Università di Modena e Reggio Emilia
Dipartimento di Scienze e Metodi dell'Ingegneria

Corso di Dottorato in ingegneria dell'innovazione industriale

Certified management of competences in web 3.0

Supervisor: Franco Zambonelli

PhD candidate: Alberto Francia

A.A. 2022/2023

All’ing. Nardo Francia

Summary

Abstract

The management of competencies is a crucial concern for both students and workers, as well as for training institutions and companies. For the former, it allows users to track and certify acquired skills to apply for positions; for the latter, it enables better organization of business processes. However, currently, most software systems employed for competency management tend to be either organization-focused or centralized. This presents two main limitations: on one hand, they restrict the ability of students and workers to transfer their competencies outside the original context; on the other hand, they imply a certain dependence on users' trust, often requiring them to give up part of their privacy for the storage of personal data. This study will illustrate a user-centric, fully decentralized competency management system that enables verifiable, secure, and robust management of competencies digitalized as Open Badges through notarization on a public blockchain. In this way, anyone who acquires a competency or achievement maintains full control over it and can disclose their digital certifications only when necessary and to the required extent, migrate them across storage platforms, and allow anyone to verify the integrity and validity of such certifications independently of any centralized organization. The proposed solution is based on C-Box®, an existing application for the management of digital competencies that has been enhanced to fully support models, standards, and technologies of the so-called Web 3.0 vision—a global effort by major web organizations to "give the web back to the people," pushing for maximum decentralization of control and user-centric data ownership. Additionally, a complementary study on the energy consumption of the blockchain used in the system has revealed that, despite common concerns about intensive energy use, the specific implementation adopted optimizes energy efficiency. This aligns with the goal of maximizing the decentralization of control and user-centric data ownership, while also promoting environmental sustainability.

1. Introduction

The term "Human Resources" (HR) refers to the department or business function within a company that is responsible for managing and developing its workforce. Its main goal is thus to attract, develop, and retain the best talent available. The same can be easily said for learning institutions such as universities. To achieve this, HR needs a clear understanding of the skills necessary for the organization to function effectively as well as an understanding of the organization's internal competencies. By identifying employees (students, for universities) with specialized competencies or relevant experience, the company can effectively address changes or implement new business functions and strategies. This fosters the company's ability to adapt quickly and remain competitive in the marketplace.

According to Andrew Spencer, a UK-based HR technology consultant/researcher, the four areas where blockchain can be used more proficiently in this context are credential verification, worker payments, work matching platforms, and identity management [1]. The former and the latter are the two we focus on in this thesis with our proposed C-Box® platform.

The prevalent practice of verifications is generally handled by inner administrative human resources and/or assigned to third parties, and applicants provide contact information [1]. Talent supply, candidate fraud, and selection bias were identified as the most pressing problems that blockchain can solve in HR management by the study conducted in [2]. In particular, verification of educational career achievement, expertise acquired from previous jobs and performance thereof, as well as data sharing are the concerns mostly represented amongst surveyed participants from the HR sector.

Therein, implementation is seen as the bigger barrier to overcome for full exploitation: hence, the relevance of platforms such as C-BoX® that can be readily exploited by organisations and individuals, either manually (via a Graphical User Interface) or automatically via an integration API provided by the platform—such as the "Web API" component in C-Box® (see Section 3.2).

The ability to certify, identify, and track people's competencies is a fundamental activity for both individuals and companies. In this context, Open Badges for the digital certification of competence play a fundamental role, as they provide the softwarised representation of a given competence together with metadata about ownership, issuer organisation, and the acquisition process [3].

However, keeping track of an organization's internal competencies can be a challenge [4], especially for large companies with many employees and different divisions or locations. In addition, if the company has a well-defined hierarchical structure, it can be straightforward to identify employee competencies based on roles and responsibilities, but in more flexible and agile organizations, where employees can perform multiple tasks and roles, competency management may require a more flexible and adaptable approach. Usage of software technology, such as HR management software or competency management platforms, can streamline the competency tracking process, as these tools allow the recording and updating of employee competency information, making it easy to find and access that information when needed [5].

From the standpoint of employees and students alike, competency tracking is relevant also across organisations. For instance, when changing jobs or applying for college, information on the competencies acquired remains primarily in the hands of the previous company/school if it has been collected through internal training programs or performance evaluations. Also, the HR department or school administration may have no incentive to communicate to the employee, the new company, or other education institutions the competencies acquired. Some companies adopt open and transparent policies, allowing employees to access and maintain records of the competencies acquired during their employment. An example is represented by the web portal promoted by Unioncamere and the Chambers of Commerce in Italy: it allows the registration of competencies to an independent, accredited portal (https://certificacompetenze.unioncamere.it/, accessed on 23 October 2023). Independent competency management systems therefore safeguard the interests of the worker, who will be able to continue to access his/her certificates even after the termination of the employment relationship. However, these independent systems mostly are centralized; hence, the worker still depends on a single external authority that holds complete control of his/her own data [6,7,8]. In addition, keeping data in one place increases the risk of data loss due to technical failures, human error, or cyberattacks. Finally, employees/students are forced to share sensitive information about their competencies with the authority, raising concerns in terms of data privacy and security as that authority has control of and responsibility for protecting that information.

The emergence of blockchain technology [9] and of the concept of Self-Sovereign Identity (SSI) [10,11] provide individuals with new ways to manage their own data, including competencies. These technologies make it possible to create verifiable and immutable digital records that can be inspected by multiple parties while respecting privacy and without giving up control to a single organisation; rather, data are fully distributed and decentralised. The move to decentralized, self-managed systems addresses the limitations associated with centralized systems, allowing employees to maintain control and ownership of their competencies while making it easier, more privacy preserving, and safer to share relevant information during job changes.

Accordingly, in this study, we propose a user-centric, fully decentralised competency management system enabling verifiable, secure, and robust management of competencies digitalised as Open Badges via notarization on a public blockchain. This way, whoever acquires the competence or achievement retains full control over it and can disclose his/her own digital certifications only when needed and to the extent required, migrate them across storage platforms, and let anyone verify the integrity and validity of such certifications independently of any centralised organisation. The proposed solution is based on C-Box® (https://www.cboxiqc.com/, accessed on 23 October 2023), an existing application for the management of digital competencies developed by Italian Quality Company s.r.l. (IQC) in technological partnership with Pomiager s.r.l. C-Box® is designed for the management of Open Badges, which represent a digital recognition of the competencies or achievements obtained by an individual, and it allows issuers qualified by IQC to create and issue Open Badges to learners/employees who demonstrate that they have acquired specific competencies. C-Box® has been extended to fully support models, standards, and technologies of the so-called Web 3.0 vision—a global effort by major web organisations to “give the web back to the people”, pushing for maximum decentralisation of control and user-centric data ownership. In particular, our contributions can be articulated as follows:

We describe the notarization service implemented on a public blockchain to ensure immutability and decentralized verification of the information reported in the Open Badges.

We demonstrate that such implementation fully adheres to the requirements of the Self-Sovereign Identity (SSI) model to enable full ownership and control of the competencies acquired by learners/employees.

We motivate the addition of Non-Fungible Tokens (NFTs) [12] to Open Badges as they enhance their portability and interoperability and stimulate user engagement.

The remainder of this document is organised as follows: in Section 2, we provide to the reader the necessary background to fully appreciate our contribution: that is, what Open Badges are, what the paradigm of SSI is and why it is central to Web 3.0 developments, and what role the blockchain may play in competency management; in Section 3, we describe our contribution: that is, the solution developed and how it supports notarization and creation and verification of Open Badges, and how NFTs are exploited.

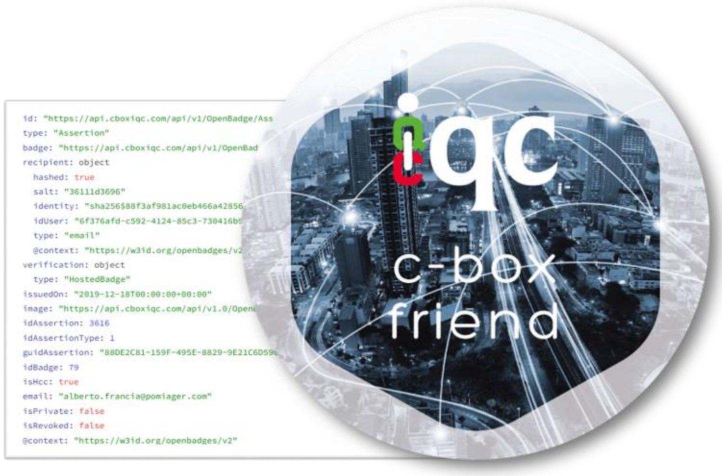
2. Background

This section provides the preliminary knowledge needed to fully appreciate the C-Box® technology presented in Section 3: what Open Badges are (Section 2.1), how the concept of Self-Sovereign Identity (SSI) relates to them (Section 2.2), and why the blockchain, Verifiable Credentials, and Non-Fungible Tokens (NFTs) are convenient choices for their software implementation (Section 2.3).

2.1. Open Badges

An Open Badge is a digital certificate that allows users to recognize and represent a person's competencies in a transparent and portable way [3]. Open badges consist of an image that represents the recognition itself, accompanied by detailed metadata that provide additional information about the competency or goal achieved, such as information about the issuer of the badge, its recipient, the award criteria, a thorough description of the competence or achievement obtained, and the date of issue. The most important feature of an Open Badge is its portability: once it is obtained, a person can keep it and share it on different digital platforms, such as social media, online resumes, or personal portfolios. This allows individuals to effectively present their competencies and accomplishments to potential employers, educators, or community members.

To achieve such portability, Open Badges are based on an open technical standard: the Open Badges standard—originally created by the Mozilla Foundation (https://web.archive.org/web/20160426204303/https://openbadgespec.org/ archived from the no longer accessible original page, accessed on 23 October 2023) and now maintained and developed by the 1EdTech organisation—defines a software format for Open Badges, including the badge image, associated metadata, and how it must be managed and shared. As an example, Figure 1 shows a representation of an Open Badge with JSON metadata—a lightweight data representation format particularly suitable for web applications.



```
id: "https://api.cboxiqc.com/api/v1/OpenBadge/Ass
type: "Assertion"
badge: "https://api.cboxiqc.com/api/v1/OpenBad
recipient: object
  hashed: true
  salt: "36111d3696"
  identity: "sha256$88f3af981ac0eb466a42856
  idUser: "6f376afd-c592-4124-85c3-730416b
  type: "email"
  @context: "https://w3id.org/openbadges/v2
verification: object
  type: "HostedBadge"
issuedOn: "2019-12-18T00:00:00+00:00"
image: "https://api.cboxiqc.com/api/v1.0/Open
idAssertion: 3616
idAssertionType: 1
guidAssertion: "88DE2C81-159F-495E-8829-9E21C6D59
idBadge: 79
isHcc: true
email: "alberto.francia@pomiager.com"
isPrivate: false
isRevoked: false
@context: "https://w3id.org/openbadges/v2"
```

***Figure 1**. Representation of an Open Badge as implemented in C-Box®: an image and metadata describing the achievement.*

Version 3.0 of Open Badges was published in July 2023 (https://1edtech.github.io/openbadges-specification/ob_v3p0.html, accessed on 23 October 2023), introducing several new features and improvements towards realising the vision of Web 3.0: that is, a global effort by major web organisations to "give the web back to the people", pushing for maximum decentralisation of control and user-centric data ownership. This update included:

- Support for Verifiable Credentials (VCs)—see Section 2.2.2;
- Interoperability with digital wallets capable of hosting users' VCs;
- A greater focus on data privacy and security through the use of technologies such as end-to-end encryption and data management based on user consent;
- Support for Linked Data (via the representation format JSON-LD), a technology that allows linking of the information contained in digital badges to other information on the web in order to provide a broader context.

Open Badges offer numerous advantages in mapping the competencies acquired by people in all training and experiential contexts, such as (i) detailed documentation of the knowledge and competencies acquired, (ii) digital portability, (ii) easy sharing, and (iv) automated verifiability—a process that guarantees the authenticity and validity of a badge awarded to a person: that is, whether the badge has been actually issued and by what organization, and that the badge has not been altered or counterfeited. As such, they have established themselves as the de-facto standard for recognising and assessing individual competencies in a transparent and certifiable way.

However, the validity of an Open Badge is closely bound to the fate of the platform that issued it in the first place: if, for any reason, such a platform discontinues its service, gets hacked, or loses data, the badge would no longer be transportable and/or verifiable [13]. Decentralized systems such as blockchains, in which the verification process does not depend on the database of the issuing platform but on all the peer nodes participating in the network, and Web 3.0 paradigms such as SSI, where users have independently stored and verifiable credentials, can fix this issue. Accordingly, C-Box® implements a notarization service and a VCs scheme—that is, verifiable and secure tracking of identities, processes, and data—in a public blockchain so as to decouple badges from issuers' platforms and add a further security layer (as described in Section 3).

2.2. Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) is a cornerstone of Web 3.0 [10], as it represents an innovative approach to digital identity management that aims to remove dependency on centralized third parties and focuses on autonomy and ownership by individuals. These identities are verified and recognized by different organizations and online services, allowing users to interact securely and privately without having to reveal sensitive information. Users have the power to decide what information to share, with whom, and for how long.

SSI is based on the concept of Decentralized IDentifiers (DIDs) [14] and Verifiable Credentials (VCs) [15], which allow individuals to create and manage their own digital identity that can be verified by others without revealing unnecessary personal information. But then we must ask how can this new freedom and the need to protect our privacy coexist. The answer is via Zero-Knowledge Proof (ZKP) [16], which allows the verification of information without revealing sensitive details.

The C-Box® certificates issued via VCs can vouch for the specific competencies they represent, which is entirely consistent with the principles of Self Sovereign Identity. This approach enables individuals to possess and manage their attestations from their personal wallet, rendering the verification processes independent of the issuing platforms.

2.2.1. Zero-Knowledge Proof (ZKP)

In cryptography, a Zero-Knowledge Proof (ZKP) [16] is a method by which one party (the demonstrator) can prove to another party (the verifier) that a given statement is true while avoiding transmission of any additional information beyond the fact that the statement is actually true. In general, when a person wants to prove that he knows something, the simplest solution would be to simply reveal the information itself. For example, if someone claims to know a secret password, they could simply reveal it to prove they have that knowledge. However, the goal of ZKP is to demonstrate knowledge without revealing that knowledge. For achieving this, the verification process generates one or more “challenges” (or “proofs”) that an individual is able to overcome only if in possession of that specific information. Fully describing such challenges is out of the scope of this thesis; it is sufficient to know that they rely on encryption algorithms that allow calculations to be performed on encrypted information without the need to decrypt it. The tools that allow ZKP verification of a statement in an SSI context are Verifiable Credentials (VCs) and Decentralised Identifiers (DID).

2.2.2. Verifiable Credentials (VCs)

A Verifiable Credential (VC) [15] is a standardized data format for representing claims that can be digitally verified. VCs can be used to represent virtually any attestation or statement, from academic or professional qualifications to citizenship. The verifiable data registry is the system that mediates the creation and verification of identifiers, cryptographic keys, and other relevant data that may be required to actually verify credentials. The use of VCs follows a three-party model as described in Figure 2: an issuer, a holder, and a verifier.

