Proceedings of the of the 17th Conference on Computer Science and Intelligence Systems pp. 685–694
DOI: 10.15439/2022F194
ISSN 2300-5963 ACSIS, Vol. 30

A Blockchain-Based Self-Sovereign Identity Approach for Inter-Organizational Business Processes

Amal Abid, Saousssen Cheikhrouhou, Slim Kallel, and Mohamed Jmaiel

***Abstract*—Blockchain presents a promising and revolutionary technology for organizations' collaboration, particularly for Inter-Organizational Business Processes (IOBP). It addresses the lack-of-trust problem thanks to its transparency and decentralized features. However, while the adoption of Blockchain technology can alleviate some of IOBP's challenges, it does so at the expense of significant privacy issues. In fact, some process execution data, such as customers' data or business secrets, cannot be shared across the collaborating organizations owing to regulatory restrictions such as the General Data Protection Regulation (GDPR). To address trust and privacy issues in IOBP, this paper presents a Blockchain-based Self-Sovereign Identity (SSI) approach. The SSI concept is combined with a registry proof smart contract to provide an efficient privacy-preserving solution. The proposed approach is applied to the pharmaceutical supply chain case study and implemented on the Ethereum Blockchain.**

***Index Terms*—Blockchain, BPMN, IOBP, Self-Sovereign Identity**

I. Introduction

BUSINESS processes have become the main factor of organizations to accomplish defined goals and to remain competitive in the dynamic marketplace. Collaboration between organizations, such as in supply chains, is considered essential in a business ecosystem in which organizations focus on their competitive strategy, perform only those operations for which they have expert skills, and enrich their services through partners and suppliers [1], [2].

In an Inter-Organizational Business Process (IOBP), independent organizations operate as collaborators and exchange messages to perform business transactions. This data exchange may be complicated, particularly when safety and confidentiality are intended to be first-class citizens. Collaborators expect to have access to complete process execution data and benefit from maintaining traceability. However, this is difficult to achieve in IOBPs since some process execution data such as customers' data or business secrets cannot be shared across the collaborating parties owing to regulations and confidentiality restrictions (e.g. General Data Protection Regulation (GDPR) [3]). Furthermore, there is an inherently lack-of-trust problem as organizations are mutually untrusted and IOBP execution can be prone to disagreements on counterfeiting operations. Additionally, IOBP can hardly be established efficiently, since companies generally rely on settled business processes and existing solutions. In fact, each party has managed information by building its own database. This has led to information silos, however, resulting in serious problems, particularly with respect to verification of data origins. Current systems use a centralized solution to organize their interoperability and cooperation. In this case, one of the actors will be the dominant partner in providing the solution and having access to the data. If instead, the parties choose a third-party solution, this would be costly and still prone to potentially exposing sensitive information.

Recently, Blockchain technology [4], [5] is proposed for IOBP execution to address the lack-of-trust problem, thanks to its nature as distributed, transparent and immutable ledger [6], [7], [8], [9]. While the adoption of Blockchain technology can alleviate some of these challenges, it does so at the expense of significant privacy issues. To overcome these problems, Blockchain can be leveraged in conjunction with Self-Sovereign Identity (SSI).

Self-Sovereign Identity (SSI) represents the recent evolution in identity management systems. In SSI systems, individuals have complete ownership and control over their data. These data that constitute an identity are known as Verifiable Credentials (VCs) and, unlike traditional systems, remain only with the individual. Verifiable credentials can also be owned by organizations as well as individuals. To protect privacy, SSI systems do not record transactions between interacting peers on ledger since they may include or reveal private information. Alternatively, the ledger is harnessed to verify claims using verifiable credentials.

In this line, some initial work is proposed for exploring the combination of Blockchain with Self-Sovereign Identity to address the issues highlighted above [10], [11], [12], [13], [14]. Unfortunately, these approaches focus particularly on the use of Blockchain-based SSI solutions for the customer side (business to customer (B2C)) and disregard their use between organizations (business to business (B2B)), and hence these approaches do not deal with IOBPs. Besides, these solutions do not address the lack of traceability concerns in SSI systems.

In this paper, we propose a Blockchain-based SSI solution for IOBP that ensures confidential inter-organization process execution while providing privacy-preserving traceability.

The main contributions of this paper can be summarized as follows :

- Propose an interoperable SSI interface between inter-organizational processes that exposes its functionality to the cooperative organizations through a common API.

A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel are with ReDCAD, ENIS, University of Sfax, Sfax, Tunisia

The objective of the proposed SSI interface is to enable confidential collaboration between organizations by providing confidential end-to-end processes without exposing any sensitive data on-chain. It also supports the use of existing systems and databases while incorporating Blockchain technology as a reference for inter-organizational process interaction.
- Propose a Transaction (Tx) Registry Proof that maintains traceability in a private manner. In particular, this Registry Proof records the hash of transactions as well as Decentralized Identifiers (DIDs) of collaborating organizations in the Blockchain to ensure integrity. This can be used as a privacy-preserving trace to validate afterward that a collaborative task was performed in case of conflicts or audits.

To validate the feasibility of the proposed approach, we applied it to a pharmaceutical supply chain as a case study. In fact, the pharmaceutical supply chain is a vastly diversified and complex ecosystem, in which, the secure management of identity and private data is a typical concern. More Precisely, collaborating entities could identify their partners and interact with them using Verifiable Credentials for compliant transactions and information disclosures. This paper also provides an initial implementation and execution. An experimental evaluation shows that the implementation can achieve good results with low gas costs as well as low latency.

The remainder of this paper is organized as follows : Section II briefly introduces some concepts upon which our work is built. Section III explains the proposed approach. Section IV illustrates the pharmaceutical supply chain case study. Section V presents a proof-of-concept implementation. Section VI evaluates our approach. Section VII summarizes related work, and section VIII concludes and suggests future directions.

