BLOCKSTAND

Annex A

BlockStand deliverable 1

"Standardisation scenarios for *Verifiable Credentials in NFTs of Qualified electronic attributes*"

By Giampiero Zito

28.06.2024

Purpose of the document

The purpose of this document is to outline and analyze the implementation and interaction scenario by decentralized identity (also EIDAS compliant) and permissionless blockchain within the skills /job verifiable credentials workflow.
This schema fits also for different types of credentials such as health records, social security benefits, etc.
Technical reports explain also how a) ***ZERO KNOWLEDGE Proof*** mechanism allows preserving privacy of users in information sharing process; and b) **pure proof of stake mechanism** of consensus and *cryptographic alghoritms (quantum resistance)* are high performing for data security

For this reason, we can try to build new work item for standardisation activities:

"Decentralized and qualified attributes of identities in NFTs- soulbound type".

Or integrated technical report into the following standards already or ongoing published:

- ISO/TC 307 - ISO/IEC JTC 1/SC 27 WG: Security, privacy and identity for Blockchain and DLT (WG 4-6-7-8) ;

- IEEE P 3221 (Standard for Technical Requirements of Digital Collection Services Based on Blockchain Technologies);

- ISO/AWI 20435 (Representing Physical Assets using Non-Fungible Tokens).

Actors

Infrastructures decentralized involved in the analysis are the following:

1. Framework managing digital identities in compliant with international frameworks and eIDAS, based on permissioned blockchain
2. Blockchain framework particularly optimised for scalability, security and decentralisation.

**in the first point reference also toward eIDAS 2 means that some actors included in permissioned consortium for decentralized identity in the world are also Identity Trust Providers for EU regulamentation. EUDI WALLET could be considered as centralized wallet but with my contribution I'm trasfer it in permissioned blockchain consortium built by States and/or Delegate Authorities that will be able to release decentralized identity based on new regulamentations.*

Decentralized application.
D-app user - Natural or Legal Person who use our application within one of the intended roles.

Roles

In the blockchain scheme, the following roles are present:
Holder - The person or institution that holds the credentials, typically in a Wallet.
Issuer - The person or entity able to create new credentials and assign them to a Holder.
Verifier - The person or entity able to request verification of a Holder's credentials.

Objectives

The aim of the investigation is to identify the entities involved in the process and Architecture and Reference Framework (ARF) and fix example of specific features of wallets (delegates) and token (**NFTs**).

Scenario

DApp built for job&skills verifiable cresdentials, takes on the role of **Oracle.**
It will manage identification credentials of its users, **natural or legal person**, but it don't verify quality of data. Compliant **eIDAS** leave it to the **ITPs** to do it. After verification ITP register, according to Blockchain **SSI schema,** relying private blockchain, the identity on permissioned wallet so Users can managed their identity with self-sovereign identity schema

and use their decentralized identity to access at Oracle platform. This takes on the role of verifier authorized by Users in only one time process of identity credentials in the platform and allow access it and services only ones with verified identity.
Not only do users access an oracle platform with a real identity, verified and registered on the blockchain, but they are not forced to provide documents to the platform and/or other attributes that are not essential for those managing certain services.
With the ***ZERO KNOWLEDGE PROOF*** **(ZKP) mechanism** they only share the identity verification credential in their wallet, safeguarding their **privacy**. Furthermore, Users avoid having the credentials for authenticating access to the platform and connected services stored in the platform database (and managed by the people who work there), managing them independently according to the SSI scheme. This process prevents the oracle platform from managing sensitive documents and data, and the user from having to register their access credentials and, as often happens, leave them unattended, causing **security problems and data breaches**.

In addition, Oracle platform will rely on public (p**ermissionless) blockchain** to provide all users verified on its platform, wallet on permissionless: the **wallet is type "delegate"** and can receive only assets because the wallet refer to **immaterial assets as, personal resume (skills and job), personal welfare benefits (health care, social security, etc.), personal medical history (visits, surgical operations, etc.) and other case uses.**

Oracle register on permissionless platform the creation of this Events (NFTs) like courses, esams, roles, projects, welfare, health events, etc and creating for each one **NFTs soulbound type and no tradeble-token.**
Users can purchase and/or receive (for donation and/or entitlement) by others Users (VETs, Corporates, Universities, Hospitals, Health Facilities, Doctors) **their unique fractional NFT** corresponding at NFT (divided a priori into n parts) generating by DApp on permissionless blockchain.

Users (holders) after completed course (attendance event), exam (result certification) or medical visits (doctor report), receive other fractional NFTs for each event completed or used in their blockchain wallet that becomes a real one verifiable digital resume (in case of skills&job credentials) or electronic health record (in case of health credentials).
Service providers (Issuers) in the field of training, job market, welfare, healthcare etc can become partners of Oracle platform (DLT based) and receiving by it wallet delegate (issuer type), only if the events are traceable and verified in quality and quantity by Oracle that will be able to active dedicated smart contract (if/then clause) for events up and linked tokens (assets).