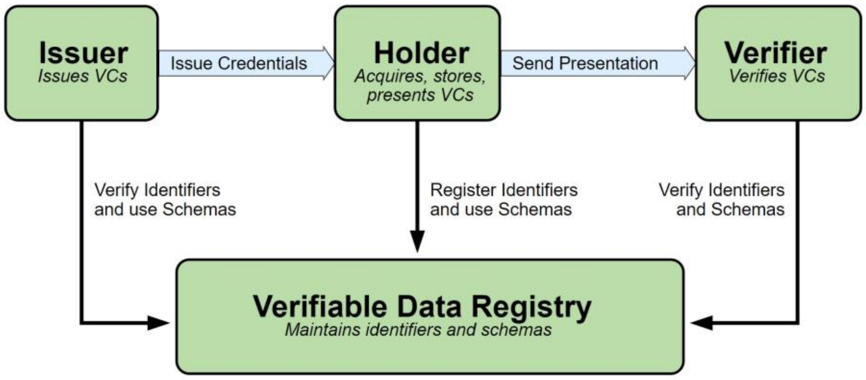

Issuer
Issues VCs
Issue Credentials
Holder
Acquires, stores, presents VCs
Send Presentation
Verifier
Verifies VCs
Verify Identifiers and use Schemas
Register Identifiers and use Schemas
Verify Identifiers and Schemas
Verifiable Data Registry
Maintains identifiers and schemas

Figure 2. *Three party verification model.*

The issuer digitally signs the VC, which can then be saved on the holder's wallet—a web or mobile app specifically designed to allow saving of VCs and that relies on standard JSON schemes registered and available in the verifiable data registry. A verifier that wants to validate the VC must trust the issuer: it must be a reliable entity capable of issuing the specific credentials relevant to the claim included in the VC. If such trust exists, the verifier can verify the signature on the VC provided by the holder without the need to make any request to the issuer platform.

2.2.3. Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) [14] play a key role in the VC model, especially when combined with ZKP. A DID is a unique identifier that can be registered and managed by the holder itself without the need for an issuing authority. This DID is used to create a sort of digital profile, called a DID Document, that can contain arbitrary data and pointers to services related to the identity of the holder. DIDs perform two main functions:

- Authentication: when the owner presents a VC to a verifier, it can use its DID to prove its identity.
- Verification: since each VC contains a reference to the issuer's DID, the verifier can check whether the issuer's digital signature is valid.

If both checks are passed, one can be sure that the VC actually belongs to the holder and that the VC has been actually issued by the issuer to that holder. DIDs therefore provide a method to authenticate both the owner and the issuer in a fully decentralized way, respecting the principle of SSI and thus the vision of Web 3.0.

Through DID it is possible to sign and verify "verifiable credentials", i.e., to create and resolve cryptographically secure evidence that attests to certain personal information such as age, qualifications, or work history. These credentials may be shared with third parties, such as employers, financial institutions, or government agencies, who can verify their authenticity without having to access other personal information.

2.2.4. Verifiable Presentation

A verifiable presentation [17] is a safe way to share VCs; it tells the verifier only what it is required to know and allows the owner to maintain different identities, such as online player, professional, etc., while only disclosing the one actually necessary at any given time. Technically, a verifiable presentation consists of three components:

- Presentation metadata that provide information about the presentation itself (such as data types and storage requirements);
- A list of VCs;
- The DID of the holder and (all of) the issuer(s) necessary to validate the authenticity of the statements.

To create a presentation, the holder must first access his/her wallet and select which statements he/she wants to add to the verifiable presentation. The holder then digitally signs the presentation to be transmitted to the verifier, who can proceed with the verification; by checking the holder's signature (available in his/her DID) on the presentation, the verifier confirms that the VCs belong to the holder, whereas by checking the individual VCs, the verifier guarantees that they are valid and that they have been issued by the indicated issuers.

C-Box® integrates a system for generating Verifiable Presentations, offering users the ability to create detailed and modular presentations of their skills. These presentations, structured as VCs, can be shared with third parties, such as employers or educational institutions, to attest to and demonstrate the individual's skills and knowledge.

2.3. Blockchain

Blockchain technology is essentially a distributed ledger with built-in transparency, decentralisation of governance, and security against tampering. Blockchains that support smart contracts also add the possibility to program general-purpose applications on top of them, and these are executed in a fully decentralised way.

In the following, we briefly describe the two main blockchain ingredients we use for C-Box®: smart contracts for notarization and NFTs.

2.3.1. Notarization

Notarization is the process that guarantees the immutability and authenticity of a document or set of data through the registration of a hash (or "fingerprint") of the document on a public or private blockchain. The process of notarization on a blockchain consists of several phases:

- Definition of the document: the document is created by the user and can be a text file, an image, a video, a transaction, etc.
- Hash calculation: the user calculates the hash of the document, which is the unique alphanumeric code that represents the fingerprint of the document itself.
- Inserting the hash into the transaction: the user inserts the hash of the document into a blockchain transaction by notarizing it.
- Verification of authenticity: at a later time, a third-party user can verify the authenticity of the document by hashing it and comparing it with the one originally registered on the blockchain.

Note that even if notarization requires the use of a distributed system, any privacy requirements demanded by the issuer or learner are respected. In fact, the process distributes on the blockchain only the hash of the data and never its content in the clear.

There are two main categories of blockchains: public blockchains and private blockchains. Public blockchains, such as Bitcoin and Ethereum, are decentralized and open to anyone who wants to participate in the network. This means that data on the blockchain are public and accessible to anyone. Private blockchains instead are controlled by a specific (group of) organization(s), which means that only authorized users can access the network.

Notarization may be implemented on both; however, a private blockchain requires trust in the blockchain technology itself (its consensus protocol, security measures adopted, etc.) as well as in the organisation(s) running the blockchain, whereas notarization on a public blockchain only requires trust in the blockchain platform itself. The price is publicity of data: no sensitive data must be stored on a public blockchain, as they will be open to scrutiny by anyone. Since in the notarization process implemented by C-Box® only a hash code computed on a given piece of data is stored on the blockchain and there is no way to trace the content of such data back from the hash code, a public blockchain is chosen as the backbone of the C-Box® application.

There is currently no recognized standard for notarizing documents on blockchain [18,19]. There are several independent implementations available on the market, but each uses a different approach and data structure. This can make it difficult to set up an interoperable system that allows different notarization services to communicate with each other. In addition, the lack of standards can make it difficult to choose the right notarization solution, as there can be significant differences between implementations in terms of security, cost, and ease of usage. Accordingly, several projects and initiatives are working to develop blockchain notarization standards in hopes of creating an interoperable and universal notarization ecosystem. For example, ISO has set up a committee to define guidelines for blockchain technologies and distributed ledgers, but no standards have yet been released (https://www.iso.org/committee/6266604.html, accessed on 23 October 2023). Instead, on Joinup—a collaboration platform created by the European Commission for the definition of interoperability solutions for public administrations—you can find a file-notarization project (Blockchain Based Notary Proof Of Concept), but at the moment, there are no practical implementations (https://joinup.ec.europa.eu/collection/blockchain-egov-services/solution/blockchain-based-notary-proof-concept/about, accessed on 23 October 2023).

In conclusion, besides standards, also no dominant design seems to have emerged yet. For C-Box®, we therefore had to develop our own notarization service for the validation of the information contained in the Open Badges (see Section 3).

2.3.2. Non-Fungible Tokens (NFTs)

Non-Fungible Tokens (NFTs) are a type of cryptographic token that represents ownership of a unique digital object or work [12]. Unlike fungible tokens, NFTs are distinct and cannot be exchanged equivalently with each other. Each NFT has a unique identifier registered on the blockchain, which guarantees the authenticity, traceability, and ownership of the digital object represented [20]. NFTs offer owners new ways to monetize their digital assets as they represent a form of exclusive ownership and digital authenticity. For example, an artist can create a unique digital artwork and sell the NFT that represents it to a collector. In this way, the buyer of the NFT owns the digital artwork and the artist can earn a commission on the sale of the NFT. This allows owners

to derive additional revenue from the resale of their digital assets.

NFTs and VCs are both emerging concepts within blockchain, and while they share a technology base, they have distinct purposes and applications (Table 1 summarizes the differences between NFTs and VCs.). In essence, NFTs are digital certificates of ownership. VCs, on the other hand, are a technology standardized by the World Wide Web Consortium (W3C) to represent and share attributes or rights of a digital identity. A key difference is that VCs require a three-party infrastructure to work properly: the issuer, the owner, and the verifier. NFTs, on the other hand, are based on the blockchain and are time-marked, which makes it easy and accessible to verify the digital ownership of the token. Another difference regards transferability: although the owner can decide where and how to share a VC, its ownership never changes. NFTs, instead, allow owners to sell, exchange, or give away the digital object represented by the token. However, in the face of a change of ownership the content of the token does not change. So regardless of the owner of the wallet to which an NFT is associated, the NFT of a certificate associated with a natural person will always remain associated with the same person. NFTs require a blockchain to be realised, while VCs can be implemented on blockchain or any other distributed storage platform that supports the required verification. Finally, an NFT is inherently indivisible due to the specific nature of the digital asset it represents. This stems from the fact that splitting the unique digital asset would compromise its intrinsic value and uniqueness. In the case of VCs, they can be divided while sharing. For example, suppose a VC contains an individual's date of birth and driver's license number. The holder can choose to share only the driver's license number with one verifier and only the date of birth with another. In this sense, VCs are divisible.

In C-Box® we foster an interpretation of NFTs and VCs as complementary concepts: in the context of competency management, in fact, NFTs can be associated to VCs to (i) incentivise users to acquire new competencies to be showcased, (ii) further decouple ownership of a competence (a responsibility of VCs) from ownership of the certification of such competence (to which NFTs may add value), (iii) improve interoperability, as NFTs are widely supported by all the major public blockchain platforms, and potentially (iv) allow users to generate revenues from ownership of their certificates. For instance, let us imagine that Professor J. R. R. Tolkien (the famous author of "The Lord of the Rings") is still alive today and that a literary award obtained by him has been notarised to a blockchain. Such a digitalised award would be bound to Prof. Tolkien's VCs to always and forever prove that such an award has been indeed achieved by him and not by another homonym. However, ownership of such a digital certificate (the certification of the award, not the award itself) may be valuable to estimators and collectors of Tolkien's memorabilia. Hence, digitalising such ownership as an NFT, decoupled from the award certificate itself (that would still "belongs" to Prof. Tolkien, even after his death), provides unprecedented market opportunities.

	NFTs	**VCs**
What it is	Publicly exposed digital property right	Private digital fact
Requires blockchain	Yes	Both with and without a blockchain
Transferable	Yes	No
Immutability	History of transactions is always immutable; content is only saved in a distributed environment	Only if based on an immutable, verifiable data registry
Implementation	Blockchain and timestamps	Symmetric key infrastructure
Purpose	Proves ownership of an entity, granting exclusive rights to the owner	Proves identity of an entity

Table 1. Main differences between NFTs and VCs.

3. The C-Box® Platform

In this section, we present our contribution: that is, the C-Box® platform for distributed and decentralised competency management. First, we enumerate the main goals and functionalities of the platform; then, we overview its conceptual architecture by describing its main components and their relationships; afterwards, we describe in detail its core processes: that is, notarisation, handling of VCs, and NFT usage.

3.1. Overview

C-Box® is an online platform designed to allow issuers to award digital skill recognitions to “learners” (or “holders”) through Open Badges. These badges can be granted for various reasons, such as the completion of training programs, participation in specific events, or in acknowledgment of skills acquired in a professional setting or based on the roles undertaken. The C-Box® platform adheres to the standards set by 1EdTech concerning the specifications of Open Badges 2.0. This means that holders have the flexibility to import and export Open Badges to and from other platforms that follow the same standard, ensuring great interoperability and simplifying the sharing and recognition of skills across platforms. A unique feature of C-Box® badges is the ability to embed multimedia attachments, such as handouts or videos, directly within the badge in order to enrich the badge’s content and provide additional evidence or details of the acquired skills.

C-Box® also already integrates a notarization service, currently based on a private blockchain, that ensures the authenticity and immutability of certifications over time. Unlike with public blockchains, using a private one eliminates the need to spend cryptocurrency for the notarization of each certification. This represents a cost-effective advantage. However, there is a downside: the private nature of the blockchain restricts access and consultation by entities external to the C-Box® platform. This hinders the transparency benefits typically associated with blockchain technology, as the data are not freely available to the public.

The notarization service has thus been re-engineered on a public blockchain in the way that we describe in the remainder of this section. Also, with the aim of increasing interest and engagement for learners, an option has been added for C-Box attestation holders to redeem NFTs representing the received open badge. Finally, given that the most-recent version of the Open Badge standard requires the use of VCs, the platform has chosen to implement this SSI technology.

The choice was driven by the desire to leverage the inherent advantages of a public blockchain, such as increased robustness to faults and absolute transparency, making the information accessible to external users. However, transitioning to a public blockchain presents challenges. One of the main ones is managing the monetary cost (in cryptocurrency) associated with transactions and smart contract execution. This calls for a thorough review of procedures and smart contracts’ source code to ensure resource-efficient use and cost minimization. Furthermore, another pivotal aspect is privacy. With the shift to a public blockchain, it is crucial to ensure that users' sensitive information remains protected and that their privacy is not jeopardized.

3.2. Architecture

C-Box® consists of two main components (Figure 3): one that exposes APIs to its many services, such as notarization and Open Badges management ("Web API"), and another one that provides the web interface for human users ("Web Application").

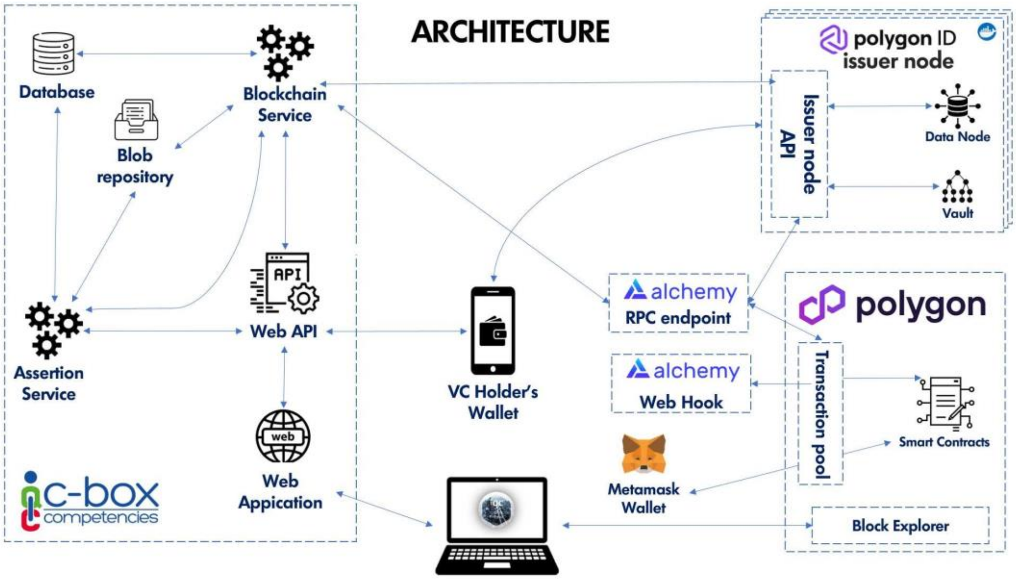


Figure 3. C-Box® system architecture.

The Web API component includes the Blockchain Service, which interacts with the Polygon blockchain through a node provider called Alchemy (https://docs.alchemy.com/reference/api-overview, accessed on 23 October 2023), that receives API requests and automatically returns the responses. Polygon has been chosen for many reasons. First, Polygon ID is a useful tool to implement a Self-Sovereign Identity (SSI) infrastructure in a decentralized context. Although it was not originally developed with a specific orientation towards Open Badges 3.0, it proves capable of meeting many of the requirements of this standard. Moreover, Polygon is a second-layer blockchain, meaning it operates on top of a primary blockchain like Ethereum, offering a scaling solution. This characteristic brings with it two significant advantages. Firstly, transactions on Polygon are considerably faster. While primary networks can suffer from congestion, leading to transaction delays, Polygon, due to its structure, manages to process transactions with greater efficiency and speed. Secondly, another tangible benefit of using Polygon is the reduced transaction cost. Primary networks, especially during times of high demand, can have high fees. In contrast, Polygon offers significantly lower transaction fees, making operations not only faster but also more cost-effective. These two aspects combined make Polygon a preferable choice for many seeking efficiency and affordability in the blockchain. Finally, Polygon allows for the management of Verifiable Credentials (VCs) and the implementation of claim verification in accordance with Web 3.0 principles and technologies.

