# The Future of Document Verification: Leveraging Blockchain and Self-Sovereign Identity for Enhanced Security and Transparency

***Abstract*—Attestation of documents like legal papers, professional qualifications, medical records, and commercial documents is crucial in global transactions, ensuring their authenticity, integrity, and trustworthiness. Companies expanding operations internationally need to submit attested financial statements and incorporation documents to foreign governments or business partners to prove the authenticity, legal validity and regulatory compliance of their businesses and operations. Attestation also plays a critical role in education, overseas employment and legal documents such as testaments and medical records. Traditional attestation process is plagued by several challenges including time-consuming procedures, circulation of counterfeit documents and concerns over privacy of data in the attested records. Covid-19 pandemic brought into light another challenge which is ensuring physical presence for attestation which caused significant delay in the attestation process. Traditional methods also lack real-time tracking capabilities for attesting entities and requesters. This paper aims to propose a new strategy using decentralized technologies such as blockchain and self-sovereign identity to overcome the identified hurdles and provide an efficient, secure and user-friendly attestation ecosystem.**

***Index Terms*—Attestation, Blockchain technology, Self-sovereign identity technology**

## I. Introduction

Attestation of records is the important first step to verification and certification of documents to confirm that the information contained in it is correct, authentic and was issued by a legitimate authority. Legal, education and commercial documents often need to be attested when they need to be used for international purposes such as employment, business expansion to foreign countries and global transactions [1]. For instance, in the context of legal documentation, records such as birth certificates, marriage certificates and power of attorney require attestation to verify and assert the legitimacy of the record when they are used in legal proceedings or administrative reasons in a foreign country [2]. Attested documents prove that they can be accepted in jurisdictions outside of the country of origin. In the educational sector, diplomas , degrees, transcripts and certificates need to be attested if the students wish to study or apply for employment opportunity in a foreign country. An attested educational record confirms that student's academic achievements and qualifications are trustworthy and have been awarded by an accredited educational institution. Attestation is therefore a vital step in confirming the credibility and global acceptance of different types of documents [1].

The current manual verification faces numerous challenges and problems. Some of the significant challenges are delay in the completion of process due to the number of steps, personnel and time required for completing the process. The traditional system used for the process is also prone to human error which is difficult to track due to the inability to perform real time transparent and tamper evident tracking of each attestation step. In addition to this, Covid-19 pandemic added the difficulty in ensuring physical presence of record owner or attesting officer. Another problem is reliance on the traditional system alone to attest paper-based documents makes it susceptible to fraud and forgery. There have been several instances of fake educational certificates used for employment or visa applications [2]. In addition to this, it is often a complex and bureaucratic process, prone to delays and inefficiencies. Geographical limitations can also be a hurdle when individuals in remote areas require attestation from authorities in a far away location.

This work is organized as follows: Related work section delves into some of the existing systems used for attesting different types of records and how it aims to prevent forgery and reduce time-delays involved in the process. The section also explores the underlying issues in the system which makes the process complex not only for record owners but also for attesting officers and entities across international borders. The proposed system explains how an integration of blockchain and self-sovereign identity technology can be used to create a more interconnected and trustworthy attestation system that can create transparent tracking of the process while preserving the privacy of record owners and confidentiality of information in the record.

## II. Related Work

Attestation process provides a standardized method to verify and certify documents facilitating global mobility, employment, business and education. Absence of a formalized attestation process can increase the risk of fake documents being used for cross-border transactions and interactions. Traditional attestation systems involve multi-step process that is used to verify and assert the authenticity of different records such as legal documents, educational certificates and business documents. The primary purpose of attestation is to prevent fraud and forgery thereby ensuring that the the document and the information contained in it was verified by a trusted entity to be credible.

Even though a standardized system exists to verify the documents, fraudulent practices are prevalent especially in the

