

Automated Medical Document Verification on Cloud Computing Platform: Blockchain-Based Soulbound Tokens

Ashish Khanna , Yogesh Sharma , Devansh Singh , Ria Monga , Tarun Kumar 

Department of Computer Science and Engineering, Maharaja Agrasen Institute of Technology, Delhi, India

Corresponding author: Tarun Kumar (tarunkumar.sbb@gmail.com)

Abstract

Medical document verification is a critical and expensive process that often relies on centralized databases. However, manual verification of such documents is time-consuming and lacks credibility. Deep learning and blockchain technology can be employed to address this issue by reducing fraud and increasing efficiency. The use of non-transferable soulbound tokens (SBTs) can provide a secure and tamper-proof system for verifying medical records. The authors have proposed an algorithm for automated document verification and authenticity using blockchain-based SBTs. The system uses cloud computing to access the decentralized database, reducing the time taken to verify each document to 2-3 minutes in comparison to the related non-automated techniques discussed in the literature review. The aim of this research paper is to provide a secure and tamper-proof system for verifying medical records, such as prescriptions and test results, on the cloud using decentralized databases and blockchain technology. The use of deep learning algorithms can be used to determine the best way to allocate resources in a decentralized network or to minimize the costs of a blockchain platform. The adoption of blockchain technology can reduce fraud and improve efficiency. The proposed system can significantly improve the efficiency and credibility of medical document verification, reduce fraud, and ensure tamper-proof authenticity. The use of SBTs and cloud computing can simplify the process and provide easy access to decentralized databases. Future research can explore the scalability of the proposed system and its potential application in other sectors.

Keywords

Blockchain; Soulbound token; Cloud computing; Medical document verification; Deep learning.

Citation: Khanna, A., Sharma, Y., Singh, D., Monga, R., & Kumar, T. (2023). Automated Medical Document Verification on Cloud Computing Platform: Blockchain-Based Soulbound Tokens. *Acta Informatica Pragensia*, 12(2), 342–356. <https://doi.org/10.18267/j.aip.218>

Academic Editor: Zdenek Smutny, Prague University of Economics and Business, Czech Republic

Copyright: © 2023 by the author(s). Licensee Prague University of Economics and Business, Czech Republic.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution License (CC BY 4.0).

1 Introduction

Several traditional methods are available for medical document verification; however, one of the major problems in the Web2 industry is identifying modified fraudulent documents. The need of the hour is the latest automated technologies. The Web3 industry is experiencing a significant compound annual growth rate of 43.7%, with the potential for even further expansion as governments begin to adopt and integrate emerging technologies into sectors such as finance and governance (Emergen Research, 2022). Blockchain can be used to store the state and actions of a deep learning system. This can enable the creation of decentralized reinforcement learning algorithms, where multiple agents can learn and make decisions together. Smart healthcare technologies aim to offer a range of features and services that make it easier for clients to access accurate, real-time healthcare services in a convenient and seamless manner. However, it is important to ensure that these services are also secure and cautious in handling sensitive health information. With the promising future of Web3, blockchain can act as a potent solution to the proposed problem. Some features of blockchain technology are immutability, trustless contracts and decentralized nature. Blockchain offers cryptographic assets called non-fungible tokens (NFTs), which are unique and transferrable. NFTs can be used to prove ownership of assets such as collectibles and digital art. Soulbound tokens (SBTs), which are an extension of NFTs, are designed to be non-transferable and tied to a specific individual or entity. Like other NFTs, SBTs are stored in a digital wallet or account, can be publicly visible and authenticated on a blockchain. They can be created and managed using smart contracts on a blockchain platform such as Ethereum. SBTs do not hold any monetary value. They can be used to represent affiliations, credentials, commitments or other personal attributes or characteristics of the wallet holder (Weyl et al., 2022).

Souls can identify themselves via their native Web3 identities using SBTs issued by institutions such as hospitals, businesses and governments. This enables third parties to verify this information quickly and easily without the need for intervention from the issuer.

A system is explored where medical prescriptions/reports or any other verifiable document are issued by any institute/hospital/government in the form of a unique soulbound token. Since soulbound tokens are non-transferable, they can be used to determine the authenticity of the medical history or record of any individual, since the SBTs are issued on the blockchain.

The above-mentioned soulbound token technology is implemented by Binance. In September 2022, Binance started issuing account-bound tokens on the Binance chain to their users. Binance account-bound (BAB) tokens (BNB Chain, 2022) are the first-ever soulbound token (SBT) built on the BNB chain. It will function as a digital verification tool for Binance users who have completed identity verification. Binance users who have completed identity verification can mint their BAB directly in their wallets.

SBTs can form the social graph of a user through a combination of public and private information. This information is in the form of SBT properties. Some of the properties can be publicly visible while others can be private (encrypted), and can only be accessible to users with explicit permissions. This allows the SBT issuer to control the information that they want to share through SBTs.

1.1 Application

An application of soulbound tokens in medical document verification in blockchain technology is to create a secure system for storing and verifying patient records and medical documents. People may use forged medical documents for various reasons, such as obtaining medical treatment or medication without a valid prescription or insurance coverage, claiming disability benefits or time off work, avoiding military service or other mandatory service, gaining admission to a school or programme with special accommodation, or defrauding insurance companies by claiming to have received certain treatment or medications (Grolleau et al., 2008, pp. 673-693). In this system, each patient would be assigned a unique soulbound token that

would be linked to their medical records and documents. This token would be stored on the blockchain. This system could allow healthcare providers to access and verify patient records in real time, improving the accuracy and efficiency of healthcare delivery.

A potential solution based on blockchain technology using SBTs has been explored: a platform where documents can be verified easily. This verification would need fewer resources than the currently available means and it would be faster and more reliable since the power of blockchain has been exploited to achieve the immutability of documents.