In the context of our re-engineering of C-Box®, we adapted and applied Polygon functionalities to issue competencies in the form of badges thanks to its ability to meet the standards imposed by Open Badges 3.0. On purpose, we use two services provided by Alchemy: one that exposes an endpoint useful for querying a node via Remote Procedure Call (RPC), and one that provides web hooks to react to transactions made to a specific RPC endpoint. For each issuer with a subscription to C-Box®, an Issuer Node is created on Polygon. Each issuer node provides an API meant to support Decentralised Identifier (DID) creation and management, such as defining new credential schemes, and creating and verifying VCs. The issuer node also has a database that stores the DID identities and the VCs, while a secure vault is used to store sensitive issuer information, such as the private key of its wallet (to allow it to sign blockchain transactions).

In Figure 3, two external applications are also depicted in order to comprehensively depict the overall working logic of C-Box® explained in the following sections. The VC Holder Wallet is an application capable of storing and managing user credentials. It can be either C-Box®'s custom one or Polygon ID's one (e.g., https://play.google.com/store/apps/details?id=com.polygonid.wallet, accessed on 23 October 2023). Based on the principles of SSI, the wallet enables its holder to carefully select which data to share with others without exposing other sensitive private information (in compliance with verifiable presentation principles). Metamask (https://metamask.io/, accessed on 23 October 2023) instead is an extension that any user can add to her/his browser to create and interact with his/her own wallet via the Web.

Finally, as regards ZKP, to both generate and verify ZKPs, the Iden3 framework (https://docs.iden3.io, accessed on 23 October 2023) has been used. It is an open-source framework that employs various tools developed to operate in decentralized environments with reduced trust. Specifically, Iden3 uses SnarkJS, an independent implementation of the zk-SNARKs protocol [21] written in JavaScript and thus browser compatible. Zero-Knowledge-Succinct Non-Interactive Arguments of Knowledge (zkSNARK) are "succinct" zero-knowledge proofs that can be verified in a few milliseconds, with a proof length of only a few hundred bytes even for statements about very large programs (https://github.com/iden3/snarkjs, accessed on 23 October 2023). In addition to being fast and directly executable from a browser, zkSnarks proofs allow for the verification of a proof without gaining knowledge of the solution, and they do not require interactions between the prover and the verifier.

3.3. Business Logic

In the following subsections, we zoom in on the specific interactions between the C-Box® inner services and external platforms implemented to achieve our goals.

3.3.1. Notarization Process

Figure 4 illustrates the process of notarization triggered whenever an issuer wants to deliver a badge to a learner.

- From the Web Application, the issuer releases a badge (1), and the application makes an HTTP call to the Web API component to perform authorization (does the user have the right to access this feature?) and validation (can the learner for whom the badge is to be issued receive this badge from this issuer?, etc.) checks (2).

- Then, the Web API component instantiates the services necessary for the release (3): specifically, the Assertion Service creates the badge image and saves it in blob storage and creates the necessary database records for the description and Open Badge standards, any files attached to the certification are saved, and a notification email is sent to the learner (3–5).
- Following these procedures, the Assertion Service queries the Blockchain Service (6) that will take care of the notarization.
- This amounts first of all to the creation of the JSON that represents the certification. For this, required data are retrieved from the database (7) and from the blob repository (8). This JSON contains the descriptive information of the certification, and the hash of each attachment is made and added to the JSON.
- Then, the hash of this JSON is calculated (9) and added as an input parameter to the transaction executing the notarization. This transaction is a function of the smart contract (called Notarize), which uniquely associates the assertion identifier with the obtained hash string.
- Through the Alchemy RPC service, the gas cost required to mint the transaction is estimated (this value is indeed variable because it depends on the state of the Polygon network). The Blockchain service signs the transaction with the private key of the smart contract owner and sends the transaction again through the Alchemy RPC endpoint (10).
- Mind that the time required for the transaction to be mined is variable (and also depends on the amount of gas associated with the transaction). To avoid blocking the user in a process that could also take minutes, the Blockchain Service sends the transaction without worrying about its actual mining (12). Instead, the transaction hash (which uniquely identifies it) is saved to the local database with a “pending” status (11).
- Asynchronously, Alchemy queues the transaction to its own transaction mempool (13). If for any reason the transaction should be rejected by the network (dropped), a specific webhook is used to notify the C-Box® Web API component, which will take care of retrying the transaction.
- If instead the transaction is mined (14), Alchemy’s webhook service will make an API call to C-Box® containing the transaction hash, the actual gas used, the gas cost, and the block number (15).
- This information is saved in the C-Box® application’s cloud database by the Blockchain Service (16, 17).
- Finally, through a websocket connection, if the issuer is still connected to C-Box®, he/she will be informed of the successful notarization of the assertion in the blockchain.

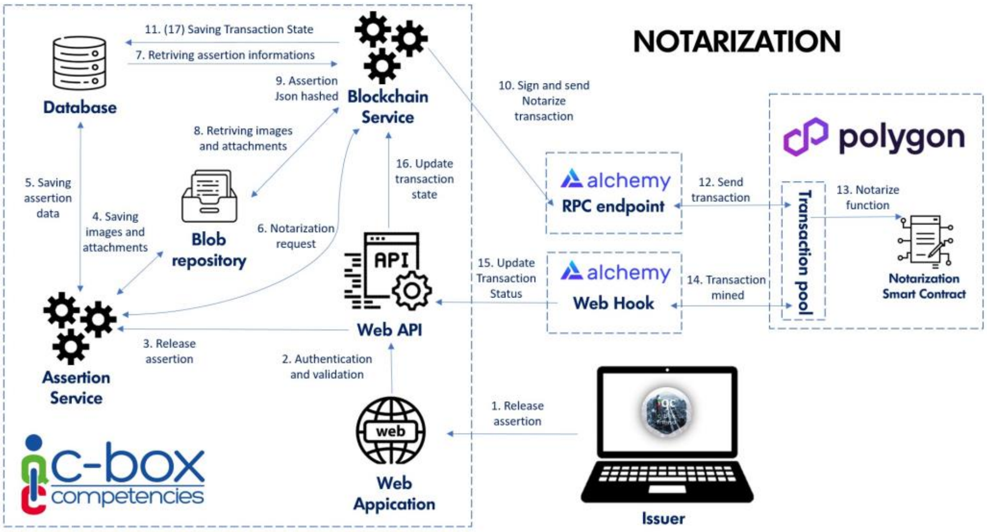


Figure 4. Notarization of an Open Badge released by an issuer organisation.

Figure 5 describes the process of verifying the integrity of a C-Box digital badge after notarization.

- The verification carried out through a notarization check can be performed by any user (Verifier) by consulting the dedicated verification section on the C-Box portal (1).
- The C-Box Web application queries the API application, which through the Assertion service retrieves from the database all the data necessary for verification and page display (2, 3), such as the smart contract address or the assertion's identification code.
- The Verifier user can then use a Polygon block explorer or directly use the verification page to interact with the getAssertionUri function of the Notarization Smart Contract (4).
- Based on the assertion's identification code, the smart contract returns a URI from which it is possible to retrieve the JSON that describes the digital certificate (5).
- This URI points to the C-Box Web API application (6). The API can create the JSON through the blockchain service (7), which, by retrieving the details, images, and attachments of the assertion (8, 9), returns the certificate's JSON (10).
- The Verifier user can now evaluate the hash of this JSON using SHA256 through the verification page or any online hash tool (11). By accessing the GetAssertionHash function (12), the Verifier accesses the original blockchain hash string generated at the time of the assertion's release (13).
- By comparing the two obtained hashes, the absence of data modification representing the certificate can be verified (14), since even a small change would imply a completely different hash string.

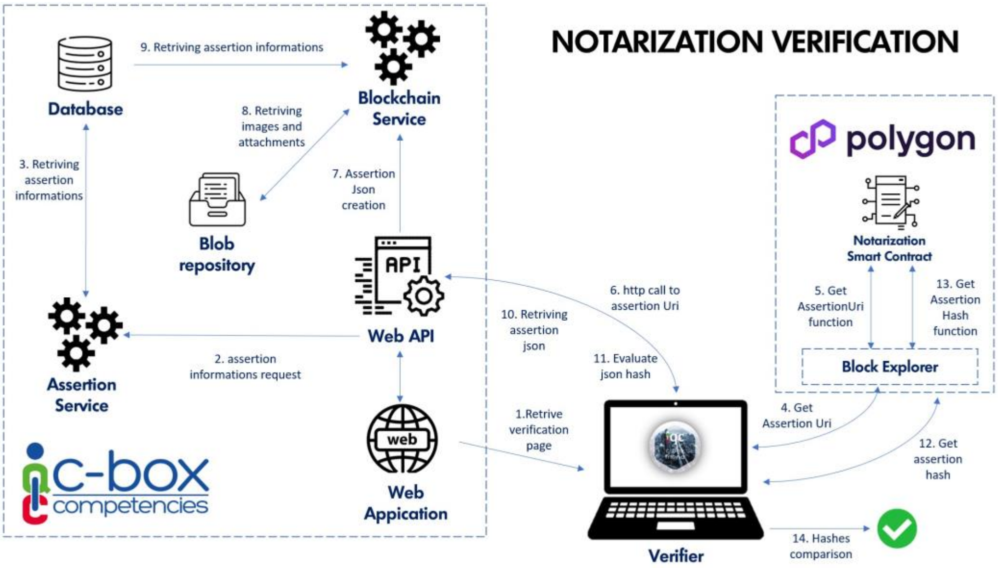

NOTARIZATION VERIFICATION
Database
9. Retriving assertion informations
Blockchain Service
8. Retriving images and attachments
3. Retriving assertion informations
7. Assertion Json creation
Blob repository
API
Web API
Assertion Service
2. assertion informations request
web
Web Appication
c-box competencies
6. http call to assertion Uri
10. Retriving assertion json
11. Evaluate json hash
1.Retrive verification page
polygon
Notarization Smart Contract
5. Get AssertionUri function
13. Get Assertion Hash function
Block Explorer
4. Get Assertion Uri
12. Get assertion hash
Verifier
14. Hashes comparison

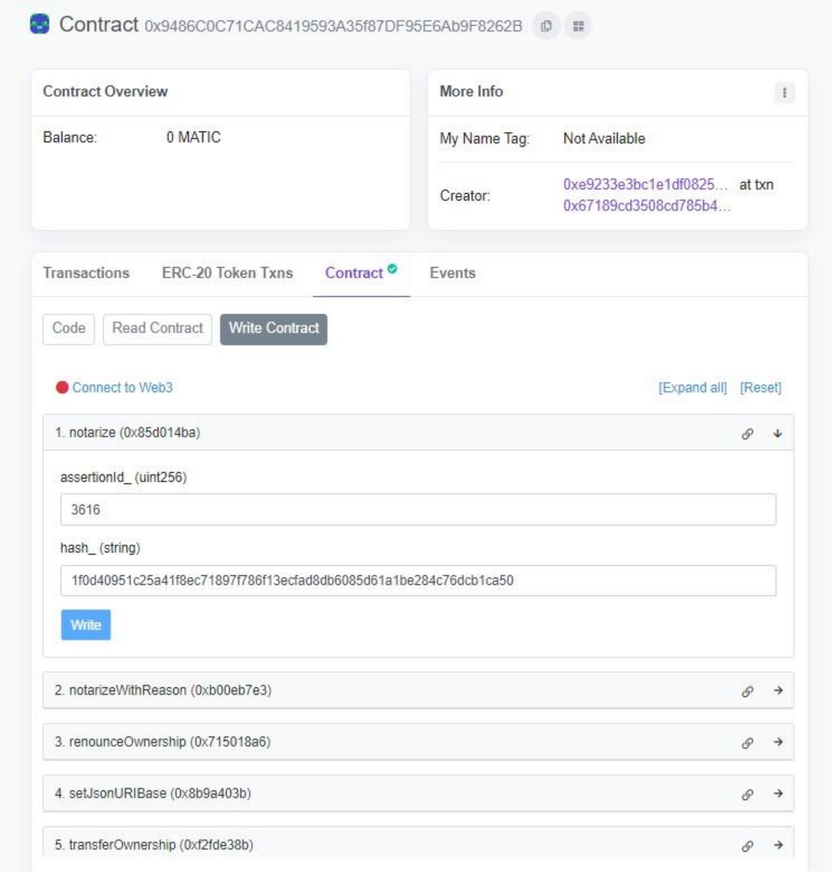
Figure 5. Verification of an Open Badge and, hence, of its notarization.

3.3.2. Developed Smart Contract

For C-Box®, a smart contract has been developed with the precise task of carrying out the notarization and verification process on a public blockchain and at the same time guaranteeing the confidentiality of the information contained therein. A challenge has been to develop source code that is computationally the least-complex as possible to allow the lowest consumption of fees (hence monetary cost) during the notarization transaction.

The main phases of notarization carried out by the smart contract are summarized below (in reference to Figure 4):

1. The C-Box® application receives a notarization request for the assertion ID, e.g., 3616 (6).
2. The C-Box® blockchain service retrieves information from the database (7) and the blob repository (8) in order to create the JSON representing the assertion with ID 3616 (Listing 1).
3. The SHA256 algorithm is executed to get the hash string corresponding to the assertion data, e.g., 1F0D4095...DCB1CA50 (9).
4. The C-Box® application authenticates itself via private key to the Polygon network (10).
5. A signed transaction sent through Alchemy (12) can proceed to the notarization method of the smart contract, providing the assertion ID and the newly computed hash string (Figure 6).
6. In the smart contract, a record with the assertion identifier and its hash string as a value has been added to a mapping (13). A smart contract event confirms that the procedure has been completed (Figure 7).
7. The miner who mined the transaction generates and sends on the blockchain network the transaction receipt. Alchemy intercepts it (14), proving that the transaction has been mined. Alchemy forwards that receipt via webhook to the C-Box API app (15).



Contract 0x9486C0C71CAC8419593A35f87DF95E6Ab9F8262B

Contract Overview

Balance: 0 MATIC

More Info

My Name Tag: Not Available

Creator: 0xe9233e3bc1e1df0825… at txn 0x67189cd3508cd785b4…

1. notarize (0x85d014ba)

assertionId_ (uint256): 3616

hash_ (string): 1f0d40951c25a41f8ec71897f786f13ecfad8db6085d61a1be284c76dcb1ca50

2. notarizeWithReason (0xb00eb7e3)

3. renounceOwnership (0x715018a6)

4. setJsonURIBase (0x8b9a403b)

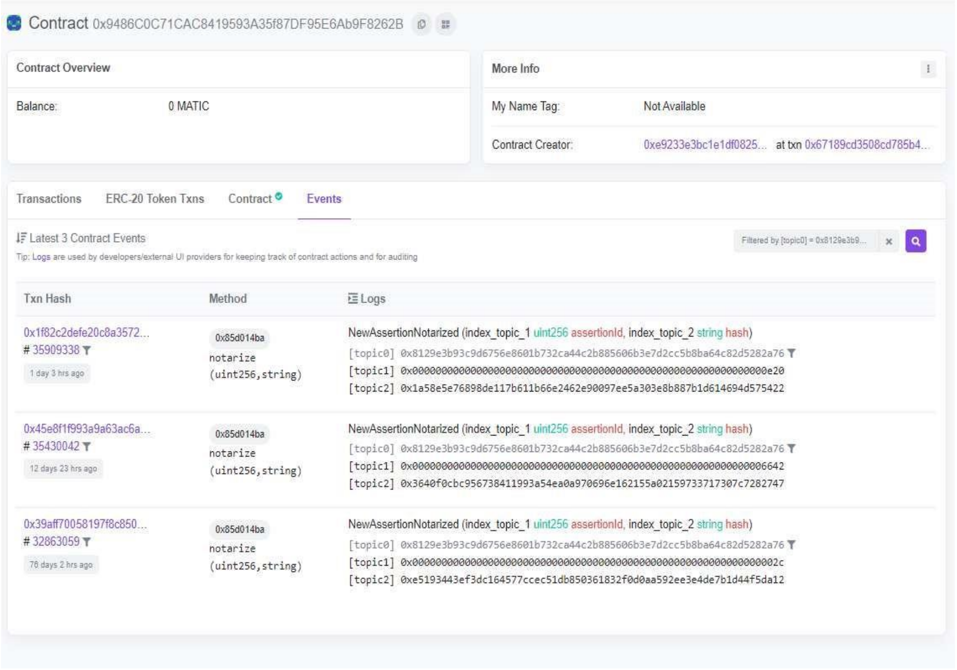
5. transferOwnership (0xf2fde38b)

Figure 6. The notarization method.

```
{
    “IssuedOn”: “12/17/2019 11:00:00 PM”,
    “LeanerEmail”: “alberto.francia@pomiager.com”,
    “Name”: “C-BOX BADGE”,
    “Description”: “I am a description”,
    “BadgeType”: “Oprb Badge”
}
```

Listing 1. JSON of the badge to be notified.