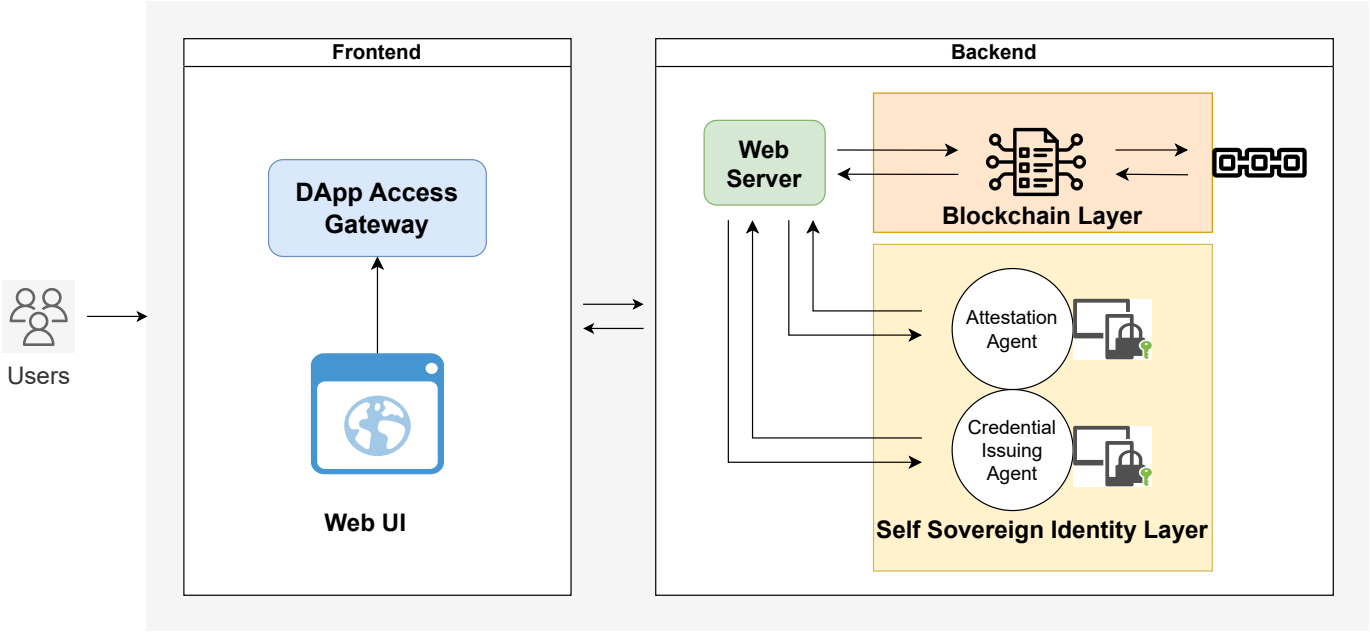


Fig. 1. Proposed Architecture Diagram

educational qualification documents. This is because of the fact that in the era of digital transformations, individuals have several ways to learn and interact with educational institutions. It is possible to complete an entire educational degree through online education where students use various online tools to learn and earn their degrees. While this makes education easily accessible to students even in remote areas, it makes it difficult for verifiers to access the credibility of qualification records provided by the students. The increased risk of circulation of fake educational qualification documents can affect the value of many of these educational certificates for courses completed online [3]. Recently, Forbes magazine conducted a study on the prevalence of fake diplomas and transcripts, revealing that the degree mill industry is illicitly generating an estimated 7 billion dollars in revenue [4]. An important group of victims is those students who saw the advertisements of these low quality, for-profit educational institutions and spent their time and money to earn the degree [4]. Fradulent practices are not the only challenge in the traditional attestation process. The complex document requirements can also be overwhelming for requesters who need to get their foreign public documents legalized [5]. Another significant challenge is lack of a transparent system to receive communication and regular updates from attesting entities regarding the progress of attestation. This lack of transparent tracking system becomes a significant hurdle for remote applicants who has no option other than to wait to receive the final update which is either a successfully legalized document or a reason for rejection.

In order to make this traditional legalization process less complex and quicker, the Hague Conference formed The Convention of 1961 which introduced the use of 'Apostille' to legalize foreign public documents for member countries [5]. But, there are still countries that are not part of the Hague Convention which affects its use in global context. Countries which are not part of this convention still requires to follow the traditional legalization process.

Many blockchain-based approaches have been proposed for document verification offering an alternate mechanism to authenticate and manage important records. A blockchain based enrollment system was proposed by Fernando et al. for University in Indonesia to solve some of the challenges related to university documents such as certificates and transcripts [6]. Authors have proposed a blockchain technology based enrollment process to monitor and control enrollment activity of each student so that it is possible to ensure that only valid students who completed the enrollment process can register for courses and get course credits for the registered and completed courses [6]. Badlani et al. has proposed an ethereum and IPFS based approach to safely store, retrieve and authenticate educational documents. They have also included mechanism to efficiently organize the complete examination process and generated of associated results [7] using mechanisms such as smart contract logic. Smart contracts have been utilized to safely execute the logic associated with the proposed system, generate tamper-evident chain of transaction records.

Blockchain based approaches have been proposed not only for academic purposes but also for secure sharing of digital assets such as wills on blockchain. Crypto-Wills is a blockchain based system proposed to verify and securely transfer deceased person's asset to assigned entity using ERC-20 and ERC-721 crypto tokens. A consensus based mechanism is used to execute the contract specified in the will, verify and transfer assets to the beneficiaries [8]. Gunit Malik et al. have provided a detailed description on how a blockchain based solution can be used to verify the authenticity of documents that are issued by the Indian Government. They have leveraged the availability of private channels in hyperledger fabric to achieve privacy of document data.

Forgery and fraudulent practices are also present in high profile areas such as international trade and business transactions, legal sector and financial and banking activities. Complexity and the time-consuming nature of traditional attestation and document verification process is also widespread in all the fore-mentioned sectors. So, there is a need of a distributed solution that can transparently and continuously monitor and track the document verification and attestation from its starting point when a user requests for attestation till the final step which produces the fully attested document. It is also important that the auditing of attestation steps does not violate the privacy of individuals and entities involved in the attestation process which includes attestation bodies and document owners. Confidentiality of document data and user information should also be ensured. Document owners should be able to get status updates via a peer-to-peer secure channel on the progress of attestation process for their document. Attestation bodies need to have the capability to contact the entity or individual who completed the previous attestation step in case additional information is required to perform verification. Once the attestation process is complete, a secure communication channel is desired for the verifier to contact the document owner or the attestation bodies if they require any additional details. All the communications need to be securely and transparently recorded in a verifiable manner.

