future internet

Article

A System Proposal for Information Management in Building Sector Based on BIM, SSI, IoT and Blockchain

Luisanna Cocco *, Roberto Tonelli and Michele Marchesi

Department of Mathematics and Computer Science, University of Cagliari, 09123 Cagliari, Italy; roberto.tonelli@unica.it (R.T.); marchesi@unica.it (M.M.)
* Correspondence: cocco@unica.it

Abstract: This work presents a Self Sovereign Identity based system proposal to show how Blockchain, Building Information Modeling, Internet of Thing devices, and Self Sovereign Identity concepts can support the process of building digitalization, guaranteeing the compliance standards and technical regulations. The proposal ensures eligibility, transparency and traceability of all information produced by stakeholders, or generated by IoT devices appropriately placed, during the entire life cycle of a building artifact. By exploiting the concepts of the Self Sovereign Identity, our proposal allows the identification of all involved stakeholders, the storage off-chain of all information, and that on-chain of the sole data necessary for the information notarization and certification, adopting multi-signature approval mechanisms where appropriate. In addition it allows the eligibility verification of the certificated information, providing also useful information for facility management. It is proposed as an innovative system and companies that adopt the Open Innovation paradigm might want to pursue it. The model proposal is designed exploiting the Veramo platform, hence the Ethereum Blockchain, and all the recommendations about Self Sovereign Identity systems given by the European Blockchain Partnership, and by the World Wide Web Consortium.

Keywords: SSI; BMI; Blockchain; IoTs; RFID tags; RFID reader

check for updates

Citation: 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. https://doi.org/10.3390/fi14050140

Academic Editor: Carlos Filipe Da Silva Portela

Received: 11 April 2022
Accepted: 29 April 2022
Published: 30 April 2022

1. Introduction

In recent years, the European Commission has revised some directives concerning the energy performance of buildings in order to tackle climate change and environmental degradation, which represent a threat to Europe and world. Such revisions regard, for example, the building of near-zero energy buildings, the promotion of e-mobility, the use of smart technologies in the building and in general a greater consideration for air pollution that is a threat for health and well-being. The EU construction sector, in all its construction, use, renovation and demolition phases, is responsible for 40% of energy consumption and 36% of greenhouse gas emissions [1,2].

In this context, the digitization of the building sector may play a crucial role in exploiting innovative technologies such as the so-called Building Information Modeling (BIM), Blockchain technology, and Internet of Things devices (IoT devices) as asserted by an interesting study, called "cup-of-water theory" [3], which explains how BIM, IoT and Blockchain can interact and contribute to the building digitization.

In our work, we take a further step forward and propose a model for the digitization of buildings that exploits, in addition to BIM, IoT and Blockchain, the concepts of the new identity management model based on Self Sovereign Identity (SSI).

BIM is a process of planning, design, construction and maintenance of a building that uses an information model that contains all the information concerning the entire life cycle of a building. It is a process that involves various figures who each operate within their own area of interest. There are numerous specialized disciplines that contribute to the design, construction and operation of a building. In such a context, the possibility of exchanging information in order to collaborate effectively in the realization of a shared project assumes strategic importance for the various stakeholders involved. Today the use of common data environments (CDE), which are single environments for sharing all the information content needed for the management of a property during its life cycle, and the use of the Industry Foundation Classes (IFC) open format, promoted by the concept of openBIM, which assumes strategic importance to break down the technological barriers that prevent different stakeholders from working together in synergy, enable the sharing information and the collaboration effectively.

Our model proposal also moves in this direction, but it contrasts with traditional models based, for example, on trusted organizations that issue digital certificates for websites, on the so called certification authorities and organizations that create, maintain, and manage user's identity information, providing authentication services, the so called identity providers, and on browser or app providers, which work using certificates and servers always connected and dictating the terms and conditions of their APIs to which the users must comply. So for contrasting any form of centralization, our proposal exploits the blockchain and the peer-to-peer network in which the participants communicate with each other directly, more or less "on an equal footing" (ref. https://veramo.io/docs/veramo_agent/messages and https://identity.foundation/didcomm-messaging/spec/ (accessed on 8 April 2022)), for data notarization and information sharing.

In more detail, the model proposal presents a decentralized system based on the Ethereum Blockchain, which manages the flow of information relating to buildings, such as blueprints, construction, maintenance, and management. The proposal manages information generated by all stakeholders, including data generated through IoT devices.

By exploiting the SSI concepts, the proposal represents stakeholders and buildings as Decentralized IDentifiers, and IoT devices as delegates of buildings. It manages the storage of all building information through off-chain database and blockchain. Precisely, it stores all useful information in off-chain database/wallet, and manages the storage on-chain by dividing information into notarized and certificated. Certificated information is notarized but it is also certified by a certified entity, which must leave on-chain the proofs to allow the check of the information validity. Our proposal manages the storage of the proofs to prove the certification validity and friendly graphic user interfaces (GUIs) that allow third parties to verify the validity of certified information.

The use of such a system would imply advantages in terms of greater security, greater efficiency, lower costs and no disadvantages related to the concept of vendor lock-in for all stakeholders. Further, thanks to the four technologies above mentioned, the proposed model intends to contain the risk of fraud, manipulation and corruption, favoring the transparency and verifiability of information; to automate various processes that take time if performed manually; and to reduce human errors, loss and manipulation of data, ensuring its integrity and quality. Furthermore, exploiting the concepts of the SSI, it stands out as a novelty in the international construction scenario.

2. An Overview

Today, any type of intervention that is carried out on the front building, for the construction, demolition, or modification of a property, requires special documentation that authorizes it. This documentation is usually produced starting from the "state of affairs" in the records in the archives of the Private Building Sector, hence in the municipality where the property is located. Digitizing building practices is a necessary process to preserve the important documents that can be requested even many years after their realization. The construction of a digital archive alongside the paper one is important for citizens and professionals to quickly access documents; to streamline the search process for the aforementioned documentation by the staff employed in the technical offices; but also to guarantee the integrity and protection of the archives over time. For any market sector, [4–7], and in particular in construction, the digitization of business processes is no longer a mere strategic choice but also a choice to meet the requirements of the regulations in force and to increase competitiveness.

The regulatory context in which the construction industry operates is very complex. It includes the procurement code, the digitization of the public administration, sustainability and energy efficiency, safety of buildings and in the workplace, technical standards for construction, qualification of the system and operators, traceability of payments and the introduction of BIM in tenders. A framework of this type places companies in front of the need to adapt their internal and external procedures, while increasing the levels of transparency, safety and efficiency. Digitization in the construction sector is today synonymous with electronic and well organized processes of the sharing of information, from which the maximum advantage can be taken only when all the stakeholders align themselves in using it.

In this work, we propose a system for the digitization of buildings that exploits Blockchain, BIM, IoT, and the concepts of the new identity management model based on Self Sovereign Identity (SSI).

2.1. Blockchain, BIM and IoT

Blockchain technology, born from the world of cryptocurrencies with Bitcoin, has started a real digital revolution that embraces numerous sectors from the banking and finance sector to insurance, from retail to agrifood, passing through the tracking of goods, and the public administration sector [8–20].

In particular, the implementation of the Blockchain in the public administration and business sectors would help citizens to have a secure and shared digital identity. It would allow us to solve some problems considered crucial in relations with public administrations and businesses, such as trust, transparency and security, and to implement the so-called Once Only Principle according to which citizens, institutions and companies must provide the authorities with certifications, attestations, declarations, or other documents once.

Blockchain represents a great opportunity for the digitization of the public and private sectors as it not only reduces costs, waste of time and bureaucratic complexity, but also the distance between citizens, companies and institutions, strengthening trust in digital services and fostering their diffusion. All this means that public and private digital services must comply with the requirements of a model based on interoperability, must be inclusive and accessible in order to respond efficiently to the different needs of people and individual territories, and must be provided in a secure way guaranteeing the personal data protection.

Looking at the public and private construction sectors, Blockchain technology, or distributed systems in general, offer a great potential when combined with innovative technologies such as BIM and IoT [21–24] and could start a completely new era of collaboration.

Today, on construction sites, communication in paper format is still very widespread and is strictly connected to evident inefficiencies and enormous costs. Consider, for example, that when the prospects of a given electrical or hydraulic system are printed, they could already be outdated due to changes that have become necessary during construction. Thanks to these technologies, it is possible to collect useful data to detect unexpected changes from what was designed, to detect delays in the execution of the project, to detect the causes of the delay that may be due to the failure to deliver the materials on time or to an incorrect order. Further, it is possible to collect data useful for detecting whether the work has been carried out through correct management between the various teams involved in compliance with the provisions of the project and therefore with what has been approved by the appropriate competent bodies.

Concerning BIM, it is a methodology that uses a shared digital representation of a building to facilitate the design, construction, maintenance and in general the making of decisions regarding any aspect of its operating life [25,26].

Therefore, BIM is essentially an IT methodology that can be used by insiders, professionals and, in theory, by any stakeholder linked to physical and non-physical design parts of a given building. It is a digital representation of all data relating to a building, such as geographic coordinates, floor plans, types and related properties of construction materials, the characteristics of individual systems, the chronology of the various construction, maintenance and demolition phases, and energy analysis.