Every writing action on a public blockchain must be paid for via cryptocurrency. The gas fee is a fee paid for the use of the network and its nodes. The gas fee is paid in cryptocurrency, such as Eth (for the Ethereum blockchain) or Matic (for the Polygon blockchain), and its value can vary depending on supply and demand on the network as well as on the complexity of the transaction itself. The gas fee is a fee paid by users on the blockchain network to ensure the efficiency and security of the system. Since network nodes are managed by volunteer users (miners), the gas fee provides an incentive to motivate users to contribute their computing power to the network. By paying this fee, users can ensure priority in verifying and recording their transactions. The gas fee contributes to the efficiency of the network, avoiding abuses and congestion, and ensures a fair allocation of resources. It is important to keep in mind that the gas fee is only required for write operations (transactions) and never for reading.



Contract 0x9486C0C71CAC8419593A35f87DF95E6Ab9F8262B

Contract Overview

Balance: 0 MATIC

More Info

My Name Tag: Not Available

Contract Creator: 0xe9233e3bc1e1df0825... at txn 0x67189cd3508cd785b4...

Transactions | ERC-20 Token Txns | Contract | Events

Latest 3 Contract Events

Tip: Logs are used by developers/external UI providers for keeping track of contract actions and for auditing

Filtered by [topic0] = 0x8129e3b9...

Txn Hash	Method	Logs
0x1f82c2defe20c8a3572... # 35909338 1 day 3 hrs ago	0x85d014ba notarize (uint256,string)	NewAssertionNotarized (index_topic_1 uint256 assertionId, index_topic_2 string hash) [topic0] 0x8129e3b93c9d6756e8601b732ca44c2b885606b3e7d2cc5b8ba64c82d5282a76 [topic1] 0x0000000000000000000000000000000000000000000000000000000000000e20 [topic2] 0x1a58e5e76898de117b611b66e2462e90097ee5a303e8b887b1d614694d575422
0x45e8f1f993a9a63ac6a... # 35430042 12 days 23 hrs ago	0x85d014ba notarize (uint256,string)	NewAssertionNotarized (index_topic_1 uint256 assertionId, index_topic_2 string hash) [topic0] 0x8129e3b93c9d6756e8601b732ca44c2b885606b3e7d2cc5b8ba64c82d5282a76 [topic1] 0x0000000000000000000000000000000000000000000000000000000000006642 [topic2] 0x3640f0cbc956738411993a54ea0a970696e162155a02159733717307c7282747
0x39aff70058197f8c850... # 32863059 76 days 2 hrs ago	0x85d014ba notarize (uint256,string)	NewAssertionNotarized (index_topic_1 uint256 assertionId, index_topic_2 string hash) [topic0] 0x8129e3b93c9d6756e8601b732ca44c2b885606b3e7d2cc5b8ba64c82d5282a76 [topic1] 0x000000000000000000000000000000000000000000000000000000000000002c [topic2] 0xe5193443ef3dc164577ccec51db850361832f0d0aa592ee3e4de7b1d44f5da12

Figure 7. Confirmation from the smart contract.

3.3.3. Creation and Verification Workflows

Figure 8 shows the process by which an Issuer can issue Verifiable Credentials with the C-Box application.

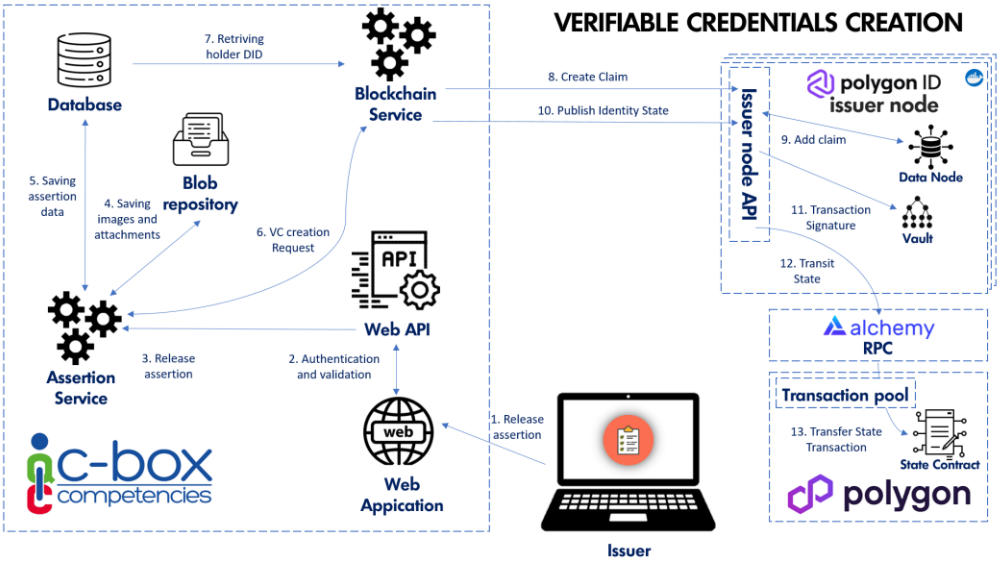


Figure 8. Creation of verifiable credentials in C-Box®.

- The Issuer user issues a digital badge to multiple users from the dedicated page of the platform (1) in the case of a human user issuing the badge manually, or by using the C-Box® API services in the case of a third-party application integrated with C-Box®.
- Following the usual authentication and validation checks (2), the Assertion Service handles all release procedures (3), including the creation and saving of images in the blob repository (4) and saving the related data in the database (5).
- The Verifiable Credentials release procedure is carried out by the Blockchain Service (6): that is, the C-Box® module provides access to all the functions belonging to the blockchain, such as the smart contract, which first retrieves the DID files of the learners (7) saved in the Database.
- Now, the Blockchain Service can query the relevant issuer node and create the VC through the CreateClaim API, specifying the learner’s DID, the reference scheme, and the information related to the certification to be issued (8).
- The Issuer node adds this information to its storage system (9).
- Once the claims have been added for all learners, the Blockchain Service takes care of saving the addition of the new claims in the blockchain (10).
- “Publish Identity State” is an API of the Issuer node that retrieves the current state of the database in which the clear information has been saved. Using an algorithm that employs merkle tree roots, the storage system obtains a string describing the current state of the issuer node’s storage system. This string is saved on a dedicated smart contract (11–13) specifying the previous and current states of the issuer node. This asynchronous blockchain publishing procedure minimizes the number of transactions made on Polygon, thus avoiding excessive and unnecessary gas consumption in Polygon.

Figure 9 describes the process by which a verifier can request a user (holder) to prove possession of a particular certification.

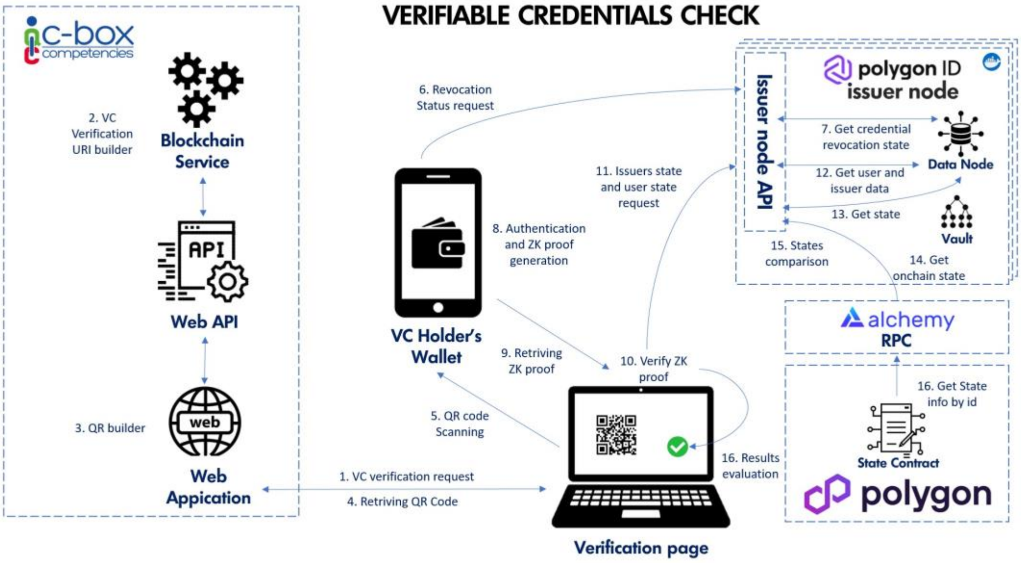


Figure 9. Verification of verifiable credentials in C-Box®.

Before our re-engineering effort, in C-Box®, the verification of the validity of a competence was carried out through the consultation of badges that attest to the competencies held by the badge holder whose skills one wants to verify. Polygon Id changes this process: verifiers can set up queries based on claims mapped by Open Badges issued by a set of issuers. The query encapsulates the criteria that a user must meet in order to meet the requirements of the verifier and can include multiple requirements. As shown in Figure 10, the verifier request is encapsulated in a QR code (generate zk request) and is shown to the user. The user scans the QR code with his/her wallet application to generate a ZKP. Note that the verification process does not involve any interaction between the verifier and the issuer that issued the claim but is a simple query to the verifiable data registry (Polygon) that verifies that the verifiable credentials that certify compliance with the required criteria are valid and not revoked. The Verifier thus obtains cryptographic proof that the user fulfils the requests without the user having to share additional information beyond that requested.

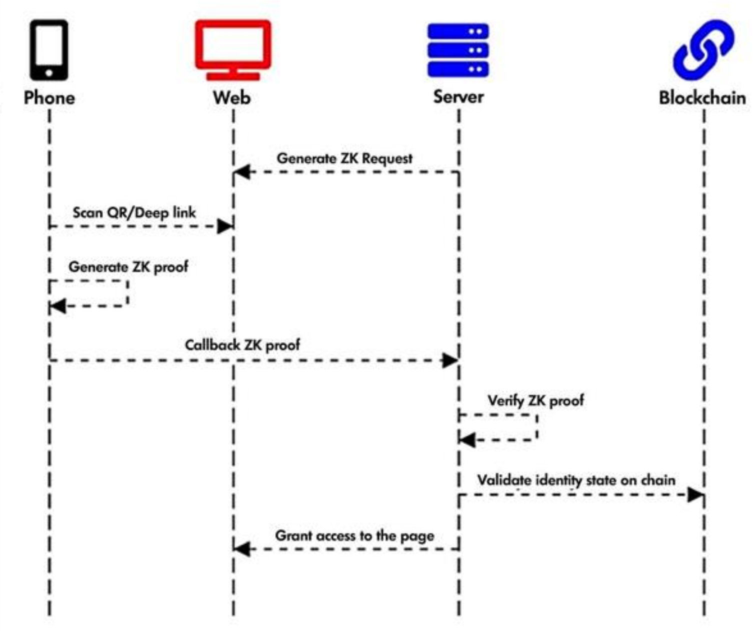


Figure 10. Polygon ID workflow.

Back to Figure 9, a verifier user can decide to set up a check based on verifiable credentials using either an SDK provided by Polygon Id or directly from the C-Box portal.

- The verifier first chooses the type of credential to check, creating the request based on a specific credential schema. He then advance a “VC verification request” to the web application (1).

- The blockchain service translates the request into a query and generates a URI (2) from which a QR code is produced (3) and displayed on the screen (4).
- The holder scans the QR code (5). Upon scanning, the Wallet analyses the query generated by the Verifier.
- The Wallet makes a call to the issuer node to ensure the certification has not been revoked (6–7).
- After successfully completing the authentication (a pin or biometric data), the Wallet initiates the process of generating a zero-knowledge proof to present to the Verifier (8).
- The circuit sends its response to the Verifier via the callbackUrl specified in the QR Code (9).
- After the proof has been sent to the Verifier, it analyses this proof to verify its authenticity and, based on its analysis, validates the proof (10).
- The Verifier finally checks that the Issuer's credential status and the User's status are still valid (8–14) and have not been revoked.
- If the verification is successful, the Verifier grants access to the user or activates any custom logics (15).

Notice how the user is able to demonstrate that he/she possesses his/her credentials (the competency digitally represented by the Open Badge) by providing only the requested information. He/she does not have to provide his/her first name, surname, email, or other information out of the context examined by the verifier (the employer). All is in full compliance with the ZKP paradigm. The user also explicitly choses what information to provide to the verifier and does not have to request any resources from the issuer or submit any request, which is in full fulfilment of identity verification in the context of SSI.

Finally, Figure 11 describes the process by which the holder can redeem his/her verifiable credentials on his/her wallet.

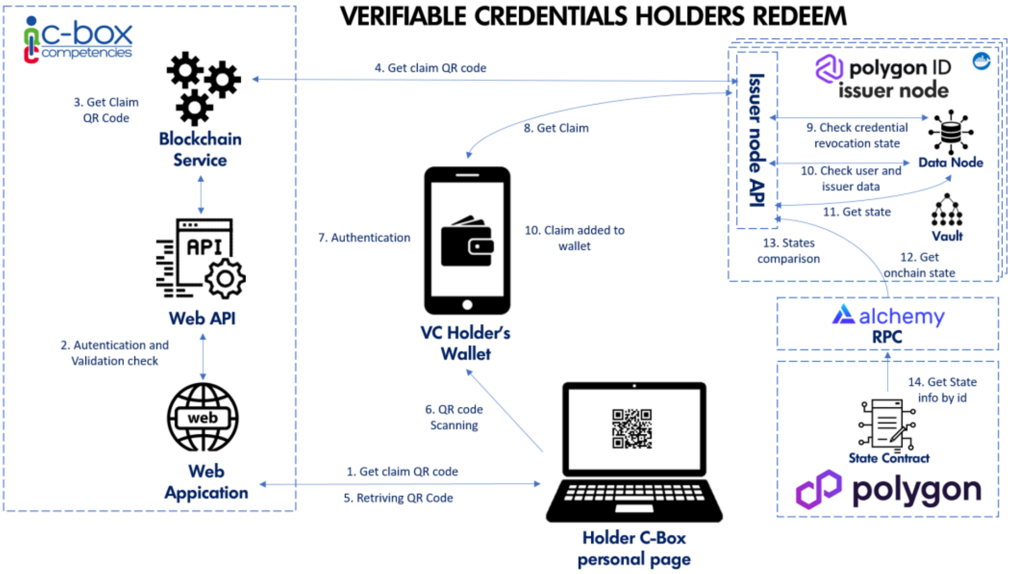


Figure 11. Redeeming of verifiable credentials.

