MADITRACE

Guidelines for Methodology implementation

Deliverable D3.3

Version N°1.0

Authors: Rouwaida ABDALLAH (CEA) , Doruk SAHINEL (Spherity)

Disclaimer

The content of this report reflects only the author's view. The European Commission is not responsible for any use that may be made of the information it contains.

Funded by
the European Union

Document information

Grant Agreement	101091502
Project Title	Material and digital traceability for the certification of critical raw materials
Project Acronym	MaDiTraCe
Project Coordinator	Daniel Monfort, BRGM
Project Duration	1 January 2023 – 30 June 2026 (42 months)
Related Work Package	WP3
Related Task(s)	T3.3: Guidelines for methodology implementation
Lead Organisation	CEA
Contributing Partner(s)	BRGM, Spherity
Authors	Rouwaida ABDALLAH and Doruk SAHINEL
Due Date	M30
Submission Date	07/07/2025
Dissemination level	PU

History

Date	Version	Submitted by	Reviewed by	Comments
20/01/25	0.1	Rouwaida A.		First draft , skeleton
20/04/25	0.2	Doruk S.		DPP inputs
23/05/25	0.3	Rouwaida A.		BC input
15/06/25	0.5	Rouwaida A.		Full Draft
27/06/25	0.9	Doruk S.		First Review
04/07/25	1.0	Rouwaida A.	Daniel M., LGI	Final Review

Funded by
the European Union

Table of contents

Funded by
the European Union

List of figures

Summary

This deliverable provides practical guidelines for implementing a Digital Product Passport (DPP) to ensure traceability, transparency, and certification of critical raw materials (CRM) throughout their lifecycle. It presents a step-by-step methodology for generating, managing, and maintaining DPPs, including technical components such as decentralized identifiers (DIDs), verifiable credentials, and QR code integration. The architecture proposed within this project will be detailed in Deliverable 3.6.

The document also introduces a blockchain-based notarization module to guarantee the integrity and auditability of data using cryptographic hashing and Merkle trees.

The guidelines are grounded in the architectural model defined in D3.2, and will be further expanded in upcoming deliverables such as D3.7, which will offer deployment feedback and refined recommendations on blockchain selection.

Keywords

Digital Product Passport, material Fingerprint, blockchain, traceability

Abbreviations and acronyms

API	Application Programming Interface
CRM	Critical Raw Material
DID	Decentralized Identity
DLT	Distributed Ledger Technology
EBSI	European Blockchain Service Infrastructure
GDPR	General Data Protection Regulation
QR	Quick Response
SSI	Self-Sovereign Identity
VC	Verifiable Credentials
W3C	World Wide Web Consortium

Funded by the European Union

1 Introduction

The growing demand for transparency and sustainability in the critical raw materials (CRM) sector has led to the emergence of digital solutions capable of ensuring reliable and verifiable traceability across the supply chain. Among these, the Digital Product Passport (DPP) stands out as a key enabler, offering a structured approach to track the origin, transformation, and environmental impact of raw materials throughout their lifecycle.

This deliverable (D3.3) provides a set of methodological guidelines and technical steps for the implementation of the DPP, aligned with European regulations and interoperability standards (like ESPP, W3C DID, ..). It integrates digital identity principles, blockchain-based notarization, and secure data exchange mechanisms to support certification, verification, and compliance efforts. The approach is grounded in the reference architecture defined in the deliverable D3.4 and illustrated through smart contract-based prototype (deliverable D3.5) and traceability workflows.

2 Implementation Steps

To ensure reliable, transparent, and verifiable traceability of critical raw materials, the implementation of the reference architecture requires a combination of structured data management and secure integrity mechanisms. This section outlines two key pillars of the methodology: first, the creation and deployment of Digital Product Passports (DPPs) that serve as digital containers of lifecycle data for raw materials (Section 2.1); and second, the use of blockchain-based notarization to guarantee the immutability and verifiability of selected datasets and certification events (Section 2.2). Together, these components establish a robust foundation for data traceability, integrity, and stakeholder trust across the supply chain. The architecture proposed within this project will be detailed in Deliverable 3.6.

