Blockchain as an enabler Technology of Self-Sovereign Identities & Verifiable Credential

Dr. Adnan IMERI
Research &Technology Associate
04.05.2023

ABSTRACT

Blockchain enables technological transformation by enhancing digitalization aspects from a software connector (enabler) standpoint.

It demonstrates the ability to replace conventional aspects of activities, such as authentication mechanisms, via decentralized digital identities.

Decentralized digital identities are currently seen to be advantageous for persons, applications, devices, and society to cope with the digital era.

Decentralized digital identities and verifiable credentials are replacing trusted third parties and paper-based authentications in identifying persons (humans), documents (e.g., diplomas), and devices in swarm computing, leveraging the trust and reliability of the digital world.

PRESENTATION OUTLINE

- Context
- Identity, Digital Identity, Current Approaches for Managing Digital Identity
- Self-Sovereign Identity - SSI
- Digital Wallets
- Distributed Ledger Technologies and Blockchain as Enabler of Self Sovereign Identity
- Trust Model: Blockchain and Web3 Paradigm
- SSI pattern for information sharing
- Diploma use case
- SSI and associated challenges

CONTEXT

- **Decentralized Digital Identity**
  - An initiative to provide **subjects** with enhanced **control**, **privacy**, and **portability** of their **digital identities**.

CONTROL

PRIVACY

PORTABILITY

IDENTITY

- Everything that characterizes a person, organization, process or thing is known as identity [3]. According to ISO (ISO/IEC 24760-1) “Identity is a set of attributes related to an entity”.
  - Person identity attributes: biometric information, titles, property, and any attribute linked to a person.
  - Collection of these attributes enables identification of persons differently and allows them to proof uniquely their identity.
    - → Authentication

Passport

- Authentication
  - Process of convincing (“verifying”) someone or something (“device”) that it’s really “you” based on some “documents” issued by third parties (“authorities”), e.g., a Passport [3]

DIGITAL IDENTITY

- The **digital identity is:**
  - Sum of all digitally available data
  - Unique representation of a subject

    that allows a person, thing, process, or animal to be identified uniquely and authenticated by others electronically (NIST, OIX, EU-BDID, 2019).
- Benefits
  - unique identification
  - authenticate by other digital services
  - allows access to remote digital services

CURRENT APPROACH OF DIGITAL IDENTITY MANAGEMENT

Identity Management Approach

1 Centralized Identity

- Client-Server approach. Identities stored in a database.

2 Federated Identity

- Agreement (based on eIDAS) between several identity providers enable multiple authentications, e.g., government services, banking, hospitals…

3 User-Centric Identity

- Third-Party Identity Provider
- Using a third party for authentication e.g., “log in with Gmail”…
- OAuth, OpenID, OpenID Connect 2.0, SAML,…

4 Self-Sovereign Identity (SSI)

- User administrate information about their identity, user autonomy
- In SSI user has much more control over data compared to other (third parties)
- The user decides with whom they share information

Issues

Regulation and Standards

- Lack of standards and rules to support the evolution of digital identity
- Most advanced ones: eIDAS, GDPR,…

Technology

X.509 Certificates

Stored in a specific location, makes portability an issues

Security

- Users have no control over their digital identities
- Users do not own information stored in the “internet” (third-party databases)
- Memorize or store multiple usernames/passwords
- No guarantee of **data protection**, right to be forgotten, pseudo anonymization, **portability, accessibility, …**
- Expose to vulnerability, hacks, theft, misuse,…

SELF-SOVEREIGN IDENTITY (SSI)

SSI is an identity related approach which enables user control of digital identity. User has full autonomy is the ruler over his digital identity [2].

To accomplish SSI must be portable, therefore avoiding to be locked down in specific site/device [2].

Main Principles of SSI [6].