Thanks to BIM it is possible to know, in real time and unambiguously, for example the characteristics of the windows, or insulating materials used, or the performance of the air conditioning system installed, without the need to conduct a redundant inspection. The advantage is not of the individual designer, but of all those involved, such as builders, managers, property owners, public administrators and therefore of all stakeholders.

With the use of these technologies, thanks to the tracking and updating of information continuously in real time, everyone within the team know who did what, when, where and how. Everything is tracked for the entire life cycle of the building. Through the IoT, the BIM can be redefined and recontextualized [27–29]. The IoT allows us to locate people, machines and materials, allowing us to extract useful information to know how and when people, machines and materials interact. Building sites equipped with suitable sensors allow us to know, for example, where and for how long there is the greatest influx of personnel, how the machines are used and if the materials have been delivered or installed. Thanks to radio frequency identification (RFID), people/machines/materials, plants can be monitored, and useful data can be stored and exploited also for example by the facility management, that is the company discipline that deals with the management of the physical work spaces and all those activities necessary to make buildings operational, productive and safe.

2.2. Self Sovereign Identity and Building Artifacts

Within the framework outlined so far, the concepts of SSI, and in particular the concepts of digital identities applied both to individuals and to building artifacts, could play a key role. The principle behind SSIs is that of digital identity managed directly by the user, and no longer digital identity centrally managed [30].

When the Internet was created, the main problem was to create a network of networks, identifying the address of the computer that is connected to the network through the TCP/IP protocol, which, however, does not allow us to trace the identity of the person, organization, or thing that uses computer. To solve this problem, several models have been introduced to identify users online. The first is the centralized model in which to create an identity it is necessary to register an account with the subject providing the online services (service provider). With this model, there is the total absence of control over the data by the person who owns the account. The next model is that of the federated identity and this is the case of SPID. In this model, a third party, the identity provider (IdP) is inserted between the service provider and the person who intends to use them. The latter has an identity (account) registered with the IdP and can use the services provided by third-party sites without having to re-register at their sites, but by logging in through the identity registered with the IdP. Also with this model, there is the absence of control over the data by the person holding the account, and it is better not to entrust the sharing of user information in a secure manner, in particular the sharing of sensitive information, such as identity documents, health data, financial data, to IdPs, such as Google or Facebook.

The decentralized model based on SSIs is made possible thanks to distributed ledger technologies, in particular the Blockchain, and solves the above mentioned problems. It is not based on accounts, but it operates in the same way as real identity. There is a direct relationship with the party that must verify the so-called claims (statements) belonging to a precise digital identity.

The SSI model is based on some key concepts, in particular on the concept of digital identity that can be associate both to natural or legal entity and to thing, of decentralized identifier that allows for the identification of the parties and is an address, of verifiable identifier that contains information about an entity and allows for identification and authentication of such entity, of verifiable attestations that are issued by an issuer, held by a holder and contain information, for example about attestation or authorization received, and on the concept of verifiable presentations that are created by transforming information extracted from Verifiable IDs and/or Attestations. The links among these concepts, given by the European Blockchain Partnership (EBP), are shown in Figure 1. It is extracted from the EBSI's technical specification on their website https://ecas.ec.europa.eu/ (accessed on 8 April 2022).

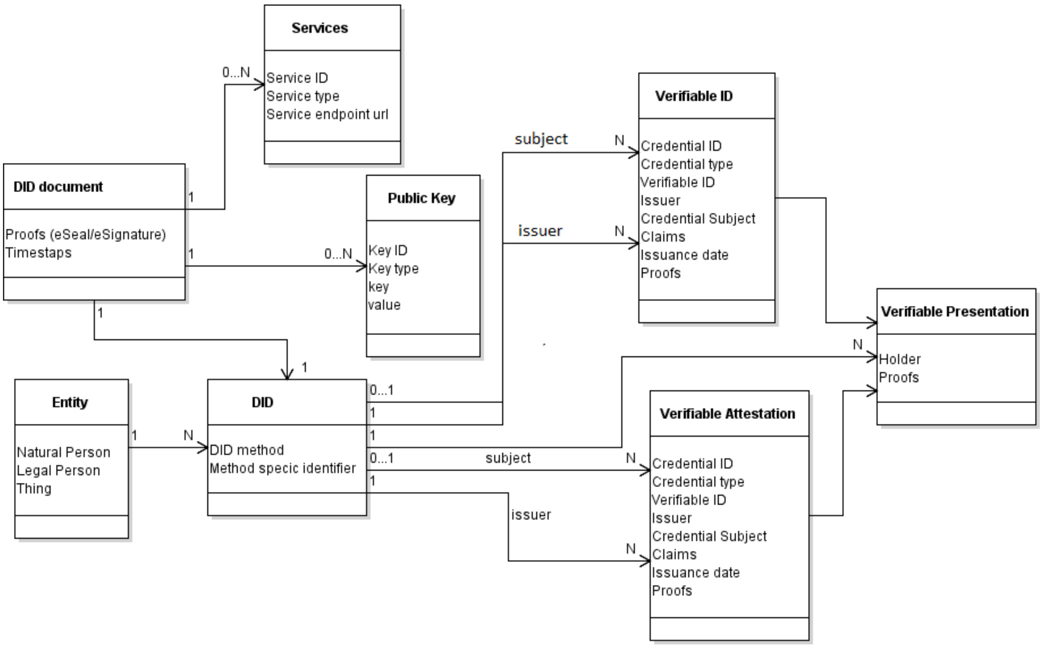


Figure 1. SSI data model proposed by EBSI.

The two main elements for the management systems of these digital identities are highlighted by Lopez [30]:

> *SSI leverages two essential elements for identity management: decentralized registers of information and digital wallets. Decentralized ledgers: The SSI model relies on decentralized registers of information, in which the proofs of ownership of decentralized identifiers and the verifiable credentials are stored within a decentralized ledger. Unlike the centralized, third-party, federated, and user-centric models, which require the verifying entity to somehow reach out to the issuer to verify digital credentials presented to them by the subjects, the SSI model allows the issuer to leave all necessary proofs (cryptographic proofs such as digital signatures and timestamps) in a decentralized public ledger so that anyone can verify them against it. . . . Digital wallets: Digital wallets are portable and secure personal repositories; ideally in the form of a mobile app, they allow us to manage our identifiers, authenticators, data, and verifiable credentials within our phones, which are completely protected and under our control. We decide what information we disclose to whom in the form of verifiable presentations. . . .”*

In the proposed building digitization model, we assume that the building artifacts and all the individuals/organizations that are involved in its design/construction/maintenance during its entire life cycle, which goes from its conception to its demolition, are identified through a digital identity, precisely through a DID. This is because, as defined above, a digital identity, hence his/her/its corresponding identifier, allows for unique identification of an entity that can correspond to both a natural person or legal entity but also to things, i.e., building artifacts.

Each digital identity owns precise Verifiable Credentials (VC) with which some of its attributes are certified, for example the possession of a driving license, the possession of a school diploma and a birth certificate, in the case of a natural person, the possession of certificates of super parties, of competence, independence and impartiality in the case of certification bodies or Public Administrations, the possession of certifications of professionalism in the case of engineers, architects and surveyors, or the possession of energy performance certificates, certificates of town planning compliance, or electrical system certificates in the case of building artifacts.

From this model arises a trilateral relationship, in which there is the *issuer* who issues the credentials, which can be the public or private body, or the identity itself, that certifies a certain status, the *holder* of the credentials that stores them in his/her/its wallet and presents them to third parties when needed, and finally the *verifier* to whom the credentials are presented.

Through the use of DIDs and their DID documents, the SSI model provides for checking the validity of the credentials of a digital identity. These credentials have the characteristic of being permanent, cryptographically verifiable, decentralized and solvable, i.e., able to identify not only the public key of the issuer but also the address connected to it. The DIDs have already been implemented in the W3C context and, therefore, already constitute a standard.

3. Related Work

Many European countries and enterprises are currently working on the development of SSI platforms. Among the most popular SSI platforms there are European Self-Sovereign Identity framework (ESSIF) (ref. https://ecas.ec.europa.eu/ (accessed on 8 April 2022)), uPort/Veramo (ref. https://www.uport.me, https://veramo.io/docs/basics/introduction (accessed on 8 April 2022), and [31,32]), Sovrin (ref. https://sovrin.org/ (accessed on 8 April 2022)), and Civic (ref. https://www.civic.com/ (accessed on 8 April 2022), and [33]), and the first wallets conformant with EBSI have been announced (ref. https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Conformant+wallets (accessed on 8 April 2022)).

Regarding the literature on SSI, recently Cocco et al. [34] presented a system based on SSI to support food supply chains providing full visibility of process/food certifications. Tim et al. [35] proposed an approach based on Blockchain and DIDs to resolve the problem of the reliable identification of the IoT devices. Bartolomeu et al. [36] and Niya et al. [37] discussed the advantages of the SSI systems in combination with industrial IoT applications. Liu et al. [38] proposed and discussed design patterns to be applied in the SSI management system design. Nguyen et al. [39] and Bouras et al. [40] did not take into account the SSI concepts, but only those of the decentralized systems. Precisely the former presented a Blockchain-based authentication system to face the problem of fake educational certificates in Vietnam, while the latter presented an access control architecture for IoT networks.