Integration scenarios with Decentralized identity and wallet

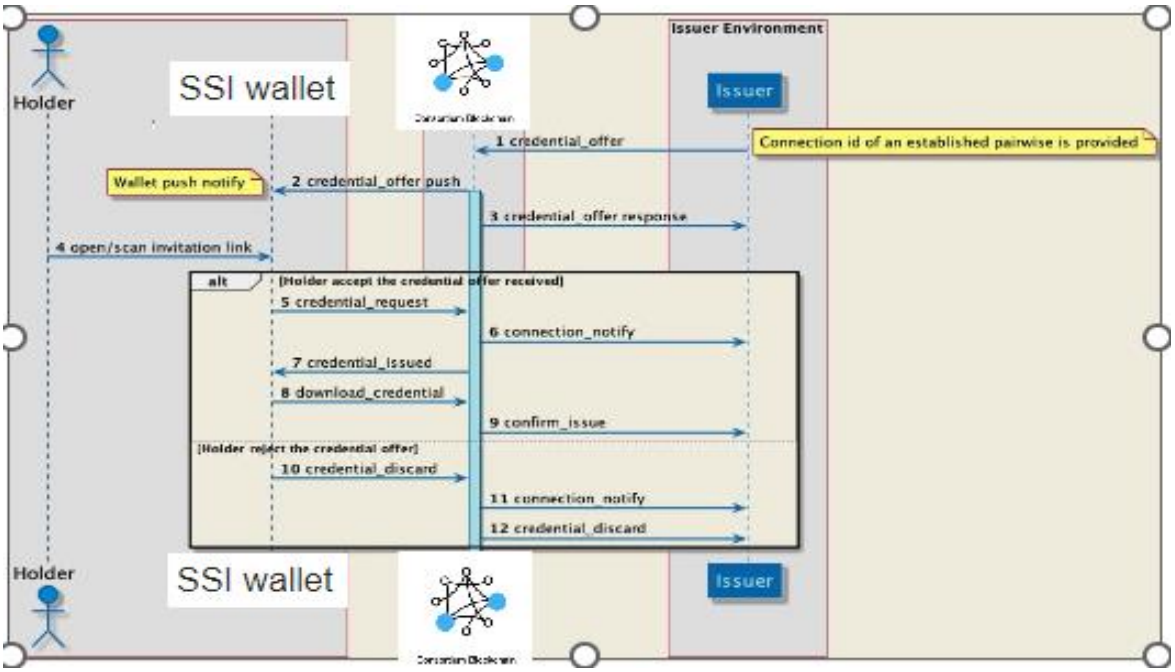
It will then be necessary to create two Proofs with the relative claims/attributes, to be requested to the user intending to register. Oracle platform will set the Proof with REVEALED claims/attributes only for the data needed to correctly identify the user, while all other data unnecessary to the purpose will stay UNREVEALED.

Scenarios for verifying identity credentials of a natural person

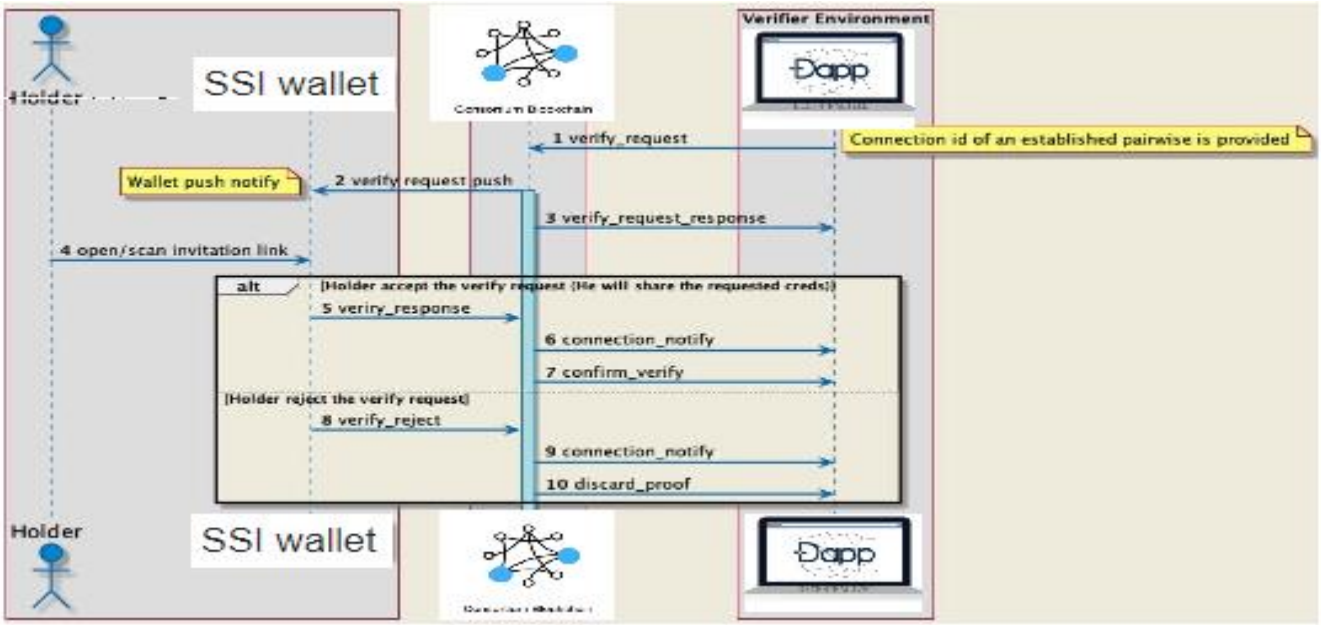
The WorkersBadge system will invite users at the first login to register their credentials on Infocert (Issuer) via a QRCode. The user will then be guided by WorkersBadge, through navigation and tutorials, to the download of Dizme app and of the appropriate QRCode, depending on whether they are a natural or a legal person. Once the Infocert credentials have been completed and verified, WorkersBadge will create its own credentials for the user, through which it will authorise the user to log in to its system via a Proof Request, as outlined above.
Dizme also offers applications registered in its ecosystem with Issuer/Verifier roles, such as WorkersBadge, to request an Invitation to connect to their environment. This Invitation, in turn, can then be sent to the end user via QRCode. At that point, once the user has accepted the Invitation and connected an existing or new Wallet through certified credentials, Dizme will notify WorkersBadge that the connection has been made.

Epic	ID Req fun.	User story	Acceptance Criteria	Blockchain
REGISTRATION NATURAL PERSON	1.1, 1.2	Site registration. Verification of credentials: As a new user I want to be able to register for the Oracle platform so that I can access the portal	The user (not logged in) accesses the main page and the login form. After answering questions, the user must continue through decentralized app of ITP in order to proceed and start the registration and authentication process on DLT (permissioned blockchain)	A request for all data necessary to verify the identity of the natural person (KYC) will be initiated. Upon completion of the predefined checks, a wallet will be created for the applicant and credentials will be issued on the blockchain wallet SSI If the credentials cannot be verified in blockchain, the user will be notified. Without blockchain registration of identity credential it will not be possible to access Oracle Platform (D-App)
LOGIN NATURAL PERSON		Access to the site (Login), Verification of credentials: As a registered user, I want to be able to log in so that I can access the portal.	The user (not logged in) accesses the main page and the login form. He scans the QRCode. To proceed, he continues on the DApp of ITP (Member of permissioned blockchain Consortium) and confirms he wants to send to Oracle (only one time verifier) his ID credentials. The system verifies the credentials and logs him in by redirecting him to the homepage.	Verification of ID and registration of it on the permissioned blockchain Wallet will be required. If it is not possible to verify credentials in blockchain, the user will be notified. Without blockchain ID credential it will not be possible to access Oracle platform and its (or Partners) services.