1.2 Roadblocks in existing methods

There are several potential problems with existing methods of document verification. Some common issues include the potential for fake or forged documents, the difficulty of verifying the authenticity of certain types of documents, and the time and resources that may be required to properly verify a record. Additionally, some verification methods may not be effective at detecting all forms of fraud or forgery, which can leave organizations and individuals vulnerable to scams or other types of deception. Many existing methods of document verification are time-consuming, unreliable and labour-intensive, which can make the process slow and expensive.

Highlights of the proposed work:

- Explores the use of soulbound tokens in medical document verification.
- Explores a system to make the verification of medical records automatic, secure and time-efficient.
- Explores the use of cloud computing for easy access to a decentralized database and efficient verification of medical documents.
- Proposes a soulbound token algorithm *Docu_Verification_using_SBT* for medical document verification.

2 Literature Review

This section discusses the potential of blockchain technology and deep learning in healthcare, as well as the use of blockchain for digital document verification. The review highlights the advantages of blockchain technology, including decentralization, data sharing and security, and its potential applications in various domains, such as healthcare, smart government, e-government and business. The review also discusses the challenges associated with traditional methods of record-keeping and the potential of blockchain technology to address these challenges. The use of blockchain technology in healthcare is explored, including its potential to improve data integrity, medical image classification and disease prediction, as well as to prevent counterfeiting of drugs in the supply chain management process.

The review also introduces the concept of soulbound tokens, which are unique digital tokens that are tied to a specific individual and can be used to verify their identity or ownership of a particular asset. The use of soulbound tokens in verifying digital documents is discussed as an alternative to centralized systems. Overall, the literature review provides a solid foundation for the research paper and highlights the potential of blockchain technology and deep learning in improving the accuracy, security and efficiency of medical document verification.

Blockchain technology aims to create a decentralized environment where third-party control is not necessary (Yli-Huumo et al., 2016). It has been introduced in various domains due to its advantages, such as the healthcare industry (Roehrs et al., 2017, pp. 70-81), smart government (Arendsen et al., 2011), e-government (Hou, 2017, pp. 1-4) and business (Sidhu, 2017, pp. 1-6).

Deep learning, which is a type of artificial intelligence that is based on artificial neural networks, has the ability to learn from data and has been applied in a variety of fields including healthcare, visual

recognition, text analytics and cybersecurity (Sarker, 2021, pp. 1-20). The convergence of machine learning and blockchain technology can lead to highly accurate and secure results. Machine learning requires sufficient data and the reliability of these data is crucial for accuracy. Blockchain technology, with its decentralized database and emphasis on data sharing, can enhance the accuracy of machine learning while also ensuring the security and legitimacy of the data through consensus (Vyas et al., 2019). Mani et al. (2022, pp. 1-15) proposed a framework that exploits cloud-based blockchain technology to address the need for traceability, data storage and data privacy in the pharmaceutical industry. This system helps identify fake or illegally imported products by tracking the manufacturer and country of origin. Li et al. (2021, pp. 1-34) has conducted research on the use of blockchain technology to address trust and security issues in the context of cloud computing systems. The survey focuses on the use of blockchain to create a decentralized and distributed trust architecture in order to improve the traceability and integrity of transactions in the cloud.

Several challenges associated with traditional methods of record-keeping, including the need for large physical storage spaces and the difficulties that can arise in trying to retrieve records have been identified. The availability of these medical records is currently restricted. Requests for medical records by patients or authorized attendants should be acknowledged and documents should be issued within 72 hours (Thomas, 2009, pp. 384-388).

Jamil et al. (2019) presented research on the use of blockchain technology to prevent counterfeiting of drugs in the supply chain management process. This innovative application of blockchain has the potential to improve the safety and effectiveness of the drug supply chain by providing a secure and transparent record of the movement and handling of drugs from manufacturer to patient. A study on the potential uses of machine learning and blockchain in the healthcare industry by conducting a survey of 150 medical professionals with expertise in these areas was carried out by Umamaheswaran et al. (2022). The study revealed data integrity in blockchain and improved accuracy in medical image classification and disease prediction. BinDaaS (Bhattacharya et al., 2019, pp. 1242-1255) is a system that utilizes blockchain technology and deep learning techniques to share electronic health records (EHR) among multiple healthcare providers. It operates in two phases: first, an authentication and signature scheme based on lattice cryptography is implemented to prevent collusion among $N-1$ healthcare authorities from a group of N . In the second phase, deep learning as a service is applied to stored EHR datasets to predict future diseases based on current patient indicators and features. Blockchain technology can be used to improve healthcare systems by using frameworks and tools to measure performance, implementing an access control policy algorithm for data accessibility, and optimizing performance metrics such as latency and throughput (Tanwar et al., 2020). Luo and Choi (2021, pp. 1-26) investigated how deep learning and blockchain together can help improve business operations. Akter et al. (2020, pp. 1-33) explored digital business transformation through emerging technology fields: artificial intelligence, blockchain, cloud and data analytics using a multidisciplinary approach.

Blockchain technology has been gaining increasing attention in recent years due to its potential to revolutionize various industries owing to its decentralized and secure nature. One area where blockchain has shown promise is in the field of digital document verification (Imam et al., 2021, pp. 1262-1267; Yumna et al., 2019, pp. 191-202). In this context, a digital document can be any type of electronic file that needs to be authenticated, such as contracts, certificates or identity documents. There are also more traditional methods that can be used to ensure the authenticity of a document, such as using watermarks, holograms and other physical security features. These methods can be effective in preventing counterfeiting and falsification, but they may not be as secure as digital methods and may be more difficult for the general public to verify.

Soulbound tokens are unique digital tokens that are tied to a specific individual and can be used to verify their identity or ownership of a particular asset. They are based on blockchain technology and are secured

through cryptographic techniques, making them resistant to counterfeiting and tampering. Weyl et al. (2022) discussed that soulbound tokens that represent education credentials, work history and rental contracts could serve as a persistent record of credit-relevant history, allowing souls to stake meaningful reputations.