With regards to the literature on BIM, Turk et al. [25] discussed about the utility of blockchain technology, also in combination with BIM, to provide an infrastructure able to manage in reliable way the information of a building during all its life cycle stages. Zheng et al. [22] proposed a system model, called bcBIM, based on BIM data and blockchain technology, to guarantee data provenance and open sharing, and to prevent tampering in mobile cloud architectures. Hargaden et al. [23] provided insights into the potential of the blockchain technology to improve the efficiency of the processes in the construction industry. Olawumi et al. [24] investigated the factors that influence the adoption of the blockchain in this industry using the system dynamics approach and highlighted the necessity to integrate blockchain technology with those already in use in this sector. Yang et al. [21] applied Blockchain technology to two construction industry cases. Specifically they applied private Blockchain technology to the design process of the suitable external cladding of an apartment and public Blockchain to the acquiring process of the distillation tower of an international big project that has to be bought overseas.

Sattineni et al. [27] explored the possibility of combining RFID technology with BIM to track workers and materials in real time on site. Wang et al. [29] presented the M-ConRDSCM system that manages and improves the flow of information in the construction supply chain, for example, between the offices and the sites, by integrating RFID technology, mobile devices and web portals. Ma et al. [28] proposed a system that integrates BIM and RFID data, following the IFC standards, to display information of the prefabricated components, and monitor their quality during the building life cycle.

4. The System Proposal: An Introduction

In our system proposal, each building, from the moment in which it is conceived to its demolition, is identified by means of a DID. Each building has a BIM model associated with it, therefore multiple files that can be represented through the so-called claims of the SSI model, becoming when necessary verifiable attestations. Not only engineers and architects contribute to associating files to a given building/DID but also appropriate IoT devices, located at strategic points such as the entrance to a construction site in the case of a building under construction. These devices, equipped with suitable RFID readers, take useful data from the RFID tags that detect and associate such data to the building and therefore to the specific DID.

Hence a building under construction could be equipped with RFID readers that, placed at the entrance to the construction site, must detect the RFID tags associated with each material/product/item entering the construction site. These latter tags must be carefully prepared by the manufacturer in such a way that their memory contains detailed information on the technical characteristics with which they are associated. The building could also include a set of cameras that can be used to record crucial moments in the life cycle of a building, such as the installation of insulated panels on the roof, or the installation of windows and air conditioners. In this way, all the characteristics of the materials chosen during the design phase can be compared with those of the products that have actually entered and used on the construction site, and the certifications, for example the energy performance certificates, can thus be drawn up using information extracted both from the BIM files but also from the data collected from the RFID tags and cameras.

The BIM files, all data collected by IoT devices, and all useful files produced by stakeholders support themselves in the various activities that they must conduct in the different stages of the life cycle of a building, such as design, construction, certification and maintenance. For example, temperature and humidity information of some components belonging to the building could be collected in real time, through appropriate sensors, providing a reliable reference for the maintenance personnel to evaluate and maintain the quality of such components making correct decisions. In addition, thanks to data collected by IoT devices, artificial intelligence could be applied to detect operational problems in buildings by monitoring data in real time, and to establish correlations between existing performance and potential malfunctions allowing predictive maintenance or component replacement first problems to occur.

Exploiting the SSI concepts and the Blockchain technology the model proposal ensures audit and provenance of all information associated with a building. First, the model proposal assumes that all building information, which can be requested to the building owner even many years after its realization, is stored in off-chain databases. Each building refers to a precise database at the level of the municipality in which it is located, and refers to a digital wallet, which is a digital portable and secure repository, belonging to building DID. Then the proposal assumes that the hashes of all files stored on the databases/wallet are stored on the Blockchain, and associated with the DID of the building they refer to. Hence for example data extracted reading the RFID tags is automatically collected and stored in the digital wallet of the building DID and its hash is computed and automatically stored on-chain assigning it to that precise DID.

The BIM files generated through specific software by a given stakeholder are also stored in a digital personal wallet belonging to the stakeholder DID. The stakeholders can share these files with other stakeholders through secure and protected digital channels. The stakeholders authorized can load them in the digital wallet of the building DID and their hashes on the chain in the data structure associated with the building DID. In this way, the system allows individual professionals, who are obliged to keep documentation for many years from the end of the assignment, to store all the documentation in clear text in personal repositories and to demonstrate that the information exists from a very specific date, has been notarized by a very precise asymmetric key, and has not been altered.

So in our proposal, the municipality manages an on-chain registry, a DID registry, implemented through a smart contract, which contains the list of all buildings located in its territory. In addition to the DID registry, the municipality manages another registry, implemented again through a smart contract to store the hashes of all files associated with a given building/DID, as well as to store the proofs necessary to prove the validity of all certificated files as expected from a model based on the SSI concepts.

In this way, all files associated to a given building/DID, are notarised and if they are certificated, they become verifiable files, hence as the verifiable credentials of the SSI model, they become permanent, cryptographically verifiable, decentralized and "solvable". In contrast with traditional methods that may take days or months to verify the certification validity, within a SSI-based system this verification process works out smoothly and efficiently. In Figure 2, the two methods are illustrated, showing the steps to be executed to prove the validity of a digital certification issued by a certification authority.

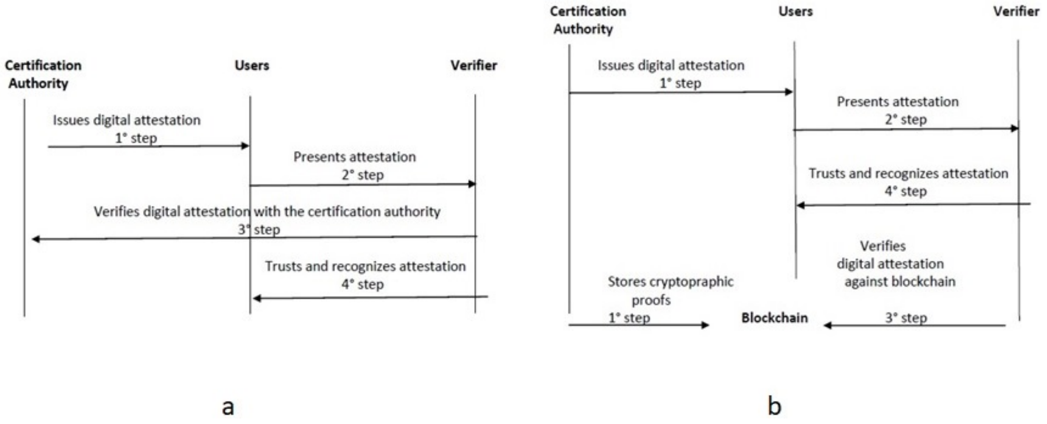

Certification Authority
Users
Verifier
Issues digital attestation 1° step
Presents attestation 2° step
Verifies digital attestation with the certification authority 3° step
Trusts and recognizes attestation 4° step
a
Certification Authority
Users
Verifier
Issues digital attestation 1° step
Presents attestation 2° step
Trusts and recognizes attestation 4° step
Verifies digital attestation against blockchain
Stores cryptopraphic proofs
1° step
Blockchain
3° step
b

Figure 2. (**a**) Traditional Process of verification and (**b**) Process of verification in SSI system.

In the next sections a detailed description of the goal of the system, its actors and user stories is reported, illustrating the details of one of its possible implementations. The design of the system proposal was carried out following the ABCDE method [41].

4.1. ABCDE Method: Goal and Actors

The goal of the system proposal is the digitization of the building sector, exploiting, in addition to BIM, IoT and to Blockchain, the concepts of the new identity management model based on SSI, to contain the risk of fraud, manipulation and corruption, and favor the transparency and verifiability of information related to a building artifact during all its life cycle.

The proposed system is the result of the integration of three different subsystems, each with their own actors and features:

1. Blockchain subsystem: it provides a decentralized infrastructure based on Smart Contracts for managing information relating to a building product throughout its life cycle;
2. IoT device subsystem: system of IoT devices for structural monitoring, for monitoring all systems, electrical, photovoltaic, heating, or for example for monitoring the presence of people or things;
3. Information management platform: web platform that allows authorized users to access information relating to a given building, verify its validity and upload documentation.

Regarding the actors of the system, they are who interact with the system. They can play human roles but also devices and external systems. Actors are outside the system. They interact with it, initiate the use case activity, provide input to it, and/or receive outputs from it. So, for example, a timer that triggers an action is an actor, a smart contract that interacts with the dApp is an actor.

The actors of the system are listed below.