Credential Request natural person schema



Credential Verifyng natural person schema

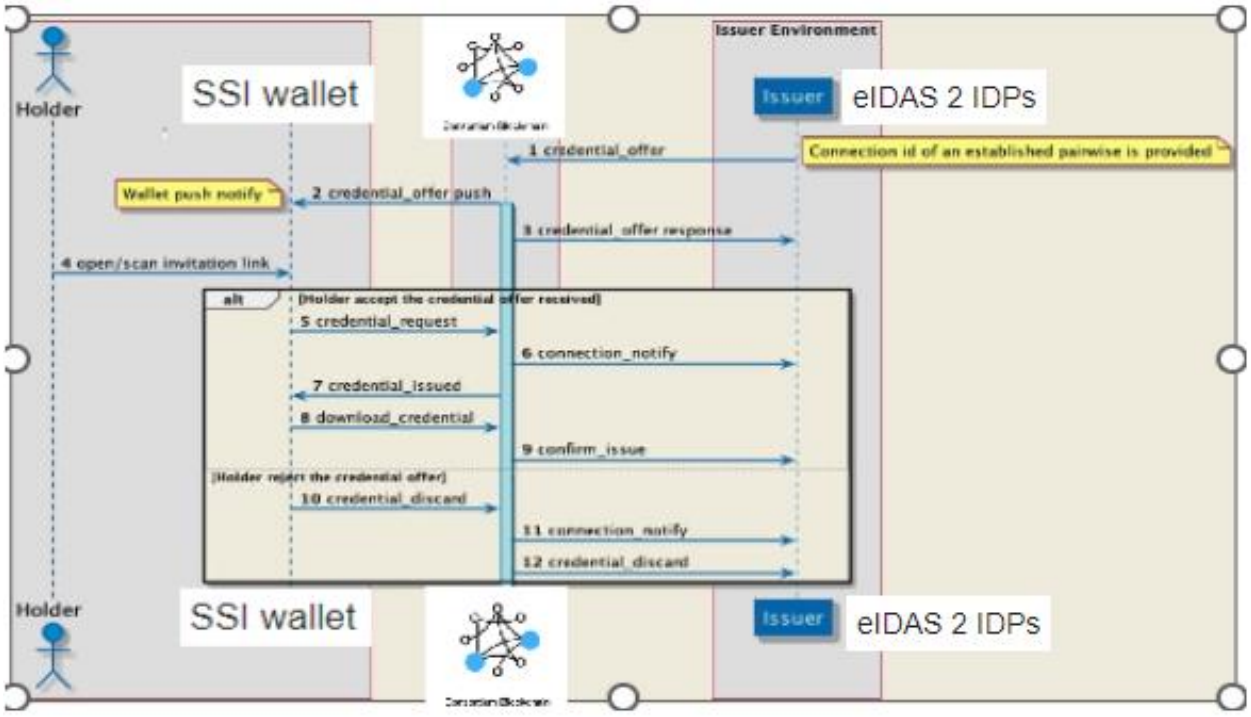


This schema refer to international consortium blockchain in which there is no regulamentation about ID quality credentials as eIDAS for Europe and new EUDI wallet. So it will be useful for standardisation decentralized identity SSI on Blockchain permissioned consortium used by Oracle platform and their decentralized apps for verifiability of identity

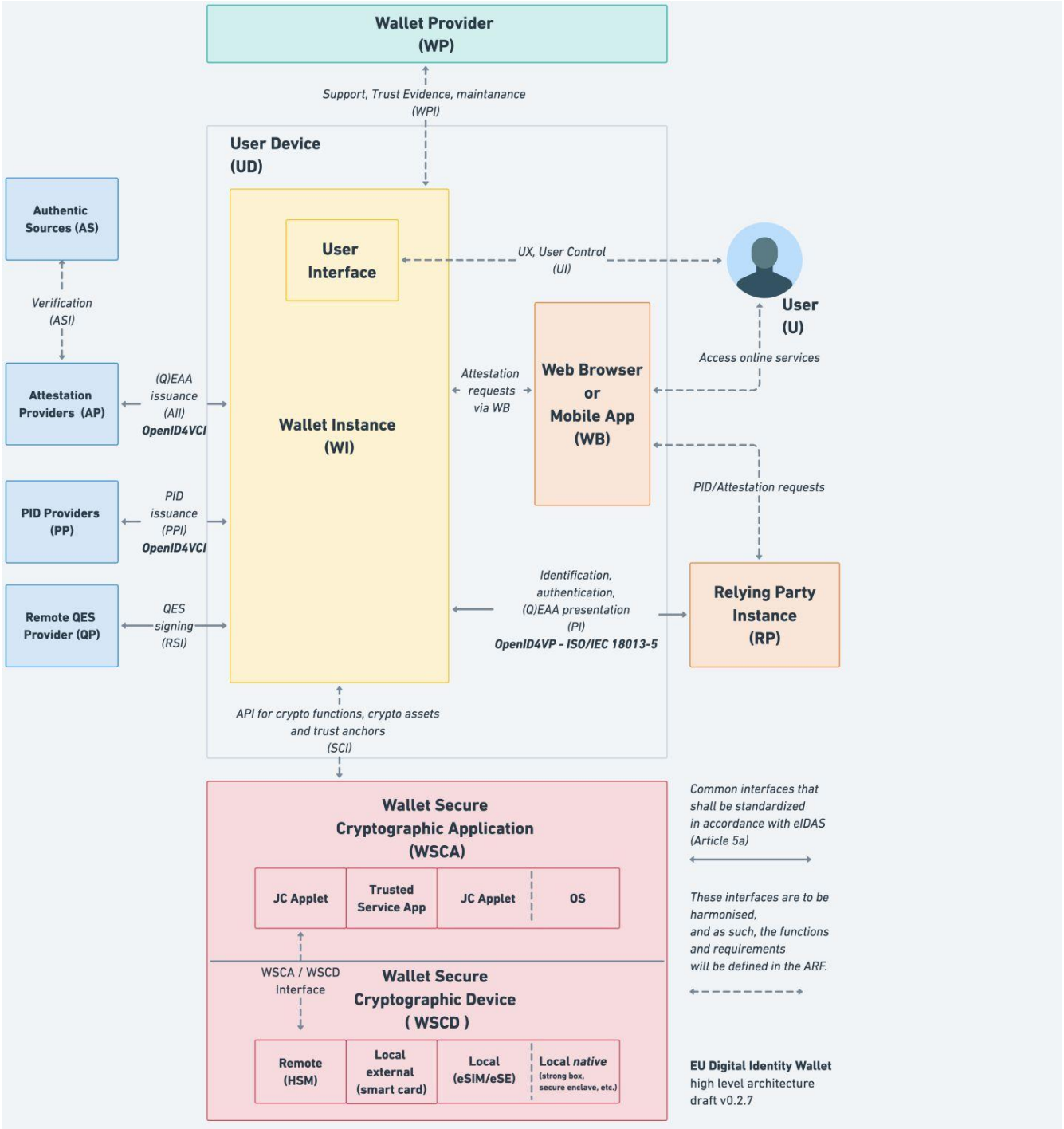
and use dlt credential as verifier for accessing services.