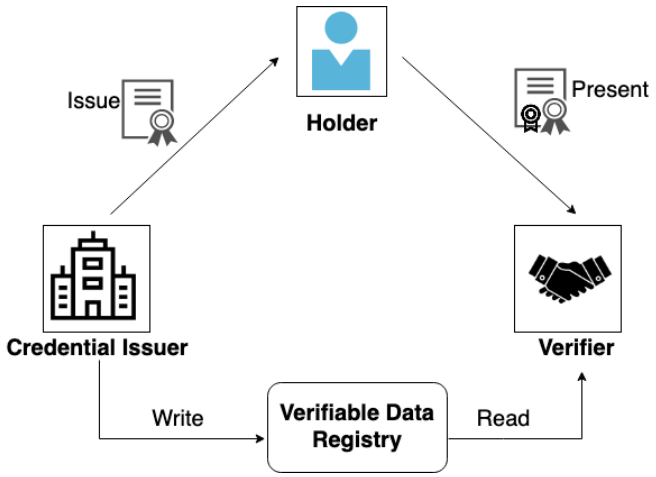


Fig. 2. Triangle of Trust for Verifiable Credentials

## III. Proposed System

This section is organized in two parts: in the first part, a brief introduction to the unique features of blockchain technology, self-sovereign identity technology and micro-credentials is provided. The second part offers a detailed description on the working of the proposed system and its key features.

### *A. Overview of Key Technologies and Concepts used in the Proposed System*

*1) Blockchain Technology:* Blockchain has proven to be useful beyond the financial sector and has demonstrated its applicability in areas such as supply chain, real-estate, insurance, voting and governance and Internet of Things (IoT). Some of the important features that made blockchain technology useful in sectors beyond finance are transparency, immutability, autonomy,security and also it's decentralized nature. At the core, blockchain is a distributed ledger in which each transaction is recorded in a block and linked to the previous block thereby forming a chain that is visible to all the participants in the blockchain network [9]. This visibility makes sure that every transaction on-chain is open to all network participants for verification creating a transparent environment for all interactions between participants of blockchain network. Anyone on the network can see the details and history of transactions on the blockchain depending on several key factors such as accessibility, consensus and control mechanisms. This characteristic of blockchain enhances the accountability and integrity of the information recorded on chain, making any attempt at unauthorized altering of data easily detectable [9]. Moreover, the entire blockchain ledger is distributed across multiple computers referred to as nodes operating in a peer to peer manner. Modifying data on the blockchain would require simultaneous modification of the ledger on more than half of the nodes operating on the network which is extremely difficult to achieve on large and well-distributed networks [9]. Consensus mechanisms such as Proof of Work or Proof of Stake are used to perform validation and addition of transactions to the ledger [10]. These mechanisms help to make sure that all nodes on the blockchain network are in agreement on the current state of the ledger, rejecting unauthorized attempts at modifying data on the network [10].

Every transaction performed on blockchain is cryptographically encrypted and signed. Digital signatures used to sign each transaction helps in verifying the authenticity of transaction. The signature can be generated only by the holder of the private key thereby confirming the identity of the parties involved in the transaction. The use of asymmetric cryptography ensures that public key part of cryptographic key pair is visible to anyone on the network and private key part is restricted to the owner of key pair.

Data traceability is another important feature of blockchain which made it really valuable in areas such as financial transactions, supply chain management and clinical trials [9]. Every transaction entered into the blockchain network is timestamped. This helps to prevent fraud and counterfeiting because it allows stakeholders to verify the authenticity of transactions at any time to detect any fraudulent activity or to ensure that a product on the supply chain is not counterfeit.

*2) Smart Contracts:* Smart contracts are self-executing contracts that contain the terms of agreement between two involved parties represented by lines of code written in the chosen programming language. They can store information, process input data and generate output based on pre-defined conditions represented by functions in smart contract. Smart contracts automatically execute the contractual agreement when the pre-defined conditions are met [11]. When executed, they enforce an agreement between two unknown and potentially untrustworthy parties without the involvement of any external party. Therefore, smart contracts provide the blockchain

an automated and secure way to translate contracts on paper to their digital counterparts. To ensure that no unauthorized modification of smart contracts occur, they are stored on the blockchain network itself. Automatic execution of pre-defined conditions on the smart contract reduces human error and the chance of disputes. Ethereum is the first blockchain platform that started the development of smart contracts [12]. Some other blockchain platforms that support smart contracts are NXT, Hyperledger Fabric, Cardano and Polkadot.