Traditionally, the verification of digital documents has relied on centralized systems, such as banks or government agencies, to act as trusted third parties. However, these centralized systems can be vulnerable to fraud and tampering, and they often require significant time and resources to verify documents.

One approach is to use a public blockchain, where anyone can participate in the network and verify the authenticity of the soulbound tokens. This approach has the advantage of being more decentralized and transparent, as it allows anyone to verify the authenticity of digital documents. However, it also has the potential to be less secure, as it relies on the security of the entire network rather than a smaller, more controlled group of entities.

One of the earliest efforts in this area was the work by Nakamoto (2008) on bitcoin, which introduced the concept of a decentralized digital currency using blockchain technology. The bitcoin system uses a distributed ledger to record and verify transactions, ensuring integrity and security of recorded data. Other notable examples include the work by Liu and Wang (2017) on blockchain-based electronic voting systems and the work by Dursan et al. (2022, pp. 203-217) on the use of blockchain in supply chain management. Both these efforts highlight the potential of blockchain technology to securely store and verify electronic data, ensuring authenticity and integrity of recorded information.

Satybaldy et al. (2022) demonstrated the use of self-sovereign identity (SSI) to create tamper-proof verifiable credentials in online loan processing. Sun et al. (2022) explored a know-your-customer (KYC) identity scheme using Merkle trees and smart contracts.

Several attempts have been made to establish a decentralized society based on soulbound tokens. For example, Prabhakar and Jain (2022), in their whitepaper on the DeSoc governance protocol, illustrated how soulbound tokens representing commitments, affiliations and credentials can encode trust in the real economy to establish provenance and reputation. They presented a multi-chain application that enables a decentralized network environment to solve key issues of identity security, data integrity, inclusive governance and asset recovery. They aim to provide under-collateralized lending where people will be able to take loans under their on-chain identity while establishing trustworthy behaviour.

Non-fungible token marketplaces (NFTM) currently determine the NFT ecosystem but they pose security issues. Das et al. (2021) presented NFTM Dapp platforms, where NFTs are traded. The methodology poses a lot of security risks. They discussed how the NFTs listed on various platforms such as OpenSea and Rarible may or may not be verified. While listing an NFT, the NFTM takes control of the token so that when a sale is executed, it can transfer the ownership of the NFT from the seller to the buyer. To this end, the NFTM needs to be either the owner of the NFT, a controller, or an operator.

The escrow model in this case is risky because one single escrow contract/wallet managed by the NFTM holds all assets being traded on the platform. Therefore, the security of all assets in a marketplace depends on the security of the escrow contract or the external account that manages such a contract (Das et al., 2021).

The existing technologies for establishing a digital identity – decentralized identifiers (DIDs) and verifiable credentials (VCs) – are currently insufficiently standardized, leaving room for vulnerabilities such as the exposure of user information and composability issues. This leaves users vulnerable to negative reputation and immutable "scarlet letter" effects. In contrast, SBTs are yet to be defined and have the potential to offer stronger security and immunity to these challenges (Jain et al., 2022).

The University of Nicosia (UNIC, 2018) utilizes a program that generates and stores certificates on the bitcoin platform. Furthermore, the UNIC accepts bitcoin as a method of payment for degree programmes. However, this approach can be costly for platform users as it requires the storage of large data and documents such as diplomas, certificates and transcripts.

To overcome the above shortcomings in the available NFT methodology, the presented paper explores SBTs. Overall, the use of soulbound tokens (Weyl et al., 2022) for digital document verification has the potential to enhance the security and verifiability of digital documents and has been an active area of research in recent years.

3 Proposed Methodology

The methodology proposed is conceptual and built upon the previous studies by examining the use of soulbound tokens in the context of Web3, where they can be used to represent digital assets that are native to the decentralized web. Here, a system for creating medical digital documents in the form of soulbound tokens and managing these tokens using Web3 technologies is explored and the potential benefits of using this approach in practice are discussed. We have developed and proposed an algorithm under the title of *Docu_Verification_using_SBT* to automate the verification of medical history using available blockchain technology.

3.1 Sample fields of an SBT

Table 1. Sample SBT fields.

SBT title	Medical examination
SBT type	Report
Issuer name	Maharaja Agrasen Hospital
Issuer type	Hospital
Issuer wallet address	0x269a92881693e64f55468760A3B1C696CD3d1ea3
Receiver name	Santosh Deewan
Receiver wallet address	0x122aBA6957Fe4F5c997De23CFBb980F71b3E6B0C
Issuing date	12/02/2023
Patient ID	10014802719
Entitlement	Report Generated
Token smart contract address	0x3E2B3fab95a1bDfB72316c31471Ce9c70230693A
Claim date	14/02/2023

3.2 Working of Docu_Verification_using_SBT

Automated medical document verification is one of the cumbersome problems of the present world. A system is proposed to overcome this. In the presented methodology, the hospital is first verified and

registered on the platform to access the services using soulbound tokens. After successful verification and registration, the SBT-enabled hospital can proceed further to deploy its smart contract and can start issuing prescriptions/reports in the form of SBTs. As hospital-issued documents are SBT-enabled, they are non-transferable. Furthermore, patients can prepare their medical records on the basis of SBT-enabled documents, which are self-verifiable on the SBT-enabled blockchain.

3.3 Pseudo code for medical document verification on blockchain using soulbound tokens

Begin:

Step 1 – SBT_Enabled_Hospital

1. Initialize the blockchain and create a new soulbound token contract.
2. Verify the hospitals that are allowed to issue SBTs.
3. Set up a user interface for uploading and verifying documents.

