



Article

Digital Transformation in the Construction Sector: Blockchain, BIM and SSI for a More Sustainable and Transparent System

Luisanna Cocco * and Roberto Tonelli

Department of Mathematics and Computer Science, University of Cagliari, 09124 Cagliari, Italy; roberto.tonelli@unica.it

* Correspondence: cocco@unica.it

Abstract: This article presents a model built for deep digitalization in the construction industry and for making building information modeling achieve a greater level of transparency, verifiability and effectiveness for the benefit of all stakeholders. Thanks to blockchain and the self-sovereign identity paradigm, the model guarantees data integrity and transaction reliability, enabling the generation of more efficient and productive businesses. The model includes a decentralized application for notarization of the information flow in building information modeling processes; the application is implemented and tested on a local blockchain. The proposed model represents a so-called digital twin and is, hence, a huge system that manages all the information flow associated with a building throughout its life cycle, returning to individuals the control of their own data. In this model, all stakeholders operate based on so-called decentralized identifiers and DID documents, which store on-chain the fingerprints of the information flow in a common data environment.

Keywords: self-sovereign identity; DID; blockchain; building information modeling; common data environment



Citation: Cocco, L.; Tonelli, R. Digital Transformation in the Construction Sector: Blockchain, BIM and SSI for a More Sustainable and Transparent System. *Future Internet* **2024**, *16*, 232. <https://doi.org/10.3390/fi16070232>

Academic Editor: Yuansong Qiao

Received: 14 May 2024

Revised: 23 June 2024

Accepted: 24 June 2024

Published: 28 June 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Over the past few decades, there has been a global and cross-industry digitization process. While it initially began modestly, the advent of smartphones greatly accelerated this trend. The COVID outbreak further intensified this shift, compelling a transition from in-person to digital interactions.

In this digitization process, the construction industry (CI) lags compared to other sectors. Apart from the adoption of building information modeling (BIM), which is, however, often limited to the design phase and only for large projects, the adoption of digital technologies is limited. A recent report by the European Commission [1] underscores the critical and immediate necessity for a digital transformation in the CI to encompass aspects like data collection, process automation and the integration of advanced technologies for digital information and analysis.

Thanks to the BIM methodology, it is possible to manage a complex and varied amount of data throughout the entire lifecycle of a building, from the material production phase, to installation and commissioning, up to decommissioning. A tool for implementing BIM is the so-called common data environment (CDE), which is a shared working environment that is capable of making the management of real estate more efficient through transparent and shared processes ([2–4]). CDEs are regulated internationally by ISO 19650 [5]. Reference [5] identifies a CDE of the appointing party and a CDE of the appointed parties. The latter are, for example, the companies, the designers, or the construction supervisors ([2]). (The Italian legislation accurately describes the methods and procedures that have to be executed so that this transfer can take place [3]. CDEs are regulated in Italy by UNI 11337.)

However, today, CDEs are centralized systems that do not offer guarantees against tampering with their contents or with their history of updates (Refs. [6–9]), and often,

legal implications hinder their use, thus also hindering the adoption of BIM to streamline processes and speed up operations (Refs. [10–14]).

In addition, within this digitization process, a crucial role is played by identity management. It is widely acknowledged that the internet was constructed without a foundational identity layer. Consequently, as the world becomes increasingly digitalized, we face seemingly insurmountable challenges such as a lack of control over data, privacy concerns, compliance issues, security vulnerabilities, fraud, identity theft and a cumbersome user experience.

In the literature, many works describe how BIM, IoT and blockchain can interact to contribute to digital transformation in CI (see, for example, the “cup of water theory” [15] and works [16–21]).

This article takes a further step forward and, for deep digitalization of CI, in addition to BIM, IoT and blockchain, exploits a new identity management paradigm based on self-sovereign identities (SSIs) that empowers users to take control of their data while facilitating seamless, private, secure sharing of data on users’ own terms. This presupposes a huge system, and, hence, it would be a digital twin as defined by Su et al. [22]:

Digital twin is not just a single platform, technology or model, but a huge system that requires a lot of advanced technical support. For digital twin applied in the whole life cycle of buildings, with the characteristics of larger system and wider stakeholders, more support is required (extracted by [22]).

Our model leverages blockchain, BIM and SSI to tackle counterfeiting, waste, supply chain inefficiencies, lack of transparency, lack of trust, constant use of paper, long lead times for the processing of different activities and the lack of efficient sharing of documents and information.

Precisely, we present a model in which all users can operate through their decentralized digital identities and exchange data using the typical mechanisms of the SSI paradigm. Through the SSI paradigm, two entities (digital identities) can exchange data with each other, trace the entities behind the digital identities involved in the data exchange thanks to the so-called decentralized identifiers (DIDs) and DID documents, and verify the validity of the exchanged data.

The proposed model includes a decentralized application (dApp) for the notarization of the information flow in common data environments (CDEs). The dApp notarizes on-chain the information flow relating to a given job order (precisely relating to a design commission in the proposed system and, henceforth, simply commission) within a CDE, i.e., the space on a server in which data and files related to a specific commission are stored. Specifically, it is made up of two subsystems: one on-chain and another off-chain. The on-chain subsystem consists of the smart contract, which implements the logic for notarizing the information flow within a CDE and for triggering the passage from one area of the CDE to the next thanks to the events emission. The off-chain subsystem consists of an application that includes the software that calculates the hash of the content of the information to be notarized, the server side software, which listens to the events issued by the contract to trigger the automatic transfer of contents from one area of the CDE to the next when the contractual conditions implemented in the smart contract are all respected, and the graphic user interface (GUI), which allows users to interact with the on-chain subsystem. Note that, to date, there are no CDEs that implement APIs for managing the automatic transfer of contents in response to external triggers. For this reason, in this article, only the complete implementation of the on-chain system and the latter and former application of the off-chain subsystem are presented. (As of today, there are no APIs for this interaction, but there are several initiatives moving in this direction. For example, Harpaceas and Chainplug—the former being a leader in the software market for large construction and the second being an innovator in the field of blockchain technology for workflow automation—have started a collaboration with the aim of offering digital and complete technological solutions based on BIM and blockchain for the construction market [4].)

Differently from the proposed model, Nizamuddin et al. and Tao et al. [6,7] proposed blockchain-IPFS-based solutions for document sharing and version control without the involvement of a centralized third party, and Ciotta et al. [23] presented a proof of concept based on blockchain technology for the certification of information flow between CDEs in applications related to structural design.

