. Sequence Diagram of the code

Table 2. Sample Patient Data Verification Table of Ecrecover hash function

Original Text	Ecrecover Hash
"PatientID: 123, BloodType: A+"	0x5Aaeb6053F3E94C9b9A09f33669435E7ef1bEAeD
"PatientID: 250, BloodType: 0+"	0x7Dc6D9C1b94a89C42b0f2A6c4999281ac1EaF00D
"PatientID: 338, BloodType: AB+"	0xF8b31A41E6B64F69575E6BcaDf9e77d7c43Fd0e0

Table 2 displays a sample of unique Ethereum addresses generated from patient data to ensure its integrity and authenticity. This is achieved through a process that involves digitally signing the patient information using a private key and then employing the ecrecover function to verify the signature and create a corresponding address. This address serves as a secure identifier, as only the holder of the private key could have produced a valid signature. This indicates the importance of digital signatures in ensuring the authenticity and integrity of sensitive data through a secure and tamper-proof process.

6. EVALUATION

6.1. Challenges and Considerations

While blockchain's potential for securing NHS patient data is exciting, implementing it demands careful consideration. Extensive training and system updates are required for the NHS to widely adopt blockchain technology. While blockchain can provide robust security, it is not a guaranteed solution for all problems. Designing and testing smart contracts requires precision and attention, just like any other code. Compatibility with existing systems and adherence to regulatory compliance are crucial for successful data exchange. For managing patient consent via smart contracts, it is important to have clear legal frameworks. Moreover, the scalability of algorithms and their impact on the environment need to be addressed. It is also important to balance the advantages of decentralisation with a trustworthy governance system. Finally, addressing privacy concerns and educating patients about blockchain are critical for its success in transforming healthcare data management. It can be difficult to guarantee transparency and maintain the integrity of data in identity management systems, but blockchain technology offers a solution by providing transparent and tamper-proof records (Aydar et al., 2020).

6.2. Results and Discussion

The proposed blockchain-based solution offers multiple advantages over traditional methods of managing digital identities and consent in healthcare. By using decentralisation, cryptographic security, smart contracts, and patient-controlled identities, this solution gives patients greater control over their medical records while enhancing data privacy and consent management. Using blockchain technology offers multiple advantages, such as removing central points of failure and greatly increasing system security against cyberattacks by spreading data between blockchain nodes. Smart contracts allow patients to control access permissions to their records, ensuring consent-based sharing only with authorised providers. SSI gives patients exclusive ownership over their credentials, reducing identity theft risks. Advanced cryptographic techniques also secure end-to-end privacy while enabling verification of transactions. PBFT uses cryptography to provide strong security even with malicious nodes. This consensus approach promotes quick confirmation times, energy efficiency, and resilience against attacks.

According to T et al. (2022), utilising decentralised identifiers and verifiable credentials based on blockchain can enhance the authentication and consent management for patients in Electronic Health Records. This approach helps minimise the risks of single points of failure, loss of privacy, and interoperability challenges. Blockchain technology can improve the management of patient data and identity in the

healthcare sector by providing self-sovereign identity and granting individuals control over their data (Houtan, 2020).

Compared to other blockchain-based solution examined in this paper, this proposed solution uniquely integrates self-sovereign identity, smart contract-based access controls, and Practical Byzantine Fault Tolerance (PBFT) consensus within the healthcare context. The integration of self-sovereign identity gives patients exclusive ownership over their medical credentials and histories, eliminating reliance on external third parties. The design of the smart contract allows patients to manage their own consent, giving them more control over who has access to their healthcare information. This allows for more detailed access control for healthcare providers. Use of PBFT consensus for identity verification ensures multi-party agreement on the validity of transactions, enhancing security and accuracy.

Previous solution of digital identity management system was limited, and they did not explore smart contract-based consent management. They also did not examine PBFT consensus for digital identity management scenarios. This solution presents a comprehensive architecture that covers identity ownership, access controls, and consensus mechanisms customised for the NHS. The network is decentralised yet permissioned, which gives patients more control, and builds trust between them and verified providers. This solution differentiates itself from other medical data storage options by using a layered security model and a patient-centric approach. These measures help address the risks associated with centralised data storage.

7. CONCLUSION

In conclusion, the blockchain-based solution offered a robust architecture to secure the digital identity management in the NHS systems. The integrated solution mitigates the vulnerability of centralised databases by using decentralisation, cryptographic techniques, SSI, PBFT consensus and smart contract logic to provide multilayered protection while enabling patient control over consent. The system offers multilayered protection against cyber threats and gives patients control over their medical records and consent. This can be achieved through a unique combination of SSI, which ensures complete control of medical credentials, smart contracts that enable detailed access controls, and PBFT consensus, which provides a secure and accurate transaction validation process. This solution is different from other approaches as it provides a decentralised yet permissioned network, building trust between patients and verified NHS providers. This architecture mitigates the risks associated with centralised data storage and sets a new standard for secure and patient-centred digital identity management in healthcare.