1. System administrator is the one who carries out the deployment on the Blockchain of the contracts used by all users and initializes the system;
2. DIDs are Decentralized IDentifiers representing building artifacts, and users/ stakeholders. They have an owner, whose address can also be replaced by the address of a multi-signature contract, which activates the execution of certain actions only with the multiple signatures, therefore with the approval of multiple users. This functionality will be used in our system by DIDs representing building artifacts. Stakeholders can be Architects / Engineers / Safety Managers / Managers of public bodies. They are the people or companies, identified through a DID in our case an Ethereum address, who use the platform to acquire a document, to notarize a document or to verify the validity of a document;
3. Smart Contracts are the only actors who interact directly with the Blockchain. They are the smart contracts that implement the application logic of the system. For the implementation of the smart contracts listed refer to https://eips.ethereum.org/EIPS/eip-1056, https://github.com/ethereum/EIPs/issues/780, https://docs.soliditylang.org/en/v0.8.4/solidity-by-example.html, and https://solidity-by-example.org/app/multi-sig-wallet/ (accessed on 8 April 2022);
   (a) The *EthereumDIDRegistry.sol* contract tracks all DIDs;
   (b) The *EthereumClaimsRegistry.sol* contract tracks all claims/certificates of DIDs that identify the building artifacts;
   (c) The *Verifier.sol* contract implements the logic for verifying the validity of building artifacts certifications;
   (d) The *MultiSignWallet .sol* contract implements the logic for multiple approval of a given on-chain transaction;
4. IoT Devices interact with the platform by communicating data to be stored on-chain and are identified by an Ethereum address and associated with a given DID;
5. External System is the platform for information management during the entire life cycle of a building artifact. It is the web interface that allows the use of the system, interfacing with the application logic defined by smart contracts.

4.2. ABCDE Method: User Stories and Use Case Diagram

In the following, the user stories used to define the requirements of the system proposal are listed:

- Owners, engineers, architects, installation companies, construction companies, qualified certifiers and managers or managers of specific municipal offices contribute to produce files for a given building/DID;
- Appropriate IoT devices, located in strategic points and equipped with suitable RFID readers, take useful data from the RFID tags that detect and associate such data to the building and therefore to a specific DID;
- Appropriate IoT devices, located in strategic points collect useful data and associate such data to the building and therefore to a specific DID, to track workers, equipment and materials on site;
- Appropriate IoT devices, located in strategic points collect useful data to prepare maintenance actions or other facility management activities during the life cycle of a building;
- The certifications are drawn up using information extracted both from the BIM files and from the data taken from the IoT devices;
- All data/files belonging to a building are stored in a database/wallet off-chain. Hence the system manages the storage in clear text of files in off-chain mode using appropriate databases/structure data;
- Some data/files hashes belonging to a building are stored on-chain;

- The hashes of the notarised files are stored on-chain performing a notarization-only function. In this way we have a timestamping of data by identifiable entities with asymmetric keys. Some files must be notarised but only some are certified;
- The hashes of the certified files are stored on-chain, in the Blockchain, with the proofs that prove their validity. In this way a file becomes a verifiable file;
- All the potential verifiers can verify the validity of the files/certifications since they are permanent, cryptographically verifiable, decentralized and "solvable";
- A process of multiple authorized signatories allows the storage of some files only after having reached a precise number of signatures, hence multiple approval;
- The system must improve, enhance the management of the information flow between offices and locations where the property is located, and/or between these and all the nodes that make up the building chain that revolves around a given property. To this end, friendly dashboards are opportunely prearranged to allow users access to all system functions;
- The system includes analysis software and visualization dashboards. All the information collected is processed to obtain valuable information in the context of decision making, with the possibility of obtaining a centralized and immediate consultation view of the entire building.

From the user stories we extracted some use cases (see Figure 3) and the different classes that make up the system, that are shown in an UML (unified model language) class diagram in Figure 4, and described as follows.

- *Creator/Admin*: the one who deploys the contracts and the external system;
- *Entity*: class representing the natural person, legal person or thing that is below a DID;
- *DID*: class representing stakeholders and construction products;
- *Information Management Platform*: class representing the Information Management Platform that allows all stakeholders to access and manage information relating to a DID;
- *IoT Device*: class representing IoT devices owned by a DID;
- *Notarized File*: It contains information used to prove who is behind the entity that has created this file;
- *Verifiable File*: This type of file is issued by an entity certified and contain information used to prove attributes or properties issued by this entity. This file is accepted as true. In the SSI models there are both data self certifications and 3rd party data certifications.

4.3. ABCDE Method: On-Chain Subsystem

We start analysing in detail the two typologies of files that our system must manage, given that we present a system proposal for the information flow management among offices and building and in general for facility management, hence for managing everything concerning the management of buildings, for example, plants (electrical, mechanical, plumbing), green areas, cleaning, surveillance but also company catering and concierge services in the case of company buildings. So the way in which the system manages data and information plays a key role.

Let us see in detail the mechanisms by which the data are stored, focusing on the newest and most innovative part of the proposal, hence let us analyze data notarisation and data certification.

The first mechanism guarantees *timestamp*, that is, certain data have existed for a certain time; *authentication*, that is, the data have been created by an asymmetric key; *non-repudation*, that is, the sender cannot deny having sent the information; and *integrity*, that is, the information has not been altered. In addition, it guarantees that data can be verified by every verifiers but that data has been created only by the owner of the key.

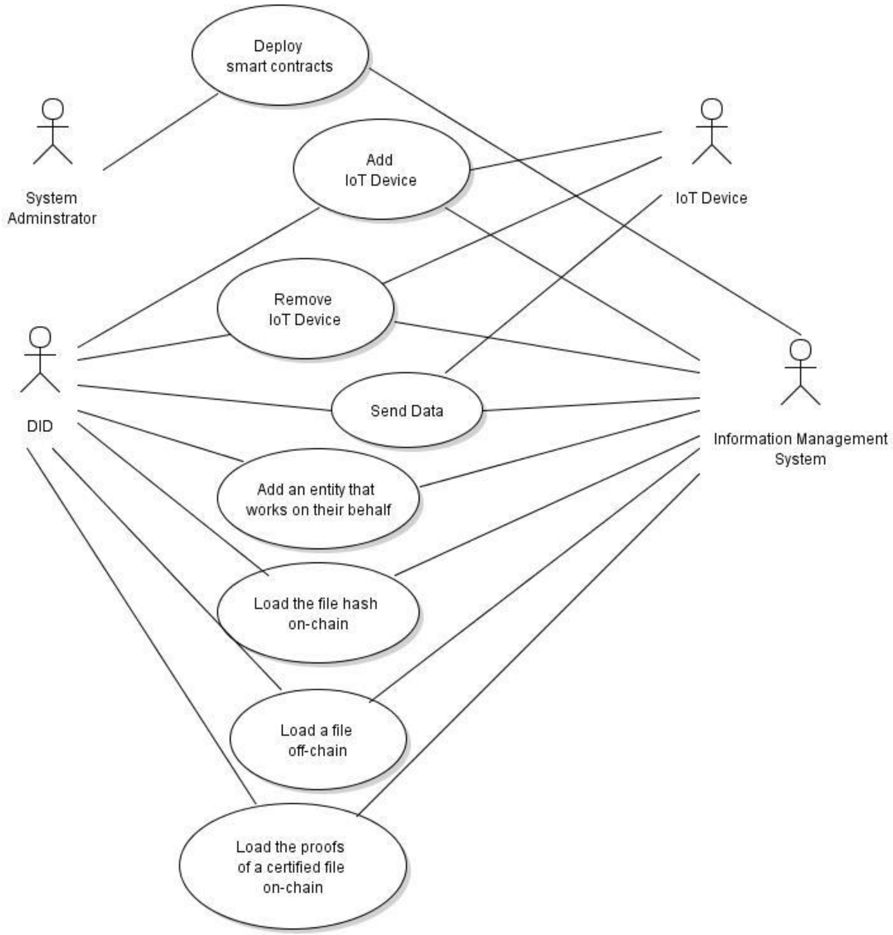

Deploy smart contracts
System Adminstrator
Add IoT Device
IoT Device
Remove IoT Device
DID
Send Data
Information Management System
Add an entity that works on their behalf
Load the file hash on-chain
Load a file off-chain
Load the proofs of a certified file on-chain

Figure 3. Format for Verifiable ID and Attestation signed with a DID Key.