II. Background

This section introduces the main concepts and definitions related to Self-Sovereign Identity (SSI).

Digital identities in today's world rely on the username-password combination method or the federated identity management method. Users are struggling to handle the growing number of passwords within the username-password combination method. Besides, they are vulnerable to password theft techniques including phishing, key-logging, viruses, and malware. They are also unable to efficiently transfer identity-related information from one account to another, and they must go through the hard registration procedure repeatedly, disclosing ID cards, driver's licenses, bank account details, and other personal information [15].

On the other hand, the federated identity management method attempts to alleviate some of these drawbacks with Single Sign-On platforms that transfer identity-related information between services that are linked to the platform. However, users are obliged to accept the terms and conditions because, otherwise, they will be unable to use the system. Additionally, during registration, users should disclose a significant amount of personal information, which causes privacy issues. This personal information is not protected from unauthorized secondary use [13].

Self-sovereign Identity (SSI) represents the latest evolution and most current stage of digital identities, which is designed to address the issues of all previous stages. Thanks to SSI, users have full control over their data when using enterprises' systems. Besides, they can share only the required piece of information with their consent.

SSI's standards, architecture, and lifecycle are presented as follows.

A. SSI Standards

SSI is based on two standardized pillars. Decentralized Identifiers (DIDs) and their cryptographic counterparts, Verifiable Credentials (VCs), provide a decentralized and privacy-preserving form of digital identity.

- **Decentralized Identifier:** A decentralized identifier (DID) is an innovative type of globally unique identifier created by the World Wide Web Consortium (W3C) working group [16]. The DIDs approach has proven to be popular for associating a globally unique identifier to cryptographic keys and other interaction metadata necessary to prove control of the identifier.
- **Verifiable Credential:** A credential is a document that details the qualification, ability, or authority granted to an individual by a third party having the requisite authority or assumed ability. For example, a driver's license is used to prove that a person is capable of driving a vehicle, a university degree can be used to prove the education level of a person, and a government-issued passport permits people to travel between nations. These physical credentials may include information related to the identifier (e.g., identification number, photo), the issuing authority, particular attributes asserted by the issuing authority, and credential constraints. All the same information that a physical credential represents can be represented by a verifiable credential (VC), defined as a tamper evident credential that has authorship which can be cryptographically verified. The Verifiable Credential Data Model specification became a recommended standard by W3C in 2019 [16].

B. SSI Architecture

Figure 1 depicts the SSI architecture. In this architecture, there are three principal roles: issuer, verifier, and holder. They are briefly presented below:

- **Issuer:** An entity that creates claims within a VC about a subject. Such an entity can be organizations like governments, universities, but also private individuals or objects such as sensors. An issuer transfers VCs to holders.
- **Holder:** An entity that requests or receives VCs from issuers and maintains them in a credential repository/ digital wallet. A holder may not always be the (credential) subject. For example, a parent (holder) holding VCs for its child (subject) or a friend (holder) obtaining a prescription at the pharmacy for its sick friend (subject).

Holders can also create Verifiable Presentations (VPs) from Verifiable Credentials and disclose them to a verifier.

- **Verifier:** An entity that intends to verify specific attributes or claims of a subject. It may receive these in the form of VP, which may include those claims from one or more VCs. However, holders have control at all times over which attributes are transferred to the verifier.

As a recent SSI development, DID Communication (DIDComm) [17] presents an asynchronous encrypted communication protocol. It establishes a cryptographically secure channel for any two software agents (peers) to interact directly or via intermediary cloud agents. In DIDComm, peers who are parties to the connection are individually responsible for the generation of their DID, the key pairs in a DID document, and the subsequent key rotation or revocation of those keys. DIDComm uses information from the DID document, such as the public key and its associated endpoint, to exchange secure messages. It enables distinct entities to connect with each other in a peer-to-peer manner, eliminating the need for a middleman.

This credential exchange protocol supports zero-knowledge proof (ZKP) cryptography using the Camenisch-Lysyanskaya (CL) signature scheme, which enables credential holders to selectively reveal claims to verifiers without any linkage.

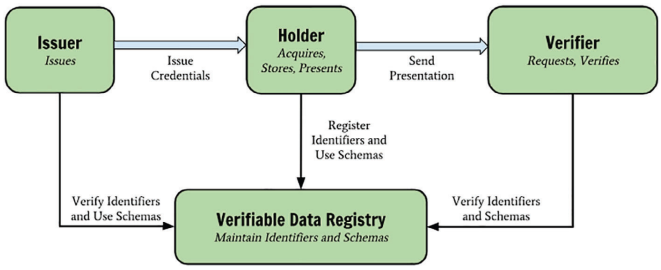

Fig. 1: SSI Architecture [16]

C. SSI Lifecycle Process

The lifecycle of a VC with Camenisch-Lysyanskaya (CL) signature which enables the zero-knowledge proof (ZKP) is detailed as follows:

- The issuer specifies the credential's schema, publishes the credential definition which indicates the intention to post a credential from schema X, signed using key Y, and with revocation strategy Z.
- The issuer generates a DID and correlates it with a public-private key pair. Afterwards, the issuer generates a DID document, signs it, and publishes it to the distributed ledger.
- The issuer collects all the information it intends to include in the credential, containing the information for each attribute specified in the schema defined previously. The issuer constructs the credential by creating a numeric representation of each field and then signs the numeric as well as the text formats of each of the claims using the CL Signature.
- The credential anchors a "link secret" that is known only to the holder (recorded in the holder's wallet), and when a credential is issued to the holder, it encapsulates a cryptographic promise to the "link secret" within another long number that the issuer serves as the credential ID. The "link secret" acts similarly to a watermark stamp. Therefore, the certificate's content is extremely difficult to falsify, proving that the holder owns the stamp and is able to create such a watermark.
- Once the holder owns the VC in his/her digital wallet, he/she can communicate with a verifier and may seek to prove a set of claims created by a specific issuer regarding a subject. The holder receives a request from the verifier for the type of credential it is looking for.
- The holder conducts certain calculations on the VC to prepare it for sharing in a proof presentation. The holder creates a new, never-before-seen credential wrapped inside a proof presentation. This later aggregates and discloses whatever attributes from issued credentials are requested, as well as any predicates, while hiding everything else. The 'proof' block of this new VC is a mathematical proof that the holder actually owns VCs signed by the appropriate issuer, containing the revealed attributes, and conforming to the specified schema.
- The proof also proves that the issuer has not revoked the credentials and that they are bound to the holder because the holder knows the "link secret" that was utilized at issuance. Afterwards, the verifier uses the information received from the holder in the form of a proof presentation to do certain calculations. It should cryptographically verify the validity of the proof. The verifier resolves the issuer's DID and identifies its public key. Then, using the issuer's public key, it validates the provided attributes. The presentation proof may comprise attributes from more than one credential. For each shared attribute, the verifier checks its corresponding credential schema, as well as the issuer's DID/DID document. It employs these two pieces of information to verify the presentation attribute. Each attribute statement in the proof presentation must follow this process. The verifier can be assured that all of the attributes are issued to the holder of the same "link secret".

III. Blockchain-Based SSI Approach for IOBP

This section provides a detailed description of the proposed approach. This description covers the proposed platform, the involved actors as well as the main process to ensure a secure IOBP communication (see Figure 2).

The main objective of the proposed Blockchain-based SSI solution is to ensure confidential inter-organization process execution while providing privacy-preserving traceability.

A. Platform components

The proposed platform includes three main components: an SSI interface, a private permissioned Blockchain and a Registry Proof smart contract which are described as follows.

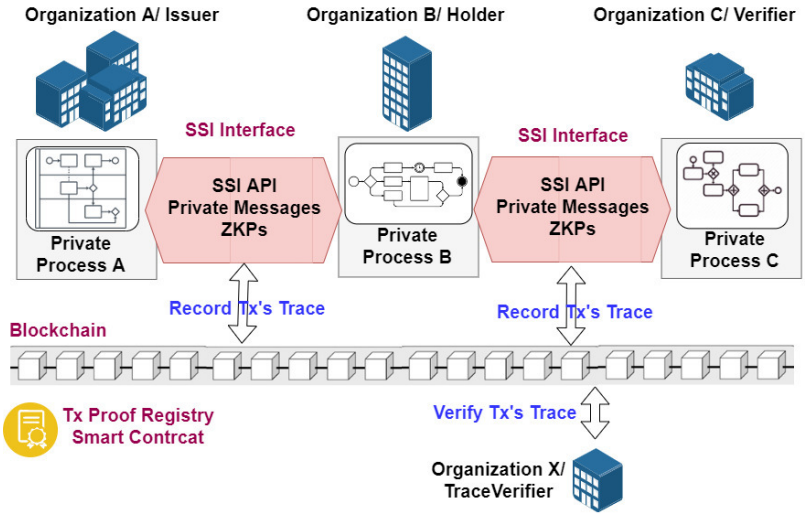

Fig. 2: Proposed approach Overview

- **SSI Interface:** The SSI Interface between processes involved in the inter-organizational process presents modular libraries and APIs for Decentralized Identifiers (DID) and Verifiable Credentials (VC). It exposes its functionality to the cooperative organizations through a common interface API (i.e. RESTful API) to ensure interoperability. Therefore, collaborative organizations can keep using existing systems and databases while integrating this RESTful API as a common interface. The proposed SSI interface is aligned with the W3C specification and ensures JWT-based VC issuance, Selective Disclosure Request (SDR), and Verifiable Presentations (VP).
  Through the proposed SSI interface, each organization can present a DID document maintaining verification methods (i.e. public keys) and service endpoints (e.g., details of messaging service) that other organizations can use to establish interactions. Thus, before engaging in any formal activity in a relationship, two organizations should first mutually resolve each other's DID and acquire the interaction information preserved in the DID document.
- **Private permissioned Blockchain:** The proposed platform relies on Ethereum [5] private permissioned Blockchain (i.e. Ethereum Private net) to allow only authorized users to access to the system by verifying their cryptographic keys. Furthermore, in the proposed platform, the Blockchain serves as a tamper-proof verifiable data registry as well as transactions' proof registry.
- **Registry Proof Smart Contract:** The transactions' Proof Registry smart contract is proposed to record transactions' trace. Indeed, SSI systems do not offer a native way to record issuance and verification transactions on the Blockchain in order to ensure privacy and protect sensitive data. This can present a gap when audits are needed. Therefore, we propose to record only DIDs of interacting organizations as well as transaction hash to maintain a privacy-preserving trace. The data itself is stored locally off-chain for private process execution.
  While the proposed approach requires the use of a permissioned Blockchain, a public Blockchain may also be used as a shared reference between collaborative organizations by recording the hash of each DID and the transaction hash.

B. Involved Actors

Many actors are involved in our proposed approach:

- **Organizations:** In the proposed approach, each organization can play the role of issuer, holder or verifier when taking part in an inter-organizational process.
  - **Issuer** (i.e., Organization A): When an organization issues a verifiable credential, its DID is associated with this credential for further verification. Here the issuer is trusted by different actors belonging to the permissioned Blockchain.
  - **Holder** (i.e., Organization B): An organization has full control over its data including sensitive information and any request for accessing these data must necessarily require its confirmation.
    When performing a collaborative process, an organization can use the Selective Disclosure concept, during message exchange, to share selected pieces of information with interacting parties.
  - **Verifier** (i.e., Organization C): An organization can verify the origin of exchanged data by checking digital signatures. Hence, it can confirm the validity and authenticity of shared verifiable credentials.
- **Trace Verifier:** A Trace Verifier is an authorized organization (i.e., Organization X) that has access to the trace provided by the Tx Registry Proof. It can check if an inter-organizational task/activity (i.e., exchange of message) was performed between collaborating parties.
  We note here that the TraceVerifier is distinct from the Verifier role belonging to the SSI concept.

