SBTCert: A Soulbound Token Certificate Verification System

Tarun Vihar Tumati
Department of Computer Science
California State University, Northridge
Northridge, CA 91330
tarun-vihar.tumati.208@my.csun.edu

***Abstract*—Certificate authentication is considered to be one of the most tedious and complex processes. Moreover, different types of documents like banking documents, education certificates, and government documents might need a specific type of authentication and verification. For example, the process of verifying the authenticity of education certificates with conclusive evidence can take up to months and consumes a lot of human effort. Hence, universities and colleges have no option but to consider the documents submitted by students, even if they might be fabricated. Sometimes an artfully generated forged certificate is almost impossible to detect and can be treated as the original. With the increase of forged documents, the credibility of both the document holder and the issuing authority is jeopardized. On the other hand, from students' perspective, as they go through multiple phases of education, they are compelled to submit several documents to secure admission to universities/colleges, or sometimes even more frequently for scholarships and tuition concessions. Therefore, hosting these certificates in a secure and tamper-proof manner on a decentralized network (blockchain) only allows participating parties to read/verify data to reduce errors and make it more transparent. In this paper, we analyze the limitations and shortcomings in the current certificate verification solutions and proposes the SBTCert (Soulbound Token Certification) Verification System, Blockchain-based digital certificate platform that aims to enhance the verification model without compromising security, authentication, decentralization, and confidentiality.**

***Index Terms*—Blockchain Technology, Authentication, Signed Documents, Security.**

I. Introduction

In the first paragraph, talk about: importance of the topic with supporting evidence; existing problems or gaps in the chosen topic; the problem that will be addressed in this project.

Global mobility has become common in education and professional area that increasingly people studying and working abroad. The increased mobility of individuals has made it essential for employers and educational institutes to verify the academic and/or professional qualifications of applicants. Meanwhile, students also need to share with higher education institutions their personal information (such as financial details, academic records, etc.), which must be securely stored, unaltered, and could be verified. There were people that forge certificates to gain employment or admission, making it difficult for organizations to verify the authenticity of the certificate. To address these issues, secure certificate verification systems were introduced which could efficiently handle and verify certificates.

Blockchain technology has been a major asset in the process of verifying academic qualifications, due to its built-in resistance to data manipulation. All network members must agree on any changes to the blockchain, and all validated transactions are recorded. In order to successfully issue digital certificates in the blockchain, it is essential that authentication, authorization, ownership, and privacy confidentiality are all taken into consideration. Currently, there are many research models and theories on the generation and issuance of digital certificates [1]–[4], but most of them lack some of the necessary factors.

In this paper, we propose SBTCert (Soulbound Token Certification) Verification System, a Blockchain-based digital certificate platform. SBTCert takes advantage of the blockchain's decentralized nature, security, and scalability by introducing SBTCert based on Soulbound Tokens. A web application is built to mints the certificates as SBTCert on the Block chain and transfer to the students. SBTCert requires verified participants to join. To obtain certification-related services, educational institutions, overseas universities, or companies must obtain permission to join the private Blockchain. Furthermore, SBTCert defines its own digital certificate data format and adds the signature of students' personal information and certificate information before issuing the certificate to students and storing it in the digital wallet. This ensures that the SBT certificate does not contain any students' personal information, thus protecting the privacy of SBT Cert holders. InterPlanetary File System (IPFS) is used to store the certificates. During the certificate verification process, overseas universities or companies can clearly view which academic credentials of the students

based on the SBT tokens stored in their digital wallets.

User authorization controls that only verified academic institute users are able to upload certificates, and only student users could initiate transactions.

The rest of this paper is organized as the following: Section II discusses related work; Section IV presents the framework of the project; Section III discusses the methodologies that will be used for this project; Section V illustrates the preliminary implementation results; and Section VI shows the timeline for this project.

II. Related Works

In this section, we discuss the existing work on document verification using blockchain technology and the blockchain tokens that had been used for document verification systems.

A. Document Verification Exsiting methodology

A paragraph at the beginning of each category/subsection that summarizes the work discussed in this subsection.

Xunfei: Drawback of this work: in your introduction, you said existing work lack some of the necessary factors

Shrivastava proposed a decentralized private Blockchain system for storing and verifying academic documents [1]. It uses credit tokens to make transactions, and universities initiate mark sheet processes for individuals. Whenever a third party requests a mark sheet, a token is generated and stored over the Blockchain, and the third party must accept it with their private key to view the credit token.