But if we link new ARF EUDI wallet (eIDAS 2) at SSI wallet of Blockchain permissioned Consortium composed by EU States and/or their (figure with flow in following page) delegated Authorites, that registerd ID credentials also in decentralized wallet, it allow to Users deciding if manage centralized or decentralized identity according SSI schema and manage credentials of wallet with sovereign data, greater privacy and data security.

Credential Verifyng natural person schema by IDP (eIDAS 2 compliant)



EIDAS 2 IDP refer to Identity Trust Providers that will use published ARF of EUDI wallet (following image). Result of identification process of this id credential in wallet (ARF compliant) can be transfer also decentralized wallet of permissioned Blockchain Consortium of EU IDPs and favour transition to verifiable credentials on DLT and enablier WEB3.



Scenarios for verifying credentials of a legal person

For the identification process of a legal person or company, the WorkersBadge platform will make use of the Amlet (Issuer) certification body which will collect the information necessary to verify the correct digital identity of a company and/or legal person, then check the accuracy of the information through proprietary processes and finally issue a specific credential on the Dizme wallet of the user who requested it.

Epic	ID Req fun.	User story	Acceptance Criteria	Blockchain
LEGAL PERSON REGISTRATION		Registration as a legal person	The user (logged in) accesses his dashboard and clicks on the 'Register as a Legal Person' button. He fills in the required fields and clicks on the 'Send Request' button to start the registration process.	The Issuer of ID of legal person (entity) will initiate the procedure of identification (KYB) and validation of applicant's informations (Legal Rapresentative, VAT, etc.) and once validated it will issue the new credential directly on the applicant's wallet, on DLT (permissioned blockchain) Consortium. If credentials cannot be verified in the blockchain, the legal user will be notified. Without blockchain ID business credential it will not be possible to access Oracle platform and its (or Partners) services.
LOGIN LEGAL PERSON		Access to the site (Login), Verification of credentials: As a registered user, I want to be able to log in as a legal entity	The user (not logged in) accesses the main page and the login form specifying that he wants to authenticate as a Legal Person.	Verification of business ID (by KYB process) and registration of it on the permissioned blockchain Wallet will be required. If it is not possible to verify credentials in blockchain, the user will be notified. Without blockchain business ID credential it will not be possible to access Oracle platform and its services and become Accredited Partners (delegated issuer)

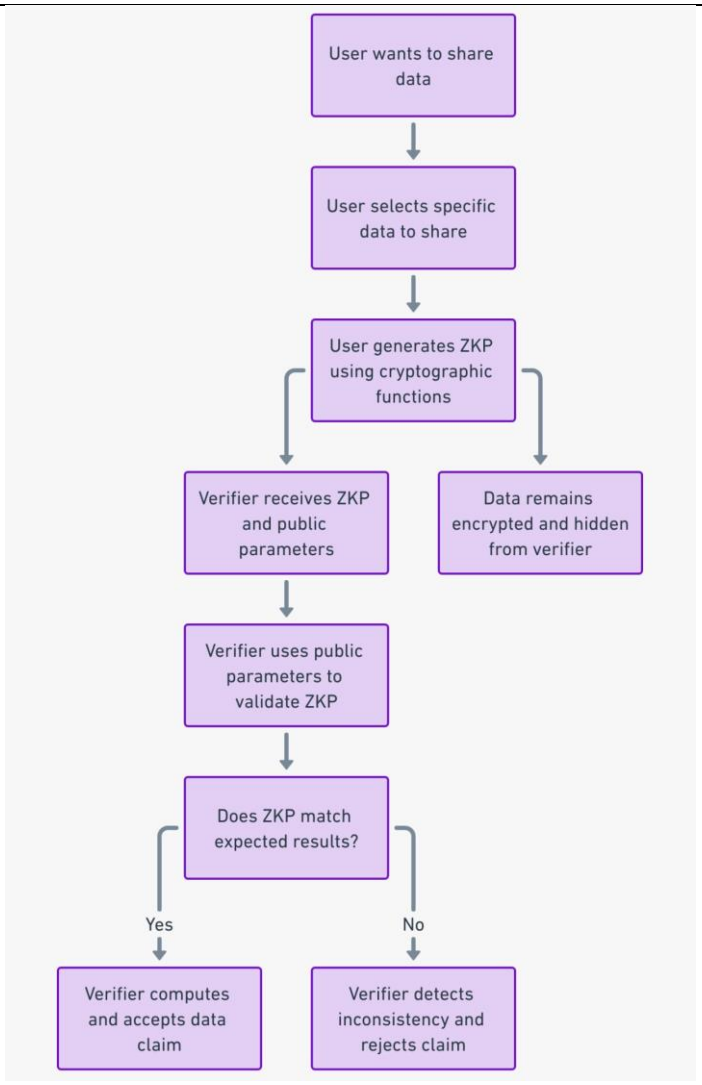
		so that I can access the portal.	He scans the QRCode. To proceed, he continues on the decentralized wallet app and confirms he wants to send Oracle platform (as only one time Verifier) his credentials. The system verifies the credentials and logs him in by redirecting him to the homepage as business users and/or Partner of service	