*3) Self-sovereign Identity Technology:* Existing identity systems are still not mature enough to handle the wide variety of digital identities that are being used for various online transactions [13]. They fail to provide users with one of the most desired feature which is sovereignty over their own personal information. Trying to achieve it, many user-centric designs proposed turning centralized identities into inter-operable federated identities with centralized control, allowing users to have some level of control over how and with whom their identity information is shared [14]. Achieving user autonomy is the next important step for identity systems to move closer to *user controlled identity*.

Recently proposed self-sovereign identity (SSI) systems promise to deliver this exact capability: instead of users being at the center of identity systems, self-sovereign identity systems advocate that users should be the rulers of their identity [14]. Self-sovereign identity systems are founded on the principle that users should be central to managing their own identities. However, the goal of SSI systems extends further, aiming to ensure not only the interoperability of user identities but also to guarantee user consent whenever their identity information is shared with other parties, such as service providers or other users. SSI based systems should also provide users with the ability to make claims which can include personally identifying information (PII) or other facts about their capability. These include license information (proving their right to operate vehicles), work authorizations and security clearance. Figure 5 shows the roles involved in a typical self-sovereign identity ecosystem and their interactions.

The main building blocks of SSI system consist of 1) an SSI-compatible digital wallet, and 2) Decentralized identifiers (DID). In addition to securely store and maintain digital identities, the wallet held by the identity owner must also be able of maintaining a history of all identities issued to their holder. They can also function as agents that facilitate secure peer-to-peer communication with other entities in the self-sovereign identity ecosystem. Another important functionality of the wallets is that they help users to decide how, when, with whom their identity information is shared and control how much information is shared with requesting entities. Decentralized identifiers (DID) are globally unique, verifiable and persistent identifiers that help users to cryptographically prove that they are indeed the ones controlling the identity stored in their digital wallet.

Decentralized Identifiers (DIDs) facilitate key functions for controllers, requesting parties, and subjects. Controllers may be individuals, organizations, or agents, managing DIDs. These DIDs enable reliable cryptographic verification of the source of information without third-party involvement, enhancing privacy and autonomy in identity management. Verifiable credentials (VCs) package all the details related to the identity of the DID subject and also the cryptographic proof associated with the details into a single file which can be stored in an SSI based digital wallet [15]. VCs are capable of digitally representing any traditional certifications or credential such as university degree, driver's license or certificate of employment. The use of digital signatures makes verifiable credentials tamper-evident.

*4) Micro-credentials:* According to Pickard, Shah and De Simone, microcredentials (also known as micro-degrees, digital badges or nanodegrees) are defined educationally as credentials that emcompass the completion of multiple courses by a student, yet do not equate to a full educational degree. The educational platform *edX* was the first to introduce micro-credentials in the year of 2013. Following up, many mass open online course (MOOC) platforms now offer different types of microcredentials [16]. Microcredentials allow sutdents to incrementally accumulate certification of skills that they have gained through learning platforms. These types of credentials provide better support for self-regulated learning abilities, allowing students to create learning goals and paths for themselves, while still receiving the certification for completed stages [16].

When powered by SSI technology, micro-credentials can be useful to provide more security and control to these individual pieces of certification. The benefit of SSI technology lies primarily in its two key components: decentralized identifiers and verifiable credentials, The World Wide Web Consortium (W3C) is currently standardizing decentralized identifiers [17], which will offer a unified framework for their creation and management. Similarly, verifiable credentials, the other fundamental component of this technology, have also been standardized by W3C. These standards provide a framework to generate, issue, hold and verify these digital credentials in a secure, private and interoperable manner [15].

### *B. Design of Proposed Approach*

The proposed system leverages the transparent and tamper-evident nature of blockchain technology to generate an attestation chain for each document submitted for verification and authentication. Attestation chain is a secure, tamper-evident, transparent sequence that represents the series of steps, verifications, and approvals associated with every document that is submitted by users for attestation. Figure 3 shows an example of the attestation chain for a document. Each block in the chain shows a distinct phase in the attestation process capturing non-confidential details related to that step. The primary purpose of the attestation chain is to provide a reliable ledger of attestation journey that each document has gone through to prove the integrity, authenticity and legitimacy of document and process. The blockchain technology ensures that the attestation chain cannot be controlled by any single entity and requires all involved parties to come into consensus