Buchmann et al. improved the long-term security of breeder documents (like birth certificates) by utilizing blockchain technology [2]. It captures biometric information of a newborn baby and then generates a cryptographic hash. The hash value will be stored in the metadata of a Bitcoin transaction made by an official birth certificate issuer of the member state.

Cheng et al. implemented a blockchain-based digital certificate system to reduce the risk of forgeries for graduation certificates [3]. The system involves universities entering student data, which is then recorded in a blockchain. Students receive an E-certificate with a QR code, which can be used to verify the authenticity of the certificate when applying for a job. The QR code also prevents tampering or forgery.

Leka et al. conducted a survey and proposed a solution called BCerts to increase trustworthiness of certificates [4]. It implements IPFS and has three functionalities - University Interface for creating and signing certificates, Verification Interface to validate certificates and Accrediting Interface to add accreditors and universities.

Potential drawbacks of the approaches described in the above research include reliance on credit tokens, vulnerability to forgeries or tampering, reliance on accurate student data, significant resources needed for implementation and maintenance, and reliance on a decentralized network.

A comparison of the works in this category and with your proposed solution.

B. Blockchain Tokens

A paragraph at the beginning of each category/subsection that summarizes the work discussed in this subsection.

For international students, the process of having paper certificates issued in their native language translated by a central agency can be tedious and open to document forgery. The authors proposed a new methodology of document verification, particularly in the educational field, using NFT certs (digital assets developed according to Blockchain architecture). This approach could potentially speed up the verification process. To address the shortcomings of using cryptos, which are not yet approved in some countries, the authors proposed integrating the application with payment providers such as Paypal for making transactions. [5]

Most recently, a group of researchers proposed the decentralized society using Soul Bound Tokens [6]. A Soul Bound Token is a type of Non-Fungible Token (NFT) that is designed to remain in the possession of one individual or entity. Unlike other NFTs, which can be exchanged freely, a Soul Bound Token cannot be transferred or sold. Instead, it is used to represent a unique virtual asset, such as a digital art piece, collectible, or game item. Soul Bound Tokens provide a secure and verifiable way to store and transact digital assets.

A comparison of the works in this category and with your proposed solution.

III. Blockchain Technology

A. Features and Characteristics

Blockchain technology is a combination of various approaches including cryptography, mathematics, algorithms, and distributed consensus algorithms. The main core elements, namely:

1) Decentralized: In a blockchain, no single node is necessary to act as a ”master” node; instead, all the nodes in the network are able to record, store, and update the ledger, allowing the blockchain to operate without relying on a single centralized node.

2) Transparency: The data stored in each block, which is distributed among the other connected nodes, is visible to each node, creating transparency among the connected nodes.

3) Immutable : All records on a blockchain are permanent and cannot be altered unless someone can take control of more than 51% of the nodes on the blockchain network simultaneously.

4) Consensus based: All nodes connected on the blockchain are eligible to safely transfer and update data, as changes can only take place when the majority of the nodes agree to the change, creating a consensus-based system.

B. Blockchain Structure

Each block in the blockchain consists of five components: the primary data, the hash of the preceding block, the hash of the current block, the timestamp, and any other relevant information.

The main data is the actual information stored in the block. This could be a transaction, a message, a digital asset, or any other data. The hash of the previous block is a unique cryptographic hash that is used to reference the previous block. The hash of the current block is a unique cryptographic hash that is used to reference the current block. The timestamp is used to indicate when the block was created. Any other relevant information is any additional information that may be associated with the block. This could include the miner’s address, the transaction fees, or other relevant data.

C. Blockchain Types

Blockchain are majorly classified into four types:

1) Public Blockchains: A public blockchain is a distributed and decentralized ledger that allows anyone to participate. It is open to the public, and its transactions are recorded in a distributed ledger that is visible to all participants.

2) Private Blockchains: A private blockchain is a distributed ledger system that is managed by a single entity or organization. It is closed off to the public, and only approved users can participate in its transactions.

3) Consortium Blockchains: A consortium blockchain is a distributed ledger system managed by a group of organizations. It is open to anyone, but its transactions are only visible to the consortium members.

4) Hybrid Blockchains: A hybrid blockchain is a combination of a public and private blockchain. It is open to the public, with some parts of the blockchain are restricted to certain users.

D. Security for Educational Certificate in Blockchain

Educational certificates stored on a blockchain must include the following essential elements:

1) Authentication: In order to access and verify the certificates stored on the blockchain, users such as students, universities, institutes, and employers must be authenticated. This can be accomplished by requiring each user to provide a username and password, or in some cases, multiple authentication systems such as biometrics may be used. For example, an employer wishing to view and verify a certificate must first join the blockchain and then receive authorization from the recipient to do so.