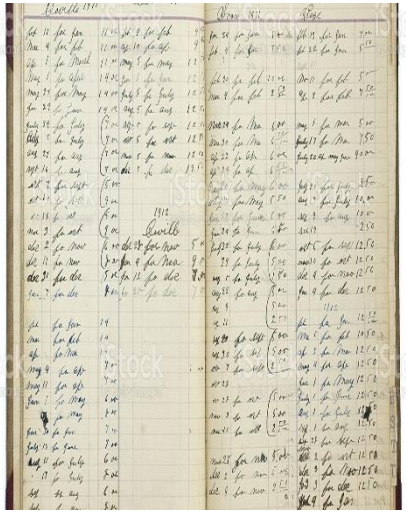
Security	Protection
	Persistence
	Minimisation
Controllability	Existence
	Control
	Consent
Portability	Interoperability
	Transparency
	Access

DLT AND BLOCKCHAIN AS ENABLER OF SELF SOVEREIGN IDENTITY

- **Decentralized Digital Identity**
  - An initiative to provide subjects with enhanced **control**, **privacy**, and **portability** of their digital identities.

- **Blockchain and the Web3 Paradigm**
  - A new paradigm where user **controls** their data and **decide who to share it with** and **when**, contrary to Web2 paradigm.
  - Wab3 enables users' control over their data.

DISTRIBUTED LEDGER TECHNOLOGIES & BLOCKCHAIN



Ledgers

"Distributed ledger technology (DLT) presents a distributed and decentralized database, shared among multiples parties, known as network participants"

"Ledgers have existed since ancient times and have served as record-keeping of transactions" [1]

- a pen and paper ledger
- a large database maintained by a central authority e.g., Banks

Blockchain

BC technology is an instance of the distributed ledger

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

BENEFITS OF USING BLOCKCHAIN TECHNOLOGY

Blockchain (BC) is a distributed decentralized database that allows storing immutable cryptographically signed transaction data.

Transaction data are gathered into blocks and chained together with the previous block, thus forming a blockchain.

- Trust and Transparency
- Data Security
- Data Immutability & Non-Repudiation properties
- Auditability/Timestamped
- Smart Contracts (SC)

BLOCKCHAIN AND WEB 3 PARADIGM AS ENABLERS OF SSI

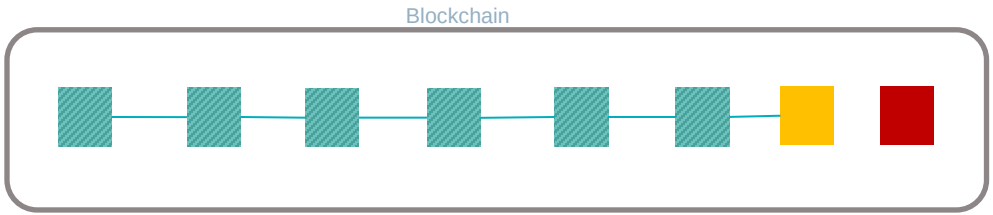
- **Web3 is composed of concepts and combination of technologies:**
  - Decentralization
    - distributed ledgers/ blockchains for registration of claims/identifiers
  - Transparency
    - Smart Contract
      - Replace “Authority” for proofing identity via decentralized algorithm
  - Cryptographic Tools
    - Enabling principles of self-sovereignty identity, e.g., sharing public key
  - Interoperability

    APIs, Business-driven policies.

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

TRUST MODEL: BLOCKCHAIN AND WEB3 PARADIGM

- **Trust Model** based on proofs, i.e., verifiable information



DID

Public Key

Private Key

Verifiable Credentials

Digital Wallets

DECENTRALIZED IDENTIFIERS AND VERIFIABLE CREDENTIALS – SSI APPROACH

- Decentralized Identifiers (DIDs)
  - A new way for individuals to generate unique identifiers that allows interacting with the digital world.
- Verifiable Credentials (VC)
  - Are digital credentials containing attributes (person name, birthdate, address, …).
  - Self-Issued or Third-Party (government)

- World Wide Web Consortium (W3C)

Decentralized Identifiers (DIDs) v1.0

Core architecture, data model, and representations

W3C Recommendation 19 July 2022

▼ More details about this document

This version:
https://www.w3.org/TR/2022/REC-did-core-20220719/

Latest published version:
https://www.w3.org/TR/did-core/

Verifiable Credentials Data Model v1.1

W3C Recommendation 03 March 2022

▼ More details about this document

This version:
https://www.w3.org/TR/2022/REC-vc-data-model-20220303/

Latest published version:
https://www.w3.org/TR/vc-data-model/

DIGITAL WALLETS

- Software (Mobile and/or Web Application) that is used to manage digital credentials:

CREATION OF THE USER PROFILES

STORING VERIFIABLE CREDENTIALS

SIGNING VERIFIABLE PRESENTATION

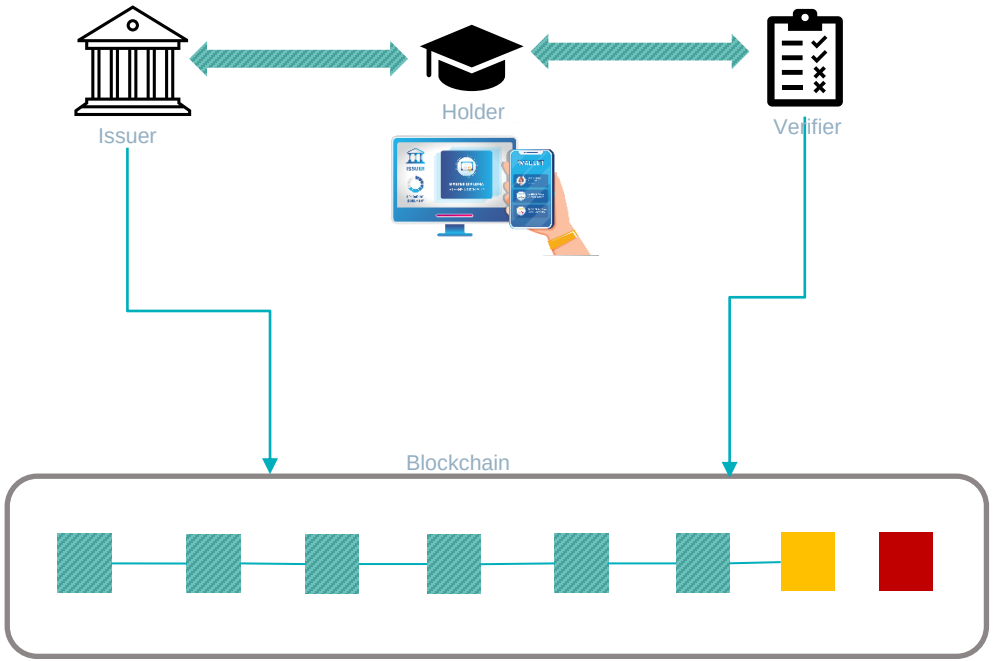
Image source: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

SSI PATTERN FOR INFORMATION SHARING SCENARIO

ISSUER e.g., University- the one who **issues verifiable credentials (VC)** (information) upon request of holders.

HODERS e.g., Student – users/things **that holds a verifiable credential (VC)** (information).

VERIFIER e.g., Private Firm or cross-border University or even a device which **verifies the issued verifiable credentials** (information).



LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

DECENTRALIZED IDENTIFIES (DID) AND VERIFIABLE CREDENTIALS (VC)

- DID refer to any **subject**, e.g., person, document, data, organization, thing, abstract entity, etc., as determined by the controller of DID.
- DID is just a string. It **does not show any meaningful information about the natural or juridical person**. DIDs are pseudonyms. Every person might have several DIDs

`did:ebsi:zk4bhCepWSYp9RhZkRPiwUL`

DID method-specific identifier

RANDOM UNIQUE IDENTIFIER

DECENTRALIZED IDENTIFIES (DID) AND VERIFIABLE CREDENTIALS (VC)

- DID are used in machine-verifiable documents, known as **Verifiable Credentials (VC)**.
  - Used to **ensure authenticity** of ISSUERS and HOLDERS
- VC feature is a **set of claims** by an **ISSUER** about a person (subject) that can be cryptographically verified.
- For example, a diploma is a set of verifiable claims by a University (ISSUER) for a natural person (HOLDER)

→ DIDs are embedded into VC

Example of an EBSI Verifiable Credential


```
{
 "@context": [
  "https://www.w3.org/2018/credentials/v1",
  "https://essif.europa.eu/schemas/vc/2020/v1"
 ],
 "id": "https://essif.europa.eu/tsr/53",
 "type": [
  "VerifiableCredential",
  "VerifiableAttestation",
  "VerifiableAccreditation",
  "DiplomaVerifiableAccreditation"
 ],
 "issuer": "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1",
 "issuanceDate": "2020-06-22T14:11:44Z",
 "credentialSubject": {
  "id": "did:ebsi:zk4bhCepWSYp9RhZkRPiwUL",

 (....)
```