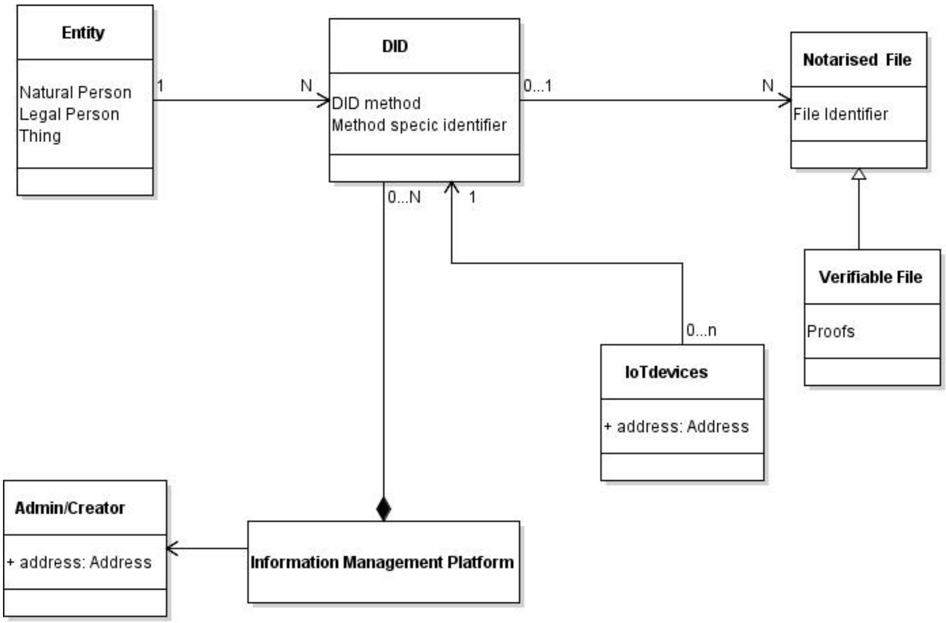


Figure 4. Class Diagram of the whole system without taking into account the methodology used for its implementation.

In turn, the second mechanism guarantees that data are notarised by a certified identity and this type of data is accepted as true and valid and contains the proofs to prove their validity. In addition through multi-signature mechanisms, data that are associated with a given certification or building practice, can be notarised by multiple identities, such as qualified certifiers together with executives or managers of the competent municipal offices.

4.3.1. Notarized and Verifiable Files

Regarding the notarized files, hence in the case of the sole notarisation, the entity that wants to certify to third parties, the so-called verifiers, the possession of a document on a certain date, and that this is not subsequently modified, must proceed as follows. It must compute the document hash digest using a standard algorithm, write the hash on a public Blockchain and disseminated, and keep the digital document, making sure it remains unaltered. The verifier entity, at any time after the hash has been registered in the Blockchain, can verify the document validity if it is provided with the original document, the hash algorithm and the data of the transaction that wrote the hash on the Blockchain.

Instead, as specified by Lopez [30], in the case of verifiable files the entity that wants to certify to verifiers the possession of a certified document must make available them the following data:

- *URI to uniquely identify the credential—Credential: representation of an identity for use in authentication. A credential is a set of one or more claims made by an issuer about a subject. A credential is associated with an identifier and/or the subject of the credential (e.g., DIDs);*
- *URI to identify the issuer (e.g., a DID);*
- *URI to identify the credential type;*
- *URI to identify terminology and protocols that allow parties to read the credential;*
- *Cryptographic proof of the issuer;*
- *Claims data—Claim: characteristic or statement about a subject made by an issuer as part of a credential—or metadata;*
- *Issuance date;*
- *Expiration conditions;*
- *Location of the credential status (e.g., a smart contract in a Blockchain network).*

4.3.2. Format for Verifiable Files

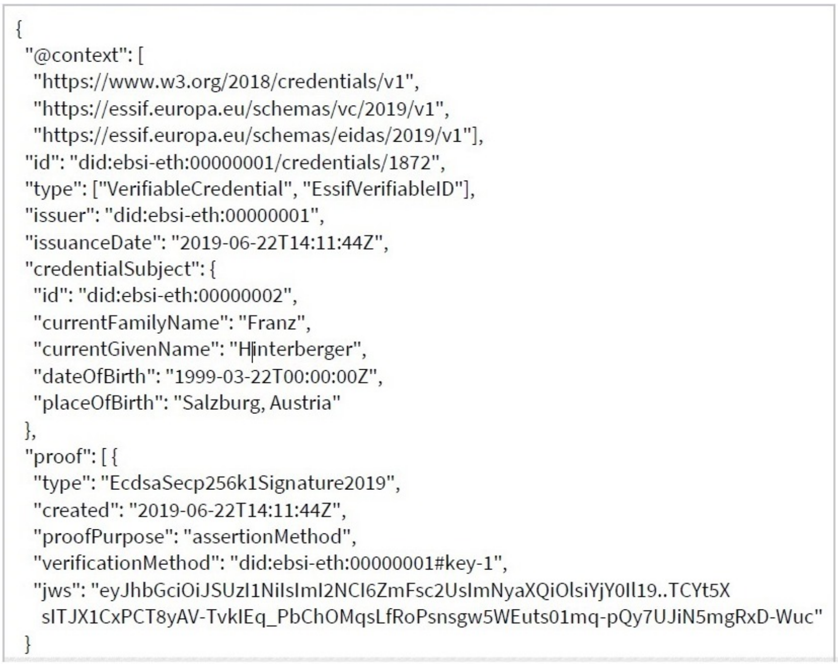
The system proposal assumes that both the typologies of files that stem from the mechanisms of notarization and certification, mentioned above, can be exchanged using secure and protected digital channel and using the suggested formats by EBSI, such as JSON-LD. This format is also in accordance with the DIDs standard developed by the W3C. In Figure 5, an example of Verifiable ID in Json-ld format signed with a DID Key is shown, the definition of its properties, such as Contexts, Identifiers, Types, Issuers, Credential Subject, Issuer, Issuance Date, Expiration, Status and Proofs, follows. It is extracted from the EBSI's technical specification in web site https://ecas.ec.europa.eu/ (accessed on 8 April 2022).

- *Contexts: JSON-LD contexts define the terminology used to describe data, in order to ensure that both producers and consumers of data have a shared understanding of the semantics; . . .*
- *Identifiers: The W3C specification requires the use of URIs to unambiguously refer to a person or other subject of a Verifiable ID or Attestation. ESSIF further constrains this by requiring the use of Decentralized Identifiers (DIDs) for both the Issuer and Credential Subject;*
- *Types: The W3C specification requires at a minimum a single type to be used (VerifiableCredential) and allows additional types. ESSIF defines the following additional types. EssifVerifiableID: To be used in the case of an ESSIF Verifiable ID. EssifVerifiableAttestation: To be used in the case of an ESSIF Verifiable Attestation; . . .*
- *Issuer: The Issuer of an ESSIF Verifiable ID or Verifiable Attestation is a public institution, company, or other organization that is a trusted source of claims of a certain type. For example, a university may be an Issuer for Verifiable Attestations of type DiplomaVerifiableAttestation. A bank may be an Issuer for a credit score. An employer may issue confirmations of employment. A government may be an Issuer for Verifiable IDs. In ESSIF, Issuers of Verifiable IDs and Verifiable Attestations are identified by DIDs;*

- *Credential Subject: The Credential Subject is the individual (or organization, thing, animal, etc.) described by a Verifiable ID or Verifiable Attestation. In ESSIF, Credential Subjects of Verifiable IDs and Verifiable Attestations are identified by DIDs;*
- *Claims: Claims constitute the 'substance' of a Verifiable ID or Attestation - they are semantic statements that express a certain value for an attribute of the DID Subject. For example, if an attribute is placeOfBirth, then a claim could be "The Credential Subject identified by did:ebsi-eth:00000001 has an attribute placeOfBirth with the value Vienna";*
- *Issuance Date:... Even though this property is called issuanceDate, it actually indicates the date and time when the credential becomes valid. This may or may not be the same as the date and time when the credential is issued;*

  Expiration Date: The Expiration Date property (expirationDate) has the purpose of expressing expiration information of a Verifiable ID or Attestation, i.e., if and when it expires. If present, the value of this property must be a string value of an combined date and time string representing the date and time the credential ceases to be valid;

  Status: The Status property (credentialStatus) has the purpose of allowing the discovery of information about the current status of a Verifiable ID or Attestation, such as whether it is suspended or revoked. The value of this property must include a) the id property (which must be a URL) and the b) type property, which expresses the credential status type (also referred to as the credential status method);
- *Proofs: The W3C specification requires at least one proof mechanism to be used for Verifiable IDs or Attestations, and allows multiple proof mechanisms. For ESSIF, the following proofs will be used: An ESSIF Verifiable ID or Attestation MUST contain a Linked Data Proof that is a signature by the Issuer, according to the Issuer's DID method;*
- *Extensibility: The W3C specification allows the data model to be extended, e.g., by introducing additional properties and vocabularies.*



```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://essif.europa.eu/schemas/vc/2019/v1",
  "https://essif.europa.eu/schemas/eidas/2019/v1"],
 "id": "did:ebsi-eth:00000001/credentials/1872",
 "type": ["VerifiableCredential", "EssifVerifiableID"],
 "issuer": "did:ebsi-eth:00000001",
 "issuanceDate": "2019-06-22T14:11:44Z",
 "credentialSubject": {
  "id": "did:ebsi-eth:00000002",
  "currentFamilyName": "Franz",
  "currentGivenName": "Hinterberger",
  "dateOfBirth": "1999-03-22T00:00:00Z",
  "placeOfBirth": "Salzburg, Austria"
 },
 "proof": [ {
  "type": "EcdsaSecp256k1Signature2019",
  "created": "2019-06-22T14:11:44Z",
  "proofPurpose": "assertionMethod",
  "verificationMethod": "did:ebsi-eth:00000001#key-1",
  "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
   sITJX1CxPCT8yAV-TvkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-Wuc"
 }
```

Figure 5. Format for Verifiable ID and Attestation signed with a DID Key.