2) Authorization: Provides users with the necessary permissions to perform transactions within the blockchain. For example, a student is given authority to share their certificate with an employer after it has been issued. All actions and functions related to the certificate must be authorized within the system.

3) Confidentiality: The academic institute and the student are responsible for maintaining the confidentiality of the student's private information. The student has the authority to decide which information should be shared with third parties, such as employers, for verification purposes.

4) Ownership: The ownership of a digital certificate in a blockchain ledger is vested in the users. For example, in the case of an educational certificate, the recipient has full ownership of the certificate, which requires the use of public and private keys to be shared among all the users who own the blockchain.

5) Privacy: Anonymity must be maintained when it comes to public keys. This is done through the use of cryptographic algorithms and the creation of hash functions. As a result, employers can verify the credentials claimed by the student on the blockchain, which helps to ensure that the certificate is not a fake.

IV. Design

As shown in Fig. 1, this project consists of three components: IPFS (InterPlanetary File System), Blockchain, and a Web Application.

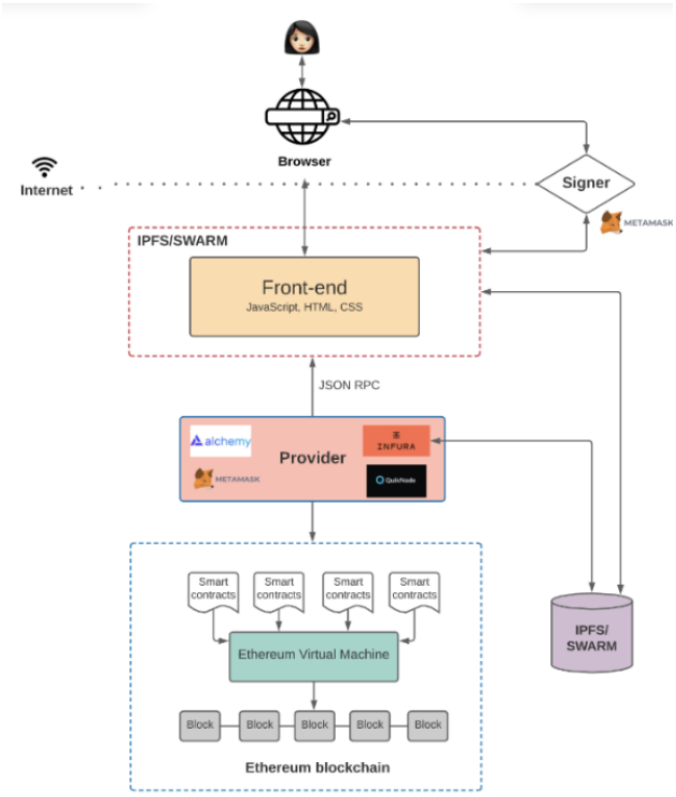

Fig. 1. Framework of the Project.

IPFS (InterPlanetary File System) is a decentralized, peer-to-peer file sharing system that aims to be a more efficient and secure way of storing certificates/documents.

Blockchain technology is used to create a secure, tamper-proof system for document verification.

A web application that is built on top of a decentralized, blockchain-based platform. It allows users to interact with blockchain to facilitate the exchange of data between the users and stakeholders.

When a user upload a certificate file, it is processed by the web application and stored on IPFS, and a hash value will be returned by IPFS. The metadata of the user's data is then sent to the blockchain, where a smart contract is used to mint an SBTCert token. This token is then used to authenticate the user and validate their data. The SBTCert token is unique and can be used for any future authentication.

In this paper, we present SBTCert, a novel certificates management framework leveraging SBT, as a solution to prevent fake or illegal certificates. This framework facilitates overseas universities and companies to access student's educational certificates using the functionalities of SBT. This proposal is based on a Blockchain, open only to authenticated and verified educational institutions, universities, and companies to ensure the security of the system.

As illustrated in the Fig. 2, educational institutions are incorporating Blockchain technology to issue SBT-based certificates to their students. Each educational institution joins the network

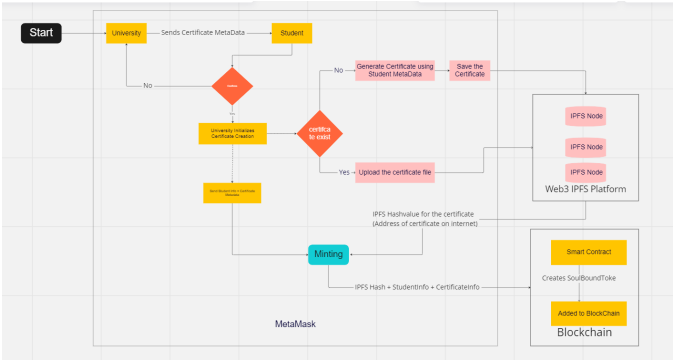

Fig. 2. Flowchart of the Project

as a node, thus ensuring the trustworthiness and validity of the certificates. The certificate minting process involves the following steps.