2.1 DPP

While the DPP is formally defined under EU regulations (e.g. ESPR and Battery Regulation) as a publicly accessible data record that satisfies regulatory requirements for a final product, its concept is increasingly extended upstream in supply chains. In the case of critical raw materials, traceability and compliance require documentation at earlier stages, and the notion of a Digital Raw Material Passport has emerged to address this issue.

Digital Raw Material Passports aim to document the origin, extraction, processing, and transportation of raw materials, providing a clear and traceable path from the source to the final product. This level of traceability is essential for ensuring that raw materials are sourced responsibly and sustainably, respecting national and international regulations, and it supports various compliance and certification requirements. The implementation of the Raw Material Digital Product Passport involves several key implementation steps, which are outlined in the following subsection. In addition, for the technical deployment, a postman-based step-by-step DPP generation workflow is presented in the second sub-section.

2.1.1 Digital Product Passport Implementation Steps

2.1.1.1 Establish Stakeholder Collaboration with Trusted Data Exchange Mechanisms

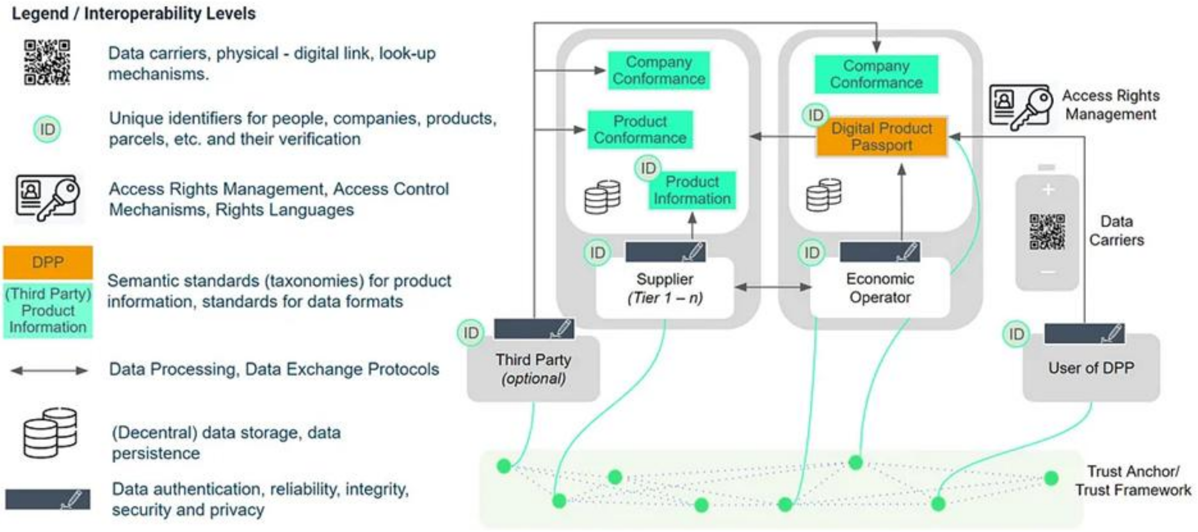

Legend / Interoperability Levels
Data carriers, physical - digital link, look-up mechanisms.
ID
Unique identifiers for people, companies, products, parcels, etc. and their verification
Access Rights Management, Access Control Mechanisms, Rights Languages
DPP
(Third Party) Product Information
Semantic standards (taxonomies) for product information, standards for data formats
Data Processing, Data Exchange Protocols
(Decentral) data storage, data persistence
Data authentication, reliability, integrity, security and privacy
Company Conformance
Product Conformance
Product Information
Supplier (Tier 1 – n)
Company Conformance
Digital Product Passport
Economic Operator
Third Party (optional)
Access Rights Management
Data Carriers
User of DPP
Trust Anchor/ Trust Framework

Figure 1 - Architectural overview and areas of standardization for the DPP [1]

Article 14 (1) of the Batteries Regulation [2] states that: "The digital product passport shall be created by the economic operator that places the battery or battery component on the market." As can be seen from the regulation, the DPP requirement comes from the ESPR for batteries; however, it is expected that the same principle applies to other products under the broader scope of the ESPR framework such as raw materials, where the economic operator responsible for placing the product on the EU market is tasked with creating the

DPP. Alternatively, a DPP service provider can take over this task on behalf of the economic operator.