- Upon accessing the private area of the user who received the credential, the holder requests the QR code for importing the credential (1) into his/her wallet.
- Following authentication and validation checks (2), the web application forwards the request to the application.
- The Blockchain service then traces back to the issuer who issued the certification and, by querying the relevant issuer node, retrieves the correct QR code (4).
- The code is returned to the application (5) and is displayed on the screen.
- The holder can now open his/her C-Box Verifiable Credentials wallet application installed on his/her device and scan the QR Code (6).
- The app extracts from the QR Code and performs authentication checks via biometrics or a pin code (7).
- The wallet can now make the call to the issuer node (8).
- The node first checks the status of the credential, ensuring that it has not been revoked (9), then retrieves the information related to the credential in the storage system (10).
- Finally, the status of the latter is evaluated (11) and compared with the status published on the blockchain (12–13), thus validating the integrity of the issuer node.
- The wallet application can then finally save the credential within its storage system (10).

3.3.4. NFTs as Incentives

NFTs provide a unique solution for digitizing and authenticating objects or competencies in the virtual world [12] that, when applied to Open Badges, bring a number of advantages:

- The possibility to unequivocally verify the ownership of a badge;
- The ability to be transferred between wallets, thus offering the possibility to move a badge to different wallets;
- The ability to be imported and exchanged on different platforms, offering wide interoperability and portability;
- The ability to be easily transported and recognized on any platform that supports NFT standards. This means that an individual can “carry” his Open Badge with him all over the web, demonstrating his competencies or achievements wherever he goes. In addition, NFT portability can help reduce reliance on a single vendor or platform, giving individuals greater autonomy and control over their data and accomplishments.

However, there are also some potential disadvantages to consider. Since NFTs are public and traceable on the blockchain, if an Open Badge contains personal information, a privacy issue may arise. As mentioned earlier, using NFTs to manage personal data can present compliance issues with the General Data Protection Regulation (GDPR). However, to ensure the immutability of the content of an NFT, it is necessary that it points to an independent and immutable resource. In fact, the content of the Open Badge does not reside in the blockchain but in the server that makes it available at a given URL. Hence NFTs can be saved to an IPFS (InterPlanetary File System) (https://ipfs.tech/, accessed on 23 October 2023), which is a distributed, decentralized network used for permanent storage. An IPFS allows any user participating in its peer-to-peer network to save information persistently on all its component nodes. However, it is impossible by design to remove such information with certainty once it has been uploaded. If this approach were followed, the owner of the Open Badge would not have the ability to make the badge private, since an IPFS does not support this feature.

Thus, to obtain the aforementioned advantages of NFTs while solving this problem, we designed the NFTs of the C-Box® platform to point to an HTTPS resource in the C-Box® domain. Even if the content of the NFT can no longer take advantage of the immutability guaranteed by an IPFS in this way, (i) it becomes possible for the user, if he/she wishes, to make the information contained in the NFT private or to restrict access to it through an authentication process, and (ii) immutability is nevertheless preserved thanks to integrating a reference to the notarization verification portal into the NFT information. This system, implemented on C-Box®, blends NFT technology with privacy and confidentiality requirements, offering an effective and efficient solution to the challenges posed by the interaction between blockchain and personal data protection.

Finally, it is important to underline the fact that the creation of an NFT for each individual assertion on the C-Box® platform takes place only at the explicit request of the user. This process requires the user to connect his/her blockchain wallet to his/her C-Box® profile. This choice respects the user's right to have active and conscious control over the creation and management of his/her information.

Of course, an NFT representing an Open Badge does not directly represent the competence, but it provides digital proof of its acquisition. Whoever buys the NFT does not become the subject of the competence but the owner of the certificate attesting to that competence. The application of NFTs to Open Badges thus introduces an element of collectability that can open up new business opportunities for issuers. This can stimulate learners to acquire a variety of Open Badges, increasing their professional training and, consequently, the offer of courses by issuers. NFTs on Open Badges have a potentially much wider value, as they can be used to create a market of competencies and experience. In this way, ownership of an NFT could become a status sign, indicating that an individual has acquired an asset describing a high-value competence.

In Figure 12, the process of a user (learner) wanting to redeem the NFT of the badge previously assigned to him/her is described.

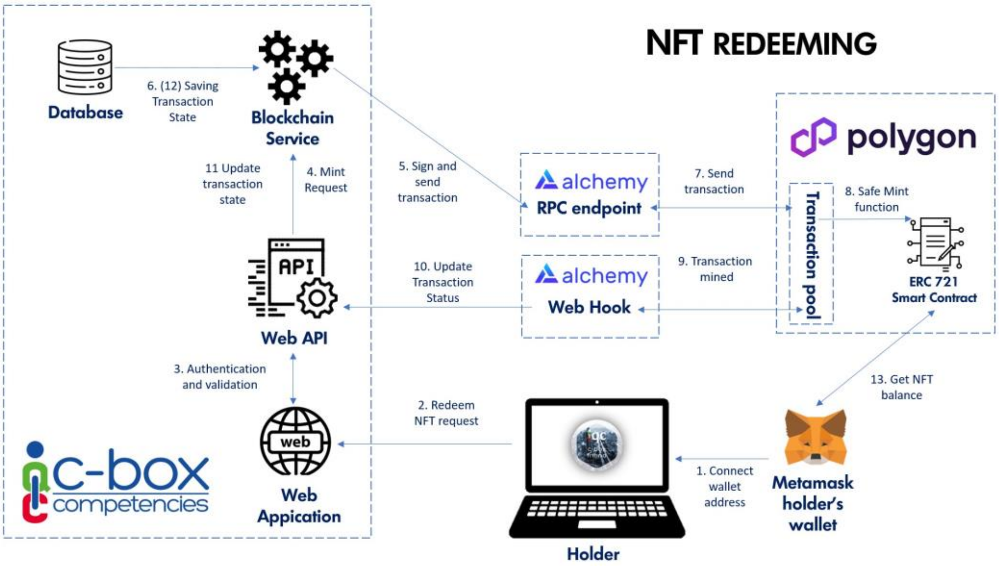


Figure 12. *Redeeming of the NFT associated with an owned Open Badge.*

- The Web Application searches for the Metamask extension on the user's browser. If it is not installed, the user is prompted to install it, and the application provides the necessary instructions. The user is prompted to connect his/her wallet to the C-Box site (1). This allows the web page to read the user's public key via JavaScript. If necessary, the user is prompted to switch the Metamask network to Polygon Mainnet.
- The webpage can now make a call to the C-Box web application (2) containing the assertion's identifier and the user's public key.
- The call is then forwarded to the Web API component (3), which checks authentication and validation requirements (i.e., that the logged-in user owns the assertion and that an NFT has not already been redeemed for that assertion).
- The Blockchain service then estimates the gas required for the minting operation and makes the transaction via Alchemy's RPC (4–7).
- Similarly to the notarization process, the transaction status is asynchronously updated via webhook (9–12).
- The transaction invokes the "safeMint" method (8) of the smart contract related to the NFT collection under the jurisdiction of this specific issuer. The function passes parameters such as the newly created unique identifier of the assertion and the address of the learner's wallet to which the NFT should be sent.
- The Metamask wallet can now recognize the newly minted token now in the user's possession (13). From now on, the user can conveniently access the NFT from the "NFT" section of Metamask.

Third-party applications that host NFTs–OpenSea (https://opensea.io/, accessed on 23 October 2023), for instance—can now query the smart contract and retrieve the URL to access specific metadata (description of the NFT, any attributes, and the image), as depicted in Figure 13.

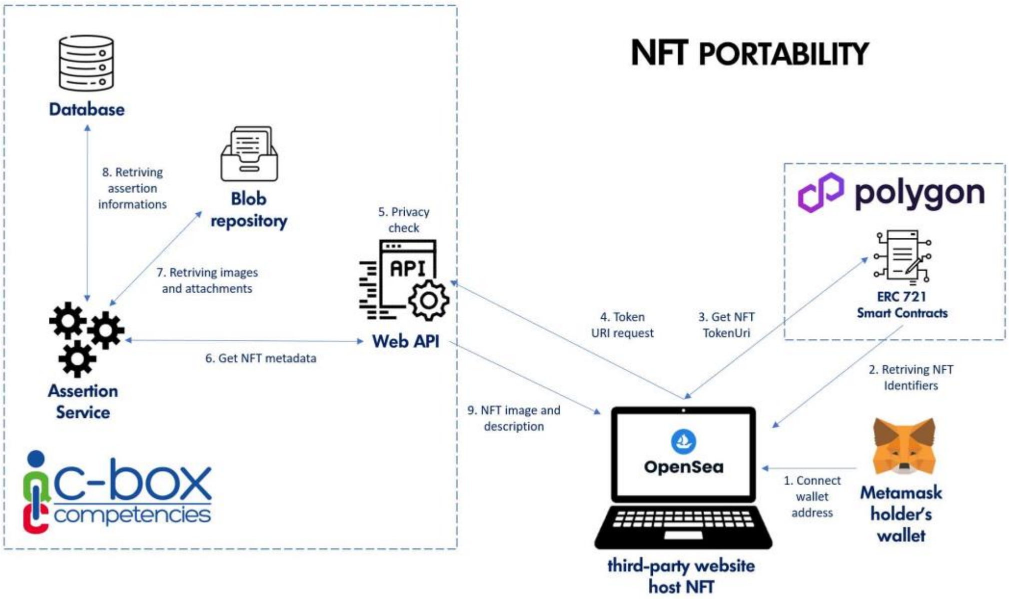
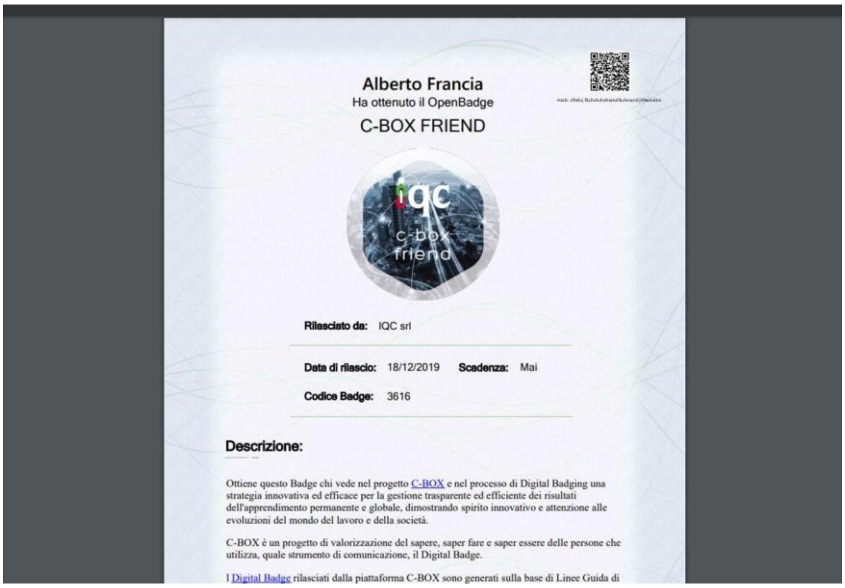


Figure 13. *NFT portability across hosting platforms.*

- By connecting the wallet (1), the hosting webpage can use Metamask to read the user's address and query the NFT smart contracts that have interacted with it.
- The page can then retrieve the NFT Identifiers that identify the tokens owned by the user (2).
- To display the description and image of each individual NFT, the hosting platform retrieves the "NFT token URI" by querying the smart contract with the NFT Identifiers (3).
- The NFT token URI is indeed the address where a JSON containing the NFT's descriptive metadata can be found. These metadata are exposed through a specific API call provided by the C-Box API application (4–8). To protect privacy, such metadata can be obscured by the user through the C-Box platform at any time.

3.3.5. Support for Printed Badges

Issuer organizations often need to provide their learners with a physical version of the open badge, but ensuring the authenticity of these paper versions is a challenge. The goal is to provide a tool that can verify the authenticity of a physical document in a fast and user-friendly way. For this purpose, C-Box® provides QR codes on the printable version of the attestation (Figure 14).



Hash: [illegible]

Alberto Francia
Ha ottenuto il OpenBadge
C-BOX FRIEND

Rilasciato da: IQC srl

Data di rilascio: 18/12/2019 **Scadenza:** Mai

Codice Badge: 3616

Descrizione:

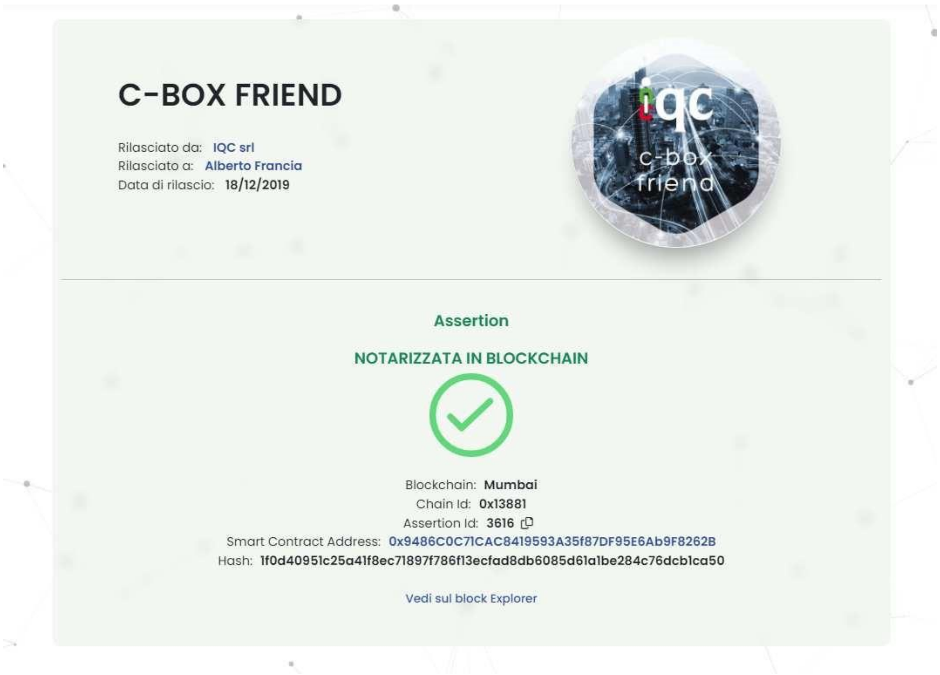
Ottiene questo Badge chi vede nel progetto C-BOX e nel processo di Digital Badging una strategia innovativa ed efficace per la gestione trasparente ed efficiente dei risultati dell'apprendimento permanente e globale, dimostrando spirito innovativo e attenzione alle evoluzioni del mondo del lavoro e della società.

C-BOX è un progetto di valorizzazione del sapere, saper fare e saper essere delle persone che utilizza, quale strumento di comunicazione, il Digital Badge.

I Digital Badge rilasciati dalla piattaforma C-BOX sono generati sulla base di Linee Guida di

Figure 14. *QR code provided for the paper attestation.*

Upon scanning the QR code, the user is redirected to the blockchain verification page (Figure 15). On this page, the user can access the digital and immutable version of the assertion and can directly access the details saved on the blockchain and the notarized JSON (Figure 16). Confidentiality requirements are respected since the digital version and metadata are only shown if the open badge has been made public either by the learner or by the issuer. In the case of a private badge, access to online information will be allowed only against a login procedure by a user with specific authorization policies.