DID of Issuer

DID of Holder

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

INTERACTION WITH VC

Presentation of VC (to HOLDER)

- Credentials Metadata (expiration data, issuance data, other info)
- Claims
- Proof of Signature of ISSUER

Presentation of VC (to be verified)

- DID of HOLDER
- Credential Metadata
- Claims

Stored/Shared via Wallet

- Signature of ISSUER (proof)
- Signature of HOLDER (proof)
- Additional checks on ISSUER

Stored/Shared via Ledger

Example of EBSI DID document


```
{
 "@context": "https://w3id.org/did/v1",
 "id": "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1",
 "verificationMethod": [
  {
   "id": "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1#keys-1",
   "type": "EcdsaSecp256k1VerificationKey2019",
   "controller": "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1",
   "publicKeyJwk": {
    "kty": "EC",
    "crv": "secp256k1",
    "x": "n03trG-1sWidluyYQ2gcKrgYE94rMkLIArZCHjv2GpI",
    "y": "6__x_vqe0nBGYf7azbQ1_VvvuCafG5MhhUPNvYp-Mak"
   }
  }
 ],
 "authentication": [
  "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1#keys-1"
 ],
 "assertionMethod": [
  "did:ebsi:zsSgDXeYPhZ3AuKhTFneDf1#keys-1"
 ]
}
```


Public key

Reference to Public key

Reference to Public key

Cryptographic Keys are associated with DID Document

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

ENABLER OF SELF-SOVEREIGN IDENTITY: BLOCKCHAIN AS DID AND VC REGISTER

- Uniqueness of DIDs
- Non-Repudiation and immutability of the DIDs
- Only the controlling key can manage the DID
- The same controlling key is not registering two different DIDs

SUMMARY OF DECENTRALIZED TRUST MODEL

- Decentralized Identifiers (DID) mainly based on W3C.
- Blockchain as DID Registry (Trusted Registries).
- Using blockchain immutability.
- Information to support the verification of credentials (VC).
- Requires the role of Trusted Accreditation Authority to verify and register trusted ISSUES.

BLOCKCHAIN FRAMEWORK FOR THE SSI APPROACH

- There exist many blockchain frameworks/research project supporting digital identity.
  - EBSI; ID Union; Hyperledger Indy; SSI IOTA; Consensys, …
- We refer to the one built to improve public services at the European Level.
  - European Blockchain Service Infrastructure [5]
- Use Cases:
  - Notarisation
  - Diplomas
  - European Digital Identity
  - Trusted Data Sharing
  - Traceability