Regarding digital identities and, precisely, digital identities of things such as IoT devices and buildings, Cocco et al. [24] discussed the benefits of SSIs in CI and presented a blockchain-based model for notarizing and certifying the information related to a building without entering into the details of the notarization of data flow in CDEs, as this article does. In [24], the authors present a decentralized system based on the Ethereum blockchain that manages the information associated with a building and is generated by stakeholders, natural or legal entities and IoT devices. In this system, stakeholders and buildings are identified through their DIDs, and the storage of all building information is managed both through a centralized database and blockchain. Niya et al. [25] and Weingärtner et al. [26] investigated and proposed SSI-blockchain-based approaches for IoT devices. Precisely, Niya et al. presented a platform, named the Know Your IoT device platform (KYIoT), that leverages the ERC 734 and 735 standards of the Ethereum blockchain for SSI (now dated) and the SRAM-based physically unclonable functions (PUFs) of these devices for the identification of Arduino devices within IoT networks such as networks for supply chain tracing and IoT data marketplaces. Weingärtner et al. presented a prototype for which IoT devices own identities that are stored both in a trusted execution environment by their manufacturer and on-chain to guarantee integrity.

Following the SSI paradigm, many organizations, such as Trinsic (<https://trinsic.id/trinsic-ecosystems/#>, accessed on 20 May 2024), Connect (<https://connect.me/>, accessed on 20 May 2024), Dock (<https://www.dock.io/post/self-sovereign-identity>, accessed on 20 May 2024), Esatus (<https://esatus.com/index.html%3Fp=7663&lang=en.html>, accessed on 20 May 2024), Talao (<https://talao.co/sandbox/saas4ssi>, accessed on 20 May 2024), Veramo [27–29], and ESSIF (<https://essif-lab.eu/> (accessed on 20 May 2024) and [30]), have been working on SSI solutions; they have been adopting different underlying technologies and, as a result, have been creating interoperability problems. The effective adoption of these solutions, including also the proposed model, will be possible only after the standardization of all the underlying protocols and the diffusion of the governance models and trust frameworks (Refs. [31–33]) that have to provide technical, syntactical, semantic and organizational interoperability, as discussed in an interesting work by Yildiz et al. [34].

The uniqueness of this work is that it presents and promotes a model that, thanks to the SSI paradigm, gives control of individuals' data back to them and aims for deep digitalization in the construction industry and of the all sectors that revolve around it. In addition, it focuses on the digital processes of building design—precisely, on the notarization of the related workflow—but it can be applied to notarize the information flow related to the construction phase of a building and also to the operation, maintenance and demolition phases. Hence, it can be applied to notarize information along the entire lifecycle of a building.

The combination of SSI concepts with dApps proposed for notarization of the information flow in CDE allows the exchange of documents with third parties that are not involved in the development of a commission—hence, with individuals that do not have access to the commission CDE—and the verification of the validity of exchanged documents by relying on the proofs left on-chain, as provided by the triangular model of the SSI paradigm in which the holders, issuer and verifier operate.

Figure 1 shows the information flow of the proposed model, in which legal and natural persons and buildings (precisely, their owners) interact among each other and with the blockchain and CDE to exchange data/documents as verifiable credentials through the DIDComm protocol, which is a standard for data exchange between DIDs. All stakeholders store data in the CDE, in a digital wallet and on the blockchain, where data are never recorded in plain text.

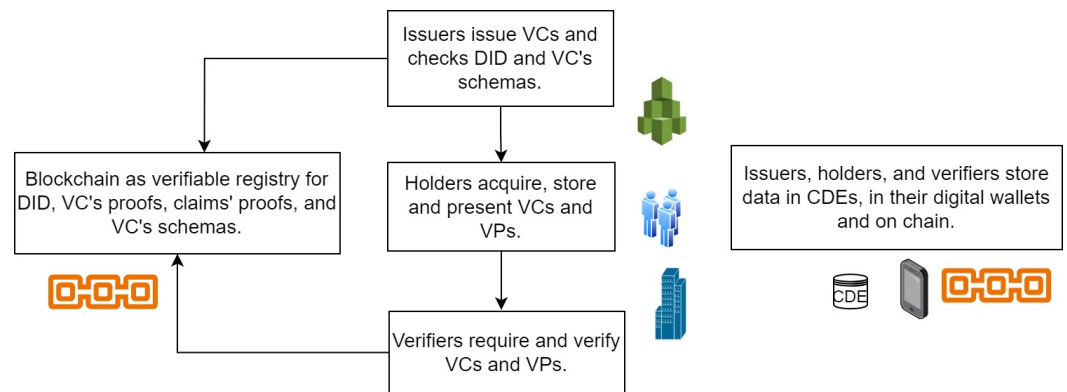


Figure 1. SSI-based model.

2. Proposed Model: An Overview

In the following, the proposed dApp, which implements the logic related to the notarization of the information flow related to a given commission within a CDE, is described. In such applications, a smart contract has to implement the logic to manage file versioning, the logic to store the information flow among the different areas of a CDE and the logic to manage the verification and coordination procedures, thus allowing users to identify who did what and allowing content to pass from one area to the next area of the CDE. (In a CDE, the following four processing states/areas for information are defined:

- The work-in-progress area, in which the information is being processed and is only available to the person responsible for that content;
- The shared area, in which the information is complete for one or more disciplines and can be shared with other users in addition to the responsible user;
- The published area, in which the information is concluded and nobody needs to modify it;
- The archived area, in which the information is related to a completed process.

In general, in a CDE, information can be in different states. In the work-in-progress directory, it is in progress, which is indicated with S0/WIP, and in the shared directory, it can be suitable for coordination S1/SfC, suitable for information S2/SfI, suitable for review S3/SfR or suitable for approval S4/SfA. Finally, in the published directory, it is suitable for manufacture D4/SfM.

In addition, an approval status is associated with all information: A0, for which the content has not yet been submitted to the approval procedure; A1, for which the content was successfully approved; A2, for which the content has been approved with comments, and changes to the content are required; and finally, A3 for which the information has not been approved.