The economic operator must bring the required information from all the stakeholders in the supply chain into the DPP. Thus, it is essential to identify all economic operators involved at various points within the raw material supply chain, including miners, processors, transporters, and recyclers. This implies that the economic operator is responsible for creating a data exchange mechanism among trusted partners, with clear definition of roles and responsibilities for the provision, verification, and updating of data. Furthermore, tailored data sharing agreements should be developed and formalized among stakeholders. The technical components required to establish this communication such as organizational identity wallet, enterprise credentials, etc. are provided in Maditrace Deliverable 3.4: Architecture definitions for POC implementation – Intermediate Report [3].

2.1.1.2 Assign a Unique Identifier to DPP

Each raw material batch or lot defined as a product should be assigned a Decentralized Identifier (DID) to serve as a unique digital identity. A DID is a globally unique identifier, which is resolvable with high availability and cryptographically verifiable [4].

W3C DID specification [5] details the framework for decentralized identifiers, including the architecture, data model, and representation of DIDs, and highlights their role in enabling individuals and organizations to create identifiers. DID issuance must follow these specification standards to ensure operability, and the content should be adapted to the context of the supply chain, for instance, allowing miners to issue initial identifiers and processors to append transformation credentials. When creating a DID, an organizational identity wallet that implements the standards around decentralized identifiers is used to follow this specification. This wallet is a secure software application that manages DIDs, cryptographic keys, and verifiable credentials, enabling the organization to create, store, and control its decentralized digital identity.

In the European context, the W3C DID standard has been adopted and operationalized through several EU initiatives, including the European Blockchain Services Infrastructure (EBSI)[1]. EBSI operates under the European Blockchain Services Infrastructure, governed by EU member states, and it supports DIDs as part of its trust framework and defines a DID method (did:ebsi)[2] aligned with EU legal and technical requirements. The use of the

[1] https://ec.europa.eu/digital-building-blocks/sites/display/EBSI/Home

[2] https://hub.ebsi.eu/vc-framework/did

Funded by the European Union

did:ebsi method for Raw Material Digital Product Passports offers several key advantages. It ensures long-term stability, as it is not tied to specific web domains and remains accessible even if websites go offline—an important feature given the long lifecycle of regulatory records. It also allows for the secure and seamless transfer of control, enabling ownership changes to be managed through blockchain-based key rotation. Furthermore, anchoring DIDs on the blockchain provides a tamper-proof and auditable record of updates and ownership, enhancing trust and traceability.