Following the recommendation by EBP and by Lopez [30], the system proposal presented in this work assumes that the DIDs of all entities can be found and resolved in the Blockchain as described in the next section. In addition it assumes that a file in clear text is never registered in the Blockchain, but in clear text in an off-chain database/wallet having an adequate access control system, and that the file's status, that can be *active* or *revoked* and modified only by the issuer, and the hash of the file and the signature of the hash of the file, that is stored in clear text in the off-chain database, are stored on-chain.

4.3.3. Decentralized IDentities and Their Registry

To design the system we refer to one of the most popular DID platforms, Veramo. It evolved from Uport in 2021. Contrary to uPort, Veramo is a more flexible and modular architecture, can run on web, mobile, and backend stack and can be easilier extended through add-on packages [42–44].

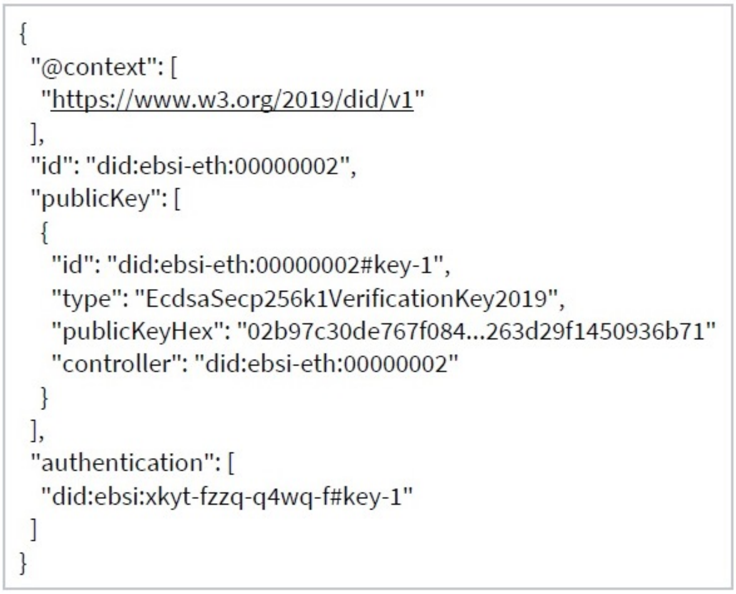
Veramo consists of identity and messaging protocols that together form a layer of interoperable identity for the decentralized web to return ownership of the identity to the individual (see web site https://veramo.io/docs/basics/introduction and https://developer.uport.me/#platform (accessed on 8 April 2022) and [31,33,43]). It is a DID platform designed to be compatible with any distributed ledger or network, as specified in [43] in which the authors wrote

> *Decentralized Identifiers are designed to be compatible with any distributed ledger or network. In the Ethereum community, a pattern known as ERC1056 utilizes a smart contract for a lightweight identifier management system intended explicitly for off-chain usage.*
> *The described DID method allows any Ethereum smart contract or key pair account, or any secp256k1 public key to become a valid identifier. Such an identifier needs no registration. In case that key management or additional attributes such as "service endpoints" are required, they are resolved using ERC1056 smart contracts deployed on the networks listed in the registry repository.... ERC1056 proposes a way of a smart contract or regular key pair delegating signing for various purposes to externally managed key pairs. Any Ethereum account regardless of whether it's a key pair or smart contract based is considered to be an account identifier. An identity needs no registration. Each identity has a single address which maintains ultimate control over it. By default, each identity is controlled by itself. As ongoing technological and security improvements occur, an owner can replace themselves with any other Ethereum address, such as an advanced multi-signature contract. There is only ever a single identity owner. More advanced ownership models are managed through a multi-signature contract. ...Delegates are addresses that are delegated for a specific time to perform a function on behalf of an identity. ...The type of function is simply a string that is determined by a protocol or application higher up.*

The ERC1056 is an Ethereum standard proposed for creating and updating identities. It allows identities to have an unlimited number of delegates and attributes associated with it. This standard is fully DID compliant hence it follows the W3C proposed recommendations.

4.3.4. Decentralised IDentities and DID Document

By a method, the so called DID method, *did:ethr*, each Ethereum address is associated with an identity in the the DID registry (ERC1056 contract), and with its DID document stored for example on IPFS (ref. https://veramo.io/docs/veramo_agent/did_methods and https://developer.uport.me/pki/diddocument (accessed on 8 April 2022)). In Figure 6, an example of a DID document with some of its properties is shown. The *Contexts* property describes the terminology used to represent data, to ensure that the shared data is understood; *DID Subject* is the entity identified by the DID; *Public Keys* are the public keys associated with the DID and are need for secure and authenticated communications; and finally the *Authentication* property refers to public keys and serves for proving both the control and the ownership of a DID, for example during a data exchange between a Holder and a Verifier. There are also other two properties, *Proof* and *Extensibility* that are optional. *Proof* can be used to add data necessary to prove for example aspects of integrity or trust; while the *Extensibility* property can be used to add useful metadata about the DID Subject.



```
{
 "@context": [
  "https://www.w3.org/2019/did/v1"
 ],
 "id": "did:ebsi-eth:00000002",
 "publicKey": [
  {
   "id": "did:ebsi-eth:00000002#key-1",
   "type": "EcdsaSecp256k1VerificationKey2019",
   "publicKeyHex": "02b97c30de767f084...263d29f1450936b71"
   "controller": "did:ebsi-eth:00000002"
  }
 ],
 "authentication": [
  "did:ebsi:xkyt-fzzq-q4wq-f#key-1"
 ]
}
```

Figure 6. ESSIF DID document.

4.3.5. Decentralised IDentities and Verifiable Files

Veramo uses ERC1056 as the DID standard, and EIP-1812 as the standard for the claims registry (ref. [45] and https://eips.ethereum.org/EIPS/eip-1056 (accessed on 8 April 2022)). EIP-1812 is the method proposed for the management of Off-Chain Verifiable Claims [46,47]. Through this EIP the claims can be stored off chain and verified on-chain by Solidity Smart Contracts, by the implementation of state channel, or by the use of off-chain libraries. The previous standards are ERC-735 and ERC-780. These standards manage claims living on chain (ref. [48] and https://github.com/ethereum/EIPs/issues/780 (accessed on 8 April 2022)), as a result in some circumstances, for example where the EU GDPR rules must be respected, storing claims on chain containing personal information on a public database is illegal.

To implement the logic that manages the storage of the files's hashes, and some of their key features, such as their status, we can refer to the Ethereum claims registry implemented by ERC780, that must be customized to accomplish the requirements of our system and that just has to memorize the information in agreement with the EU GDPR rules. For example, regarding the notarised files, we can assume that only the owner of the identity, which the file's hash refers to, can add the hash in the registry. Regarding the verifiable files, we can assume that only the owner of the identity, which the features refer to, can add these data in the registry, and only the issuer of these files can modify their status. We can customize the ERC780 contract, called `EthereumClaimsRegistry.sol` contract, replacing the `mapping` named *registry* with two mappings, the *notarisedFilesRegistry* and *verifiableFilesRegistry* mapping. In solidity the `mapping` is a data structure. The first mapping manages the notarised files and could be defined as follows:

$$mapping(address => mapping(uint => string))$$

$$public \quad notarisedFilesRegistry;$$

where *notarisedFilesRegistry* maps keys of type *address* to a new mapping, that maps *uint*, that is a counter, to *string*. The keys are the addresses of the DID to which the values of type *string* refers. The values of type *string* are the hashes of the files uploaded in the external database. So, for example this data structure could be defined as:

$$notarisedFilesRegistry[identity][counter][hash].$$

The second mapping manages the verifiable files and could be defined as:

$$mapping(address => mapping(uint =>$$

$$mapping(string => mapping(address => mapping(bytes => string)))$$

$$public \quad verifiableFilesRegistry;$$

where *notarisedFilesRegistry* is similar to the previous one but it adds to the previous structure data another mapping that maps values of type *address*, that refer to the address of the issuer that issued the file associated with the hash, to the mapping that maps values of type *bytes*, that refer to the proofs generated by the issuer, to values of type *string* that represent the status of that file. So, for example this second data structure could be defined as:

$$verifiableFilesRegistry[identity][counter][hash]$$

$$[issuer][proof][status].$$

Through this standard the proposal could implement a public distributed registry to collect useful data about building DID files and manage the stored data. In fact the ECR780 defines for example the functions for adding claims, for getting claims, and for removing claims, and defines two events, to track the claims issued and removed. The proposal provides that the identity of the verifiable files' issuer is recovered through his/her address, the so called *msg.sender* in Solidity language. Specifically by a smart contract and using the *v, r, s* signature parameters the issuer's identity can be recovered (ref. to web site https://docs.soliditylang.org/en/v0.8.4/solidity-by-example.html (accessed on 8 April 2022)).