The application aims to support digital processes for the construction chain—precisely, digital processes for building design—and thus, it aims to notarize the related workflow. So it is related to the design phase, but it can be easily modified, for example, to notarize the information flow related to the construction phase. It is assumed that the administrator of the application is the contractor of the commission and has both the burden of arranging a CDE, as required by the information specifications (the information specifications are the document that allows the winners of a tender to draw up the so-called information management plan.), and the burden of arranging an on-chain system that allows notarizing the information flows and sending the necessary notifications to the off-chain system.

Specifically, the dApp is composed of an on-chain subsystem and an off-chain subsystem. The on-chain subsystem consists of a smart contract that implements the logic for notarizing the information flow among the areas of the CDE. The progress of a design is, hence, notarized through the smart contract, which contains appropriate data structures to store all the data need to verify whether the contractual obligations have been respected and the design can go ahead (see the data structures named «struct»model and

«struct»version in Figure 2). The off-chain subsystem consists of a graphic user interface (GUI) that provides user-friendly access to all the functionalities of the on-chain subsystem, the application that computes the hash of the information to store, and the server-side software that allow users to listen for events and communicate with CDEs. Only the first two applications were developed in this work, as mentioned previously.

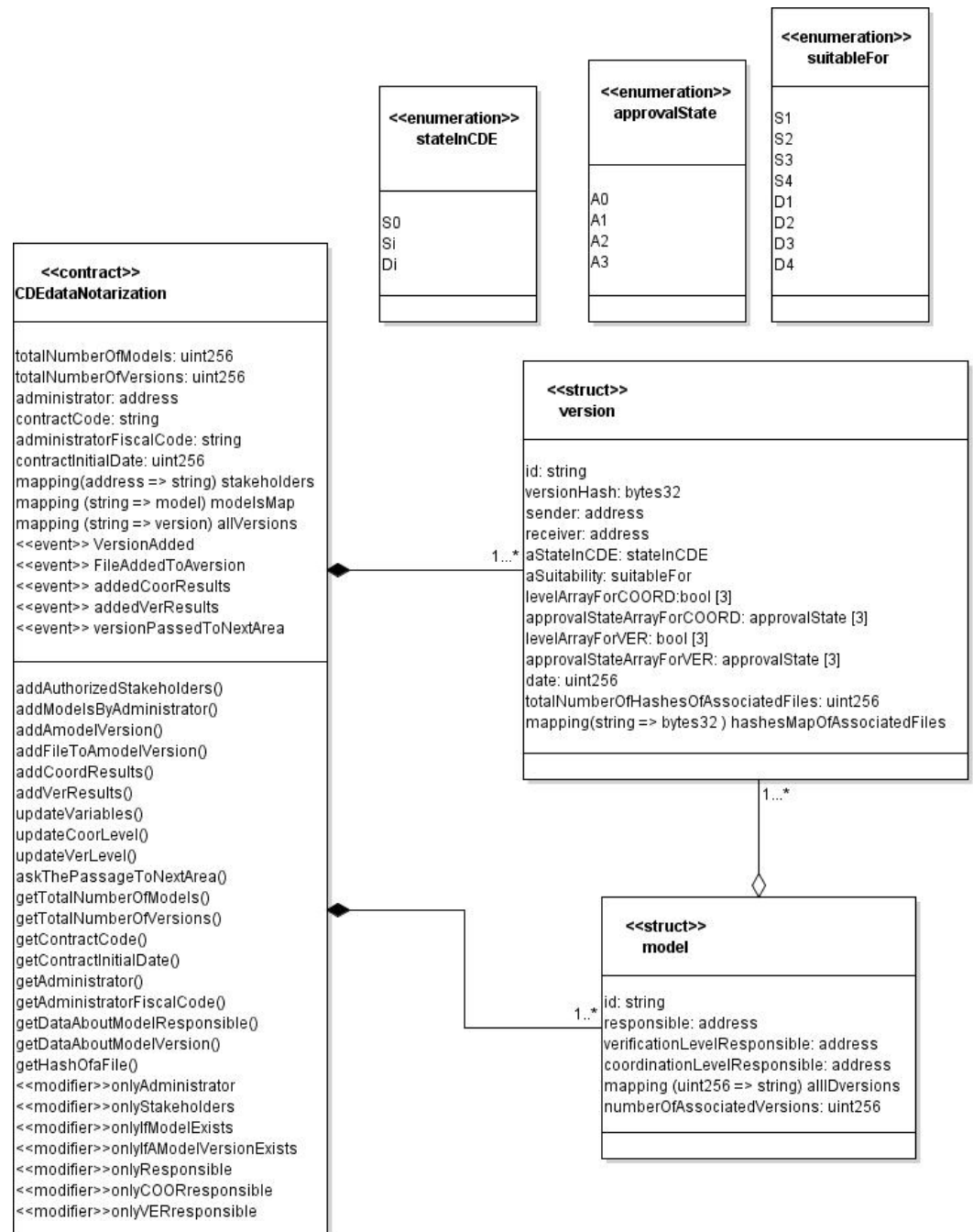


Figure 2. UML class diagram describing the proposed smart contract.

For the design of the decentralized application, the agile blockchain dApp engineering (ABCDE) method, which is an innovative process for the development and testing of blockchain applications [35], was adopted. This method proceeds by steps.

First, the goal, the actors and the requirements of the system are identified and defined. Then, the system to be realized is divided into the on-chain subsystem, which is composed of the smart contracts, and the off-chain subsystem, which is composed of the external

component, which contains the server-side code and the components for allowing users to interact with the whole system, comprising the blockchain as described above. Finally, security assessments that take into account the issue of gas optimization have to be done, and testing, integration and releasing of the two subsystems have to be executed.

Note that the proposed application, including the on-chain subsystem, was designed following the principles of software engineering and the patterns and best practices presented in works [35–37]. This is because developing applications running on blockchain implies the writing of code for the so-called smart contracts, for which the bytecode is public, and the generation of transactions, which implies a cost given the smart contracts can modify the blockchain state, and, as a result, this implies the consumption of gas. Consequently, it is important to allow only authorized users to interact with the code. So the on-chain subsystem is designed in such a way that some of its functions are accessible only to authorized users thanks to the use of address mapping and modifiers that manage access (see the three mappings stakeholders, modelsMap and allVersions and the seven modifiers in «contract»CDEdataNotarization in Figure 2) in such a way as to optimize costs thanks to the adoption of the best practices known to date. In the following, the application of the ABCDE method's steps are described in detail.