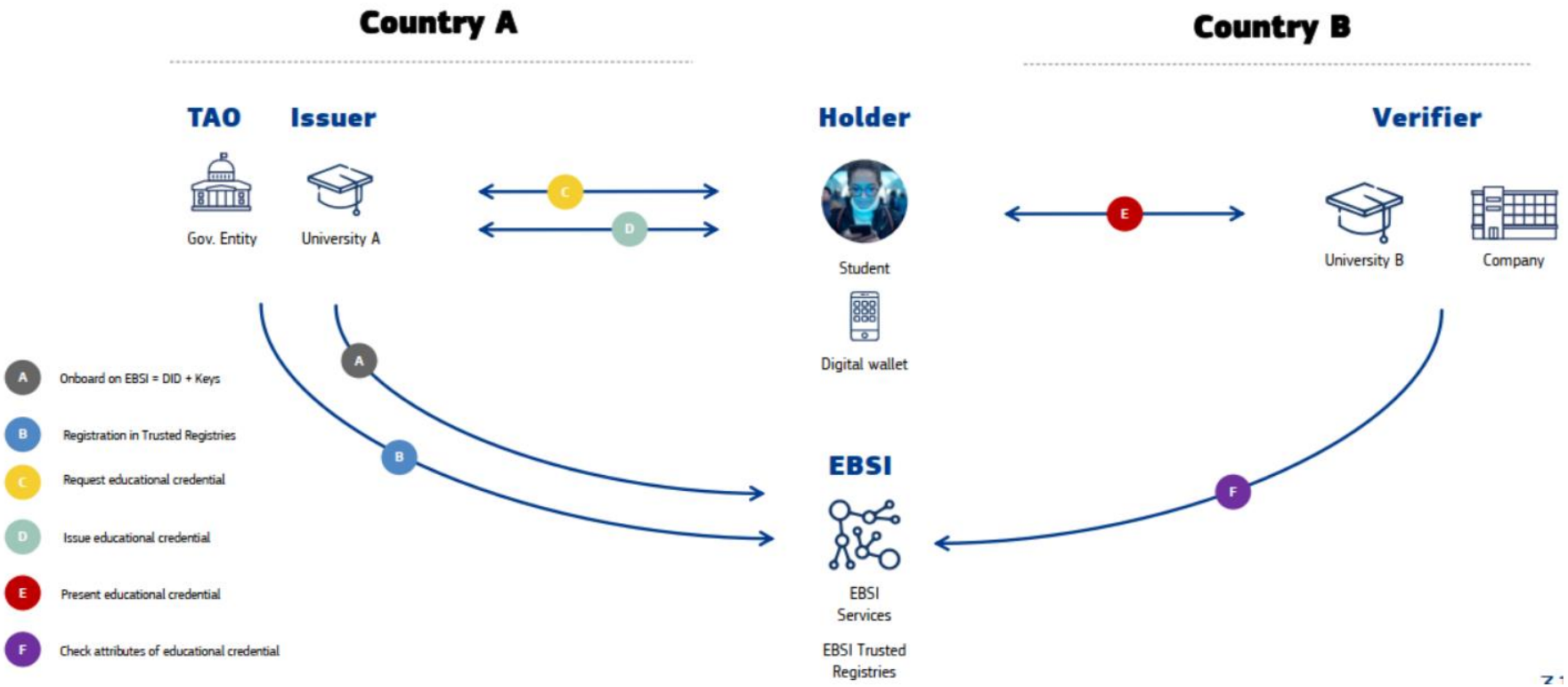
ebsi
European Blockchain

Image source: https://ec.europa.eu/digital-building-blocks/wikis/display/EBSI/Home

DIPLOMA USE CASE

- Long process of issuing the diploma
- Fraud/Fake Diplomas
- Unstructured documents and long verification time
- Inefficient verification process

DIPLOMA USE CASE



Source [8]

SSI AND ASSOCIATED CHALLENGES

- Trust over the ISSUERS
  - Challenging process of certifying ISSUERS
- Trust over the presenter of VC.
  - Is the person who is presenting VC the real one of “private key” has been compromised.
- Regulatory Framework ambiguity on using DLT and Smart Contract

SUMMARY

- The combination of DID-VC with blockchain technology is a game changer in **Digital Identity Management**
- **Decentralized Digital Identity**
  - An initiative to provide subjects with enhanced control, privacy, and portability of their digital identities
  - **Improvements towards different domains, e.g., Education**
    - Trust and Transparency
    - Administrative Process
    - Efficiency in cross-border

THANK YOU FOR YOUR ATTENTION

Adnan Imeri, PhD

R&T Associate | Technical Lead at Infrachain | Innovation Manager | Software Engineer-Architect | Blockchain Expert

Luxembourg · Contact info

LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY LIST

REFERENCES

[1] W3C DID: https://www.w3.org/TR/did-core/

[2] C. Allen. (2016) The path to self-sovereign identity. http://www.lifewithalacrity.com/2016/04/the- path- to- self- soverereign-identity.htm

[3] Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain. (2022). Retrieved 26 October 2022, from https://publications.iadb.org/en/self-sovereign-identity-future-identity-self-sovereignity-digital-wallets-and-blockchain

[4] SO/IEC 24760-1:2019 IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts https://www.iso.org/standard/77582.html

[5] https://digital-strategy.ec.europa.eu/en/policies/european-blockchain-services-infrastructure

[6] Proof of Work: https://www.ledger.com/academy/blockchain/what-is-proof-of-work/

[7] A. Tobin and D. Reed, “The inevitable rise of self-sovereign identity,” The Sovrin Foundation, 2016.

[8] Tan, Evrim, et al. "Verification of Education Credentials on European Blockchain Services Infrastructure (EBSI): Action Research in a Cross-Border Use Case between Belgium and Italy." Big Data and Cognitive Computing 7.2 (2023): 79.