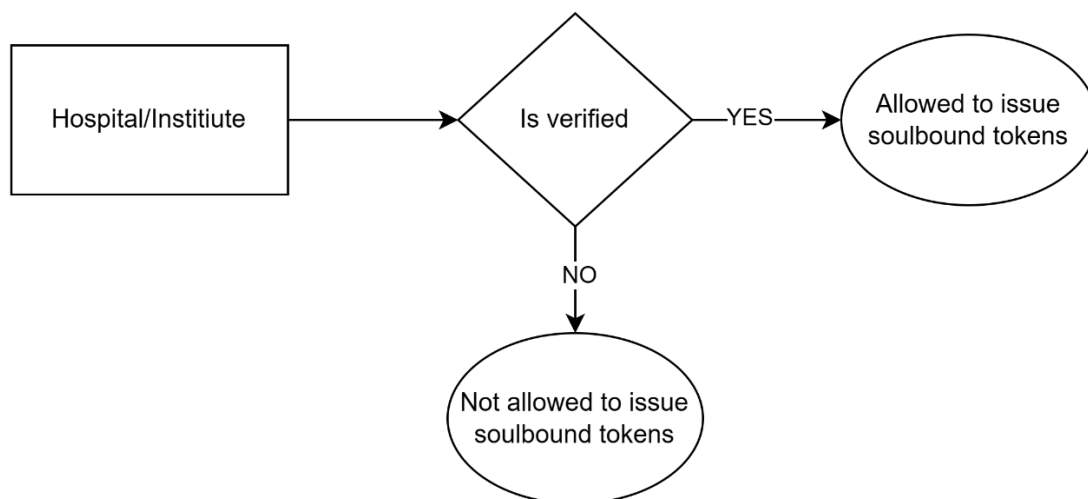


Figure 1. Verification of institutions allowed to mint SBTs.

The hospitals/institutions that want to issue soulbound tokens (SBTs) are first verified. Only verified hospitals are allowed to issue SBTs. Any hospital is able to issue SBTs to its patients using its smart contract, which is made available only to verified hospitals.

Step 2 – SBT_Enabled_Document

Part A: Document uploading process:

Input: Digital document

Output: Soulbound token

Process:

1. The hospital uploads the document to the interface.
2. The document is hashed and stored on the blockchain as a soulbound token.
3. The soulbound token is linked to the user's identity.

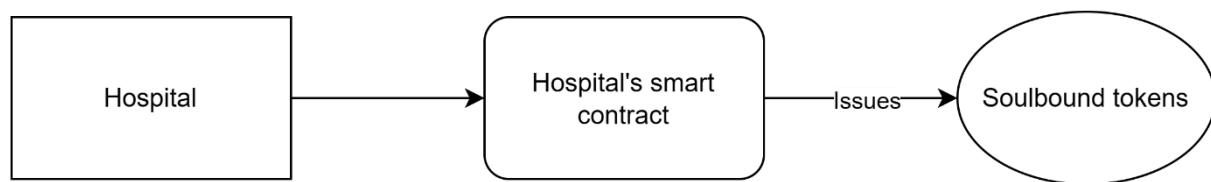


Figure 2. Hospital issuing SBTs.

The verified hospitals and institutions are allowed to issue new SBTs to their patients. These SBTs contain the URL where the document (in the form of a prescription/report) is hosted on a decentralized network.

Part B: Formation of the digital medical record:

Input: Soulbound tokens

Output: Hash of the soulbound tokens

Process:

1. The address of the user is accessed, requesting the formation of a medical record.
2. The ownership of soulbound tokens is verified for the user.
3. After the verification process, a hash of the soulbound tokens is generated using the SHA-256 algorithm (IPFS; Benet, 2014).

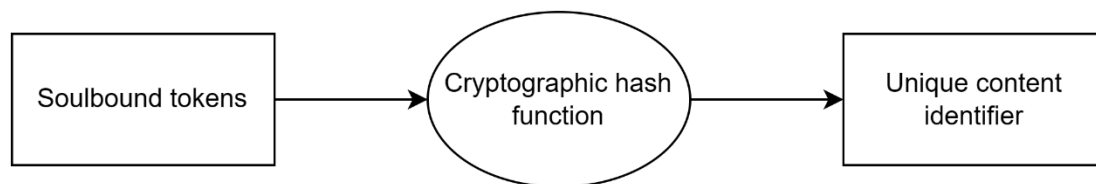


Figure 3. Generation of a hash of soulbound tokens on IPFS.

A collection of the SBTs issued to patients can be treated as a digital medical record by hashing all the SBTs and the owner of the SBTs. A cryptographic hash of listed SBTs is generated using IPFS. The IPFS link generated contains a JSON file of soulbound tokens, which can be efficiently verified by the doctor on the platform.

Step 3 - SBT_Enabled_Document_Verification

Input: Digital medical record link

Output: Document verified/not verified

Process:

1. The user presents the medical record and their identity to the verification system.
2. The system retrieves the soulbound tokens associated with the presented record.
3. The system checks the link between the soulbound token and the user's identity.
4. If the link is valid, the document is verified and the verification is recorded on the blockchain.
5. If the link is invalid, the verification request is rejected.