3. Proposed Model: ABCDE Method and Integration with SSI Concepts

In this section, the development of the decentralized application by the application of the ABCDE method's steps and the integration of this application with the concepts of the SSI paradigm are described.

3.1. Definition of the Application's Goal

As already mentioned, the goal of the application is the implementation of a dApp for the notarization of the information flow related to a given commission within a CDE, with a focus on the design phase of the work.

3.2. Actor Identification

The actors of the system are identified and briefly described as follows.

- System administrator: He/she deploys the smart contract on the blockchain and initializes the off-chain platform for information management. He/she may be the appointing party.
- Client: He/she represents the appointing party of the commission.
- Designers, architects, structural engineers and named authorized stakeholders in Figure 3: They are the subjects in charge of carrying out a given activity within the commission.
- Smart contract: It represents the only actor who interacts directly with the blockchain, and it implements the application logic of the on-chain system described above.
- Off-chain platform: It is the platform that allows for management of the information flow and contains the user interface for interacting with the blockchain. So the off-chain system allows, for example, a user to create the hash of the information and to store it on the blockchain with a transaction by using the smart contract.

3.3. Definition of User Stories

Let us describe some user stories that the proposed application implements.

1. The system administrator deploys the smart contracts and initializes the platform.
2. The platform manages the user identifications. Each participant has a public and a private key. The platform has to associate a given address with a precise entity and has to allow the identification of the responsibilities of a given entity within the development of the commission.
3. The smart contract implements the logic for managing read and write access in its data structure.

4. The administrator enters the identification data of all the models envisaged by the commission in the smart contract, specifying for each of them the phase of the project in which it has to be inserted.
5. The platform and the smart contract, including the CDE, have to use the same naming convention for all information.
6. The administrator assigns to each model the subject responsible for carrying out it.
7. Stakeholders create BIM models, BCF files, approval documents or change-request documents and notarize them on the blockchain.
8. Each stakeholder receives a notification when a model/file that is addressed to them is entered into the system.
9. The smart contract has to associate a given level of coordination and verification with each model, and it allows only authorized actors to change the approval status of a given model after a coordination or verification procedure.
10. The smart contract signals to the off-chain system when a given model can pass a given gate.

3.4. Division of the System into On-Chain and Off-Chain Systems

The on-chain subsystem consists of a smart contract that was developed in the Solidity language and tested using Chai, which is a behavior-driven development (BDD)/test-driven development (TDD) assertion library for node.js and browsers using JavaScript scripts. Specifically, the application was tested on Ganache by the Truffle suite.

On the other hand, the off-chain subsystem consists of a software application that includes the GUI that allows the user to interact with the smart contract and, hence, with the Ethereum virtual machine, and the application that calculates the information's hash to be uploaded on-chain.

This external subsystem is implemented using node.js, web3.js and the JavaScript language, and it is connected to an Ethereum node: in our case, to Ganache through Metamask, which is a browser plugin that injects a web3 instance into the browser and allows users to select the Ethereum network to connect the proposed subsystem to. Therefore, before a user launches the dApp, he/she has to ensure that Metamask is enabled in his/her browser so that he can manage his Ethereum account and private keys.

The proposed dApp was tested by uploading the BIM file's hash, which was calculated by an application developed in node.js, and by storing on-chain all the data necessary for the notarization of the information flow, which obviously have to be congruent with those stored in the CDE. The proposed prototype, like that of Ciotta et al., is based on the Ethereum blockchain. The system was tested on a local blockchain that allows the execution of transactions towards the smart contract without incurring any cost for the gas necessary for the deployment of the contract and for subsequent transactions towards the smart contract.

Some Explicative Diagrams

All data necessary for implementing the logic that manages the passage of content from one area of the CDE to another—and, therefore, the overcoming of the so-called gates—are stored on-chain. A given model passes from one area to the next one only if it passes appropriate checks, the so-called coordination levels CLs, and only if it passes appropriate verifications, the so-called verification levels VLs. After these checks, reports are drawn up with the results of the analyses, and an approval status is assigned to the model. So the approval status allows (or disallows) the passage of the model to the next area of the CDE.

In particular, each model is subjected to verification VL1 if it is in the work-in-progress directory, VL2 if it is in the shared directory, and finally, VL3 if it is in the published directory. Regarding the coordination analysis, typically, the information specifications are required in order to carry out a periodic activity of coordination of the models.

Only the subject responsible for a given model can modify that model according to the results of the verification and coordination procedures and according to any requests by the appointing party and/or other stakeholders. A given model is completed if it has passed through all levels of coordination and verification with approval status A0. The proposed application assumes that the subject responsible for a given model's version makes a blockchain transaction to ask the smart contract for passage to the next area when he/she believes that all the contractual constraints have been satisfied and the model has been modified according to all requests by the stakeholders involved in the design process. The smart contract, by querying its data structure, decides if the model's version can or cannot pass to next area. All the versions of a given model and all other information, such as information exchange type documents, are stored in plain text in the CDE, while their hashes are stored in the blockchain, so the transparency of all the design activities is guaranteed. Note that all of the assumptions for the proposed dApp can be customized to create a coherent dApp with the requirements that have to be realized for a specific commission.

Figures 2 and 3 show the UML class diagram and the UML use-case diagram, respectively, of the smart contract proposed in this work. Note that the use cases in this figure are for the user stories listed above, and many of them also correspond to the methods for the smart contract (see the methods listed for the stereotypical «contract» CDEdataNotarization in Figure 2).