C-BOX FRIEND

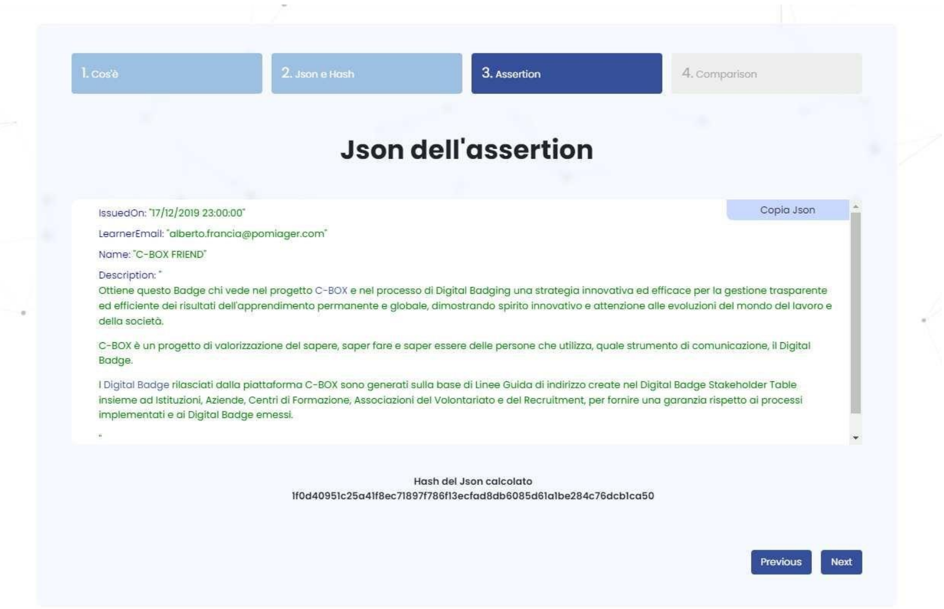
Rilasciato da: IQC srl
Rilasciato a: Alberto Francia
Data di rilascio: 18/12/2019

Assertion

NOTARIZZATA IN BLOCKCHAIN

Blockchain: Mumbai
Chain Id: 0x13881
Assertion Id: 3616
Smart Contract Address: 0x9486C0C71CAC8419593A35f87DF95E6Ab9F8262B
Hash: 1f0d40951c25a41f8ec71897f786f13ecfad8db6085d61a1be284c76dcb1ca50

Figure 15. *Verification page.*



Json dell'assertion

IssuedOn: "17/12/2019 23:00:00"

LearnerEmail: "alberto.francia@pomiager.com"

Name: "C-BOX FRIEND"

Description: "
Ottiene questo Badge chi vede nel progetto C-BOX e nel processo di Digital Badging una strategia innovativa ed efficace per la gestione trasparente ed efficiente dei risultati dell'apprendimento permanente e globale, dimostrando spirito innovativo e attenzione alle evoluzioni del mondo del lavoro e della società.

C-BOX è un progetto di valorizzazione del sapere, saper fare e saper essere delle persone che utilizza, quale strumento di comunicazione, il Digital Badge.

I Digital Badge rilasciati dalla piattaforma C-BOX sono generati sulla base di Linee Guida di indirizzo create nel Digital Badge Stakeholder Table insieme ad Istituzioni, Aziende, Centri di Formazione, Associazioni del Volontariato e del Recruitment, per fornire una garanzia rispetto ai processi implementati e ai Digital Badge emessi.

"

Hash del Json calcolato
1f0d40951c25a41f8ec71897f786f13ecfad8db6085d61a1be284c76dcb1ca50

Figure 16. *Notarized JSON.*

4. Advantages and Limitations of C-Box

In this section, we delve into the strengths and challenges of C-Box®, a platform transforming competency verification. We'll explore how it streamlines processes and respects privacy while also addressing its limitations, such as blockchain dependency and smart contract execution.

4.1 Advantages and Applications

C-Box® enhances a company's internal competency management system in several ways. First, the verifiable and reliable nature of the information contained in VCs simplifies the process of verifying employee competencies. This means that employees can quickly and easily provide information about their training and qualifications without having to perform manual checks or checks by the company's HR. Second, C-Box® provides employees with more control and autonomy over their digital identities. This means that employees can decide to share only relevant information about their competencies and qualifications, protecting their privacy and ensuring that personal information is only used for legitimate purposes. In addition, C-Box® simplifies the sharing of competency and qualification information among employees, improving collaboration and productivity within the company. This is especially useful for large companies with multiple locations, as it allows employees to quickly and easily share their competencies and qualifications with their peers around the world. Finally, C-Box® streamlines the onboarding of new employees, allowing them to easily share information about their competencies and qualifications with the company. This can speed up the process of integrating new employees into the organization, ensuring that they are quickly assigned to appropriate positions based on their competencies and qualifications.

Imagine a healthcare professional named Laura. She owns a number of VCs that attest to her various competencies, training, and certifications in the field of medicine. Now suppose Laura wants to apply for a position in a hospital that specifically requires expertise in cardiology. In this case, Laura has a VC attesting to her specialization in cardiology. Suppose that throughout her career, Laura has also acquired competencies and certifications in other medical areas, such as psychiatry and orthopaedics. These other competencies, while valid and important, are not directly relevant to the specific position Laura is currently applying to. In addition, it may be in Laura's best interest not to immediately share the full spectrum of her competencies for various reasons, including the possibility of appearing overqualified or wanting to focus on the most-relevant competencies. In this context, Laura can exploit the benefits of ZKP to demonstrate to the hospital that she has the cardiology specialization, without revealing the other competencies or qualifications present in her VC. With the use of the ZKP, Laura can provide cryptographic proof that confirms the validity of her specialization in cardiology while keeping other competencies or certifications private. This way, the hospital can verify the required competence without having to access additional information about Laura's other competencies.

From the point of view of the verifier, C-Box® provides a competency verification system that allows the control of multiple competencies in a rapid and certified way: continuing the previous example, the hospital will be able to create a QR code that, once scanned, starts a query to verify the specific competencies required for the role of a cardiologist. Using her smartphone, Laura can scan the QR code, which automatically launches her digital wallet app (her User Agent). At this point, Laura’s User Agent will search her VCs for proof of attestation in cardiology. Once the corresponding VC is found, C-Box® will create a Verifiable Presentation, which includes the ZKP. The latter allows Laura to demonstrate that she has the required competence without having to disclose the other competencies or qualifications. Laura’s digital wallet will then send the Verifiable Presentation to the hospital for verification. The hospital can then verify the authenticity of the presentation, checking if the entity that issued the credential is a reliable source and that the presentation has not been altered or falsified. In addition, the hospital can verify that the VC meets the criteria specified in the original query initiated through the QR code. If everything is successfully verified, the hospital can then confirm that Laura does indeed possess the cardiology specialization required for the position. This example illustrates how the use of ZKP for VCs enables assessment of competencies that respects the individual’s privacy, allowing selective sharing of information without compromising the confidentiality of other competencies or qualifications. The use of ZKP in this context balances the need to demonstrate the required competencies and the privacy of the individual, ensuring that only relevant information is shared without compromising the confidentiality of other personal information.

4.2 Limitations

C-Box® also has some limitations and open issues that provide starting points for future improvement.

For instance, the choice of re-engineering the platform on top of a public blockchain provides the benefits of wider adoption, maximum transparency, and full decentralised control (as already discussed). However, it also poses some open issues that we are currently dealing with and which will be the subject of further work: mostly, its dependency on a native cryptocurrency for both transactions and smart contract execution. Every operation registered on the blockchain will spend some blockchain cryptocurrency to be carried out (even if in the slightest amount). Ensuring that all of the stakeholders have the right incentive to still adopt C-Box® as a remunerative investment must be a priority. Notice, remuneration need not be monetary or financial: certificate holders (e.g., students), for instance, have incentives to adopt the platform to preserve and exploit their curriculum and careers despite any monetary return.

Execution of smart contracts brings us to other potential issues and limitations: First, as already said, smart contracts also spend money to execute; hence, such expenditures must be predictable and sufficiently low so as not to scare users away. Second, smart contracts are immutable and thus must be carefully and extensively tested before deployment, as it is yet unclear and not standardised how to “deactivate” or remove a deployed smart contract or the implications of this. Related to the monetary cost of smart contracts’ execution is the need to carefully optimize the smart contract’s source code to limit expenditures as much as possible. In C-Box®, the smart contract devoted to notarization has been carefully designed, implemented, and then optimised to keep transaction fees at the lowest and to devise upper bounds on related expenditures. A rigorous description of the process and analysis of computational performance as well as average costs is the subject of ongoing work and will be published separately.

Another open issue is a precise evaluation of the role of NFTs as complementary incentives to Open Badges. Our hope is that NFTs stimulate and incentivize people to acquire skills and competencies to showcase on, e.g., social platforms, but also to potentially gain monetary and financial value from them—as exemplified in Section 2.3.2. In perspective, a whole market can grow out of NFT exchange targeted at collectors of others' certificates.

Finally, we have identified another open issue related to evaluation regarding the whole C-Box® platform. A rigorous assessment of C-Box®'s performance and adoption is needed to confirm its strengths and uncover potential issues. Such an endeavour is currently underway.

4.3 Evaluation Methodologies

In this section, we explore the comprehensive strategies employed to assess the impact of transitioning C-Box to a public blockchain infrastructure. This evaluation not only highlights the technical reengineering efforts but also outlines the key performance indicators used to measure the success and challenges of the implementation, ensuring a holistic understanding of both the technological shift and its real-world outcomes.

The restructuring of the C-Box service necessitated the switch from the previously used blockchain provider. The original service was developed on a private Quorum blockchain, offered as a service by Azure, which provided a blockchain composed of three nodes. The need to deploy a new notarization system on a public blockchain became evident when Azure announced the discontinuation of its blockchain service, transferring the management of C-Box blockchain nodes to another private entity specializing in cloud and distributed solutions, Kaleido. This situation prompted Pomiager and IQC to demand a service capable of ensuring data immutability, regardless of changes in external providers. The limitation of a private entity with only three nodes did not meet the security and redundancy requirements ensured by public blockchains such as Polygon or Ethereum. It is noteworthy how a giant like Microsoft's Azure decided to cease a service linked to an emerging technology, implicitly suggesting that the future of blockchain leans towards public rather than private solutions.

Adopting a broad public blockchain like Polygon has provided C-Box users with greater service continuity and security. However, despite the restructuring being operational for three months, user trust in the system has not reflected the expected stability and immutability. Reports of malfunctions in the notarization system were frequent, necessitating on-the-fly improvements. Specifically, issues arose due to the high volume of requests to Alchemy's RPC service, causing temporary inaccessibility of blockchain information. Moreover, a mismatch between the hash calculated from off-chain data and that recorded on the blockchain raised concerns, even though no information was altered or lost. These "false positives" led to numerous reports to technical support but also demonstrated the notarization service's effectiveness in signaling any discrepancies in certified information, thereby allowing C-Box developers to address and resolve the identified issues.

While it is true that adopting a public blockchain subjects the system to the volatility and price susceptibility of the necessary cryptocurrency to keep the system running, it is also true that, currently, the use of a public blockchain service is significantly less costly compared to the previous private blockchain solution, with a cost reduction that can reach two orders of magnitude. This makes the choice of a public blockchain not only economically advantageous but also does not compromise the security and confidentiality of the managed information.

The data handled through these blockchain services are sensitive and thus are protected under data protection regulations such as the GDPR. This ensures that the right to be forgotten and the storage of data within European borders are always upheld. Indeed, the information recorded on the distributed ledger is both compressed and encrypted (effectively hashed), making it practically impossible to trace back to the public information, which remains readable only within the databases and servers managed by Pomiager. This ensures that access to and ownership of the data are always exclusive to the users who hold the rights to that information.

At the time this thesis was written, the notarization system has been operational for three months, whereas the development of a wallet based on Polygon ID is still in progress. This ongoing development process is due to the emergence of new standards related to verifiable credentials, such as the European digital wallet and the IT-Wallet, which have been identified as strategic targets by IQC and Pomiager. These entities are keen on adopting these novel technologies early, positioning themselves as first movers in the field. Consequently, the development of their proprietary wallet solution integrated with Polygon ID has been somewhat deprioritized. The overarching goal remains to deliver a service that excellently balances reliability, performance, privacy, and the incorporation of avant-garde technologies.

To effectively measure the performance and the impact of these implementations, several key indicators have been outlined:

Evaluation and download numbers of the wallet app: This metric is crucial for gauging the influence that Self-Sovereign Identity (SSI) technologies may have on digital badge holders. By analyzing the app's reception and its adoption rate, insights into user engagement and the perceived value of SSI technologies can be gleaned. It reflects the users' trust in and the usability of the platform, indicating the potential for widespread acceptance of digital wallets in managing digital identities.

Number of new issuers signing up for C-Box: This indicator is essential to determine whether the recent developments and functionalities indeed translate into a competitive edge over other platforms. An increase in the number of issuers opting for C-Box could signal that the platform offers distinct advantages, such as enhanced security, greater efficiency, or more seamless integration with emerging digital identity standards. This metric helps to understand the platform's market positioning and its attractiveness to organizations seeking blockchain-based notarization services.

Percentage of badges converted into NFTs by users: Understanding users' interest in converting their attestations into NFTs is vital, as it reveals the demand for tokenizing digital credentials for enhanced ownership and transferability. This metric also sheds light on the user-friendliness of the process, especially in the context of Web3 technologies. If the processes required for account activation and badge conversion are sufficiently streamlined, it could indicate the platform's success in making complex blockchain functionalities accessible to the average user.

So far, the NFT minting service has been made available to a select group of issuers, allowing approximately 2300 users the option to redeem an NFT. Out of these, 51 users have redeemed an NFT, which corresponds to a redemption rate of about 2%. It's noteworthy that this feature has not yet been extensively marketed, as the intention is to conduct a pilot test with a smaller user base to identify areas for improvement and ensure the system's stability before a broader rollout. This cautious approach reflects a commitment to quality and user satisfaction, aiming to refine the service based on real-world usage and feedback.

5. Blockchain energy cost analysis

In this section, I have detailed the evidence gathered from literature pertaining to the critical issue of energy consumption demanded by blockchain technology. This technology has been criticized and vilified for its characteristic of being extremely energy-intensive. Initially, (1) we will examine why it consumes so much energy, then (2) we will review the actions that have been implemented over time to reduce its impact, and finally, (3) we will attempt to determine the energy consumption required for validating transactions executed by the blockchain used by C-Box.

To understand where and why a blockchain consumes so much energy we need to introduce the concept of mining, a crucial component of cryptocurrencies like Bitcoin and Ethereum and their respective blockchain networks. Transactions are actions carried out by users, such as transferring cryptocurrency, which need to be confirmed and recorded. A block is a set of these transactions, bundled together along with a unique code that links it to the previous block in the chain, thus forming the blockchain. Mining involves validating these transactions and ensuring they are legitimate before adding them to the blockchain. This process prevents issues like double-spending and maintains the decentralized, secure nature of the cryptocurrency network. As a reward for their efforts, miners receive a certain amount of the cryptocurrency, along with transaction fees, which incentivizes them to continue supporting the network.
The efforts required by miners in a blockchain network are dictated by its specific consensus algorithm, a fundamental aspect that varies for each blockchain. This algorithm defines the rules and processes that miners must follow to validate transactions and add new blocks to the blockchain. In essence, it is the consensus algorithm that determines how miners participate in the network, the nature of the computational challenges they must solve, and how they are rewarded for their contributions.

In a Proof of Work (PoW) system, like that used by Bitcoin [36], nodes that verify transactions (known as miners) must perform a complex computation to assert the validity of entities in the network. Figure 17 describes the mining process in the Bitcoin blockchain. During the mining process, the miner computes the hash of a block of transactions. A block also contains other data, such as the hash of the latest accepted block in the blockchain, and a ‘nonce’ value that the miner can choose randomly. The aim of the miner is to find a nonce value such that the hash of the block is smaller than a target value T. In the bitcoin network, the 256-bits cryptographic hash of a block B is computed by applying the SHA-256 hash function twice, h(B) = SHA256 (SHA256(B)), which yields a hash that behaves approximately as a uniformly random value between 0 and 2^{256} - 1. Hence, the only way to find a valid hash is to randomly try nonce values. The bitcoin network controls the difficulty for finding a valid hash by adjusting the target T every 2016 blocks, with the aim of keeping the average time to mine a new block near 10 min.