2.1.1.3 Model and Collect Data

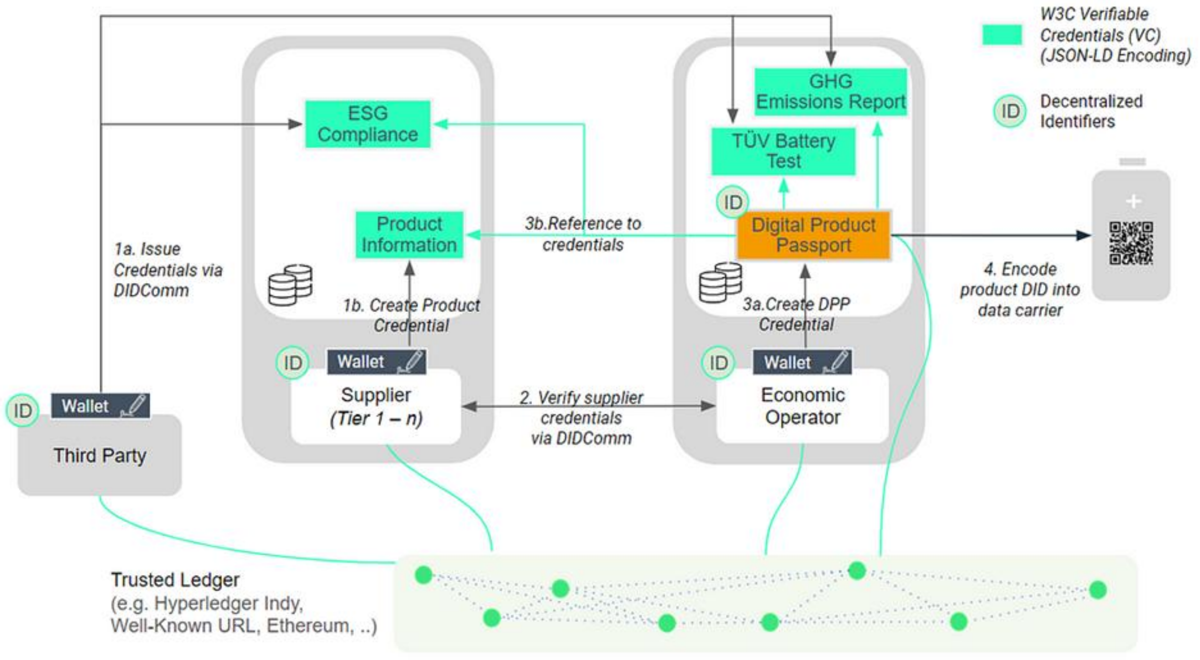

W3C Verifiable Credentials (VC) (JSON-LD Encoding)
ID Decentralized Identifiers
ESG Compliance
Product Information
GHG Emissions Report
TÜV Battery Test
Digital Product Passport
1a. Issue Credentials via DIDComm
1b. Create Product Credential
3b.Reference to credentials
3a.Create DPP Credential
4. Encode product DID into data carrier
2. Verify supplier credentials via DIDComm
ID
Wallet
Third Party
Supplier (Tier 1 – n)
Economic Operator
Trusted Ledger (e.g. Hyperledger Indy, Well-Known URL, Ethereum, ..)

Figure 2 - Third party ESG verifiable credential issuance to supplier [1]

In order to create a raw material DPP data model, firstly the required data points must be identified according to the specific stages of the supply chain, including extraction, processing, transport, and storage. Regarding raw materials, the following categories are prioritized in Maditrace:

- Product Information: Name, model, category, and ownership history.
- Material Composition: Details on raw materials, including lithium and other components.
- Manufacturing Process: Energy consumption, carbon footprint, and sustainability metrics.
- Environmental Impact: Information on hazardous substances and compliance with regulations.

Funded by the European Union

- End-of-Life Management: Recycling instructions, repairability, and disposal guidelines

The data model should incorporate regulatory requirements regarding raw materials and the data formats should be standardized to facilitate interoperability. In Deliverable 3.4 [3], a semantics layer is proposed as a conceptual framework that uses JSON-LD Contexts, established vocabularies, and trusted schema registries to provide a common semantic foundation. Furthermore, the data a DPP contains must be made available in a verifiable manner. The data model does not only contain information stored and processed in the digital twin / data catalogue of the economic operator, but it also contains verifiable data from third parties. For this reason, the responsibilities for data input should be clearly allocated to appropriate stakeholders to prevent information gaps. Third parties and suppliers provide information in the form of W3C Verifiable Credentials [6] to provide verifiable data, as shown in Figure 2. While the example in Figure 2 refers to a TÜV battery test and Greenhouse Gas (GHG) emissions report, these components are only illustrative. In practice, any accredited third-party entity—such as laboratories, auditors, or certification bodies—can issue verifiable credentials. The architecture is designed to support a wide range of issuers based on the specific trust and compliance needs of the value chain, including the integration of broader ESG-related information—such as social (e.g. labor conditions) and governance factors (e.g. audit and compliance reports) —via verifiable credentials by trusted certification bodies or auditors.

2.1.1.4 Implement Data Storage and Management

The selection of data storage architecture should consider security, transparency, and scalability. APIs and integration mechanisms should be developed to create a communication infrastructure in the supply chain for automated data exchange and updates among supply chain actors. Data validation and integrity checks are necessary to maintain trustworthiness. The data exchange protocol, digital twin / data catalogue, and organization identity wallet are the components detailed in "D3.4 Architecture and components for traceability" [3] are particularly relevant for implementing data storage and management.

2.1.1.5 Attach the QR Code

After all data attributes are filled based on the data model of the DPP, the product identifier (e.g., a DID) is encoded into a QR code. The QR code provides access to its digital passport, allowing consumers and professionals along the value chain to easily retrieve the product data.