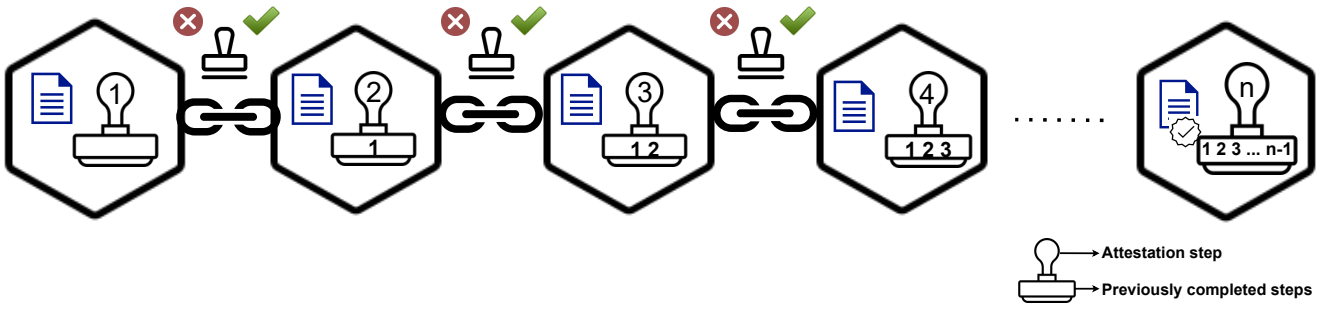


Fig. 3. Attestation Chain for a document submitted for authentication

to attest a document. All transactions within each attestation chain are stored on the blockchain and visible to all authorized parties for clear and transparent view of the attestation process. Each transaction on the blockchain is encrypted and linked to the previous transaction ensuring a secure chain of custody for the attestation steps.

The system uses SSI technology to generate micro-credentials to represent the successful completion of each attestation step. After the completion of the final step in the attestation process, a verifiable credential is generated for the document. It links all the micro-credentials together and demonstrates the completion of the attestation process. Following are the major features of the proposed system:

- Mobile based agent for peer-to-peer communication between document owner, verifying entity and attesting entity;
- On-chain transparent tracking and auditing of document attestation steps;
- User friendly interface to view non-confidential details of the document attestation status;
- Ability to revoke or expire the attestation stamp on the document;
- Ability to track the attested documents that have been expired.

### C. System Architecture

The system proposed in this paper is designed to function in parallel with the existing traditional attestation process to bring in more transparency to the manual process that is being followed currently and enhance traceability of the entire attestation process. Fig 1 shows the conceptual architecture diagram of the proposed approach. A decentralized application (DApp) is used to create and submit blockchain assets such as attestation request and non-sensitive details related to each attestation step which are linked together to form an attestation chain. The DApp Access Gateway functions as a checkpoint to ensure secure and controlled access to the DApp and services provided by the application. Web server interacts with blockchain layer to record transactions related to attestations. Web server interacts with the self-sovereign identity to initiate creation and issuance of credentials.

Attestation agent and credential issuing agents are self-sovereign identity based software agents. Attestation agent can communicate with the SSI compatible wallet which holds the verifiable credential issued to the attesting entity. The wallet helps to securely manage cryptographic keys used to sign the micro-credential. The keys can also be used to encrypt and decrypt messages that are communicated between the attesting entity, users and verifiers. Credential issuing agent will be used generate and issue verifiable credentials to authorized attesting entity, users and authorized verifiers. Credential issuer will also hold a SSI comptabile walletholding the verifiable credential of the issuer. Both credential issuing agent and the attestation agent will have a DID associated them which can be used by users or other verifiers to know the legitimacy of the entity and ensure that they still have ownership of their identity.

The proposed approach involves both blockchain and SSI layers. So, it is important to identify and assign host layer for each of the roles. This is because not all roles require identities to perform authorized actions in both layers.

The three key roles in the proposed system are *document holder*, *attesting entity* and *verifier*. The *attesting entity* is a trusted party certified by government and has the capability to verify and authenticate the submitted document. After verification is complete, the attesting entity is responsible for issuing a micro-credential proving the completion of the attestation step. The *document holder* is the owner of the document and accepts desired credentials from the attesting entity and holds the verifiable credential associated with the attestation in their SSI compatible wallet. *Verifier* can be an attesting entity trying to request any additional information from document holder or attesting entity from a previously completed step. Employers or government authorities who request proof of attestation or additional information also act as *verifiers*.

The document holder needs to have unique identities only in the SSI layer after the document has been successfully attested. This identity is issued by an issuing organization which can be a government entity. This could be a department of government which handles digital identity. For instance, identity issuer can be an agency that runs national identity program. The document holder can check the reliability and integrity of the issuing organization using the issuer's DID. The DID will have details such as their unique identifier, public keys associated with DID, privacy considerations followed by the issuer and details of revocation registry if any. Revocation registry is usually used to maintain a decentralized registry of expired and revoked credentials that were issued by the issuer in past. The SSI compatible wallet holding the verifiable credential related