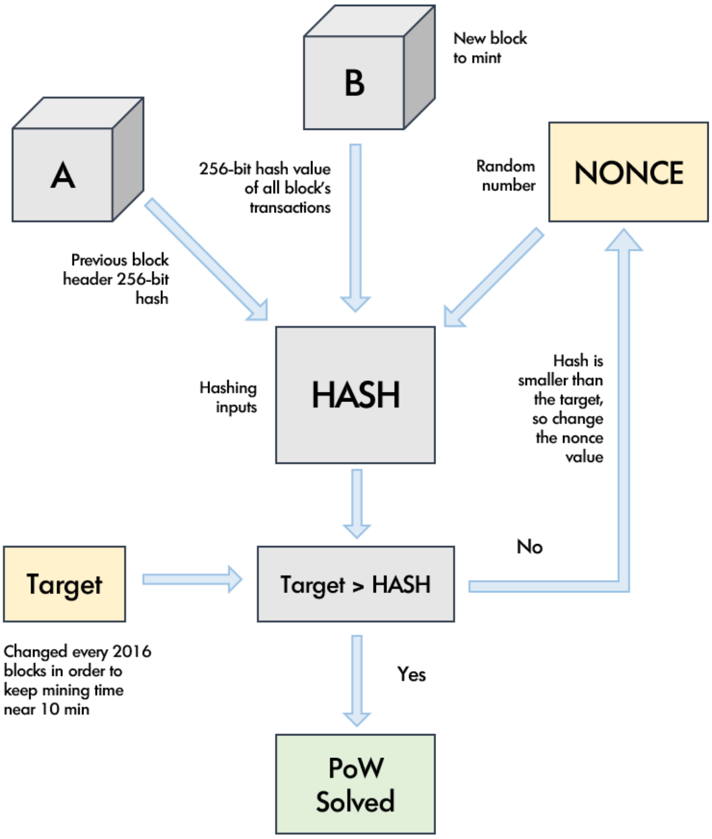

B
New block to mint
A
256-bit hash value of all block's transactions
Random number
NONCE
Previous block header 256-bit hash
HASH
Hashing inputs
Hash is smaller than the target, so change the nonce value
No
Target
Target > HASH
Changed every 2016 blocks in order to keep mining time near 10 min
Yes
PoW Solved

Figure 17. *Bitcoin PoW process.*

Proof of Work (PoW) can be viewed as a critical and somewhat controversial aspect of blockchain technology. Extensive research has been conducted to determine the actual amount of energy consumed by this process [37] [38]. Over the past decade, miners have adopted strategies to reduce the energy required for mining activities, with the aim of enhancing their profitability. This shift is primarily driven by the increasing costs associated with the energy-intensive process of mining, which directly impacts the earnings from such activities. Between 2013 and 2017, specially designed hardware significantly enhanced the hash rate for Bitcoin mining, improving from 1 million to 1 trillion hashes per second, thereby greatly increasing the energy efficiency of the mining process [39]. These changes reflect a growing awareness within the cryptocurrency community of the need to balance the economic incentives of mining with the environmental concerns associated with high energy consumption. As a result, these adaptations not only contributed to a reduction in operational costs for miners but also potentially lessen the environmental footprint of blockchain technologies, aligning economic interests with sustainable practices.

As of the date of this writing, the most recent study on Bitcoin's energy consumption, accessible via the Digital Economist website (https://digiconomist.net/bitcoin-energy-consumption), provides a comprehensive analysis of this issue. According to this study, the estimated energy consumption of the Bitcoin network is approximately 150 terawatt-hours (TWh). PoW requires a significant amount of energy, yet this energy expenditure does not directly add tangible value to the data processed or 'mined' in the blockchain.

The primary role of PoW is to ensure the immutability of data, maintaining the integrity and security of the blockchain network. However, it is not the sole method for securing data within a blockchain system. In fact, there are various consensus algorithms that do not necessarily require such a high computational effort [40].

Originally, Ethereum, one of the most prominent blockchain platforms, utilized PoW as its consensus mechanism. This changed with a significant event known as "The Merge", which occurred on September 15, 2022. During this event, Ethereum underwent a major transition through a process often referred to as a 'fork.' This transition marked the adoption of a different consensus algorithm: Proof of Stake (PoS).

Proof of Stake (PoS) was developed as an alternative to Proof of Work (PoW) primarily to address the issue of high energy consumption associated with the latter. In PoS, the mechanism for validating transactions and creating new blocks in the blockchain is significantly different. Instead of relying on computational power, as in PoW, PoS determines a participant's voting weight based on their stake in the cryptocurrency – that is, the owned units of the currency which are finite, visible, and verifiable within the blockchain network.

In PoS, validators of transactions are selected through a semi-random process that involves two main steps. Firstly, validators need to commit a certain amount of the cryptocurrency – their 'stake' – to the network. This stake is locked in the system and acts as a form of security for the validity of the new block. The probability of a validator being chosen to validate a block is proportional to the size of their stake. In other words, the more currency a participant invests as a stake, the higher their chances of being selected as a validator. Once selected, a validator's role is to scrutinize all transactions in a block to ensure they are not fraudulent. After validating these transactions, the validator adds the block to the blockchain. The reward for this process is the collection of transaction fees associated with each verified transaction. PoS is notably less energy-intensive than PoW because it does not involve the competitive mining process where participants solve complex mathematical puzzles. However, PoS systems are not without their drawbacks. For instance, the cost of carrying out an attack on a PoS network is lower compared to PoW. This is because, theoretically, an attacker would only need to acquire a sufficient amount of the cryptocurrency (the stake) to gain substantial influence over the network and potentially introduce fraudulent blocks into the chain.

According to the study of Kapengut and Mizrach, the shift to PoS reduced Ethereum's energy consumption by approximately 99.98%. This significant decrease highlights the effectiveness of PoS in addressing environmental concerns associated with blockchain technology, particularly in terms of energy efficiency [41].

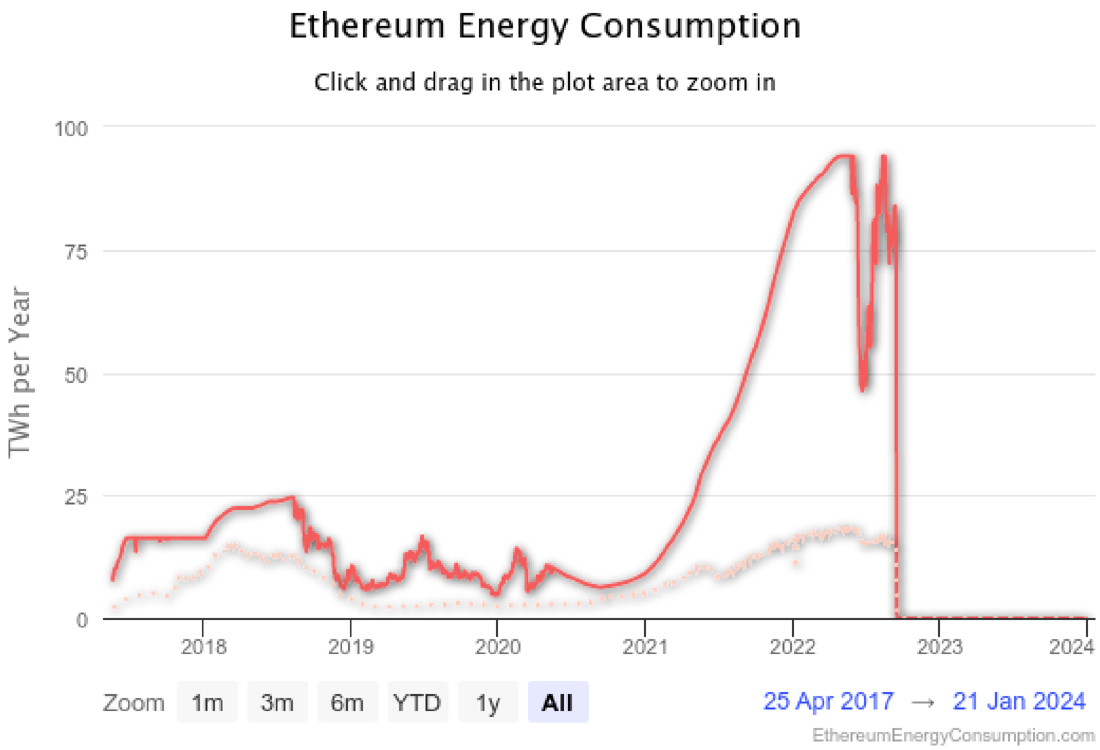


Figure 1. *Ethereum Energy Consumption*
(Ethereum Energy Consumption Index - Digiconomist)

C-Box utilizes the Polygon Blockchain, which functions as a Layer 2 scaling solution for the Ethereum network. Operating parallel to the primary Ethereum chain, Polygon establishes an independent chain rooted in the Proof of Stake (PoS) consensus algorithm. This separate chain offers enhanced speed, supporting a higher number of transactions per second, and reduces the cost per transaction, thereby optimizing performance and efficiency.

To estimate the power consumption of Polygon validators, it is possible to make a reasonable estimate of the power consumption of the current 90 validators. Validators typically operate using AWS EC2 instances. The specifics of these cases, crucial for calculating energy consumption, are outlined as follows: 8 GB RAM, 100Gb SSD x64 2.0 GHz 2v CPU. Each node in our network typically consumes around 350 watts under normal operating conditions. However, their energy consumption can peak at up to 500 watts (assuming excessively that they always work at maximum power). Therefore, the total power draw per validator node is calculated as 500 watts for the validator and another 500 watts for the accompanying node, summing up to 1000 watts per validator. With 90 validators operating globally 8760 hours (hours in a year), the annual energy consumption totals to 788,400 kilowatt-hours (kWh) equivalent to 0.00079 TWh (https://polygon.technology/). Polygon's Proof of Stake (PoS) validators are significantly more energy efficient than miners in Proof of Work (PoW)-based blockchains, resulting in a more environmentally friendly operation with significantly reduced carbon emissions. As the technology evolves, these validators are expected to no only improve the efficiency of transaction processing, but also further optimize energy consumption, thus contributing to an even more sustainable blockchain environment.

5.1 C-Box electricity consumption

In the following section, we will delve into the methodologies applied and the results garnered from our comprehensive analysis of electricity consumption associated with the c-box notarization service. Our investigation aimed to quantify the energy requirements inherent in the operation of this service, providing insights into the computational processes and their corresponding energy implications.

Since the energy required is directly correlated with the computational effort necessary for validating and executing smart contract functions, we have chosen to adopt the unit of gas as a measure in our analysis of energy consumption. Each time a block is mined, a quantity of gas for each transaction that composes the block is burned: The sender pays the miner an amount in cryptocurrency equal to the gas used multiplied by the price of gas at that time, precisely to compensate the miner for their validation activity and execution of the smart contract logics, and the energy they expended. Understanding the annual energy needs of the entire network, and being aware of the total amount of gas units expended by the network, allows us to estimate the amount of energy Polygon requires to notarize a single C-Box assertion. This estimation enables us to compare the energy efficiency of notarization on Polygon with that of other blockchains

At the time of migration, C-Box already had more than one hundred thousand assertions issued and notarized through a private blockchain, to be imported into the new smart contract. This first migration gave us the opportunity to collect information including the average number of gas used for each notarization, finding that on average a transaction cost 96,211 units of gas.

Using Polygon's block explorer, we extrapolated the amount of gas spent by the entire network in the year 2023, obtaining 2.14E+14 gas units. The previously used figure of 788,400 kWh per year reported by Polygon as the annual consumption of the entire network overestimates that reported by the Crypto Carbon Ratings Institute (CCRI https://indices.carbon-ratings.com/), which estimates Polygon's consumption at 126,287 kWh. With a simple proportion, we estimated the notarization of an assertion to be equivalent to 3.55E-04 kWh.

	CO_2 emissions	Total gas burnt (2023)	**Electricity Consumption** (annualised)	Average gas per assertion	Energy consumption per assertion	CO_2 emission per assertion
Polygon	37,781.8 Kgs	2.14E+14	788,400 kWh	96,211	0.00035 kWh	0.017g
Ethereum	2,096,754.4 kg	3.93E+13	6,171,558 kWh	96,211	0.01.51 kWh	5.13g

Table 2. Energy consumption of notarization service

As illustrated in Table 2, it is noteworthy that Ethereum exhibits lower efficiency per gas unit in comparison to Polygon. This reduced efficiency can be attributed to Ethereum's higher energy consumption, likely a consequence of its more decentralized network architecture, which comprises over nine million nodes, as opposed to Polygon's 157,200 nodes. The indices provided by the CCRI also furnish an estimate of the CO_2 emissions generated by each blockchain over the span of a year. Mirroring our methodology for evaluating energy consumption, we have appraised CO_2 emissions using a proportional approach, grounded on the average gas expenditure for a notarization transaction. This approach enables us to assess the environmental ramifications of blockchain activities, particularly focusing on the carbon footprint engendered by the notarization services facilitated by C-Box.

In conclusion, the analysis of the energy consumption associated with C-Box's notarization system reveals a compelling insight into its operational efficiency. With the system estimated to issue 100,000 assertions at an energy expenditure of 35 kWh, this level of consumption underscores the technological strides made in optimizing blockchain technology for practical, everyday applications. To put this into perspective, the average energy consumption of a standard toaster ranges from 0.8 to 1.4 kWh per hour of use. Therefore, the energy required to power C-Box's notarization for 100,000 transactions is equivalent to running a toaster continuously for approximately 25 to 44 hours.

This comparison vividly illustrates the efficiency and sustainability of the C-Box notarization system, demonstrating that advanced blockchain solutions can indeed align with our daily energy consumption patterns in a manageable and environmentally conscious manner.

6. Related Works

In [23], blockchain applications for HRM and other fields are thoroughly surveyed and commented. Out of the 12 papers collected that specifically targeted HRM, only 1 proposes a prototype blockchain-based platform: all others are conceptual studies. That one, however, proposes blockchain as a way to achieve consensus about the skills needed by a consortium of stakeholders; hence, it is much more narrow in scope compared to our proposal [24].

In [25], the QualiChain European project is presented in its initial conception and early development. Other subsequent publications mention the project, but it is unclear to us what final resulting platform it produced (e.g., whether it fulfils all the initial desiderata) and the extent of its adoption. Further, QualiChain is conceived as a comprehensive suite of APIs for the three main stakeholders of blockchain-based competency management: those who acquire them (e.g., students and employees), those who produce them (e.g., schools, training institutions, and work companies), and those who want to validate them (e.g., employers). Thus, QualiChain offers services such as profiling and recruiting that C-Box® does not offer out of the box—although it is posible to develop them on top of currently available C-Box® APIs. As such, QualiChain is surely more comprehensive than C-Box®—at least in theory. However, two peculiarities of C-Box® even when compared to such a comprehensive platform are: usage of NFTs linked to Open Badges to nurture adoption and widen participation, and supporting VCs in full compliance with the SSI paradigm and technological requirements—this latter aspect, in particular, is unclear in QualiChain.

In [26], a badge-awarding system for performance assessment in education is proposed, integrating a platform for badge awarding (compliant with the Open Badges 2.0 specification) and a blockchain for tamper-proof tracking and verification. The proposed system relies on the Badgr platform for Open Badge issuing while either Bitcoin or Ethereum can be used for badge-related event tracking and verification. Although this work is similar to ours in the goal pursued (integrate blockchain into competency management systems for better security and transparency while maintaining decentralisation of control), we exploit blockchain also for distributed verification (through the developed smart contract) rather than for event tracking only. Also, we incorporate NFTs in the picture and more comprehensively support the paradigm of SSI. Also in [27], the Badgr platform is taken as a reference for integration of blockchains, although the developed solution is explicitly a proof-of-concept (featuring a simple custom blockchain implementation) and is more concerned with integration with a MOOC platform than with SSI and badge sharing.

In [28,29], the authors integrate Blockcerts and Ethereum to provide decentralised governance to Open Badges issuers: smart contracts are provided to manage creation and execution of certification consortia and to deal with certificate issuing and verification. Decentralised governance is the focus of the proposed ecosystem, which essentially provides the means to create a decentralised autonomous organisation on a public blockchain. This work is very similar to ours, although we worked with an existing commercial product (C-Box®). The main differences are that we (i) also take care of decentralised credential management by offering a solution based on Polygon IDs, (ii) also provide NFTs as an added incentive to attract users, and (iii) stay open to any Open Badge certification platform, not only Blockcert. Nevertheless, the experimental evaluation carried out in this related work may serve as inspiration for a comparison to be carried out as future work. Also the work in [30] integrates Blockcerts and Bitcoin, although not many details are provided about the smart contracts developed and the processes of certification issue, redemption, and validation.