Funded by the European Union

2.1.1.6 Implement Access Control

DPPs aim to provide publicly accessible information; however, different actors such as auditors, national regulatory bodies, or the European Commission have the right to ask for further information over the DPP infrastructure, which the economic operators do not prefer to share publicly due to confidentiality and/or data protection requirements. To balance the need for transparency with these requirements, role-based access control mechanisms must be implemented to restrict data visibility and modification according to user permissions. This way, essential product information must remain accessible to authorized parties, including consumers and regulatory authorities, while protecting confidential data.

The SSI Authorization and Access Control component presented in Deliverable 3.4 [3] enables decentralized, credential-based authorization, ensuring that only verified entities access or share sensitive data within the supply chain. Using SSI principles, this building block allows permissions to be managed through verifiable credentials, empowering organizations to control data access independently. Additionally, it supports privacy compliance (e.g., GDPR) by verifying identities and authorizing access without exposing unnecessary data, securing interactions within the supply chain.

2.1.1.7 Monitor and Maintain DPP

The intermediate system architecture presented in Deliverable 3.4 [3] defines traceability monitoring tools and applications for the stakeholders that want to make use of the traceability data stored and processed for the DPP. The tools comprise of the internal database, quality investigation process, and a monitoring UI. By making use of these tools, the DPP should be continuously updated to reflect any changes occurring throughout the raw material lifecycle. DPP maintenance, including updates due to regulatory changes or product lifecycle events, should be supported by either by the economic operator or the DPP service provider as part of an ongoing service model. In addition, quality investigation processes shall allow periodic audits and data verification processes to ensure data integrity. Additionally, feedback mechanisms should be established to allow stakeholders to report discrepancies or suggest improvements.

2.1.2 Postman-Based DPP Generation and Deployment Workflow

To generate DPPs for raw materials, Application Programming Interfaces (APIs) are used to create and manage structured product data in an automated way, allowing different

Funded by the European Union

software systems to communicate with each other. In the MaDiTraCe project, the widely used API platform Postman[3] is employed for this purpose. Postman is a user-friendly, cross-platform interface for working and interacting with RESTful APIs, available as a free desktop and web-based application. Postman makes it easier for developers to send DPP creation requests over these APIs[4], test the setup, and manage created DPPs. In MaDiTraCe project, the technical creation and management of Raw Material DPPs are facilitated using Postman API calls as follows:

1. Activate the Postman Environment: The relevant Postman environment and collection for raw material DPPs must be uploaded and activated within the Postman application.
2. Obtain an Access Token: An access token with appropriate permissions should be generated via the authorization tab in Postman to enable API interactions.
3. Initialize the Organization Profile: The organization profile can be retrieved or created using the "Get Organization Wallet Profile" and "Create Organization" API endpoints. Subsequently, the organization wallet must be obtained using the appropriate API call.
4. Create and Publish the Raw Material Template: A DPP template reflecting the raw material data model should be defined using a JSON schema. The data model must be structured using appropriate data types such as objects, arrays, and enumerations. Once defined, the template should be published to finalize the schema version.
5. Create and Publish the DPP Profile: The template schema properties should be mapped to display configuration elements, including tabs and sections, to define how information is presented. The DPP profile must then be published for use in subsequent DPP creation.
6. Create and Publish the Raw Material DPP: A new DPP instance should be created by referencing the published profile identifier. Raw material-specific information, such as batch identifiers, origin, and supply chain details, must be included in the creation request. Upon completion, the DPP should be published.
7. Retrieve and Verify the DPP: The created DPP can be retrieved using the "Get DPP" API endpoint. The service endpoint URL contained within the response provides a link to verify the DPP and ensure its correctness and completeness.

[3] https://www.postman.com/

[4] https://api-pegasus.susi.spherity.dev/#post-/product-passports

2.2 Blockchain based Notarization

In this section we detail the Trusted Ledger component as it appears in Fig. 2. First, we give some background concepts and definitions, then we proceed with the implementation steps and recommendations. Finally, we present a concrete implementation to illustrate these concepts.