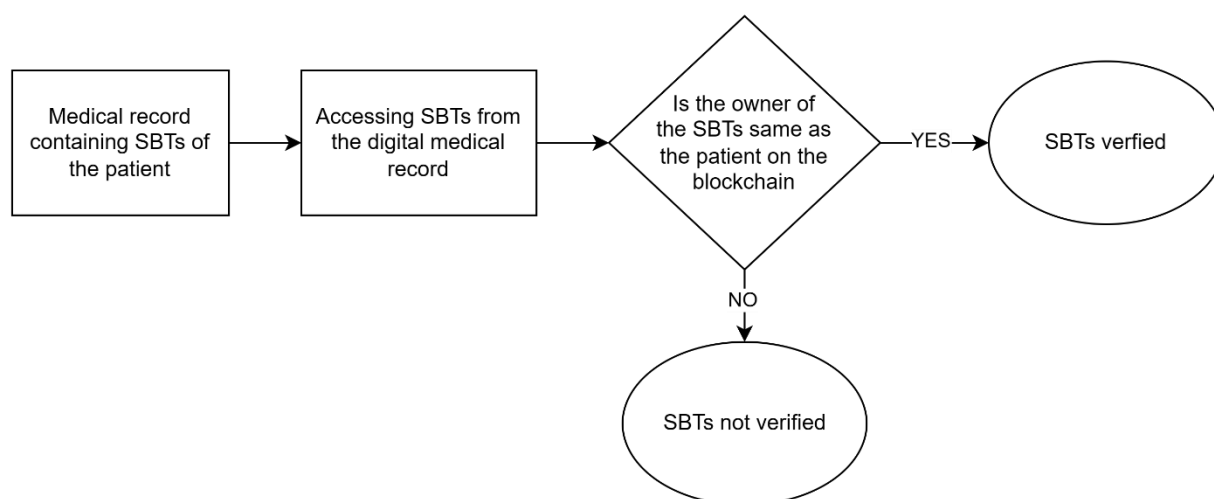


Figure 4. Verification of medical record using SBTs.

To verify a digital medical record, the SBTs contained in the medical record has an owner that can be read from the blockchain using the hospital's smart contract address and token ID. After accessing the SBT owner, it is checked whether the address of the patient is the same as the owner of the SBT. If the owner is the same, the SBTs are verified.

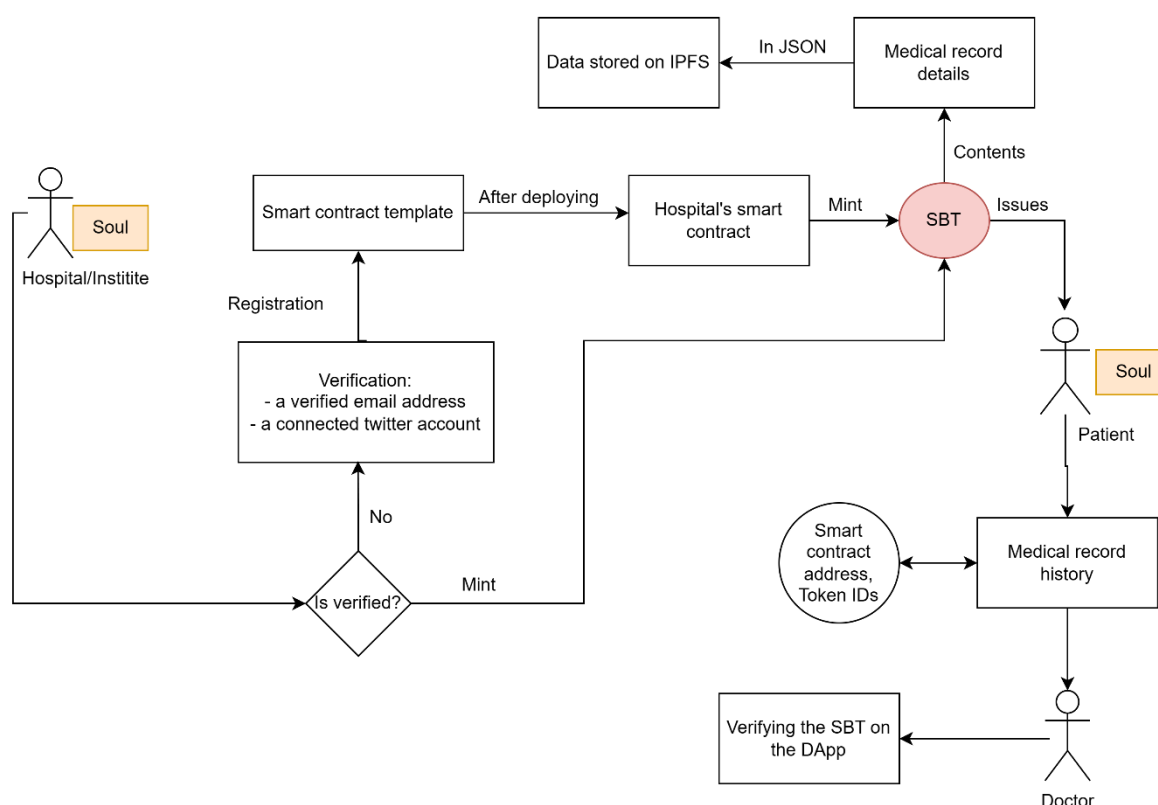


Figure 5. Flow chart of Docu_Verification_using_SBT.

3.4 Complete algorithm: Docu_Verification_using_SBT

1. To register and verify an institute/hospital, *SBT_Enabled_Hospital* is called for verification of the hospital.

$$H + SB_i \rightarrow H\#$$

- i) $H \Rightarrow$ Hospital
- ii) $SB_i \Rightarrow$ Hospital ID
- iii) $H\# \Rightarrow$ Hospital's smart contract

2. After successful verification, hospitals are allowed to issue new prescriptions/reports in the form of SBTs to their patients by calling *SBT_Enabled_Document*.

$$H\# \rightarrow SBT(i,j)$$

- i) $SBT \Rightarrow$ Soulbound token
- ii) $i \Rightarrow$ Verified hospital
- iii) $j \Rightarrow$ Token ID

3. Each patient can generate their digital medical record by cryptographic hash of their soulbound tokens, which are stored on IPFS.

$$SBT(i,j) \times n \rightarrow Docu$$

- i) $n \Rightarrow$ Number of SBTs
- ii) $Docu \Rightarrow$ Medical document on IPFS

4. To verify any SBT-enabled document, *SBT_Enabled_Document_Verification* can be called by passing in the medical record link which will automatically verify the SBTs issued to that patient.