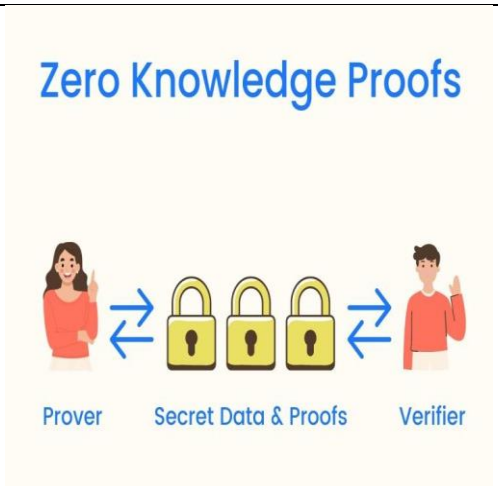
Flow chart is the same (figures upon) of natural person with different IDPs that should be accredited to KYB process by Blockchain permissione consortium and in other use cases (financial services) to AML process.
User after verification of their natural person ask another request to link their ID credential at each one business, demonstrating specific claim as role (Representative or delegated by Representative) and receive proof credentials in decentralised wallet as Legal Entity with decentralised ID in wallet.
Completed ID business process verification and register it as verifiable credential on DLT permissioned wallet, legal User can access to Oracle Platfom and its services and event registered on permissionless DLT.

Architecture based on two different DLT platform (permissioned vs permissionless) for ID credentials and others like

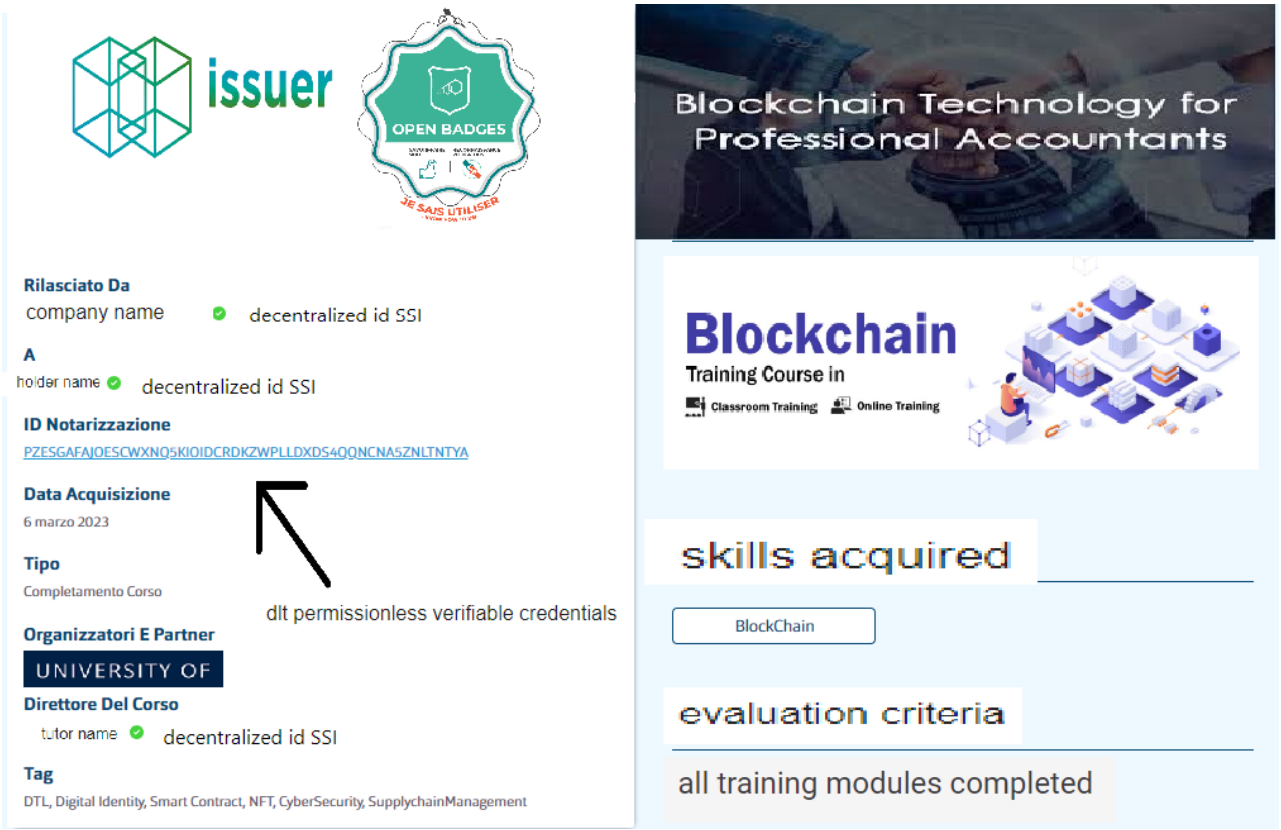
skills, job, welfare and healthcare is due also for preserving:

- **Quality of data about ID and personal assumption that only States (in our case EU) or Delegated Authorities by them can verify if identity of users (natural or legal) is real;**
- **Data and information storage of data are safer on DLT permissionless and with mechanism of consensus (pure proof of stake);**
- **Permissionless DLT platform used by Oracle and Dapps guarantee to Users principle established in the GDPR of the "right to be forgotten", as the data relating to events and/or certificates released in the form of fractional NFTs are connected to a pseudo-anonymized wallet with a cryptographic key which makes the credentials on the DLTs verifiable by all Stakeholders, not connectable to the real identity and claims of a person. Only the Oracle platform using an identity on a further permission platform knew its real identity! This architecture preserve also right of Users to take his data according DATA ACT and Oracle and DApps to keep principle most important for blockchain technology: immutable data.**