Step 1. Universities/educational institutions have two options for initiating the certificate generation process: a) Uploading a file for already created e-certificates to be minted with SBTCert, or b) For new certificates, the application provides the functionality to generate e-certificate from the given information.

Step 2: The Generated Certificate is stored on the Blockchain and its hash is then captured on IPFS.

Step 3: The returned hash along with metadata is sent to the smart contract in the Blockchain, which generates the SBT.

Step 4:The generated SBT is transferred to student's wallet and stored as SBTCert.

Step 5: Students holding SBT-based certificates have the option to share their digital wallet address with anyone who needs to verify their credentials, such as colleges, employers, or other entities. The authenticity of the SBT-based certificates can quickly and easily be confirmed.

Step 6: Yes, overseas universities or companies that are connected to the Blockchain can access the stored SBT-based certificates. As long as the university or company has access to the blockchain network, it can view and verify the stored certificates.

Insert a figure for the project framework: reflect the major components/modules of your project. You could directly save your design as a jpeg/png file, and inset the file here. Adjust the size of the figure and the font size for text in the figure so that people could easily read the text in the figure.

A. IPFS Storage

Include a figure for the design for this major component if applicable

IPFS (InterPlanetary File System) is a distributed storage protocol used to store certificates generated by the application [7]. It is used to store documents and verify their authenticity. It works by allowing users to store documents on a peer-to-peer network, and then using hash functions to verify the integrity of the documents. This means that if someone attempts to alter a document, the hash will no longer match, and it will be obvious that something has been changed. This makes it much more difficult for someone to tamper with documents and helps to ensure their authenticity. This makes it much easier for verifying the accuracy of documents and can help to reduce the potential for fraud. Therefore, IPFS is an ideal solution for storing t sharing education certificates in a secure and reliable manner.

B. Blockchain

Provide a detailed description for the major component 2.

Include a figure for the design for this major component if applicable

Soulbound Tokens and the Smart Contracts are used to provide a secure and tamper-proof way of storing and verifying the authenticity of educational certificates and to allow for the automation of certificate minting through the use of smart contracts.

Soul bound tokens are used for document verification by creating a unique identifier for each document that is stored in the blockchain.

The SBT will be associated with the document and will be used to verify the document's authenticity. It is used to ensure that the document has not been tampered with or changed in any way, as any changes to the document will be reflected in the SBT . Additionally, it can be used to verify that the document has been issued by the correct entity, as the token can be used to trace the document back to its source. Smart contract is to facilitate the secure and automated verification of the authenticity and validity of a document. It stores relevant information (such as the issuer, date of issuance, and academic performance, etc.) for a document in the form of SBTToken on the blockchain. When the verifier(individual or entity involved in the document verification process) requests verification of the document, the smart contract can retrieve this information and verify its accuracy against the information provided by the them. If the information matches, the smart contract automatically triggers the release of the verified document to the inquirer.

The algorithms and technologies used for minting Soulbound tokens include blockchain technology, smart contracts, web3 libraries or APIs, and wallet providers.

1) Setting up a blockchain network: The first step in minting Soulbound tokens is to set up a Ethereum network, on which the tokens will be created and stored. This involve installing and configuring the softwares, such as a blockchain node and wallet, as well as joining an existing network or creating a new network.

2) Creating a smart contract: The next step is to create a smart contract that defines the properties and rules of the Soulbound tokens. This involve programming the smart contract code in Solidity, and deploying it to the blockchain network using web3 libraries or APIs.

3) Minting the tokens: Once the smart contract is deployed, the next step is to mint the Soulbound tokens by calling the appropriate functions in the smart contract which may involve

metadata of student or any addtional custom parameters that are required.

4) Storing and managing the tokens: After minting the tokens, they must be stored and managed securely. To achieve that we use a MetaMask wallet provider, to store the tokens and manage the minted SBTs, as well as using web3 libraries or APIs to interact with the smart contract.

C. Web Application

Insert a figure for the component 3.

There are six modules in the web application to mint soulbound tokens:

1) Wallet integration module: This module enables users to connect their wallets to the web application, allowing them to securely store and manage their soulbound tokens. The module may also include support for popular wallet providers, such as MetaMask and Ledger.