2.2.1 Background and definitions

2.2.1.1 Blockchain

Blockchain is a distributed ledger technology (DLT) that enables the secure and immutable recording of transactions across a decentralized network of nodes. First introduced by Nakamoto in 2008 [7] as the foundational infrastructure for Bitcoin, blockchain has since evolved into a general-purpose technology with applications far beyond cryptocurrencies. A blockchain consists of a chain of blocks, each containing a list of transactions that are cryptographically linked and secured using consensus mechanisms such as Proof of Work (PoW), Proof of Stake (PoS), or other Byzantine Fault Tolerant protocols [8].

Blockchain offers several key benefits over traditional centralized systems [9]:

- Decentralization: Eliminates the need for a central authority, enhancing resilience and trustlessness.
- Immutability: Once recorded, data cannot be altered retroactively, ensuring integrity and auditability.
- Transparency and Traceability: All participants have access to the same version of the ledger, promoting accountability.
- Security: Cryptographic techniques and consensus protocols make the system robust against unauthorized modifications and attacks.

2.2.1.2 Smart Contract

Smart contracts are self-executing agreements encoded on a blockchain that automatically enforce the terms defined by the contracting parties without the need for intermediaries. The concept was first introduced by Nick Szabo in 1997 [10], who defined them as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises.” In the context of blockchain, smart contracts gained practical relevance

Funded by
the European Union

through the Ethereum platform, which generalized their use beyond cryptocurrency transactions to complex decentralized applications [11]. A smart contract operates deterministically, meaning its execution depends solely on the inputs and its programmed logic, ensuring transparency, traceability, and irreversibility. These properties make smart contracts particularly appealing in scenarios where trust is limited, automation is desired, and legal enforcement is costly or inefficient.

2.2.1.3 Hash Functions

Cryptographic hash functions [13] are essential building blocks in blockchain systems and data integrity mechanisms. A hash function takes an input—such as a document, a file, or a data record—and produces a fixed-length output string, called a hash or digest, that uniquely represents the original input. One of the most widely used hash functions in blockchain applications is SHA-256.

- Hash functions have several key properties that make them particularly valuable for notarization and verification:
- Deterministic: The same input always produces the same output.
- Unique (collision-resistant): Even a small change in the input (like a single character) generates a completely different hash.
- Irreversible: It is computationally infeasible to reverse the process—that is, to deduce the original input from its hash.
- Efficient: Hashes can be computed quickly, regardless of input size.

In blockchain-based notarization, hashes are used instead of raw data to ensure privacy, while still allowing for integrity verification. Since the hash represents the content without exposing it, any future modification to the original data can be easily detected by recomputing and comparing hashes. This concept of "digital fingerprinting" is foundational for more complex structures such as Merkle Trees.

2.2.1.4 Merkle Tree

Merkle Trees, also known as hash trees, are a fundamental cryptographic data structure that enables efficient and secure verification of large data sets. Introduced by Ralph Merkle in 1979, they structure data as a binary tree of hashes, where each non-leaf node is the hash of its two child nodes [12]. This hierarchical organization allows for the validation of any individual data item by tracing a small set of hashes up to the root, known as the Merkle root, which acts as a compact commitment to the entire dataset.

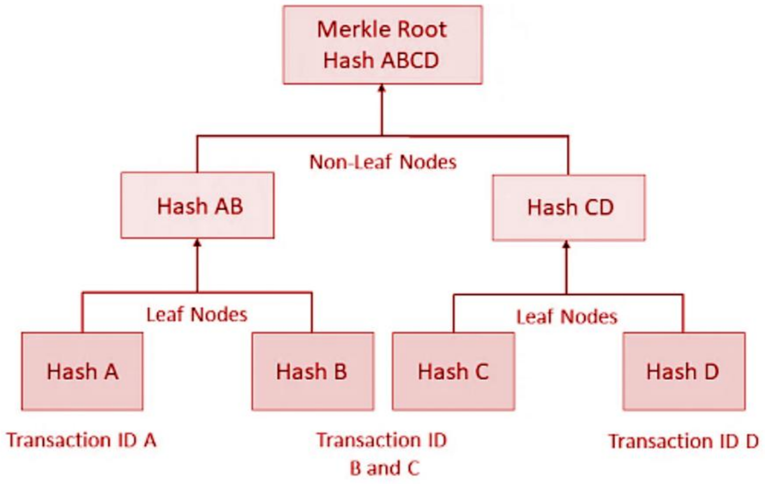


Figure 3 - How Merkle Tree works

2.2.2 Implementation Steps for a Blockchain-Based Notarization Service

To implement a blockchain-based notarization service, the following key steps are necessary:

2.2.2.1 File Preparation and Hashing

Users select one or multiple files they want to notarize. The system computes a cryptographic hash (e.g., SHA-256) for each file locally, ensuring privacy as the files themselves are never uploaded or exposed. Only the resulting hashes are recorded on the blockchain as unique, tamper-proof fingerprints

2.2.2.2 Merkle Tree Construction

The individual file hashes are organized into a Merkle tree. This structure enables a single hash (the Merkle root) to represent the integrity of the entire dataset efficiently.

2.2.2.3 Blockchain Interaction

Funded by the European Union

The Merkle root is recorded in a smart contract deployed on a blockchain. This step ensures immutability and timestamping of the notarization, making it cryptographically verifiable later.

2.2.2.4 Confirmation and Indexing

After the Merkle root is written to the smart contract, the system returns a confirmation (e.g., index or transaction ID) that can be used to verify notarization events later. Optional metadata or descriptions may also be linked to the transaction.

2.2.2.5 Verification Mechanisms

Users with all original files can re-compute the Merkle root and compare it with the one stored on-chain. An external verifier (e.g., an auditor) who has access to all the original files can verify the notarization by requesting the associated notarization index or ID. Using this ID, they retrieve the Merkle root recorded on the blockchain. They can then re-compute the Merkle root locally from the provided files and compare it with the on-chain value. A match confirms that the files are authentic and have not been altered since the original notarization.

2.2.2.6 Account Tracking (optional)

Users can view their notarization history by querying either a central server (if used) or directly the blockchain for notarization events tied to their address.

2.2.3 Technical Architecture and Tooling Choices

Having outlined the general steps involved in setting up a blockchain-based notarization service, we now turn to a concrete implementation that operationalizes these concepts. In the following section, we present the technical architecture, tools, and practical choices made to realize the notarization and verification processes.

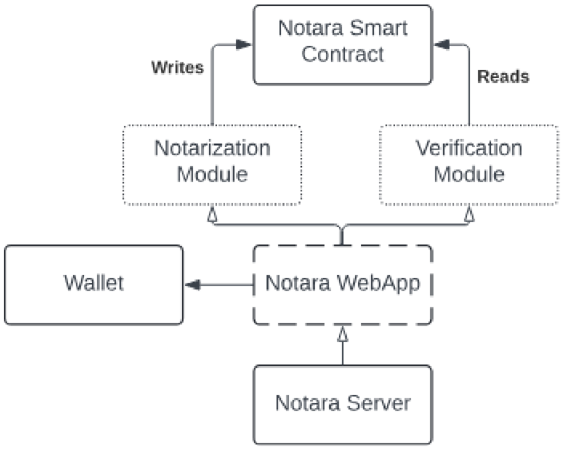


Figure 4 - Notara, Blockchain-based notarization module architecture

Notara, the Blockchain based notarization module's architecture is presented in Fig. 3. The key components are: A web server hosting a web application that provides an interface for notarization and verification, a smart contract deployed on a blockchain network, and the user's wallet.

The notarization tool we implemented provides a secure and immutable way to verify the integrity and authenticity of files by computing their hashes and notarizing the Merkle root on the Blockchain. This report details the functionalities, architecture, and verification process of this tool.

2.2.3.1 Notarization process

The notarization process ensures that file integrity is maintained without exposing the original files. The process includes:

1. Computing file hashes locally.
2. Generating a Merkle tree from these hashes.
3. Storing only the hashes and Merkle root on the server.
4. Notarizing the Merkle root on the Blockchain for immutability.

2.2.3.1.1 Steps in the notarization process

- File Selection: The user (notarizer) selects one or more documents from their local storage via the Notara web interface, and can (optional) add some description or comments.
- Local Hash Computation: The system computes a cryptographic hash locally for each selected file, ensuring that no file content ever leaves the user's device.