In the proposed solution architecture, each role may have multiple instances (i.e., multiple participating issuers, holders, verifiers, and trace verifiers).

C. Process flows

Figure 3 depicts the overview of the interaction between different actors involved in our proposed approach as a BPMN collaboration diagram.

The main interactions are as follows: An Organization A (i.e., Issuer) issues verifiable credentials to an Organization B (i.e., Holder) through message exchange in an inter-organizational collaboration. Afterwords, these verifiable credentials can be presented to an Organization C (i.e., Verifier) which confirms the validity and authenticity of data by verifying the signature of the issuer. The Tx Proof Registry records the transaction hash and the DIDs of interacting parties for both issuance and presentation activities. Consequently, an authorized Organization X (i.e., TraceVerifier) can check if the transaction between collaborating parties is performed.

Listing 1 illustrates the algorithm of the inter-organizational process of data exchange and storage.

This algorithm depicts a secure and private DIDComm between three cooperating organizations. An Organization A (i.e., Issuer) first encrypts and signs a message for Organization B (i.e., Holder). The signature and the cipher text are then sent through organization A's endpoint to organization B's endpoint. The authenticity of the message can be checked, by an Organization C (i.e., Verifier) before executing an IOBP, by resolving the DID and identifying whether it matches organization A's public key. All mentioned interactions are recorded in a privacy-preserving way on a Tx Proof Registry for further traceability by any authorized Organization X (i.e., Trace Verifier).

```
1. A process task exchanges DIDs with an Organization A (Org_A) (i.e. Issuer) to establish a DIDComm connection channel.
2. The Issuer employ the public key of the AES encryption scheme (pk_aes) to encrypt the data.
3. Data Issuer issues Verifiable Credential data (vc_data) to the process task with the (pk_aes) as an attribute of the credential.
4. Process task accepts and stores the Verifiable Credential in the Organization B (Org_B) (i.e. Holder) wallet.
5. The hash of the transaction (trans_proof) as well as Organization A (Org_A) and Organization B (Org_B) DIDs are stored on the Proof Registry.
6. Organization B (Org_B) exchange Verifiable Credential data with Organization C (Org_C) through a collaborative process within a DIDComm connection channel.
7. Organization C (Org_C) verifies the Proof Data by checking the signature and DID of the Issuer.
8. If proof data has been verified then
   . Execute the current IOBP
   . Store the hash of the transaction (trans_proof) as well as Organization B (Org_B) and Organization C (Org_C) on the Proof Registry.
9. An Organization X (Org_X) (i.e. TraceVerifier) can request transaction proof from the Proof Registry.
10. The TraceVerifier Evaluate the transaction proof and send the evaluation result for underlying organizations
```

Listing 1: Algorithm of SSI applied to IOPB

IV. Case Study: Pharmaceutical Supply Chain

The pharmaceutical supply chain is a diversified and complex ecosystem, in which the secure management of identity and sensitive data is a typical issue.

The Drug Supply Chain Security Act (DSCSA) [18] enforces specific requirements on different types of stakeholders: manufacturers, repackagers, wholesale distributors, third-party logistics providers (3PLs), and pharmacies [19]. One such requirement is an extended Know Your Customer' regulation, which requires each entity to confirm that their partners are also authorized. In many situations, the regulation requires interactions between entities without any direct business relationship.

Therefore, to enable interoperability and trust, the pharmaceutical supply chain community has harnessed the power of Blockchain and Decentralized Identifiers (DIDs). Together, they provide all parties with a 'single source of truth' to address challenges, such as master data management and counterfeit detection. At a more essential level, different entities must be able to identify their partners and interact with them using Verifiable Credentials for compliant transactions and information disclosures.

The specific goals of this case study are: (i) authentication of a verification request with a verifiable credential, and (ii) enhanced verification between pharmacies and manufacturers.

Figure 4 shows a simplified model of the pharmaceutical supply chain as a BPMN collaboration diagram. The diagram contains seven pools, one for each involved parties: Raw Material Manufacturer, Pharmaceutical Manufacturer, Hospital Pharmacy, Hospital Healthcare Professional, Patient, Tx Proof Registry, Higher Authority of Drugs, and Pharmaceutical Industry (HADPI).

This diagram depicts many examples of data exchange between cooperative organizations, in which we use verifiable credentials' issuance and verification, such as *Raw Material Credentials*, *Pharmaceutical Credentials*, and *Product Credentials*.

We use colors to explain different roles and interactions. For example, the red color designates the issuance of *Raw Material Credentials* by the *Raw Material Manufacturer* which acts as an Issuer. These credentials are issued to the *Pharmaceutical Manufacturer* which plays the role of Holder. This issuance transaction is recorded in the Tx Proof Registry after its completion. The yellow color highlights how the *Pharmaceutical Manufacturer* can become an Issuer of the *Pharmaceutical Credentials*, while the *Hospital Pharmacy* acts as a Holder. The same interaction is performed between the *Hospital Pharmacy* and the *Hospital Healthcare Provider* (green color). Finally, the *Hospital Healthcare Provider* prepares a Verifiable Presentation to the *Patient* that contains *Pharmaceutical Product Claims* (blue color). Here the *Hospital Healthcare Provider* plays the role of a Holder while the *Patient* acts as a Verifier.

All issuance and verification transactions are recorded on the Tx Proof registry. Consequently, the HADPI can play the role of Trace Verifier, and thus check if transactions are performed between interacting parties.