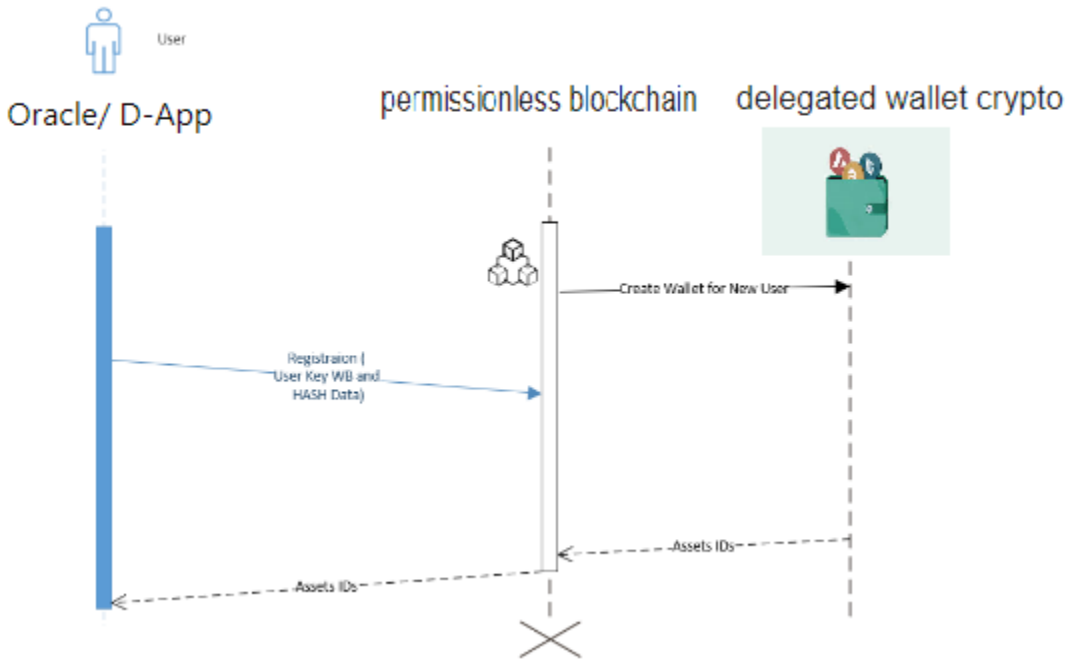
This scheme will be also visible in open badge 3.0 that allows users to demostrate possession of Fractional NFT and to Issuers (Oracle platform and accredited Partners) demonstration of release for (example) accountability process, also ESG criteria based.



In upon open badge 3.0 it's possibile verifier that issuers, holders and tutors exist and their identities was been verified by IDP permissioned blockchain consortium and registered on ID wallet decentralized and managed by users in SSI schema. D-APP only one time verify that users are identity verified by IDP and registered in decentralized wallet, After that link to single NFT (blockchain course for example) and after that user complete all courses module release fractional NFT (representative asset of the domain events and scenarios) about course attendance in decentralized wallet (delegated) that become digital resume DLT based.
ID NOTARIZATION on badge allows all stakeholders to verify on permissionless DLT timestamping of credentials for the person/user who share it without share claims about his identity and/or other skills credentials of his resume.

The Algorand Wallet will be created as the WorkersBadge platform is launched and user wallets will be created upon successful registration within the system. Wallets will be created automatically through the use of REST APIs provided by the Algorand ecosystem. The wallet's private key will be held only by the WorkersBadge platform, which will act as the sole entry point for incoming and outgoing transactions on that wallet. Activation and successful connection to a user's Wallet will be a condition required to enable the user to use WorkersBadge services and consequently to enter

transactions into their Wallet in the manner envisaged in the indicated scenarios.
User Wallet creation scenario on permissionless Blockchain after verification of identity by IDPs and Oracle for access to D-App and services



Notarisation scenarios on Permissionless Blockchain

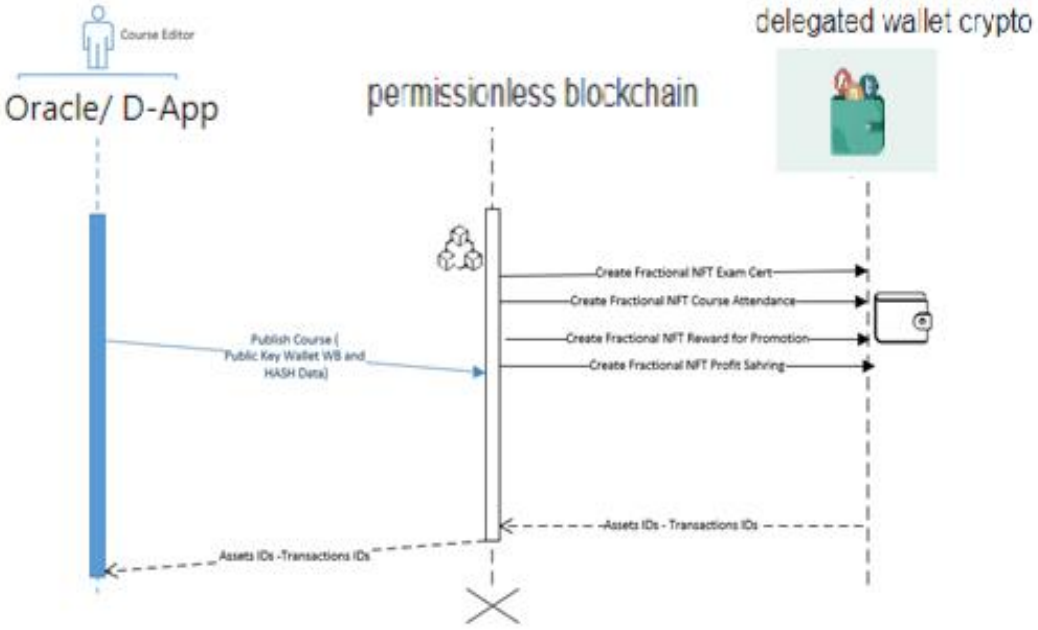
Insertion into and interaction with blockchain ecosystems will take place in the following use cases.
The goal is to certify on distributed ledgers data related to:

1. ***Participation in a training course;***
2. ***Evaluation of acquired competences through testing.***