2) Cerficate Creation: This module allows universities to generate a digital certificate from the student's metadata and his academic performance.

3) Token Minting: This module allows universities to mint their soulboundtokens and transfer them to relevant students or smart contracts.

4) Token Burning: This module produces functionality for the stakeholder to rollback the minted SBTs and avoid airdrops in the network

5) Token Management: This module provides users with the ability to manage their soulbound tokens, including the ability to view their SBTS, transfer history, and other relevant information.

6) Token Verification: This module enables users to verify the authenticity and validity of their soulbound tokens, ensuring that they are not counterfeit or fraudulent.

V. Preliminary Results

A short summarize of methodologies that will be used for this project.

A. IPFS on Web3 Storage

Web3 Storage[1] is used to store certificates on IPFS, leveraging the decentralized and distributed nature of IPFS for secure and efficient storage. This is done by using IPFS libraries/APIs to add the certificates to IPFS and retrieve them from within the application.

To configure web3 storage (IPFS provider) in an web application, the following steps may be followed:

First, the necessary dependencies for using web3 storage (IPFS provider) in Angular must be installed. This include installing the web3.js library, the IPFS.js library, and other relevant dependencies. After installing the dependencies, they must be imported into the web applications. The next step is to initialize the web3 and IPFS objects in the Angular app. Finally, the app must be configured with valid token to use web3 and IPFS for storage.

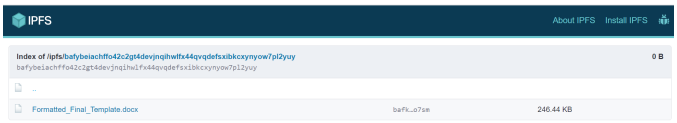

Fig. 3. IPFS Results

Fig. 4. IPFS Results

B. Web Application

VI. Timeline

The timeline for the proposed project is shown in table I.

References

[1] A. K. Shrivastava, C. Vashistth, A. Rajak, and A. K. Tripathi, "A decentralized way to store and authenticate educational documents on private blockchain," in *2019 International Conference on Issues and Challenges in Intelligent Computing Techniques (ICICT)*, vol. 1. IEEE, 2019, pp. 1–6.

[2] N. Buchmann, C. Rathgeb, H. Baier, C. Busch, and M. Margraf, "Enhancing breeder document long-term security using blockchain technology," in *2017 IEEE 41st Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2. IEEE, 2017, pp. 744–748.

[3] J.-C. Cheng, N.-Y. Lee, C. Chi, and Y.-H. Chen, "Blockchain and smart contract for digital certificate," in *2018 IEEE international conference on applied system invention (ICASI)*. IEEE, 2018, pp. 1046–1051.

[4] E. Leka, E. Kordha, and K. Hamzallari, "Towards an ipfs-blockchain based authentication/management system of academic certification in western balkans," in *2022 45th Jubilee International Convention on Information, Communication and Electronic Technology (MIPRO)*. IEEE, 2022, pp. 1448–1453.

[5] X. Zhao and Y.-W. Si, "Nftcert: Nft-based certificates with online payment gateway," in *2021 IEEE International Conference on Blockchain (Blockchain)*. IEEE, 2021, pp. 538–543.

[6] E. G. Weyl, P. Ohlhaver, and V. Buterin, "Decentralized society: Finding web3's soul," *Available at SSRN 4105763*, 2022.

[7] J. Benet, "Ipfs-content addressed, versioned, p2p file system," *arXiv preprint arXiv:1407.3561*, 2014.

[1] https://web3.storage/

TABLE I
TIMELINE FOR THE PROJECT

Month	**Schedule**		
	Tasks	***Description***	***Output***
Dec 2022 - Jan 2023	Mint SBT (Soul-bound) tokens	Create the smart contracts and deploy it on a test network to enable the minting of SBT tokens to students	Working smart contract deployed on the test network; Ability to mint SBT tokens to students
Feb 2023	FrontEnd with Blockchain	Develop the front-end interface for the certificate verification system, including any necessary integrations with the blockchain platform	Working web application for the certificate verification system
March 2023	User Management	Develop a module for managing users and assigning roles and privileges, as well as implementing authentication and authorization processes	Working user management module with functionalities for assigning roles/privileges and authentication
April 2023	Initial Version of the system	Finalize the development of the initial version of the system and prepare it for testing and deployment on main network	Initial version of the project ready for testing and deployment
May 2023	Final Paper	Document the functionalities of the certificate verification system, including any challenges or lessons learned, and any recommendations for future work	Final paper detailing overall funcationlies of certificate verification system