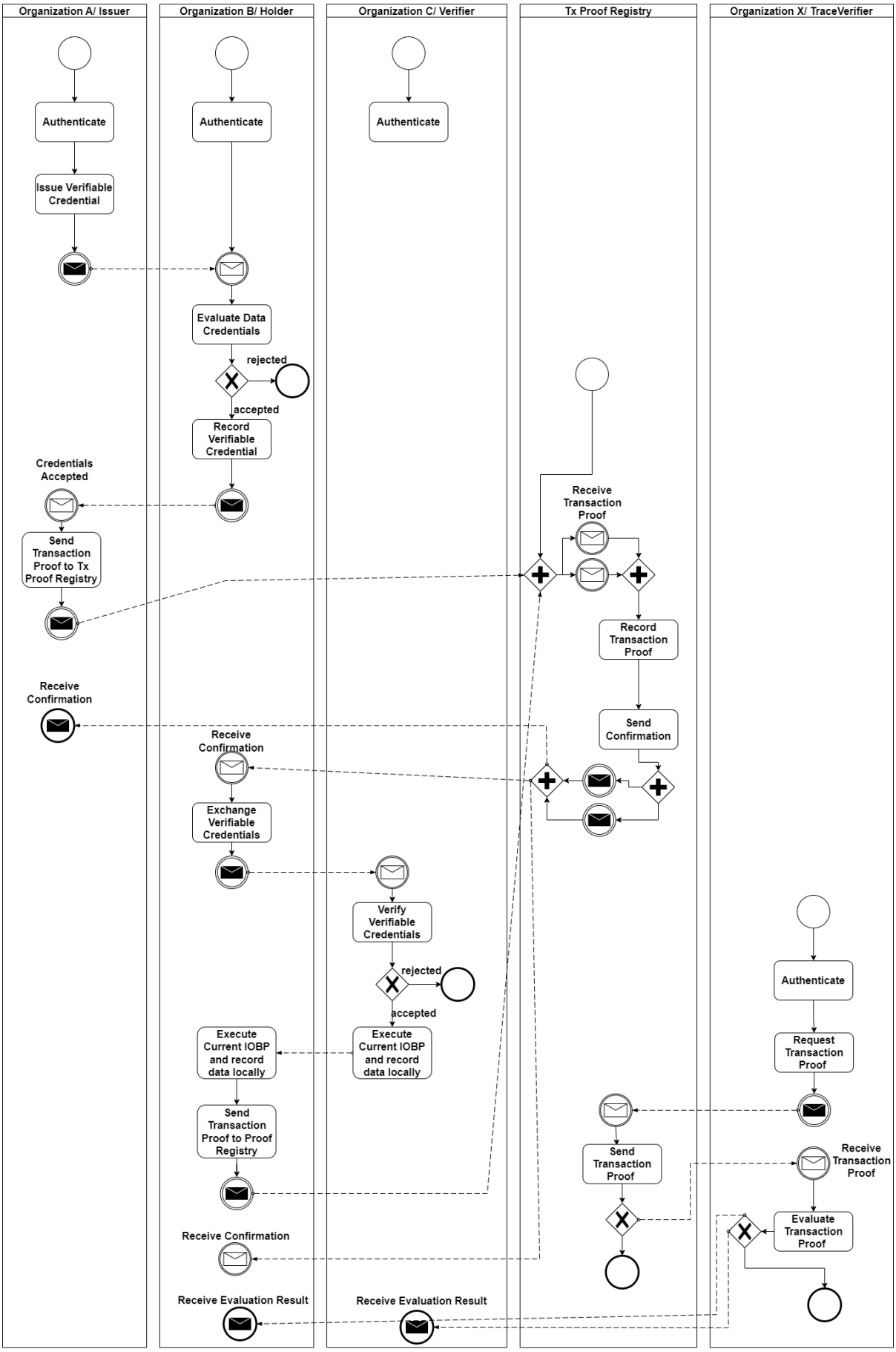

Fig. 3: Generalized BPMN diagram

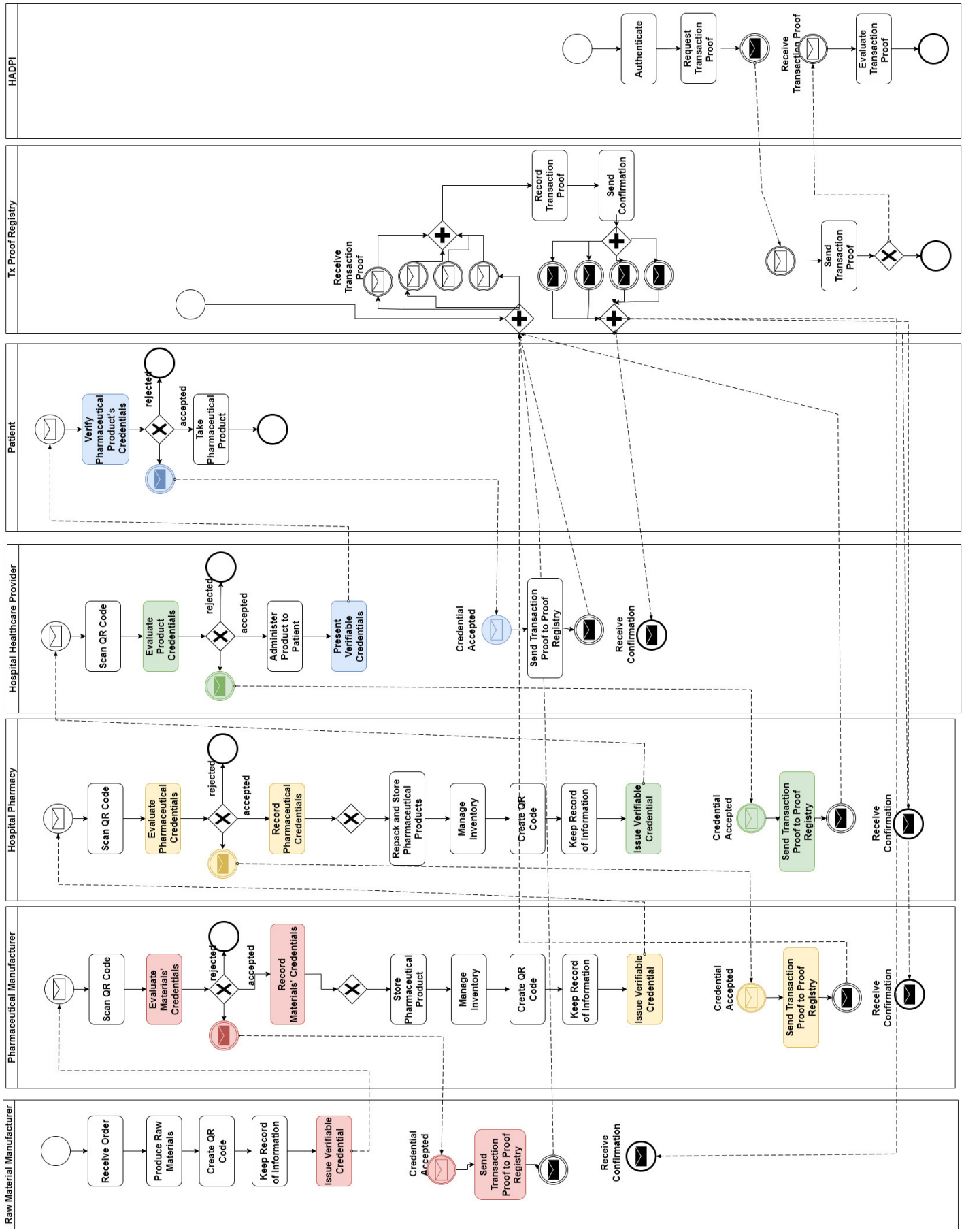

Fig. 4: Pharmaceutical Supply Chain's BPMN diagram

V. Implementation

This section presents the implementation of the proposed Blockchain-based SSI approach for IOBP. In particular, we detail the implementation of both the SSI interface and the Tx Proof Registry smart contract.

A. SSI interface

In order to implement the SSI interface, we use Veramo [20], an open-source set of modular libraries and APIs for SSI and verifiable credentials. Veramo exposes its functionalities to the cooperative organizations through a common RESTful API. Therefore, collaborative organizations can keep using existing systems and databases, while integrating Veramo RESTful API as a common interface. Additionally Veramo's API is aligned with the W3C specification, and it supports the creation of Ethereum-based and web-based DIDs as well. Besides, the SSI interface ensures JWT-based VC issuance, Selective Disclosure Request (SDR) and Verifiable Presentations (VP).

The first step towards using and accessing the methods of Veramo API is to create a Veramo Agent and export it in the 'VeramoSetup.ts'. As a result, this Agent can be imported and used in the proposed SSI interface. Listing 2 shows an excerpt of the implementation of the Veramo Agent.

```
// Core interfaces
import { createAgent, IDIDManager } from "@veramo/core";
// Core identity manager plugin
import { DIDManager } from "@veramo/did manager";
// Credential Issuer
import { CredentialIssuer, ICredentialIssuer } from "
    @veramo/credential w3c";
export const veramoAgent = createAgent<IDIDManager &
    IKeyManager & IDataStore & IResolver & ... >({ plugins:
     [  new KeyManager({
store: new KeyStore(dbConnection, new SecretBox(secretKey)
    ),
kms: {local: new KeyManagementSystem(), },
}),
new DIDManager({ store: new DIDStore(dbConnection),
    defaultProvider: "did:key",
 providers: { "did:key": new KeyDIDProvider({ defaultKms:
    "local",})}
}),
new DIDResolverPlugin({ resolver: new Resolver({ key:
    getDidKeyResolver().key, getUniversalResolverFor(["io",
     "elem", "sov"]), }),
}),
new CredentialIssuer(),