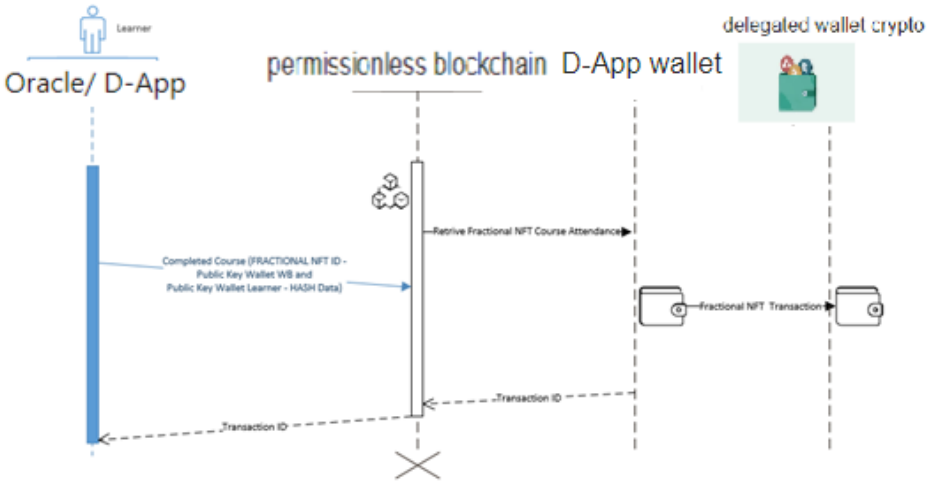
Fractional NFTs will be issued to the user's (learner/worker) wallet at the end of the above events.

Before it need that Oracle/DApp create assets link to spcific course and exam on blockchain. It create nr.2 NFTs for specific course published on his marketplace: one for course attendance and another one for certification by exam. Other NFTs could be create for trace selling of courses and rewards Tutors and/or trace promotion by Users for reward them.

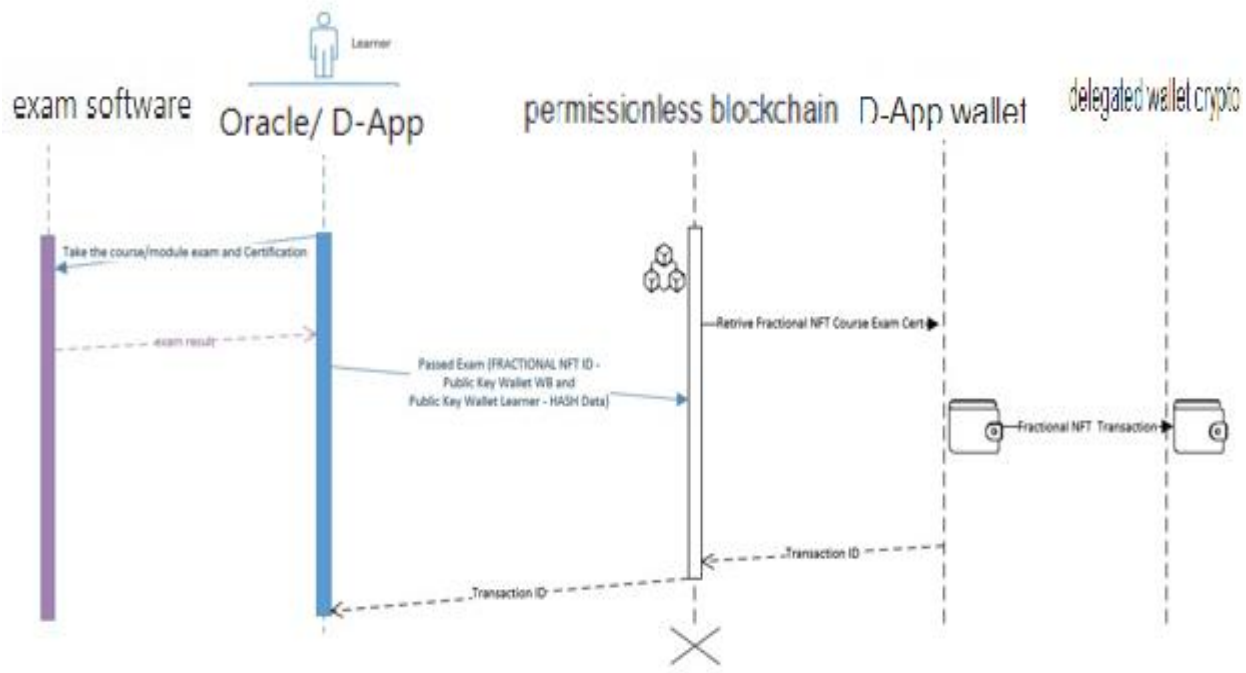
Published course and exam assets on Blockchain