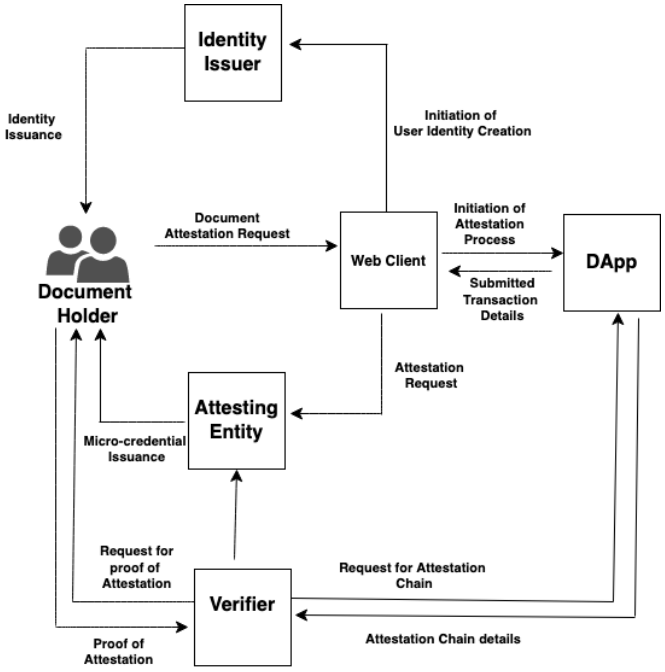


Fig. 4. Flow of Information between Entities in Attestation Process

to the identity of user will be used to receive notifications regarding the status of their attestation request. The wallet will also be used to hold micro-credential associated with each attestation step and final verifiable credential issued to prove the successful completion of attestation.

The unique identifier of the document can be used by the document holder on a user-friendly web interface to check the details related to the timeline of the attestation process that is recorded on the blockchain. Attesting entity requires identification in both blockchain layer and SSI layer. Identity on the blockchain layer will be used by the attesting entity to submit transaction on chain whenever the required verification is completed by them. This transaction will be recorded as part of the attestation chain created for the document. Identity on the SSI layer will be used by the attesting entity to create and issue micro-credential related to the completed attestation step. Every attesting entity is issued a verifiable credential that contains details such as their title, issuing organization's details, issuance and expiration date, cryptographic proof that can be used to verify the authenticity of the credential, public key associated with attesting entity. Attesting entity can store and maintain the issued credential in an SSI compatible wallet. The SSI agent associated with the wallet facilitates peer-to-peer secure communication with other entities to exchange proofs or other necessary information that the owner of the wallet authorizes to share.

Verifiers need not have any identity on the blockchain layer since they can use the document identifier to view the attestation chain related to the document. Verifier requires identity only in the SSI layer. The identity can be used for need peer-to-peer interaction with the document holder or attesting entity to collect any additional information from them after viewing the attested document.

Figure 4 demonstrates the steps followed by the proposed system in recording transactions on chain and generating credentials for user identity and document attestation.

The process starts with a user submitting a document for attestation. The unique document identifier provided as part of the request is used to search and ensure that no duplicate request has been filed for the same document in the past. If there are no duplicates, then attestation process is initiated by submitting a transaction to the blockchain. The submitted transaction contains details such as current timestamp, document identifier and destination country name. The destination country's name is added to ensure that the user's request is not rejected because the document was attested previously for a different destination country where the user pursued higher education or worked. Smart contract logic can be used to ensure that the condition stated above is checked for every incoming request.

After manual verification of attestation is performed by the attesting entity and document is authenticated, the attesting entity uses the SSI agent to generate a micro-credential proving the successful completion of the step. The user can accept and store the micro-credential in their SSI compatible wallet.

The non-sensitive details related to the completed attestation step such as micro-credential's unique identifier, DID of the user, unique identifier of the document, timestamp details, attestation phase number and DID of the attesting entity involved in that phase are stored on the blockchain. Smart contract logic can be used to ensure that no step in the attestation process is skipped.After the on-chain verification, the transaction is successfully submitted to the blockchain.

After all the individual steps in the attestation process is complete, a verifiable credential proving the completion of entire attestation is generated. The entity performing the final step of attestation has the capability to initiate the credential generation process. This verifiable credential will link all the individual micro-credential, the DID of the entity who intitiated the verifiable credential generation, cryptographic proof associated with the issuer, activation date, public key of the user. This verifiable credential can be stored in user's SSI compatible wallet and can be used to provide proofs to the verifier as needed. Fig 5 shows an example of a verifiable credential issued to the user marking the completion of attestation process. -previous space for architecture diagram–

## IV. Privacy and Ethical Considerations in the Implementation of Proposed Approach

A discussion on a new technical solution handling human data, including personal identification, educational qualifications, work experience, and sensitive health information, is incomplete without addressing its ethical and privacy implications. It is crucial to ensure that the integration of blockchain and SSI technologies does not make any assumption regarding the ethical and social outcomes of the solution. Advancements in identity management systems must not overlook the potential privacy and security concerns associated with enhancing


Fig. 5. Example Verifiable Credential containing micro-credentials of all the steps in the attestation chain.

systems that handle public data. Considering the proposed system as a whole, the rest of this section addresses parameters commonly identified in cybersecurity and data ethics:

### *A. Accountability*

Accountability can be defined in terms of both responsibility and liability. Accountability requires that there is an identified party who accounts for the way the system works and is capable of explaining the actions and decisions of the system. It encourages responsible behavior from both individuals and entities involved in the ecosystem. It also helps in identifying who is capable of fixing issues when things go wrong [18]. Linking transactions in a document's attestation to form a blockchain-recorded attestation chain simplifies audit history access and identifies parties responsible for unauthorized actions during attestation. Use of self-sovereign identity ensures that all interactions made between entities is audited securely in their wallet, generating a clear chain of consent and responsibility. Onboarding of all roles into the new system should include educating them regarding their roles and responsibilities in the system.