$$Docu \rightarrow Owner(SBT(i,j)) = Address(Patient) ? \rightarrow Verified$$

- i) $Owner(SBT) \Rightarrow$ Owner of the SBTs in digital medical document
- ii) $Address(Patient) \Rightarrow$ Wallet address of the patient

3.5 Data protection against unauthorized users

There are several ways to protect the patient's data against unauthorized access when using IPFS for decentralized storage:

1. **Encryption:** Before storing the patient's data on IPFS, it can be encrypted using a strong encryption algorithm. This would make the data unreadable to anyone who does not have the decryption key, which would only be provided to authorized individuals.
2. **Access control:** The IPFS nodes that store the patient's data can be configured to only allow access to authorized individuals. This can be achieved through the use of access control lists (ACLs) or other similar mechanisms.
3. **Decentralized identity:** A decentralized identity system such as a blockchain-based identity management system can be used to verify the identity of individuals who are authorized to access

the patient's data. This would ensure that only authorized individuals can access the data, even if they are stored in a decentralized network.

4. **Secure data sharing:** If the patient's data need to be shared with other healthcare providers or researchers, secure data sharing mechanisms such as secure data rooms or secure data sharing platforms can be used. These platforms would ensure that only authorized individuals have access to the data and that the data are encrypted and protected during transit and storage.

4 Performance Analysis

The process of evaluating the effectiveness and efficiency of the proposed algorithm is explored. The proposed system is examined and it is determined how it differs from the available manual methodologies, i.e., total man hours spent verifying. The various measuring metrics involved are time taken to verify, expenditure, authentication, security or automation, to determine the overall performance of the proposed system.

4.1 Time

The time taken to verify a medical document can vary greatly depending on several factors, including the complexity of the document, the availability of the necessary information and records, and the workload of the verifying party. In general, it may take anywhere from a few days to several weeks to fully verify a medical document.

Reading data that SBT holds from a blockchain is relatively quick, other operations such as writing data or making transactions can take longer, depending on the specific blockchain, the speed of the network and the complexity of the operation.

The average time taken to add a block to Polygon takes approximately 2.2 seconds (Polygon, 2022).

4.2 Authentication and security

Some of the factors that outweigh the necessity of having medical documents in the form of SBTs are:

1. **Immutability:** Once data have been recorded on a blockchain, they cannot be altered or deleted. This makes it difficult for anyone to tamper with the data and forge fake documents or records.
2. **Decentralization:** Blockchains are decentralized and distributed across multiple computers or nodes, which makes it difficult for a single entity to control the data or alter them without the consensus of the network.
3. **Cryptographic hashing:** Blockchains use cryptographic hashing to secure the data stored on them. Cryptographic hashing involves taking a piece of data and running it through a mathematical algorithm, which produces a unique "hash" that represents the data. This hash can be used to verify the authenticity of the data without revealing their actual content.
4. **Consensus algorithms:** Most blockchains use consensus algorithms to ensure that the data recorded on the blockchain are accurate and valid. These algorithms require multiple nodes on the network to reach a consensus about the validity of a transaction before it is added to the blockchain.

Overall, the combination of these features makes it difficult for anyone to forge or alter data on a blockchain, which helps enhance the security and reliability of the authentication process.

4.3 Automation

The verification of medical records such as prescriptions, reports and any other documents is a time-consuming process and is currently not automated. To verify a specific document of a patient, first the patient is verified using the assigned identification number, medical record number, social security number, etc. With the help of soulbound tokens, a patient holding the soulbound tokens can create a hash

of the soulbound tokens. This hash contains all the data about the patient's prescriptions and medical reports. When this hash is made available to the hospital/institute, the organization is able to know the medical history of the patient with this single hash that contains data about all the patient's soulbound tokens. This hash of the soulbound tokens may be treated as a digital medical record, which can automatically be verified with the help of the blockchain.

5 Results and Analysis

In the context of document verification, soulbound tokens can potentially be used to provide a tamper-proof record of the authenticity of a document. This would provide a secure and immutable record of the issuance of the document, which could be verified by anyone with access to the blockchain.

There are several potential implications of using soulbound tokens for medical document verification:

1. **Increased authentication:** Soulbound tokens provide a secure and tamper-proof record of the authenticity of a document, which can help reduce the risk of fraud and counterfeiting.
2. **Improved efficiency:** By using soulbound tokens, hospitals can streamline their document verification processes, as the authenticity of a document can be easily and quickly verified using the blockchain.
3. **Greater transparency:** Soulbound tokens allow anyone with access to the blockchain to verify the authenticity of a document, which can increase transparency and trust in the document verification process.
4. **Enhanced interoperability:** Soulbound tokens can be used to create a standard for medical record verification that is interoperable across different organizations and systems, which can facilitate exchange and use of digital documents.

6 Discussion

The use of soulbound tokens for medical document verification has several benefits over traditional methods. Firstly, it provides a higher level of security and immutability, as the record is stored on a decentralized blockchain that is resistant to tampering or hacking. Secondly, it can be easily and quickly verified by anyone with access to the blockchain in an automated manner without any human intervention, making the verification process faster and more efficient. Finally, it reduces the need for intermediaries, such as notaries or document verification services, which can lower the costs and time required for document verification. This is in line with Yli-Huumo et al. (2016).

There are also some challenges that need to be addressed when using soulbound tokens for medical document verification. For example, it would require the document to be converted into a digital format that can be represented by a soulbound token. While the use of blockchain technology can eliminate the need for intermediaries in document verification, the results of Grolleau et al. (2008, pp. 673-693) suggest that there would need to be a trusted issuer of the document.