new MessageHandler({ ... }),
 ]});
```

Listing 2: Excerpt of the Creation of Veramo Agent

To construct the agent, all required plugins must be imported as libraries (Listing 2 lines 1-6) and taken into consideration when the object is initialized (Listing 2 lines 7-18).

After its creation, the Veramo Agent provides basic methods for creating Verifiable Credentials, Verifiable Presentations, verifying messages like JWT credentials and sending presentation requests as Selective Disclosure Requests.

Listing 3 shows an excerpt of the creation of a VC using the Veramo Agent.

```
async issueVerifiableCredential(body:
    IssueCredentialRequest, toWallet: boolean): Promise<
    IssueCredentialResponse> {
 try {
 body.credential.issuer = {id: body.credential.issuer.
     toString()};
 const save: boolean = body.options.save?body.options.save:
     false;
 const credential: W3CCredential = body.credential;
 const verifiableCredential: W3CCredential = await
     veramoAgent.createVerifiableCredential({ save: false,
     credential, proofFormat: "jwt", });
 // Prepare response
 const result: IssueCredentialResponse = { credential:
     verifiableCredential,};
if (toWallet) {
 try { // Send VC to another Veramo agent
 const msg = await veramoAgent.sendMessageDIDCommAlpha1({
     save: true,
  data: { from: verifiableCredential.issuer.id,  to:
     verifiableCredential.credentialSubject.id, type: "jwt",
      body: verifiableCredential.proof.jwt, }, });
 result.sent = true;
 return result;
} catch (error) {
 return error; }
 }
 return result;
 } catch (error) {
 return error; }
 };
```

Listing 3: Excerpt of the Creation of a VC using the Veramo Agent

The credential object is prepared first (Listing 3 Lines 3-5), and then transformed to a VC using Veramo Agent's methods (Listing 3 line 6). Afterwards, the API response is prepared with the newly created VC (Listing 3 lines 8-10). If an error occurs during issuance, the error is returned as a response to the requester. Alternatively, if the API request specify that the VC should be sent directly to the DID's agent through the messaging endpoint (Listing 3 lines 11-16), it would be handled using the "sendMessageDIDCommAlpha1()" method.