8. REFERENCES

1. Ahmed, R., Islam, A. K. M. M., Shatabda, S., & Islam, S. (2022). Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey | IEEE Journals & Magazine | IEEE Xplore. Ieeexplore.ieee.org. https://ieeexplore.ieee.org/document/9927415
2. Aydar, M., Serkan, & Salih, A. (2020). Towards a Blockchain based digital identity verification, record attestation and record sharing system. https://arxiv.org/pdf/1906.09791.pdf
3. Houtan, B., Hafid, A. S., & Makrakis, D. (2020). A Survey on Blockchain-Based Self-Sovereign Patient Identity in Healthcare. IEEE Access, 8, 90478–90494. https://doi.org/10.1109/access.2020.2994090
4. Li, J., Hu, K., Jian, Z., Jean-Paul Bodeveix, & Ye, Y. (2022). Formal Modelling of PBFT Consensus Algorithm in Event-B. Wireless Communications and Mobile Computing, 2022, 1–17. https://doi.org/10.1155/2022/4467917
5. Rouhani, S., & Deters, R. (2019). Security, Performance, and Applications of Smart Contracts: A Systematic Survey. IEEE Access, 7, 50759–50779. https://doi.org/10.1109/access.2019.2911031
6. Saragih, T. K., Tanuwijaya, E., & Wang, G. (2022). The Use of Blockchain for Digital Identity Management in Healthcare | IEEE Conference Publication | IEEE Xplore. Ieeexplore.ieee.org. https://ieeexplore.ieee.org/document/9935935
7. Simanta Shekhar Sarmah. (2018). Understanding Blockchain Technology. Computer Science and Engineering, 8(2), 23–29. http://article.sapub.org/10.5923.j.computer.20180802.02.html
8. Singla, A., Gupta, N., Aeron, P., Jain, A., Sharma, D., & Bharadwaj, S. S. (2022). Decentralized Identity Management Using Blockchain. Journal of Global Information Management, 31(2), 1–24. https://doi.org/10.4018/jgim.315283
9. Song, Z., & Yu, Y. (2022). The Digital Identity Management System Model Based on Blockchain | IEEE Conference Publication | IEEE Xplore. Ieeexplore.ieee.org. https://ieeexplore.ieee.org/document/9845097
10. T, M., Makkithaya, K., & V G, N. (2022). A Blockchain Based Decentralized Identifiers for Entity Authentication in Electronic Health Records. Cogent Engineering, 9(1). https://doi.org/10.1080/23311916.2022.2035134
11. Thimbleby, H. (2018). Misunderstanding IT: Hospital cybersecurity and IT problems reach the courts. Digital Evidence and Electronic Signature Law Review, 15(0). https://doi.org/10.14296/deeslr.v15i0.4891
12. Ujjawal, A. (2018, August 14). How Does the Blockchain Work? GeeksforGeeks. https://www.geeksforgeeks.org/how-does-the-blockchain-work/
13. Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. National Institute of Standards and Technology, 1(1). https://doi.org/10.6028/nist.ir.8202

14. Zhao, W., Yang, N., Li, G., & Zhang, K. (2021). Research on Digital Identity Technology and Application Based on Identification Code and Trusted Account Blockchain fusion | IEEE Conference Publication | IEEE Xplore. Ieeexplore.ieee.org. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9724732

9. APPENDIX A

```
// SPDX-License-Identifier: MIT
    pragma solidity >=0.7.0 < 0.9.0;

    contract NHSDigitalIdentityConsent {
      struct Patient {
        bool isVerified;
        mapping(address => bool) nhsProviders;
        bytes32 ssiDid;
      }
      mapping(address => Patient) public patients;
      modifier onlyVerifiedPatient() {
        require(patients[msg.sender].isVerified, "Patient is not verified");
        _;
      }
      event IdentityVerification(address indexed patient, bool isVerified, bytes32 ssiDid);
      event ConsentGranted(address indexed patient, address indexed nhsProvider);
      event ConsentRevoked(address indexed patient, address indexed nhsProvider);

      function verifyPatient(bytes32 ssiDid) external {
        patients[msg.sender].isVerified = true;
        patients[msg.sender].ssiDid = ssiDid;
        emit IdentityVerification(msg.sender, true, ssiDid);
      }
      function grantConsent(address nhsProvider) external onlyVerifiedPatient {
        patients[msg.sender].nhsProviders[nhsProvider] = true;
        emit ConsentGranted(msg.sender, nhsProvider);
      }
      function revokeConsent(address nhsProvider) external onlyVerifiedPatient {
        patients[msg.sender].nhsProviders[nhsProvider] = false;
        emit ConsentRevoked(msg.sender, nhsProvider);
      }
      function implementPBFTConsensus() external {
      }
      function verifySignature(bytes32 message) internal view returns (address) {
        address signer = ecrecover(message, 0, 0, 0);
        require(signer != address(0), "Invalid signature");
        require(signer == msg.sender, "Signature does not match sender");
        return signer;
      }
    }
```