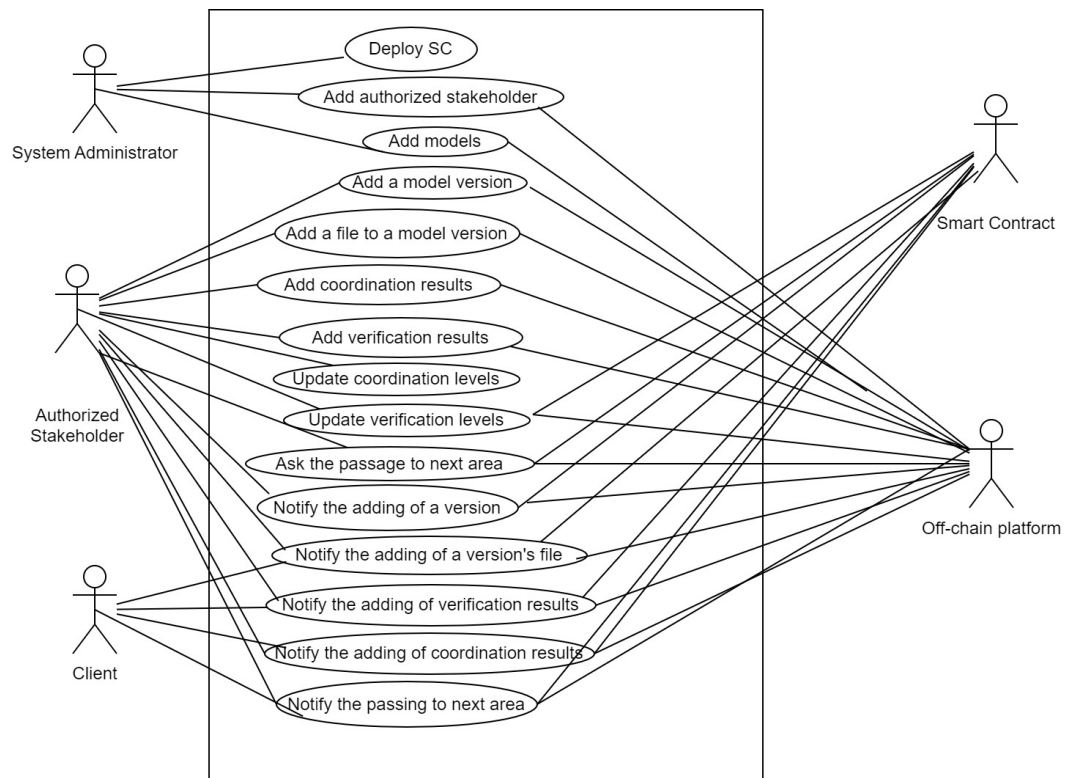


Figure 3. UML use-case diagram.

In the following, let us give a description of a typical workflow that can be implemented using the proposed dApp. A flow similar to that proposed by Tao et al. [7], who implemented a framework in Hyperledger Fabric, was followed. Unlike [7], the proposed article's goal was to notarize the information flow in a CDE and not that to implement a distributed CDE, as Tao et al. did.

Figure 4 shows the UML sequence diagram for this workflow.

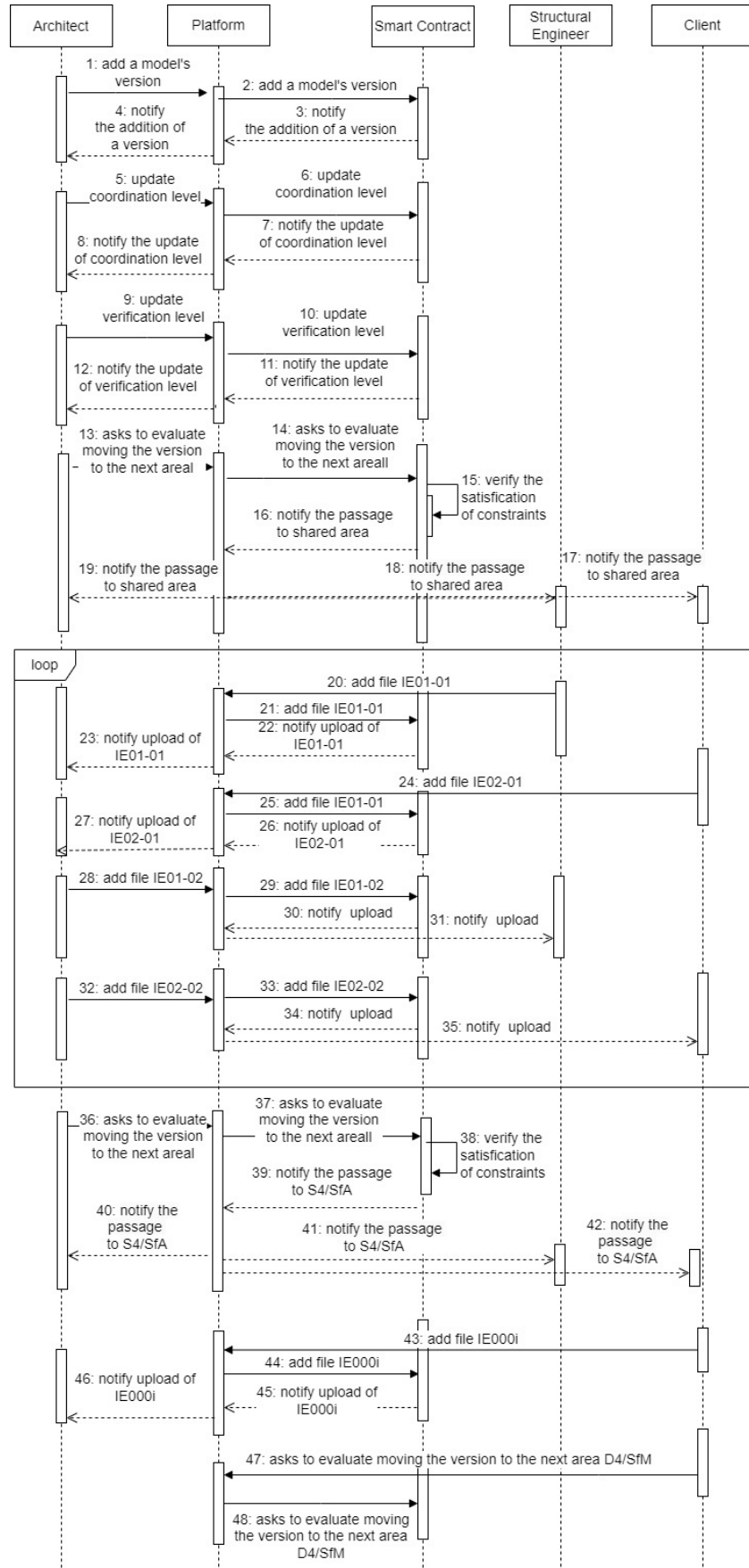


Figure 4. UML sequence diagram.