4.3.6. Decentralised IDentities and Multisignature Contract

The system proposal must manage the logic that guarantees that some types of files are stored on-chain only after having had the consent of more identities. To manage this requirement, our proposal exploits the multisignature smart contracts. This is because each identity has a single address which maintains ultimate control over it, has one only owner, but this can be replaced with any other Ethereum address, including an advanced multi-signature contract.

Our proposal uses a multisignature smart contract to interact with the `EthereumClaimsRegistry.sol` contract. In particular the `setClaim` method, of the above quoted contract, cannot be executed without a multisignature approval. To implement the multisignature contract we refer to the implementation shown on the website https://solidity-by-example.org/app/multi-sig-wallet/ (accessed on 8 April 2022).

The `MultiSigWallet.sol` contract constructor requires an array of addresses and the number of required confirmations to execute a transaction.

To submit the transaction adds a claim to the state of the `EthereumClaimsRegistry.sol` contract, to the `MultiSigWallet.sol` contract, we execute the `submitTransaction` method of the `MultiSigWallet.sol` contract. This method takes the address of the destination contract, that is the address of the `EthereumClaimsRegistry.sol` contract, the value to be send with the transaction, that is the hash to be stored, and the transaction data, which includes the encoded method signature and its input parameters.

By executing the `submitTransaction` method, the fired events, `Submission` and `Confirmation`, appear in the so-called "log" memory of Ethereum, which is what is expected. A number of confirmations equal to the number of required confirmations to execute the transaction passed to the constructor of the `MultiSigWallet.sol` contract causes the transaction to execute. As a result, the address that has updated the `EthereumClaimsRegistry.sol` contract is that of the `MultiSigWallet.sol` contract.

4.3.7. Decentralised IDentities and IoT Devices

As already mentioned, not only do entities represented by legal or natural persons contribute to associating files to a given building/DID but they also appropriate IoT devices, located in strategic points inside the building. These devices belong to the DID, and the DID sets them as its delegates through the *addDelegate* method of the *EthereumDIDRegistry.sol* contract. Hence the delegates are the addresses of the IoT devices that are delegated by the DID owner for a specific time to perform a function on behalf of its identity. The DID owner sets the type of function that IoT devices must perform. For example, the DID owner can set this variable equal to *attestor* to attest to the authenticity of the send data from this device. The system could derive a unique identifying key for each IoT device exploiting the manufacturing variability of the devices' SRAM chips, through the so-called Physically Unclonable Function (PUF) [37] to identify reliably the devices. The IoT device subsystem interacts both with the Blockchain subsytem and with the information management platform. The several sensors acquire data and, through the IoT subsystem, forward it to the information management platform, hence also to the client/Ethereum node, which in turn communicates them to the smart contract at time intervals pre-established or at the request of some stakeholders, through remote procedure calls.

5. Conclusions and Future Works

In this work, we present a system proposal that exploits the public Blockchain concepts in combination with those of the BIM, IoT and SSI to ensure the eligibility, transparency and traceability of the entire life cycle of a building artifact. We are working to its implementation by a decentralized application, designed and implemented following the so called Agile Block Chain Dapp Engineering (ABCDE) method [41].

In Figure 7, the class diagram that describes the model proposal is shown.

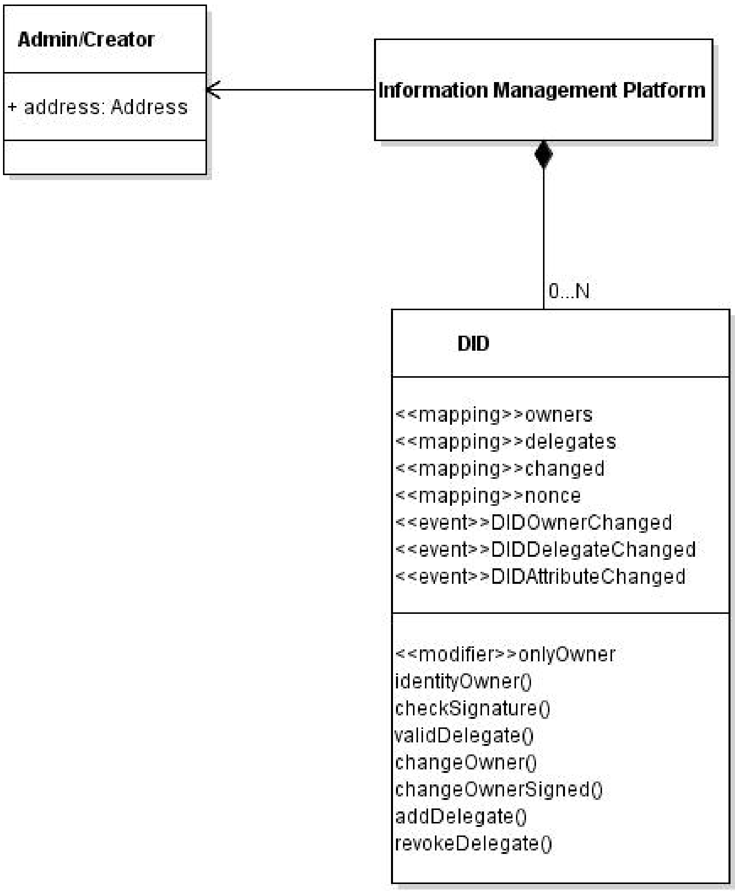


Figure 7. Class diagram of the whole system proposal.

The DID class describes all system entities, representing them with an Ethereum address. It models all stakeholders, hence all interested parties, that is, any person, group or entity that may be affected by a decision or changes during the life cycle of a building, including the building itself. So, in the model proposal, buildings are modeled through DIDs, and the IoT devices, appropriately placed in the building under construction or finished are modeled as DID delegates and are identified by an Ethereum address. The entire logic that allows entities to interact among them is implemented from the Information Management Platform. This platform includes all smart contracts, servers, and the user interfaces for a friendly information management. The proposal is designed to exploit the Veramo project, which stems from the uPort project that was split into two projects, Serto and Veramo. Both projects carry on the mission of decentralizing the internet and returning control of their data to individuals.

In this work, innovative technologies allow the development of a system for the efficient management of digital identities related to natural persons, organizations, or things, in our case building artifacts. All these digital identities can independently manage their claims/attributes also through zero knowledge proof algorithms, deciding from time to time which ones to share and with whom. So a digital identity can be the holder of the claims—the issuer—that is, the digital identity that issues a credential—or the verifier—that is, the digital identity that verifies in real time and at any time the validity of a given credential. The proposal presents a system that must manage the storage and recovery of all claims/information, the verification of their validity and in general the information management automatically.

It is an ambitious model, a novelty for international buildings, that, by exploiting the Blockchain technology together with the concepts of SSI, IoT and BIM, aims at the digitization of the construction sector, reducing not only costs, waste of time and bureaucratic complexity, but also the distance between citizens and institutions, strengthening trust in digital services and promoting their diffusion.

Future work will aim to investigate in detail the notarization of the work flow in the so called CDE. The British technical legislation has proposed an organic structuring of the CDE with the definition of four areas: "Work in Progress", "Shared", "Published Documentation" and "Archive" (ref. https://bimportal.scottishfuturestrust.org.uk/level2/stage/1/task/22/overview-of-the-common-data-environment-cde (accessed on 8 April 2022)). The transfer of information (for example, the transfer of a model or a document) from one area of the CDE to the next must take place through appropriate checks and verifications. The outcome of these checks and verifications will lead to approving or not the passage of the information to the next area. The approval procedures, therefore, are put in place to safeguard the correct flow of information. Future work will investigate a real infrastructure capable of guaranteeing a series of safety parameters in the relationship between BIM platforms with CDE, in the various delivery phases of the BIM supply chain of the documents. It will investigate a DID-based secure, private communication methodology to try to disengage from identity providers, certificate authorities, and in general from every centralization. Starting from Veramo, which works closely with the W3C and DIF, it will investigate their Messaging Protocols plugin in which "individuals on semi-connected mobile devices become full peers of highly available web servers operated by IT experts (ref. https://identity.foundation/didcomm-messaging/spec/#purpose-and-scope (accessed on 8 April 2022))".