Note that the source code of the proposed SSI interface is available on Github in [21].

B. Tx Proof Registry Smart Contract

The proposed Tx Proof Registry Smart Contract provides a privacy-preserving trace of SSI transactions. Indeed, SSI issuance and verification transactions need to be persistently recorded in a private manner for further verification (i.e. check if these transactions are actually performed). An excerpt of the proposed smart contract is presented in listing 4. It records both DIDs of interacting organizations as well as transaction hash.

```
event recordTrace ( address indexed sender , address
    indexed receiver ,
bytes32 txHash)
```

Listing 4: Excerpt of the Proposed Tx Proof Registry Smart Contract

While the proposed approach requires the use of a permissioned Blockchain, a public Blockchain may also be used as a shared reference between collaborative organizations. In this case, we recommend recording the hash of each DID instead of directly recording the DIDs on-chain (see listing 5).

```
event recordTrace ( bytes32 indexed sender , bytes32
    indexed receiver ,
bytes32 txHash)
```

Listing 5: Excerpt of Tx Proof Registry Smart Contract for public Blockchain

VI. Evaluation

This section evaluates the proposed approach and shows its feasibility and efficiency for adoption within a real-world environment including both financial cost and response time.

A. Financial Cost

Transactions on Ethereum Blockchain are subject to a certain fee. Ethereum employs a unit known as gas to calculate the amount of operations required to complete a task such as deploying a smart contract or executing an ABI function. It is always necessary to estimate gas consumption when implementing a smart contract in order to avoid unexpected costs. Therefore, storing data directly on-chain suffers not only from privacy issues but also from being costly.

In the proposed Tx Proof Registry smart contract, only the DIDs of interacting organizations and the hash of the transaction are recorded on-chain, the data itself is stored locally off-chain for private process execution. Table I shows the transaction cost for the execution of 'recordTrace' fucntion as well as the deployment of the Tx Proof Registry smart contract.

TABLE I: Operations' Gas Cost

Operation	Gas
Tx Proof Registry Smart Contract Deployment	362,525
Record Trace ABI call	64,384

B. Response time

The proposed approach is dependent on Ethereum Blockchain's latency. In fact, despite the reduction of data-size recorded on-chain, storing DIDs and transactions' hashes on-chain leads to some overheads. These overheads can be tested by sending simultaneous requests to the Tx Proof Registry Smart Contract. Figure 5 depicts the completion time in seconds (Y axis) of the "TraceRecord" operation where we send between 1 and 800 simultaneous requests (X axis).

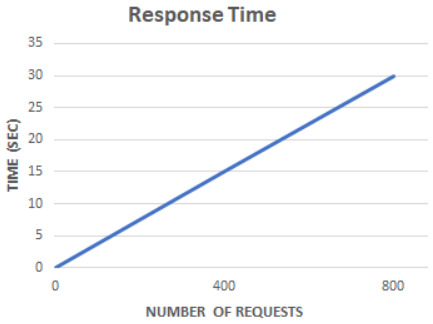

Fig. 5: Response Time Evaluation

To sum up, the experimental evaluation shows that the implementation can achieve good results with low gas costs as well as low latency.

VII. Related Work

This section provides an overview of the existing solutions for secure inter-organizational collaborations.

Authors in [10] proposed a distributed Private Data System (PDS) to achieve self-sovereign storage and sharing of private data between multiple organizations through executable choreographies. The users have complete control over their private data and are allowed to share and revoke access to organizations at any time. However, PDS does not leverage the power of Blockchain technology to address consensus problems in a distributed environment. Instead, the PDS's system is composed of nodes spread across the entire Internet managing local key-value databases. This could present a complex infrastructure and require some effort, thus may be inefficient for individuals.

Another interesting work that exploited the strength of the Blockchain technology to ensure privacy-preserving inter-organizational collaborations is proposed in [11]. Authors presented, ID-Service, a platform for designing, implementing, and executing Cross-Organization Workflows' services. It adheres to the concept of security by design in terms of trust, accountability, non-repudiation, and the system's capacity to offer forensic proof of workflow traces, critical actions, and actors' responsibilities and to maintain these features during execution. However, ID-Service does not implement the Self-Sovereign Identity (SSI) model. Consequently, it does not afford any flexibility for identity's self-possession and control.

The SSI approach has mostly been explored in the field of security, privacy, and distributed systems, with little attention paid to information systems research and process perspective. At present, there are only a few academic papers on the application of SSI in business scenarios. They include the application of SSI in know-your-customer processes in banking [22], remote management of industrial equipment [23], payback programs in retail [12], student exchange [24], e-petitions [25], access to public health services [26], assigning medical information to persons without regular identity, e.g. to combat COVID-19 [27]. The majority of these studies represent typical business processes that consider in particular the Consumer-to-Business relationship and omit dealing with inter-organizational collaborations (i.e. Business-to-Business (B2B)). For instance, authors in [12] introduced an SSI-based system for incentivized and self-determined customer-to-business data sharing in a local economy context. Here consumers are not only the owners of their data, but also they can choose what to share and in which granularity to trade their data for financial rewards. In the same direction, authors in [13] presented SSI as a solution to deal with privacy-preserving licensing of individual-controlled data to avoid unauthorized secondary customers' data usage.

The majority of the aforementioned approaches use the SSI concept to ensure data privacy and omit to propose a privacy-preserving solution to trace SSI transactions for further audit requirements. This is presented in a very broad sense in [14]. Authors proposed the concept of a proof registry through a set of technical components, data structures, and process flows, that ensures that proof data can be validated in

case of disputes or audits. However, authors did not provide any implementation nor an example of a smart contract to illustrate/show how the traceability is performed. Besides, authors do not provide a solution for inter-organizational process execution.