An architect creates the first version of a BIM model, which has been registered in the system by an administrator with the unique identifier DC-0010-INF-M2-D. A version of the model DC-0010-INF-M2-D-0001 is loaded into the system by the architect (message 1 in the sequence diagram) and is placed in the work-in-progress area identified with S0/WIP. (Note that for the stereotypical «enumeration» stateInCDE, «enumeration» approvalState and «enumeration» suitableFor, the smart contract manages the states of several instances of information in the four areas of a CDE. See footnote 8.) When the architect decides to share the model with the team of structural engineers, he records the coordination and verification analyses performed on the model (messages 5 and 9) and asks the smart contract to approve the transfer of the model to the shared area: precisely, to area S1/SfC, which is suitable for coordination (message 13). The smart contract verifies that all the data entered by the person in charge satisfy the constraints for passage to the next area, and if the constraints are all satisfied, it stores the new status of the model version, which is now in the shared area, and issues an event to communicate to the CDE that the gate can be passed (message 16).

The team of structural engineers receives the notification of the model version uploaded by the architect, performs appropriate clash detection analyses, manages the clashes detected, and creates a BCF file of the analysis results identified by IE01-01, where IE01 stands for a document of type “information exchange”, and 01 indicates the first version of that file. The team uploads the file created on-chain by associating it with the version of the model to which it refers (message 20), and the smart contract issues an event to signal the successful upload of the file (message 22).

Also, the client, who is the appointing party, receives the notification of the upload by the architect, makes a design request IE02-01 related to the BIM model, and uploads the file on-chain (message 24), associating it with the version of the model to which it refers. Also, in this case, the smart contract emits an event to signal that the file has been uploaded (message 26).

Once the notifications have been received, the architect checks the files and revises the model. At the end of the revision work, he/she uploads three files on-chain: two response files—respectively, IE01-02 for the structural engineers and IE02-02 for the client—and the DC-0010-INF-M2-D-0002 file relating to the revised BIM model, which is always located in the shared area, and precisely, in S1 suitable for coordination S1/SfC (Note that when the DC-0010-INF-M2-D-0002 file is uploaded, messages 1 to 19 are repeated.).

Multiple iterations can be done until a model that satisfies all parties is reached (indicated by the loop in the sequence diagram). Once the iterations are finished, the architect makes a transaction on-chain asking to set the new status of the model version, which is now in the S4/SfA area, to suitable for approval (message 36). The smart contract issues an event to communicate to the CDE the change to the model’s state within the shared area of the CDE (message 39).

Once the notification has been received, the client approves the BIM model and creates a document, IE000i (message 43), indicating its approval, and, hence, the completion of the model, and makes a transaction on-chain to ask the smart contract to pass the model to the next area D4/SfM (message 47).

3.5. Final Considerations

As just mentioned, the dApp described in this section can be easily customized to be applied to the several phases present along the lifecycle of a building. So a system that notarizes the information flow associated with a building over its entire lifecycle can be developed. In addition, the integration of such an application with the concepts of the SSI paradigm allows users to realize a system for which all data associated with an entity—hence, with a person or a building—become verifiable credentials. Verifiable credentials guarantee that information is certified by an authorized entity that stores on-chain the proofs to allow a third party, the so-called verifier, to prove its validity; thus, the information is accepted as true and valid.

In this model, all information is stored off-chain. So all documents/information associated with a building during its lifecycle are stored off-chain—for example, in CDEs—and also in digital wallets belonging to the owner of the building's DID. Information about all stakeholders—associated, hence, with a natural or legal, person—is stored off-chain in the digital wallets of the entity.

On the contrary, the model stores on-chain only the data necessary for the notarization and for the exchange of verifiable credentials. Precisely, it stores only the data's hash and the cryptographic proofs of the issuers.

4. Proposed Model: Use Cases

Let us describe three explicative use cases.

First use case: The home's owner, who is the so-called holder in the SSI paradigm, presents the house's energy certificate to a potential buyer: the verifier. The engineer who issued the certificate (hence, the issuer) has to store on-chain both the cryptographic proofs and the status of the credential; in this way, the energy certificate becomes a verifiable credential. It also becomes a verifiable presentation because the holder presents it to the buyer without changing it. Only the issuer of a credential (hence, only authorized bodies: in this case, the engineer) can revoke a credential following an inspection of the house in the event that the energy status no longer coincides with what was previously assigned to it. Thanks to this mechanism, the revocation does not delete the presentation delivered by the holder to the potential buyer, but a future verification of the credential by a verifier returns the non-validity of the certificate. Note that in this use case, the verifier is an external stakeholder. He cannot access the CDE and can only verify the presentation without resorting to third parties thanks to the verifiable credentials and to the public registry in which the proofs are stored.

Second use case: During construction, the home's owner wants to check the work in progress. In particular, he/she wants to verify the conformity of the electrical system. Being the owner of the house, he/she will be able to access the digital wallet of his house and verify all the credentials that have been registered by the authorized stakeholders. In particular, he/she will check the credentials regarding the electrical system, which were uploaded by the installer, who has a specific ID. Without resorting to third parties, he/she can verify the validity of all credentials and can thus check the work that has been done.

Third use case: This use case involves the person responsible for managing the work, e.g., a manager or a public official. The manager works on behalf of the client and must prepare all the documents to be presented to the municipality to obtain, for example, the certificate of habitability. By operating on behalf of the customer, who is, for example, the owner of the house under construction, he/she will have access to the digital wallet of the house and will be able to select from that wallet all the data he/she needs to request the certificate. He/she will build a presentation and present it to the public official, who, without resorting to third parties, will be able to verify that all the information presented is valid, and only in that case will the official proceed to issue the requested certificate, which, in turn, becomes a verifiable credential.

Note that the identities of the stakeholders who are authorized to issue certified content can be declared using trusted lists published in on-chain registries. Further note that energy certificates, as with every certificate and document that aims to be a verifiable credential, should be issued following a precise credentialing scheme in such a way that their content is understood by all (holder, issuer and verifiers). So proposing schemes for the main certificates and documents related to a building is crucial. Just by standardizing and by the creation of governance models that establish, for example, trusted lists, terminologies and rules, SSI systems could be realized in the near future, thus allowing the integration of current systems with SSI applications such as the proposed dApp.

5. Conclusions

By embracing cutting-edge technologies, this article proposes a model for the construction sector that is capable of optimizing the planning, realization and construction management phases by guaranteeing a greater level of transparency, verifiability and effectiveness without neglecting the aspects related to the management of identities in the relationships between businesses and other businesses, between businesses and public administrations, between citizens and the public administration, and between citizens and businesses. By exploiting BIM, the SSI paradigm and blockchain, the model is a leaner, more transparent and more efficient solution than current information systems.