### *B. Fairness*

In the context of a blockchain and SSI based document verification system, fairness can be defined as ensuring that technology and protocols involved in the system do not discriminate users within the system. This involves creating and maintaining environment that provides equal opportunity for all users within the system to access and benefit from it without any bias or discrimination [19]. Importantly, such a system should not discriminate users based on their ability to access the technologies.

The system proposed in this paper provides wider access to create, submit and track information related to attestation process regardless of the geographical location. Although internet connectivity can pose challenges in areas with low to no connectivity, the system accommodates this by not hindering manual document verification process. An offline database can be integrated into the system to record non-sensitive details that need to be stored on blockchain. When connectivity is available, users can submit their transactions, thereby triggering the issuance of micro-credentials. This ensures continuous operation of attestation process.

### *C. Privacy*

Privacy is the control individuals have over their personal information. In the proposed system, users decide on the data in their micro-credential from the attesting entity, approving or rejecting it based on privacy concerns. This can be done based on the knowledge they gained during onboarding process about what data is required by the system and how their data is collected, used, stored, and protected. Blockchain is designed to ensure that the network of participants in the system has access to data and metadata stored in the blocks. So, it is important to ensure that data collected and stored on chain does not violate the privacy of any participant in the system [20]. Attesting entities cannot make decisions regarding what information is stored on the blockchain. Pre-defined smart

contract logic governs ensures that only necessary and sufficient is collected and stored on chain. Periodical auditing of information stored on the blockchain needs to be conducted by authorized entities to ensure that the system complies with required privacy regulations. A Data Protection Impact Assessment (DPIA) under Article 35 of GDPR (DPIA) is crucial in our system, despite recording only non-sensitive verification data on-chain and storing credential data in user-controlled wallets [21]. Ensuring GDPR compliance is vital to protect necessary information during interactions.

### D. Accuracy

Accuracy requires that personal information collected from users of the system should be correct. If information collected is time-sensitive, it is important to ensure that it has not become out-of-date. Maintaining accuracy is crucial not only to ensure integrity of the system but also for the trust users have on the system. Implementing robust mechanisms to verify data that is used by attesting entity to create micro-credential after performing verification or create and submit transactions on chain is correct and up-to-date is essential. Regular auditing of information on the blockchain is also required to verify and confirm that data on chain meets all ethical standards making it reliable and trustworthy [22].

### E. Right to be Forgotten

From the ethical point of view, the 'Right to be Forgotten' allows users to request the deletion or removal of their information when it is not longer necessary or relevant. The right to be forgotten gained importance following a lawsuit that led the European Court of Justice to rule that individuals could request search engines like Google to remove their irrelevant personal information from databases and search results [23]. It is usually assumed that immutability of information on blockchain completely hinders the right to be forgotten. However, this depends on the amount of information and type of information written into it. Selecting a minimal set of required identifiers and storing them on chain can mitigate the concern about right to be forgotten [22] to an extent. This is also applicable for decentralized registries maintained as part of SSI based system. Right to erasure does not apply to SSI based verifiable credentials since the controller of the credential is the individual themselves [24].

### F. Data Access and Ownership

In identity systems, access encompasses user interaction, the extent and timing of information access, authority over data access permissions, and mechanisms securing this access [22]. Transparent nature of blockchain does not expose any private information belonging to the user since the proposed system stores only non-sensitive details on chain. SSI based system empowers individuals with the control over their own data. Data ownership addresses the questions related to who owns the data used in the system for various processes. In the proposed system, users have authority over data generated and issued in the form of credentials to them. Since the data stored on chain can be used by multiple organizations across countries to verify data on attestation chain, a consensus group can be formed to ensure that the data is processed responsibly.

### G. Governance

Governance involves organization level decisions on who is responsible for different components of a system and decisions taken by the system. In a blockchain based system, governance is shaped by its centralized or decentralized authority structure and the degree of automation in decision-making. In our proposed system, which runs alongside the current semi-automated attestation process, the attesting entity manually verifies documents before deciding on their legitimacy. Decisions will be based on the existing government policies and regulations. Inclusion of reference to policies that led to their decisions can be recorded in the blockchain transaction to enhance transparency and trust.

## V. Conclusion and Future Work

We introduce a document verification system utilizing blockchain and self-sovereign identity (SSI) technology, aimed at enhancing transparency, traceability, and tracking of verification process from inception to completion. SSI technology ensures privacy for involved parties and secures information used in decision-making. Smart contracts, combined with blockchain's tamper-evident transparency, helps processes such as enforcement of pre-defined verification rules, dispute resolution, and assist attesting entities in generating transactions.

Future work involves conducting security risk assessments before development of the system. A thorough security risk assessment should identify and evaluate potential risks that can compromise system's security, and is crucial to identify parties responsible and liable for actions of the system. This helps in developing mitigation strategies to prevent the identified attacks on a system that involves blockchain and SSI components. If technical solution involves any third party services such as cloud servers, it is important to ensure that all accountable parties reach consensus and sign agreement regarding processing of user data [25]. Security risk assessment should also be performed before deployment to analyze the impact of security measures on performance of system in real world scenario.