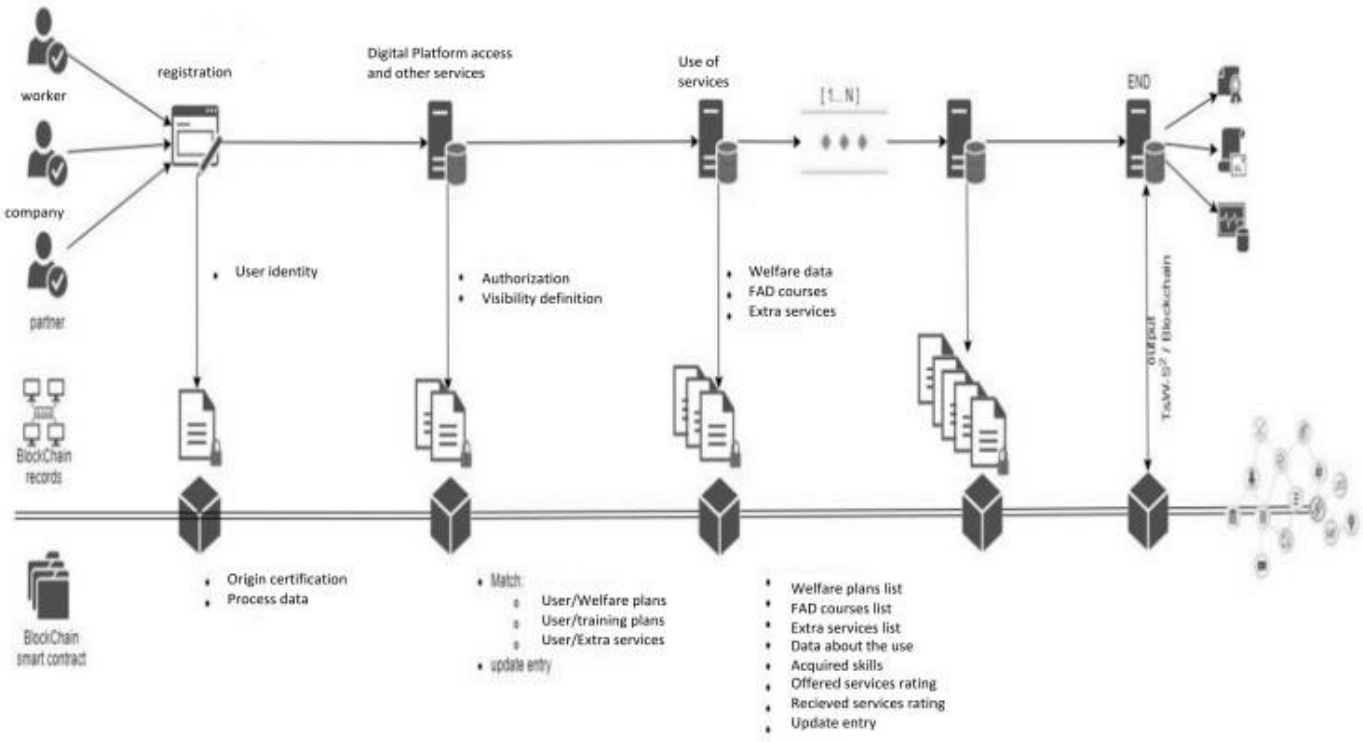
Attendance Course asset on Blockchain



Exam Cert asset on Blockchain

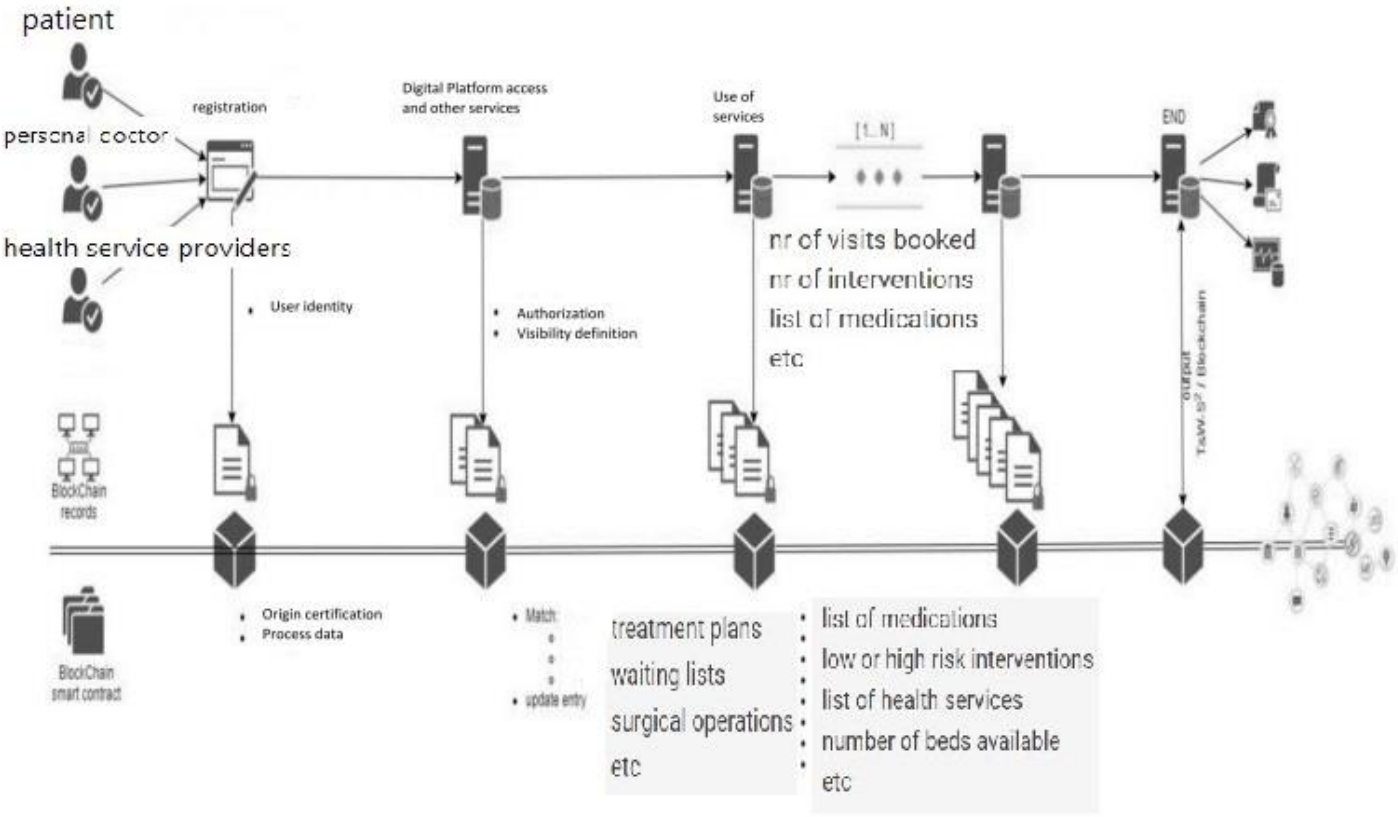


Following there is image of highlevel schema of blockchain transactions and NFTs asset for verifiable credentials on skills, job, expertices roles and welfare:



Same decentralized schema could be transferred to healthcare system in which fractional NFTs (soulbound) represent single records such as medical visit, surgical operations and main wallet of user composed by set of Fractional NFTs instead represent electronic patient health record.

Creation and transferability of assets are the same upon illustrated and actor (different for tipology and services) can be involved in healthcare process based on DLT in the same way.



28.06.2024