It aims to prevent monopolization phenomena and anti-competitive practices and aims to promote personal and economic freedoms for the benefit of the entire community and to reduce verification costs by improving confidence in the authenticity of the data used.

The system cannot disregard the presence of current document and conservation systems that guarantee that each single document is managed according to the logic of Italian and European regulations to ensure legal validity over time. So it starts from rethinking current information systems to promote user trust and personal data protection in order to help create new opportunities for dialogue between different levels of government and for sharing information for the benefit of citizens and companies. It combines different technologies in a complementary and non-competitive way, bringing to the relationship between citizens and institutions significant advantages that go far beyond those simply linked to information sharing within a CDE.

Author Contributions: Conceptualization, L.C.; methodology, L.C.; software, L.C.; validation, L.C.; formal analysis, L.C.; investigation, L.C.; resources, L.C.; data curation, L.C.; writing—original draft preparation, L.C.; writing—review and editing, L.C.; visualization, L.C.; supervision, L.C. and R.T.; project administration, R.T.; funding acquisition, R.T. All authors have read and agreed to the published version of the manuscript.

Funding: This work has been developed within the framework of the project IMASSChain, Infrastructure Management Support System Chain, under the National Military Research Plan 2020 (CIG: 884399685F-CUP: D84H22001380001). This work has been developed within the framework of the project e.INS- Ecosystem of Innovation for Next Generation Sardinia (cod. ECS 00000038) funded by the Italian Ministry for Research and Education (MUR) under the National Recovery and Resilience Plan (NRRP)-MISSION 4 COMPONENT 2, “From research to business” INVESTMENT 1.5, “Creation and strengthening of Ecosystems of innovation” and construction of “Territorial R&D Leaders”. This work was partially funded under the National Recovery and Resilience Plan (NRRP), Mission 4 Component 2 Investment 1.3-Call for tender No. 1561 of 11.10.2022 of the Ministero dell’Università e della Ricerca (MUR) funded by the European Union–NextGenerationEU, project code PE0000021, Concession Decree No. 1561 of 11.10.2022 adopted by Ministero dell’Università e della Ricerca (MUR), CUP F53C22000770007, according to attachment E of Decree No. 1561/2022, project title “Network 4 Energy Sustainable Transition–NEST”.

Data Availability Statement: No new data were created or analyzed in this study.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

MDPI	Multidisciplinary Digital Publishing Institute
DOAJ	Directory of open access journals
TLA	Three letter acronym
LD	Linear dichroism

References

1. European-Commission. A European Green Deal. Available online: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en (accessed on 15 May 2024).
2. Asprone, D.; Botta, A.; Ciotta, V.; Mariniello, G. Blockchain per la Certificazione dei Flussi Informativi tra ACData: l'Applicazione per il Collaudo delle Strutture. 2021. Available online: <https://www.ingenio-web.it/articoli/blockchain-per-la-certificazione-dei-flussi-informativi-tra-acdat-l-applicazione-per-il-collaudo-delle-strutture/> (accessed on 15 May 2023).
3. Furcola, N. ACData (Ambiente di Condivisione Dati): Cos'è e Perché è Decisivo per il BIM-Parte 3. Available online: <https://biblus.acca.it/focus/acdat-ambiente-di-condivisione-dati-cose-e-perche-e-decisivo-per-il-bim-parte-3/> (accessed on 15 May 2023).
4. Anonymous. Blockchain e BIM per le Costruzioni al Centro dell'Accordo tra Harpaceas e Chainplug. 2022. Available online: https://www.edilportale.com/news/2022/10/aziende/blockchain-e-bim-per-le-costruzioni-al-centro-dell-accordo-tra-harpaceas-e-chainplug_90733_5.html (accessed on 15 June 2024).
5. ISO 19650 Workflow. 2019. Available online: <https://plannerly.com/wp-content/uploads/2024/02/ISO-19650-Workflow-with-free-ISO-19650-templates.pdf> (accessed on 13 May 2024).
6. Nizamuddin, N.; Salah, K.; Ajmal Azad, M.; Arshad, J.; Rehman, M. Decentralized document version control using ethereum blockchain and IPFS. *Comput. Electr. Eng.* **2019**, *76*, 183–197. [CrossRef]
7. Tao, X.; Das, M.; Liu, Y.; Cheng, J.C. Distributed common data environment using blockchain and Interplanetary File System for secure BIM-based collaborative design. *Autom. Constr.* **2021**, *130*, 103851. [CrossRef]
8. Mahamadu, A.; Mahdjoubi, L.; Booth, C.A. Challenges to BIM-Cloud Integration: Implication of Security Issues on Secure Collaboration. In Proceedings of the 2013 IEEE 5th International Conference on Cloud Computing Technology and Science, Bristol, UK, 2–5 December 2013; Volume 2, pp. 209–214.
9. Das, M.; Tao, X.; Cheng, J.C.P. BIM security: A critical review and recommendations using encryption strategy and blockchain. *Autom. Constr.* **2021**, *126*, 103682. [CrossRef]
10. Sattineni, A.; Azhar, S. Techniques for Tracking RFID Tags in a BIM Model. In Proceedings of the 27th International Symposium on Automation and Robotics in Construction, Bratislava, Slovakia, 24–27 June 2010; Brno, T., Ed.; The International Association for Automation and Robotics in Construction: Edinburgh, UK, 2010; pp. 346–354. [CrossRef]
11. Wang, X.; Liang, C.J.; Menassa, C.; Kamat, V. Interactive and Immersive Process-Level Digital Twin for Collaborative Human-Robot Construction Work. *J. Comput. Civ. Eng.* **2021**, *35*, 04021023. [CrossRef]
12. Ma, G.; Jiang, J.; Shang, S. Visualization of Component Status Information of Prefabricated Concrete Building Based on Building Information Modeling and Radio Frequency Identification: A Case Study in China. In *Advances in Civil Engineering*; Wiley: Hoboken, NJ, USA, 2019. [CrossRef]
13. Turk, Ž.; Klinc, R. Potentials of Blockchain Technology for Construction Management. *Procedia Eng.* **2017**, *196*, 638–645. [CrossRef]
14. Panagiotidou, N. The Need for BIM Standards in Digital Construction. Available online: <https://www.gim-international.com/content/blog/the-need-for-bim-standards-in-digital-construction> (accessed on 15 June 2023).
15. Ye, Z.; Yin, M.; Tang, L.C.M.; Jiang, H. Cup-of-Water Theory: A Review on the Interaction of BIM, IoT and Blockchain During the Whole Building Lifecycle. In Proceedings of the 35th International Symposium on Automation and Robotics in Construction (ISARC), Berlin, Germany, 20–25 July 2018.
16. Yang, R.; Wakefield, R.; Lyu, S.; Jayasuriya, S.; Han, F.; Yi, X.; Yang, X.; Amarasinghe, G.; Chen, S. Public and private blockchain in construction business process and information integration. *Autom. Constr.* **2020**, *118*, 103276. [CrossRef]
17. Zheng, R.; Jiang, J.; Hao, X.; Ren, W.; Ren, F.X.Y. bcBIM: A Blockchain-Based Big Data Model for BIM Modification Audit and Provenance in Mobile Cloud. In *Mathematical Problems in Engineering*; Wiley: Hoboken, NJ, USA, 2019. [CrossRef]
18. Hargaden, V.; Papakostas, N.; Newell, A.; Khavia, A.; Scanlon, A. The Role of Blockchain Technologies in Construction Engineering Project Management. In Proceedings of the 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), Valbonne, France, 17–19 June 2019; pp. 1–6. [CrossRef]
19. Olawumi, T.O.; Ojo, S.; Chan, D.W.M.; Yam, M.C.H. *Factors Influencing the Adoption of Blockchain Technology in the Construction Industry: A System Dynamics Approach*; Springer: Berlin/Heidelberg, Germany, 2021; pp. 1235–1249.
20. Lee, D.; Lee, S.; Masoud, N.; Krishnan, M.S.; Li, V.C. Integrated digital twin and blockchain framework to support accountable information sharing in construction projects. *Autom. Constr.* **2021**, *127*, 103688. [CrossRef]
21. Hamledari, H.; Fischer, M.A. Measuring the Impact of Blockchain and Smart Contract on Construction Supply Chain Visibility. *Adv. Eng. Inform.* **2021**, *50*, 101444. [CrossRef]
22. Su, S.; Zhong, R.Y.; Jiang, Y.; Song, J.; Fu, Y.; Cao, H. Digital twin and its potential applications in construction industry: State-of-art review and a conceptual framework. *Adv. Eng. Inform.* **2023**, *57*, 102030. [CrossRef]
23. Ciotta, V.; Mariniello, G.; Asprone, D.; Botta, A.; Manfredi, G. Integration of blockchains and smart contracts into construction information flows: Proof-of-concept. *Autom. Constr.* **2021**, *132*, 103925. [CrossRef]
24. Cocco, L.; Tonelli, R.; Marchesi, M. A System Proposal for Information Management in Building Sector Based on BIM, SSI, IoT and Blockchain. *Future Internet* **2022**, *14*, 140. [CrossRef]
25. Niya, S.R. KYoT: Self-sovereign IoT Identification with a Physically Unclonable Function. In Proceedings of the 2020 IEEE 45th Conference on Local Computer Networks (LCN), Sydney, NSW, Australia, 16–19 November 2020.