Currently, there is no standard available for soulbound tokens to be implemented because the concept of soulbinding is still relatively new and there is no widely accepted set of protocols or standards for implementing this feature. Also, technology is changing rapidly, so solutions involving soulbound tokens may become outdated. Additionally, there are many different types of blockchain applications, each with its own unique requirements and specifications for soulbound tokens. Despite the lack of a standardized approach, many developers are working on creating their own implementations of soulbound tokens. For example, eq8 network (Prabhakar & Jain, 2022) uses SBTs, aiming to create a network that solves key issues of identity security, data integrity and inclusive governance. Some are using existing blockchain platforms and protocols, such as Ethereum and ERC-721, to create custom soulbound tokens that meet their specific

needs. Others are creating entirely new blockchain platforms and protocols specifically designed for soulbound tokens.

In comparison with other solutions discussed in the literature review, the proposed solution is unique in its use of SBTs to ensure the authenticity of medical records. While other solutions, such as BinDaaS (Bhattacharya et al., 2019), also utilize blockchain technology to share electronic health records among multiple healthcare providers, the proposed solution focuses specifically on ensuring the authenticity of medical records through the use of SBTs. Additionally, the proposed solution has the advantage of being a decentralized and secure method for medical document verification, which can improve the safety and effectiveness of the healthcare industry. However, it is also important to consider potential disadvantages of the proposed solution, such as the need for hospitals and institutions to be verified before issuing SBTs, which may cause delays in the issuance of medical records.

Compared to other blockchain-based solutions presented in the literature review, the proposed solution using SBTs offers several unique advantages. For example, Jamil et al. (2019) presented a solution for preventing counterfeiting of drugs in the supply chain management process using blockchain technology. Although the solution they discussed has the potential to improve the safety and effectiveness of the drug supply chain, it is not directly applicable to the verification of digital medical records. In contrast, the solution presented in the paper is verifiable. Tanwar et al. (2020) proposed a solution for using blockchain technology to improve healthcare systems by implementing an access control policy algorithm for data accessibility and optimizing performance metrics. Their solution addresses some of the challenges faced by healthcare systems, but it does not specifically address the problem of verifying digital medical records.

Overall, while there are some challenges to using soulbound tokens, their potential benefits in terms of security, immutability and efficiency make them a promising technology for this use case. With continued development and adoption of blockchain technology, we may see increased use of soulbound tokens for document verification in the future.

7 Conclusion and Future Scope

In conclusion, the use of blockchain-based soulbound tokens and deep learning for medical document verification has the potential to revolutionize the way healthcare records are managed and accessed. The use of blockchain technology ensures that the records are secure and cannot be altered, while in future, the use of deep learning algorithms will allow accurate and efficient verification of authenticity of documents.

There are several areas where this technology can be further developed and applied in the future. One potential application is in the area of telemedicine, where medical professionals can remotely access and verify patient records without the need for physical documents. Another possibility is in the realm of medical tourism, where individuals can easily verify the authenticity of their medical records before seeking treatment abroad.

Overall, the use of blockchain-based soulbound tokens and potentially deep learning for medical document verification has the potential to greatly improve the efficiency and security of healthcare record management. It is a technology that should be further explored and implemented in the future.

Additional Information and Declarations

Conflict of Interests: The authors declare no conflict of interest.

Author Contributions: A.K.: Project Administration, Conceptualization, Supervision, Writing – Reviewing and Editing. Y.S.: Conceptualization, Supervision, Formal Analysis, Writing – Reviewing and Editing. D.S.: Methodology, Writing – Original draft preparation,


Investigation, Writing – Reviewing and Editing. R.M.: Data curation, Writing – Reviewing and Editing, Investigation. T.K.: Data curation, Writing – Reviewing and Editing, Investigation.

Data Availability: The data that support the findings of this study are available from the corresponding author.