Author Contributions: Conceptualization, L.C. and R.T.; methodology, L.C.; software, L.C.; validation, L.C., R.T. and M.M.; 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., R.T. and M.M.; visualization, L.C., R.T. and M.M.; supervision, L.C., R.T. and M.M. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by Sardegna Ricerche-Regione Autonoma della Sardegna–R&D Program Agroindutria–POR FESR Sardegna 2014-2020–Azione 1.2.2–under Project "Complete Assessment of Smart contracts and Coin Offers (C.A.S.C.O.)" under project code: 2014IT16RFOP015.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. European-Commission. *A European Green Deal*; European-Commission: Brussels, Belgium, 2020.
2. European-Commission. *In Focus: Energy Efficiency in Buildings*; European-Commission: Brussels, Belgium, 2020.
3. 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.
4. Akram, U.; Fülöp, M.T.; Tiron-Tudor, A.; Topor, D.I.; Căpuşneanu, S. Impact of Digitalization on Customers' Well-Being in the Pandemic Period: Challenges and Opportunities for the Retail Industry. *Int. J. Environ. Res. Public Health* **2021**, *18*, 7533. [CrossRef] [PubMed]
5. Walter, L.; Denter, N.M.; Kebel, J. A review on digitalization trends in patent information databases and interrogation tools. *World Pat. Inf.* **2022**, *69*, 102107. [CrossRef]
6. Ionescu, C.A.; Fülöp, M.T.; Topor, D.I.; Căpuşneanu, S.; Breaz, T.O.; Stănescu, S.G.; Coman, M.D. The New Era of Business Digitization through the Implementation of 5G Technology in Romania. *Sustainability* **2021**, *13*, 3401. [CrossRef]
7. Matt, D.T.; Pedrini, G.; Bonfanti, A.; Orzes, G. Industrial digitalization. A systematic literature review and research agenda. *Eur. Manag. J.* 2022; *in press*. [CrossRef]
8. Aung, M.M.; Chang, Y.S. Traceability in a food supply chain: Safety and quality perspectives. *Food Control* **2014**, *39*, 172–184. [CrossRef]
9. Rejeb, A.; Keogh, J.G.; Treiblmaier, H. Leveraging the internet of things and blockchain technology in supply chain management. *Future Internet* **2019**, *11*, 161. [CrossRef]
10. Feng, T. A supply chain traceability system for food safety based on HACCP, blockchain & Internet of things. In Proceedings of the 14th International Conference on Services Systems and Services Management (ICSSSM 2017), Dalian, China, 16–18 June 2017. [CrossRef]
11. Baralla, G.; Pinna, A.; Corrias, G. Ensure Traceability in European Food Supply Chain by Using a Blockchain System. In Proceedings of the 2nd International Workshop on Emerging Trends in Software Engineering for Blockchain, Montreal, QC, Canada, 27–27 May 2019; pp. 40–47. [CrossRef]
12. Baralla, G.; Pinna, A.; Tonelli, R.; Marchesi, M.; Ibba, S. Ensuring transparency and traceability of food local products: A blockchain application to a Smart Tourism Region. *Concurr. Comput. Pract. Exp.* **2020**, *33*, e5857. [CrossRef]
13. Pranto, T.H.; Noman, A.A.; Mahmud, A.; Haque, A.B. Blockchain and smart contract for IoT enabled smart agriculture. *PeerJ Comput. Sci.* **2021**, *7*, e407. [CrossRef] [PubMed]
14. Haihui, H.; Xiuxiu, Z.; Jun, L. Food Supply Chain Traceability Scheme based on Blockchain and EPC Technology. Available online: https://easychair.org/publications/preprint_download/5x9H (accessed on 15 March 2022).
15. Xu, Q.; Song, Z.; Mong Goh, R.S.; Li, Y. Building an Ethereum and IPFS-Based Decentralized Social Network System. In Proceedings of the 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, 11–13 December 2018; pp. 1–6. [CrossRef]
16. Chen, Y.; Li, H.; Li, K.; Zhang, J. An improved P2P file system scheme based on IPFS and Blockchain. In Proceedings of the 2017 IEEE International Conference on Big Data (Big Data), Boston, MA, USA, 11–14 December 2017; pp. 2652–2657.
17. Ali, M.S.; Dolui, K.; Antonelli, F. IoT data privacy via blockchains and IPFS. In Proceedings of the Seventh international Conference on the Internet of Things, Linz, Austria, 22–25 October 2017; pp. 1–7.
18. Zheng, Q.; Li, Y.; Chen, P.; Dong, X. An innovative IPFS-based storage model for blockchain. In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), Santiago, Chile, 3–6 December 2018; pp. 704–708.
19. Norvill, R.; Fiz Pontiveros, B.B.; State, R.; Cullen, A. IPFS for Reduction of Chain Size in Ethereum. In Proceedings of the 2018 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), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1121–1128. [CrossRef]
20. Cocco, L.; Mannaro, K.; Tonelli, R.; Mariani, L.; Lodi, M.B.; Melis, A.; Simone, M.; Fanti, A. A Blockchain-Based Traceability System in Agri-Food SME: Case Study of a Traditional Bakery. *IEEE Access* **2021**, *9*, 62899–62915. [CrossRef]
21. 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]
22. 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. *Math. Probl. Eng.* **2019**, *2019*, 5349538. [CrossRef]

23. 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 Sophia-Antipolis, France, 17–19 June 2019; pp. 1–6. [CrossRef]
24. 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.
25. Turk, Ž.; Klinc, R. Potentials of Blockchain Technology for Construction Management. *Procedia Eng.* **2017**, *196*, 638–645. [CrossRef]
26. Panagiotidou, N. The Need for BIM Standards in Digital Construction. *Breakwithanarchitect*, 15 March 2019.
27. 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, 25–27 June 2010*; Brno, T., Ed.; International Association for Automation and Robotics in Construction (IAARC): Batislava, Slovakia, 2010; pp. 346–354. [CrossRef]
28. 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. *Adv. Civ. Eng.* **2019**, *2019*, 6870507. [CrossRef]
29. Wang, L.C.; Lin, Y.C.; Lin, P.H. Dynamic mobile RFID-based supply chain control and management system in construction. *Adv. Eng. Inform.* **2007**, *21*, 377–390. [CrossRef]
30. López, M.A. *Self Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain*; Technical report; Inter-American Development Bank: Washington, DC, USA, 2020.
31. Lipińska, A. uPort Serto Ecosystems: Creating Trusted Data Networks between Businesses and Individuals. Available online: https://medium.com/uport/uport-serto-ecosystems-creating-trusted-data-networks-between-businesses-and-individuals-ff21c9368d3b (accessed on 14 June 2021).
32. Braendgaard, P. Different Approaches to Ethereum Identity Standards. Available online: https://medium.com/uport/different-approaches-to-ethereum-identity-standards-a09488347c87 (accessed on 14 June 2021).
33. Coutts, V. The Who's Who of Decentralized Identity Systems. Available online: https://medium.com/linum-labs/the-whos-who-of-decentralized-identity-systems-433b2dd9a195 (accessed on 14 June 2021).
34. Cocco, L.; Tonelli, R.; Marchesi, M. Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain. *Future Internet* **2021**, *13*, 301. [CrossRef]
35. Weingaertner, T.; Camenzind, O. Identity of Things: Applying concepts from Self Sovereign Identity to IoT devices. *Peer Rev. Res.* **2021**, *4*. [CrossRef]
36. Bartolomeu, P.C.; Vieira, E.; Hosseini, S.M.; Ferreira, J. Self-Sovereign Identity: Use-cases, Technologies, and Challenes for Industrial IoT. In Proceedings of the 2019 24th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Zaragoza, Spain, 10–13 September 2019; pp. 1173–1180. [CrossRef]
37. Niya, S.R.; Jeffrey, B.; Stiller, B. 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.
38. Liu, Y.; Lu, Q.; Paik, H.Y.; Xu, X. Design Patterns for Blockchain-Based Self-Sovereign Identity. Available online: https://arxiv.org/pdf/2005.12112.pdf (accessed on 15 March 2022).
39. Nguyen, B.M.; Dao, T.C.; Do, B.L. Towards a blockchain-based certificate authentication system in Vietnam. *PeerJ Comput. Sci.* **2020**, *6*, e266. [CrossRef] [PubMed]
40. Bouras, M.A.; Xia, B.; Abuassba, A.O.; Ning, H.; Lu, Q. IoT-CCAC: A blockchain-based consortium capability access control approach for IoT. *PeerJ Comput. Sci.* **2021**, *7*, e455. [CrossRef] [PubMed]
41. Marchesi, L.; Marchesi, M.; Tonelli, R. ABCDE—Agile block chain DApp engineering. *Blockchain Res. Appl.* **2020**, *1*, 100002. [CrossRef]
42. uPort. Veramo: uPort's Open Source Evolution. 2021. Available online: https://medium.com/uport/veramo-uports-open-source-evolution-d85fa463db1f (accessed on 4 January 2022).
43. 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).
44. Bugyis. Introducing Veramo. 2021. Available online: https://medium.com/uport/introducing-veramo-5a960bf2a5fe (accessed on 4 January 2022).
45. Beregszaszi, A.; Braendgaard, P.; Zoltu, M.; Entriken, W. Ethereum Verifiable Claims. 2021. Available online: https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1812.md (accessed on 4 January 2022).
46. Braendgaard, P. EIP-1812: Ethereum Verifiable Claims, Ethereum Improvement Proposals, no. 1812. 2019. Available online: https://eips.ethereum.org/EIPS/eip-1812 (accessed on 4 January 2022).
47. Bloemen, R.; Logvinov, L.; Evans, J. EIP-712: Ethereum Typed Structured Data Hashing and Signing, Ethereum Improvement Proposals, no. 712. 2017. Available online: https://eips.ethereum.org/EIPS/eip-712 (accessed on 4 January 2022).
48. Santos, J. First Impressions with ERC 725 and 735 Identity and Claims. 2018. Available online: https://hackernoon.com/first-impressions-with-erc-725-and-erc-735-identity-and-claims-4a87ff2509c9 (accessed on 4 January 2022).