26. Weingaertner, T.; Camenzind, O. Identity of Things: Applying concepts from Self Sovereign Identity to IoT devices. *Peer Rev. Res.* **2021**. [CrossRef]
27. Veramo. ETHR DID Method Specification 2021. Available online: <https://github.com/decentralized-identity/ethr-did-resolver/blob/master/doc/did-method-spec.md> (accessed on 4 January 2022).
28. Beregszaszi, A.; Braendgaard, P.; Zoltu, M.; Entriken, W.; eth bot. Ethereum Verifiable Claims 2021. Available online: <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1812.md> (accessed on 4 January 2022).
29. Bugyis. Introducing Veramo 2021. Available online: <https://medium.com/uport/introducing-veramo-5a960bf2a5fe> (accessed on 4 January 2022).
30. Anonymous. Proposal for a Regulation of the European Parliament and of the Council Amending Regulation (EU) No 910/2014 as Regards Establishing a Framework for a European Digital Identity. 2021. Available online: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0281> (accessed on 15 June 2023).
31. López, M.A. Self Sovereign Identity the Future of Identity: Self-Sovereignty, Digital Wallets, and Blockchain. Technical Report, IDB, IDB LAB, LACCHAIN. 2020. Available online: <https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignty-digital-wallets-and-blockchain> (accessed on 15 June 2023).
32. Sroor, M.; Hickman, N.; Kolehmainen, T.; Laatikainen, G.; Abrahamsson, P. How modeling helps in developing self-sovereign identity governance framework : An experience report. In Proceedings of the International Conference on Industry Sciences and Computer Science Innovation, Gaia, Portugal, 9–11 March 2022; Cruz-Cunha, M.M., Mateus-Coelho, N., Eds.; Elsevier: Amsterdam, The Netherlands, 2022; pp. 267–277. [CrossRef]
33. Doerk, A. The Trust Infrastructure of Self-Sovereign Identity Ecosystems, 2020. Available online: <https://ssi-ambassador.medium.com/the-trust-infrastructure-of-self-sovereign-identity-ecosystems-551f46ed9e2c> (accessed on 25 June 2024.)
34. Yildiz, H.; Küpper, A.; Thatmann, D.; Göndör, S.; Herbke, P. A Tutorial on the Interoperability of Self-sovereign Identities. *arXiv* **2022**, arXiv:2208.04692.
35. Marchesi, L.; Marchesi, M.; Tonelli, R. ABCDE –agile block chain DApp engineering. *Blockchain Res. Appl.* **2020**, *1*, 100002. [CrossRef]
36. Marchesi, L.; Marchesi, M.; Pompianu, L.; Tonelli, R. Security checklists for Ethereum smart contract development: Patterns and best practices. *arXiv* **2020**, arXiv:2008.04761.
37. Marchesi, L.; Marchesi, M.; Destefanis, G.; Barabino, G.; Tigano, D. Design Patterns for Gas Optimization in Ethereum. In Proceedings of the 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), London, ON, Canada, 18 February 2020; pp. 9–15. [CrossRef]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.