In [31], another blockchain-based certificate management platform is presented; however, the focus is on students' acquisition and social sharing of certificates, not on SSI and generic competency tracking. Interestingly, though, the authors carry out a performance assessment comparing a private blockchain implementation (HyperLedger Fabric) with a public one (Ethereum), that we plan to undertake as a next step in our research.

In [32], the authors propose their own blockchain implementation for storing digital certificates, which has the drawback of needing to attract users in the first place and competing with already globally established public blockchains.

In [33], another blockchain-based system for competency management is proposed, although it is more focused on solving staff scheduling problems for an organisation than on providing a general-purpose competency management platform open to any typical stakeholder (issuers, validators, and holders). Also, it uses a consortium blockchain; hence, participation is inherently closed to elected members, and it does not rely on open standards for the digital representation of competencies (such as Open Badges). It is thus quite different from the C-Box® platform here presented.

In [34], an NFT-based solution for digital certificate issuing, tracking, and verification is proposed. The Ethereum blockchain together with its smart contracts is used by issuers to craft NFTs representing digital certificates of whatever sort (e.g., students' attestations or worker competencies) by users to acquire NFTs and by others to verify ownership of the NFTs (hence of the certificate). Such a solution shares our objective but does not make use of the Open Badges standard, which is a much more reasonable choice for representing digital certificates, nor does it fully comply with the SSI principles.

In [35], applications of NFT technology to the education sector (and others, to a lesser extent) are surveyed. Among the many applications, management of micro-certificates (i.e., certificates of any sort attesting to even a single lesson attended), learning experiences, student records, and general data collection are also considered. There, NFTs are used essentially in place of Open Badges to digitally represent the achievement of a student: a practice we already commented on as being suboptimal.

In summary, there are many recent attempts to re-engineer (generally speaking) "competency management" systems, especially in education [36], to take advantage of blockchain security, transparency, and decentralisation, or NFTs' capability to represent ownership. This witnesses the rising interest in the topic we deal with in this thesis. However, ours is the first proposal not only adopting blockchain to ease the process of certification validation but also comprehensively taking into account SSI as a cornerstone of competency management, empowering certification recipients to exert full control over their data. Additionally, we also include NFT incentives into the picture as a means to incentivise adoption.

7. Conclusions

In this thesis, we proposed C-Box®, a blockchain-based platform for competency management using Open Badges in full compliance with Self-Sovereign Identity (SSI) principles. With C-Box®, badge recipients, issuer organisations, and verifiers can carry out their goals independently while resting assured that the competencies digitalised as Open Badges, as well as their whole handling process from generation to redeeming, are authentic, correctly attributed by the responsible organisation to the right person, and uncompromised. Part of these desired properties come from the blockchain, which enables implementation of custom smart contracts for the notarization of the whole Open Badge lifecycle. But another part derives from our efforts to design and implement a solution fully compliant with the SSI paradigm: we realised the mechanisms to fully exploit verifiable presentations by using decentralised identifiers and zero-knowledge proof. This puts the user fully in control of his/her own data. Finally, we added to C-Box® the opportunity to release NFTs attached to Open Badges as a form of incentive for participation and also as an opportunity for monetization.

Future directions for the Open Badge and Web 3.0 technology sector require a thorough and methodical examination of the results obtained so far in order to fully understand the impact and potential of these tools. This not only helps to understand the real value and effectiveness of existing solutions but also offers the possibility to identify strengths, areas for improvement, and opportunities for innovation. A key aspect to consider is the analysis of computational performance. With the increasing use of blockchain technology and Web 3.0 applications, it is essential to examine their impact on system performance, both in terms of speed and efficiency. This could include analysing the efficiency of notarization in blockchain, transaction speed, resource management.

Abbreviations

The following abbreviations are used in this manuscript:

HR	Human Resources
SSI	Self-Sovereign Identity
IQC	Italian Quality Company
NFT	Non-Fungible Token
VC	Verifiable Credential
DID	Decentralized IDentifiers
ZKP	Zero-Knowledge Proof
PoW	Proof of Work
PoS	Proof of Stake
CCRI	Crypto Carbon Ratings Institute

References

[1] Yi, C.S.S.; Yung, E.; Fong, C.; Tripathi, S. Benefits and Use of Blockchain Technology to Human Resources Management: A Critical Review. Int. J. Hum. Resour. Stud. 2020, 10, 131. [https://www.macrothink.org/journal/index.php/ijhrs/article/view/16932]

[2] Mishra, H.; Venkatesan, M. Blockchain in human resource management of organizations: An empirical assessment to gauge HR and non-HR perspective. J. Organ. Chang. Manag. 2021, 34, 525–542. [https://www.emerald.com/insight/content/doi/10.1108/JOCM-08-2020-0261/full/html

[3] Clements, K.; West, R.E.; Hunsaker, E. Getting Started with Open Badges and Open Microcredentials. Int. Rev. Res. Open Distrib. Learn. 2020, 21, 154–172. [https://www.irrodl.org/index.php/irrodl/article/view/4529]

[4] Lockley, A.; Derryberry, A.; West, D. Drivers, Affordances and Challenges of Digital Badges. In Foundation of Digital Badges and Micro-Credentials: Demonstrating and Recognizing Knowledge and Competencies; Ifenthaler, D., Bellin-Mularski, N., Mah, D.K., Eds.; Springer International Publishing: Cham, Switzerland, 2016; pp. 55–70. [https://link.springer.com/chapter/10.1007/978-3-319-15425-1_4]

[5] Casper, S.; Whitley, R. Managing competences in entrepreneurial technology firms: A comparative institutional analysis of Germany, Sweden and the UK. Res. Policy 2004, 33, 89–106. [https://www.sciencedirect.com/science/article/abs/pii/S0048733303001008?via%3Dihub]

[6] Draganidis, F.; Mentzas, G. Competency based management: A review of systems and approaches. Inf. Manag. Comput. Secur. 2006, 14, 51–64. [https://www.emerald.com/insight/content/doi/10.1108/09685220610648373/full/html]

[7] Veluvali, P.; Surisetti, J. Learning Management System for Greater Learner Engagement in Higher Education—A Review. High. Educ. Future 2022, 9, 107–121. [https://journals.sagepub.com/doi/10.1177/23476311211049855]

[8] Abdelrahman, G.; Wang, Q.; Nunes, B. Knowledge Tracing: A Survey. ACM Comput. Surv. 2023, 55, 1–37. [https://dl.acm.org/doi/10.1145/3569576]

[9] Radziwill, N. Blockchain Revolution: How the Technology behind Bitcoin is Changing Money, Business, and the World. Qual. Manag. J. 2018, 25, 64–65. [https://www.tandfonline.com/doi/full/10.1080/10686967.2018.1404373]

[10] Giannopoulou, A.; Wang, F. Self-sovereign identity. Internet Policy Rev. 2021, 10, 1–10. [https://policyreview.info/glossary/self-sovereign-identity]

[11] Cucko, S.; Turkanovic, M. Decentralized and Self-Sovereign Identity: Systematic Mapping Study. IEEE Access 2021, 9, 139009–139027. [https://ieeexplore.ieee.org/document/9558805]

[12] Hammi, B.; Zeadally, S.; Perez, A.J. Non-Fungible Tokens: A Review. IEEE Internet Things Mag. 2023, 6, 46–50. [https://ieeexplore.ieee.org/document/10070402]

[13] Cuel, R.; Virili, F.; Ghiringhelli, C.; Bolici, F. An Emerging Digital Ecosystem: Blockchain Competence Certification Networks. In Proceedings of the Exploring Innovation in a Digital World; Ceci, F., Prencipe, A., Spagnoletti, P., Eds.; Springer International Publishing: Cham, Switzerland, 2021; pp. 50–61. [https://link.springer.com/chapter/10.1007/978-3-030-87842-9_5]

[14] Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. Comput. Sci. Rev. 2018, 30, 80–86. [A survey on essential components of a self-sovereign identity - ScienceDirect]

[15] Sedlmeir, J.; Smethurst, R.; Rieger, A.; Fridgen, G. Digital Identities and Verifiable Credentials. Bus. Inf. Syst. Eng. 2021, 63, 603–613. [https://link.springer.com/article/10.1007/s12599-021-00722-y]

[16] Fiege, U.; Fiat, A.; Shamir, A. Zero Knowledge Proofs of Identity. In Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing (STOC'87), New York, NY, USA, 25–27 May 1987; Association for Computing Machinery: New York, NY, USA, 1987; pp. 210–217. [https://dl.acm.org/doi/10.1145/28395.28419]

[17] Lim, S.; Rhie, M.H.; Hwang, D.; Kim, K.H. A Subject-Centric Credential Management Method based on the Verifiable Credentials. In Proceedings of the 2021 International Conference on Information Networking (ICOIN), Jeju Island, Republic of Korea, 13–16 January 2021; pp. 508–510. [https://ieeexplore.ieee.org/document/9333857]

[18] Crosby, M.; Pattanayak, P.; Verma, S.; Kalyanaraman, V. Blockchain technology: Beyond bitcoin. Appl. Innov. 2016, 2, 71. [https://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf]

[19] Casino, F.; Dasaklis, T.K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telemat. Inform. 2019, 36, 55–81. [https://www.sciencedirect.com/science/article/pii/S0736585318306324?via%3Dihub]

[20] Guidi, B.; Michienzi, A. From NFT 1.0 to NFT 2.0: A Review of the Evolution of Non-Fungible Tokens. Future Internet 2023, 15, 189. [https://www.mdpi.com/1999-5903/15/6/189]

[21] Chen, T.; Lu, H.; Kunpittaya, T.; Luo, A. A Review of zk-SNARKs. arXiv 2022, arXiv:2202.06877. [https://scholar.google.com/scholar_lookup?title=A+Review+of+zk-SNARKs&author=Chen,+T.&author=Lu,+H.&author=Kunpittaya,+T.&author=Luo,+A.&publication_year=2022&journal=arXiv]

[22] Ramachandran, R.; Babu, V.; Murugesan, V.P. The role of blockchain technology in the process of decision-making in human resource management: A review and future research agenda. Bus. Process. Manag. J. 2022, 29, 116–139. [https://www.emerald.com/insight/content/doi/10.1108/BPMJ-07-2022-0351/full/html]

[23] Crypto Carbon Ratings Institute (CCRI): cripto sustainability indices, accessed 21st Februrary 2023 [https://carbon-ratings.com/]

[24] Fachrunnisa, O.; Hussain, F.K. Blockchain-based human resource management practices for mitigating skills and competencies gap in workforce. Int. J. Eng. Bus. Manag. 2020, 12, 1847979020966400. [https://journals.sagepub.com/doi/10.1177/1847979020966400]

[25] Kontzinos, C.; Kokkinakos, P.; Kapsalis, P.; Markaki, O.; Karakolis, V.; Psarras, J. Leveraging blockchain, analytics and decision support to facilitate qualifications' verification, recruitment and competency management: The QualiChain project and initial results. Int. J. Adv. Intell. Syst. 2020, 3, 177–191. [https://nr.brage.unit.no/nr-xmlui/bitstream/handle/11250/2726733/intsys_v13_n34_2020_paged_FINAL_PUBLISHED.pdf]

[26] Choi, M.; Kiran, S.R.; Oh, S.C.; Kwon, O.Y. Blockchain-Based Badge Award with Existence Proof. Appl. Sci. 2019, 9, 2473. [https://www.mdpi.com/2076-3417/9/12/2473]

[27] Downes, S. Recognising Achievement with Badges and Blockchain in a Connectivist MOOC. J. Learn. Dev. 2019, 6, 273–286. [https://doi.org/10.56059/jl4d.v6i3.348]

[28] Serranito, D.; Vasconcelos, A.; Guerreiro, S.; Correia, M. Blockchain Ecosystem for Verifiable Qualifications. In Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Paris, France, 28–30 September 2020; pp. 192–199. [https://ieeexplore.ieee.org/document/9223305]

[29] Mikroyannidis, A.; Third, A.; Chowdhury, N.; Bachler, M.; Domingue, J. Supporting Lifelong Learning with Smart Blockchain Badges. Int. J. Adv. Intell. Syst. 2020, 13, 163–176. [https://oro.open.ac.uk/75146/]

[30] Jeong, W.; Choi, M. Design of Recruitment Management Platform Using Digital Certificate on Blockchain. J. Inf. Process. Syst. 2019, 15, 707–716. [http://xml.jips-k.org/full-text/view?doi=10.3745/JIPS.03.0121]

[31] Mainetti, L.; Paiano, R.; Pedone, M.; Quarta, M.; Dervishi, E. Digital Brick: Enhancing the Student Experience Using Blockchain, Open Badges and Recommendations. Educ. Sci. 2022, 12, 567. [https://www.mdpi.com/2227-7102/12/8/567]

[32] Huynh, T.T.; Tru Huynh, T.; Pham, D.K.; Khoa Ngo, A. Issuing and Verifying Digital Certificates with Blockchain. In Proceedings of the 2018 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 18–20 October 2018; pp. 332–336. [https://ieeexplore.ieee.org/document/8587428]

[33] Balon, B.; Kalinowski, K.; Paprocka, I. Application of Blockchain Technology in Production Scheduling and Management of Human Resources Competencies. Sensors 2022, 22, 2844. [https://www.mdpi.com/1424-8220/22/8/2844]

[34] Bayğın, N. Digital Assurance and Traceability of NFT-Based Certificates. Ileri Teknol. Çalı¸smalar Derg. 2023, 1, 17–25. [https://zenodo.org/records/8074838]

[35] Wu, C.H.; Liu, C.Y. Educational Applications of Non-Fungible Token (NFT). Sustainability 2023, 15, 7. [https://www.mdpi.com/2071-1050/15/1/7]

[36] Loukil, F.; Abed, M.; Boukadi, K. Blockchain adoption in education: A systematic literature review. Educ. Inf. Technol. 2021, 26, 5779–5797. [Blockchain adoption in education: a systematic literature review | Education and Information Technologies (springer.com)]

[37] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system", Bitcoin, vol. 4, 2008 [https://bitcoin.org/bitcoin.pdf]

[38] Christian Stoll, Lena Klaaßen,Ulrich Gallersdorfer "The Carbon Footprint of Bitcoin", July 2019 [The Carbon Footprint of Bitcoin - ScienceDirect]

[39] Küfeoglu, S., Özkuran, M., "Energy Consumption of Bitcoin Mining", May 2019 [Energy Consumption of Bitcoin Mining (cam.ac.uk)]

[40] Harald Vranken: "Sustainability of bitcoin and blockchains" October 2017 [Sustainability of bitcoin and blockchains - ScienceDirect]

[41] Abigael Okikijesu Bada; Amalia Damianou; Constantinos Marios Angelopoulos; Vasilios Katos; July 2021 "Towards a Green Blockchain: A Review of Consensus Mechanisms and their Energy Consumption" [https://ieeexplore.ieee.org/abstract/document/9600014]

[42] Elie Kapengut; Bruce Mizrach; February 2023 "An Event Study of the Ethereum Transition to Proof-of-Stake" [https://www.mdpi.com/2813-2432/2/2/6]

I would like to express my deepest gratitude to my supervisor, Franco Zambonelli, for his essential support, wise guidance and precious advice which have been a beacon in my research journey. Special thanks go to my parents, Giovanni and Lorenza, for their unconditional love, who have been my rock on this journey. Sincere appreciation is also due to Stefano Mariani, whose help and wisdom played a crucial role in my academic development. Furthermore, I would like to thank my colleagues Pomiager and IQC for their collaboration, inspiration and shared moments, which made this academic and personal experience rich and memorable. Thank you very much to all of you for helping to make this trip not only possible, but also unforgettable.

Alberto Francia