References

- Akter, S., Michael, K., Uddin, M. R., McCarthy, G., & Rahman, M. (2020). Transforming business using digital innovations: the application of AI, blockchain, cloud and data analytics. *Annals of Operations Research*, 308(1–2), 7–39. <https://doi.org/10.1007/s10479-020-03620-w>
- Arendsen, R., Ter Hedde, M., & Hermesen, H. (2011). Exploring the future of public-private e-government service delivery. In *International Conference on Electronic Government* (pp. 441–452). Springer. https://doi.org/10.1007/978-3-642-22878-0_37
- Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. *arXiv preprint arXiv:1407.3561*. <https://doi.org/10.48550/arXiv.1407.3561>
- Bhattacharya, P., Tanwar, S., Bodkhe, U., Tyagi, S., & Kumar, N. (2019). Bindaas: Blockchain-based deep-learning as-a-service in healthcare 4.0 applications. *IEEE Transactions on Network Science and Engineering*, 8(2), 1242–1255. <https://doi.org/10.1109/TNSE.2019.2961932>
- BNB Chain. (2022, September 8). Binance Account Bound (BAB) Token Holders set for Exclusive Use Cases Across BNB Chain Ecosystem. <https://www.bnbchain.org/id/blog/binance-account-bound-bab-token-holders-set-for-exclusive-usecases-across-bnb-chain-ecosystem/>
- Das, D., Bose, P., Ruaro, N., Kruegel, C., & Vigna, G. (2021). Understanding security Issues in the NFT Ecosystem. *arXiv preprint arXiv:2111.08893*. <https://doi.org/10.48550/arXiv.2111.08893>
- Dursun, T., Birinci, F., Alptekin, B., Sertkaya, I., Hasekioglu, O., Tunaboylu, B., & Zaim, S. (2022). Blockchain technology for supply chain management. In *Industrial Engineering in the Internet-of-Things World* (pp. 203–217). Springer. https://doi.org/10.1007/978-3-030-76724-2_16
- Emergen Research. (2022, May). Web3 Industry Share | Web 3.0 Market Forecast by 2030. <https://www.emergenresearch.com/industry-report/web-3-market>
- Grolleau, G., Lakhal, T., & Mzoughi, N. (2008). An introduction to the Economics of Fake Degrees. *Journal of Economic Issues*, 42(3), 673–693.
- Hou, H. (2017). The application of blockchain technology in E-government in China. In *2017 26th International Conference on Computer Communication and Networks (ICCCN)* (pp. 1–4). IEEE. <https://doi.org/10.1109/ICCCN.2017.8038519>
- Imam, I. T., Arafat, Y., Alam, K. S., & Shahriyar, S. A. (2021). DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents. In *2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV)* (pp. 1262–1267). IEEE. <https://doi.org/10.1109/ICICV50876.2021.9388428>
- IPFS. (2012, April 15). How IPFS works. IPFS Docs. <https://docs.ipfs.tech/concepts/how-ipfs-works/#content-addressing>
- Jain, S., Erichsen, L., & Weyl, G. (2022). A Plural Decentralized Identity Frontier: Abstraction v. Composability Tradeoffs in Web3. *arXiv preprint arXiv:2208.11443*. <https://doi.org/10.48550/arXiv.2208.11443>
- Jamil, F., Hang, L., Kim, K., & Kim, D. (2019). A novel medical blockchain model for drug supply chain integrity management in a smart hospital. *Electronics*, 8(5), 505. <https://doi.org/10.3390/electronics8050505>
- Li, W., Wu, J., Cao, J., Chen, N., Zhang, Q., & Buyya, R. (2021). Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. *Journal of Cloud Computing*, 10(1), Article no. 67. <https://doi.org/10.1186/s13677-021-00247-5>
- Liu, Y., & Wang, Q. (2017). An e-voting protocol based on blockchain. *Cryptology ePrint Archive*. <https://eprint.iacr.org/2017/1043.pdf>
- Luo, S., & Choi, T. (2021). Great partners: how deep learning and blockchain help improve business operations together. *Annals of Operations Research*, in press. <https://doi.org/10.1007/s10479-021-04101-4>
- Mani, V., Prakash, M., & Lai, W. (2022). Cloud-based blockchain technology to identify counterfeits. *Journal of Cloud Computing*, 11(1). <https://doi.org/10.1186/s13677-022-00341-2>
- Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. <https://bitcoin.org/bitcoin.pdf>
- Polygon. (2022, December 8). Polygon PoS Chain Average Block Time Chart. <https://polygonscan.com/chart/blocktime>
- Prabhakar, M., & Jain, N. (2022). The DeSoc Governance Protocol White Paper (v3.0). *EQ8 Network*. <https://www.eq8.network/>
- Roehrs, A., Da Costa, C. A., & Da Rosa Righi, R. (2017). OmniPHR: A distributed architecture model to integrate personal health records. *Journal of Biomedical Informatics*, 71, 70–81. <https://doi.org/10.1016/j.jbi.2017.05.012>
- Sarker, I. H. (2021). Deep Learning: a comprehensive overview on techniques, taxonomy, applications and research directions. *SN Computer Science*, 2(6). <https://doi.org/10.1007/s42979-021-00815-1>

- Satybaldy, A., Subedi, A., & Nowostawski, M.** (2022). A framework for online document verification using Self-Sovereign Identity technology. *Sensors*, 22(21), 8408. <https://doi.org/10.3390/s22218408>
- Sidhu, J.** (2017). Syscoin: A peer-to-peer electronic cash system with blockchain-based services for e-business. In *2017 26th international conference on computer communication and networks (ICCCN)* (pp. 1–6). IEEE. <https://doi.org/10.1109/ICCCN.2017.8038518>
- Sun, N., Zhang, Y., & Liu, Y.** (2022). A Privacy-Preserving KYC-Compliant identity scheme for accounts on all public blockchains. *Sustainability*, 14(21), 14584. <https://doi.org/10.3390/su142114584>
- Tanwar, S., Parekh, K., & Evans, R.** (2020). Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *Journal of Information Security and Applications*, 50, 102407. <https://doi.org/10.1016/j.jisa.2019.102407>
- Thomas, J.** (2009). Medical records and issues in negligence. *Indian Journal of Urology*, 25(3), 384–388. <https://doi.org/10.4103/0970-1591.56208>
- UmaMaheswaran, S. K., Prasad, G. L. V., Omarov, B., Abdul-Zahra, D. S., Vashistha, P., Pant, B., & Kaliyaperumal, K.** (2022). Major challenges and future approaches in the employment of blockchain and machine learning techniques in the health and medicine. *Security and Communication Networks*, 2022, Article ID 5944919. <https://doi.org/10.1155/2022/5944919>
- UNIC.** (2018). Blockchain Certificates (Academic & Others), <https://www.unic.ac.cy/iff/blockchain-certificates/>
- Vyas, S., Gupta, M., & Yadav, R.** (2019). Converging blockchain and machine learning for healthcare. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 709–711). IEEE. <https://doi.org/10.1109/AICAI.2019.8701230>
- Weyl, E. G., Ohlhaber, P., & Buterin, V.** (2022). Decentralized Society: Finding Web3's Soul. Available at SSRN 4105763. <https://doi.org/10.2139/ssrn.4105763>
- Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K.** (2016). Where is current research on blockchain Technology?—A systematic review. *PLOS ONE*, 11(10), e0163477. <https://doi.org/10.1371/journal.pone.0163477>
- Yumna, H., Khan, M. M., Ikram, M., & Ilyas, S.** (2019). Use of blockchain in education: a systematic literature review. In *Asian Conference on Intelligent Information and Database Systems* (pp. 191–202). Springer, Cham. https://doi.org/10.1007/978-3-030-14802-7_17

Editorial record: The article has been peer-reviewed. First submission received on 11 January 2023. Revisions received on 15 March 2023 and 29 April 2023. Accepted for publication on 13 May 2023. The editor in charge of coordinating the peer-review of this manuscript and approving it for publication was Zdenek Smutny .

Acta Informatica Pragensia is published by Prague University of Economics and Business, Czech Republic.

ISSN: 1805-4951