A comprehensive scalability assessment will be conducted as part of future work, verifying the capacity of decentralized registry for storage and handling of DID information of all the roles in the system. The system's scalability will also be assessed for its ability to store non-sensitive attestation details on blockchain. This work should also include user testing: In a controlled environment, users will be able to engage with the system functionalities such as request for document verification, attestation and credential management. Feedback will be gathered systematically to evaluate user experience regarding system friendliness and overall satisfaction. This feedback is crucial to refine the system, identify and rectify usability issues, and improving the functionality of the system.

## REFERENCES


[1] W. D. Team, "Attestation." https://www.law.cornell.edu/wex/attestation. Accessed: 2023-12-19.

[2] A. Ayub Khan, A. A. Laghari, A. A. Shaikh, S. Bourouis, A. M. Mamlouk, and H. Alshazly, "Educational blockchain: A secure degree attestation and verification traceability architecture for higher education commission," *Applied Sciences*, vol. 11, no. 22, p. 10917, 2021.

[3] G. M. Alam, "Does online technology provide sustainable he or aggravate diploma disease? evidence from bangladesh—a comparison of conditions before and during covid-19," *Technology in Society*, vol. 66, p. 101677, 2021.

[4] "Forbes study on fake nursing degrees." https://www.forbes.com/sites/emmawhitford/2023/02/21/how-thousands-of-nurses-got-licensed-with-fake-degrees/. Accessed: 2023-12-18.

[5] B. Hartoyo and F. Noor, "The hague convention 1961: Solution of foreign public document legalization for indonesia and asean member countries," *ABC Research Alert*, vol. 7, no. 1, 2019.

[6] E. Fernando, C. Cassandra, H. A. E. Widjaja, Y. U. Chandra, H. Prabowo, *et al.*, "A blockchain technology-based for university student enrollment process," in *2020 6th International Conference on Computing Engineering and Design (ICCED)*, pp. 1–4, IEEE, 2020.

[7] S. Badlani, T. Aditya, S. Maniar, and K. Devadkar, "Educrypto: Transforming education using blockchain," in *2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 829–836, IEEE, 2022.

[8] J. C. Shah, M. Bhagwat, D. R. Patel, and M. Conti, "Crypto-wills: Transferring digital assets by maintaining wills on the blockchain," 2019.

[9] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *Ieee Access*, vol. 9, pp. 61048–61073, 2021.

[10] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021.

[11] S. N. Khan, F. Loukil, C. Ghedira-Guegan, E. Benkhelifa, and A. Bani-Hani, "Blockchain smart contracts: Applications, challenges, and future trends," *Peer-to-peer Networking and Applications*, vol. 14, pp. 2901–2925, 2021.

[12] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[13] "Nsa identity recommendations." https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3328152/nsa-releases-recommendations-for-maturing-identity-credential-and-access-manage/.

[14] C. Allen, "ssiprinciples." https://www.lifewithalacrity.com/article/the-path-to-self-soverereign-identity/. Accessed: 2023-12-19.

[15] D. C. C. C. P. O. S. T. v. Manu Sporny (Digital Bazaar), Dave Longley (Digital Bazaar), "W3c-verifiable credentials data model." https://www.w3.org/TR/vc-data-model-2.0/. Accessed: 2023-12-19.

[16] L. Pickard, D. Shah, and J. De Simone, "Mapping microcredentials across MOOC platforms," in *2018 learning with MOOCS (LWMOOCS)*, pp. 17–21, IEEE, 2018.

[17] A. G. Kim Hamilton-Duffy, Ryan Grant, "W3C DID Working Group." https://www.w3.org/2019/did-wg/. Accessed: 2023-12-19.

[18] V. Srivastava, T. Mahara, and P. Yadav, "An analysis of the ethical challenges of blockchain-enabled e-healthcare applications in 6g networks," *International Journal of Cognitive Computing in Engineering*, vol. 2, pp. 171–179, 2021.

[19] N. Naik, P. Grace, P. Jenkins, K. Naik, and J. Song, "An evaluation of potential attack surfaces based on attack tree modelling and risk matrix applied to self-sovereign identity," *Computers & Security*, vol. 120, p. 102808, 2022.

[20] O. Tene and J. Polenetsky, "To track or" do not track": Advancing transparency and individual control in online behavioral advertising," *Minn. JL Sci. & Tech.*, vol. 13, p. 281, 2012.

[21] "Data protection impact assessment." https://gdpr.eu/data-protection-impact-assessment-template/. Accessed: 2023-12-19.

[22] C. Lapointe and L. Fishbane, "The blockchain ethical design framework," *Innovations: Technology, Governance, Globalization*, vol. 12, no. 3-4, pp. 50–71, 2019.

[23] "Right to be forgotten case." https://www.bbc.com/news/world-europe-27388289. Accessed: 2023-12-19.

[24] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the gdpr," in *Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pp. 342–345, 2020.

[25] GDPR, "General data protection regulation." https://gdpr.eu/checklist/. Accessed: 2023-12-19.