Unlike all cited previous work, the proposed approach provides a Blockchain-based SSI solution for inter-organizational processes. Particularly, it proposes an interoperable SSI interface between collaborating organizations as well as a privacy-preserving proof registry for further audits and verification.

VIII. Conclusion

In this paper, we proposed a Blockchain-based SSI approach for IOBP. It ensures confidential inter-organization process execution, particularly inter-organization message exchange without exposing any sensitive information on-chain. The SSI concept is combined with a proof registry smart contract to provide a privacy-preserving trace for further audit verification.

In future work, we aim to enhance the proposed proof registry to enable enriched analysis on private data for authorized organizations.

References

[1] R. Wehlitz, F. Jauer, I. Rößner, and B. Franczyk, "Increasing the reusability of iot-aware business processes." in *Proceedings of the Conference on Computer Science and Information Systems (FedCSIS)*, 2020, pp. 17–22.

[2] M. Nizioł, P. Wisniewski, K. Kluza, and A. Ligeza, "Characteristic and comparison of uml, bpmn and epc based on process models of a training company," in *Proceedings of the Conference on Computer Science and Information Systems (FedCSIS)*, vol. 26, 2021, pp. 193–200.

[3] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, no. 3152676, pp. 10–5555, 2017.

[4] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Cryptography Mailing list*, 2008.

[5] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum project*, vol. 151, pp. 1–32, 2014.

[6] O. López-Pintado, L. García-Bañuelos, M. Dumas, I. Weber, and A. Ponomarev, "Caterpillar: A business process execution engine on the ethereum blockchain," *Software: Practice and Experience*, vol. 49, no. 7, pp. 1162–1193, 2019.

[7] A. B. Tran, Q. Lu, and I. Weber, "Lorikeet: A model-driven engineering tool for blockchain-based business process execution and asset management." in *Proceedings of the BPM Demo Track and BPM Dissertation Award co-located with the International Conference on Business Process Modeling (BPM)*, 2018, pp. 56–60.

[8] O. López-Pintado, M. Dumas, L. García-Bañuelos, and I. Weber, "Controlled flexibility in blockchain-based collaborative business processes," *Information Systems*, p. 101622, 2020.

[9] A. Abid, S. Cheikhrouhou, and M. Jmaiel, "Modelling and executing time-aware processes in trustless blockchain environment," in *Proceedings of the International Conference on Risks and Security of Internet and Systems*, 2019, pp. 325–341.

[10] S. Alboaie and D. Cosovan, "Private data system enabling self-sovereign storage managed by executable choreographies," in *Proceedings of the International Conference on Distributed Applications and Interoperable Systems (IFIP)*. Springer, 2017, pp. 83–98.

[11] L. Argento, F. Buccafurri, A. Furfaro, S. Graziano, A. Guzzo, G. Lax, F. Pasqua, and D. Saccà, "Id-service: A blockchain-based platform to support digital-identity-aware service accountability," *Applied Sciences*, vol. 11, no. 1, p. 165, 2020.

[12] K. Wittek, L. Lazzati, D. Bothe, A.-J. Sinnaeve, and N. Pohlmann, "An ssi based system for incentivized and selfdetermined customer-to-business data sharing in a local economy context," in *Proceedings of the IEEE European Technology and Engineering Management Summit (E-TEMS)*. IEEE, 2020, pp. 1–5.

[13] M. Kang and V. Lemieux, "A decentralized identity-based blockchain solution for privacy-preserving licensing of individual-controlled data to prevent unauthorized secondary data usage," *Ledger*, vol. 6, 2021.

[14] V. Lemieux, A. Voskobojnikov, and M. Kang, "Addressing audit and accountability issues in self-sovereign identity blockchain systems using archival science principles," in *Proceedings of the IEEE Computers, Software, and Applications Conference (COMPSAC)*. IEEE, 2021, pp. 1210–1216.

[15] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital identities and verifiable credentials," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, 2021.

[16] V. C. W. Group, "Decentralized identifiers (dids) v1.0. world wide web consortium (w3c) (2020) [online]. available: https://www.w3.org/tr/vc-imp-guide/."

[17] DID, "Didcomm messaging [online]. available: https://github.com/decentralized-identity/didcomm-messaging."

[18] DSCSA, "Drug supply chain security act (dscsa) [online]. available: https://www.fda.gov/drugs/drug-supply-chain-integrity/drug-supply-chain-security-act-dscsa."

[19] V. Dods and B. Taylor, "A proposal for decentralized, global, verifiable health care credential standards grounded in pharmaceutical authorized trading partners," *Blockchain in Healthcare Today*, 2021.

[20] Veramo, "Performant and modular apis for verifiable data and ssi [online]. available: https://veramo.io/."

[21] A. Abid, "Ssi4iobp [online]. available: https://github.com/amal-abid05/ssi4iobp."

[22] R. Soltani, U. T. Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," in *Proceedings of the IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018, pp. 1129–1136.

[23] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, "Self-sovereign identity: Use-cases, technologies, and challenges for industrial iot," in *Proceedings of the IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, 2019, pp. 1173–1180.

[24] P. Kavassalis, "Designing an academic electronic identity management system for student mobility using eidas eid and self-sovereign identity technologies," 2020.

[25] R. Karatas and I. Sertkaya, "Self sovereign identity based e-petition scheme," *International Journal of Information Security Science*, vol. 9, no. 4, pp. 213–229, 2020.

[26] D. W. Chadwick, R. Laborde, A. Oglaza, R. Venant, S. Wazan, and M. Nijjar, "Improved identity management with verifiable credentials and fido," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 14–20, 2019.

[27] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "Novidchain: Blockchain-based privacy-preserving platform for covid-19 test/vaccine certificates," *Software: Practice and Experience*, vol. 52, no. 4, pp. 841–867, 2022.