Funded by the European Union

- Merkle Tree Generation:
    a. The individual file hashes are ordered then structured into a Merkle tree.
    b. A Merkle root is computed from this tree, serving as a compact, tamper-evident representation of all files.
- Submission and Blockchain Anchoring : The Merkle root, along with a user-provided description and the user's address, is sent to the notarization smart contract, that will anchor them on the Blockchain.
- Notarization Confirmation: The user receives a confirmation that their files have been notarized and receives the index of the notarization.
- Server storage: we store on the server of the application the individual hashes of the files, the locally client side computed Merkle root, the description and the index of the notarization. This step is not mandatory for the notarization itself, as only the Merkle root is anchored on the blockchain. However, this storage is used for convenience in verification scenarios – particularly when only a subset of the original files is available. In such cases, it would be impossible to recompute the full Merkle root locally. By retrieving the hashes of the missing files from the server, the verifier can reconstruct the complete Merkle tree and compare its root with the one stored on-chain to confirm authenticity and integrity.
- Proof Generation: The confirmation information received from the blockchain can be generated as json file and can be used as VC attached to a DPP to prove the authenticity of some files later.

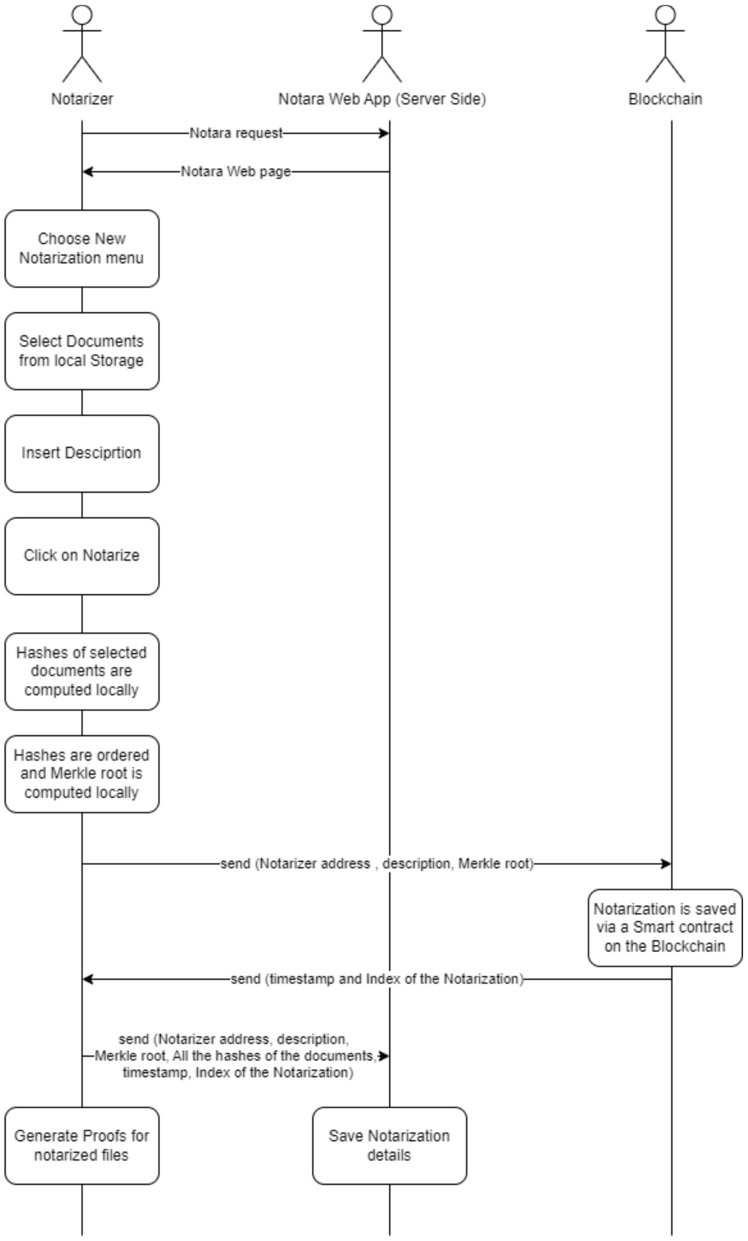
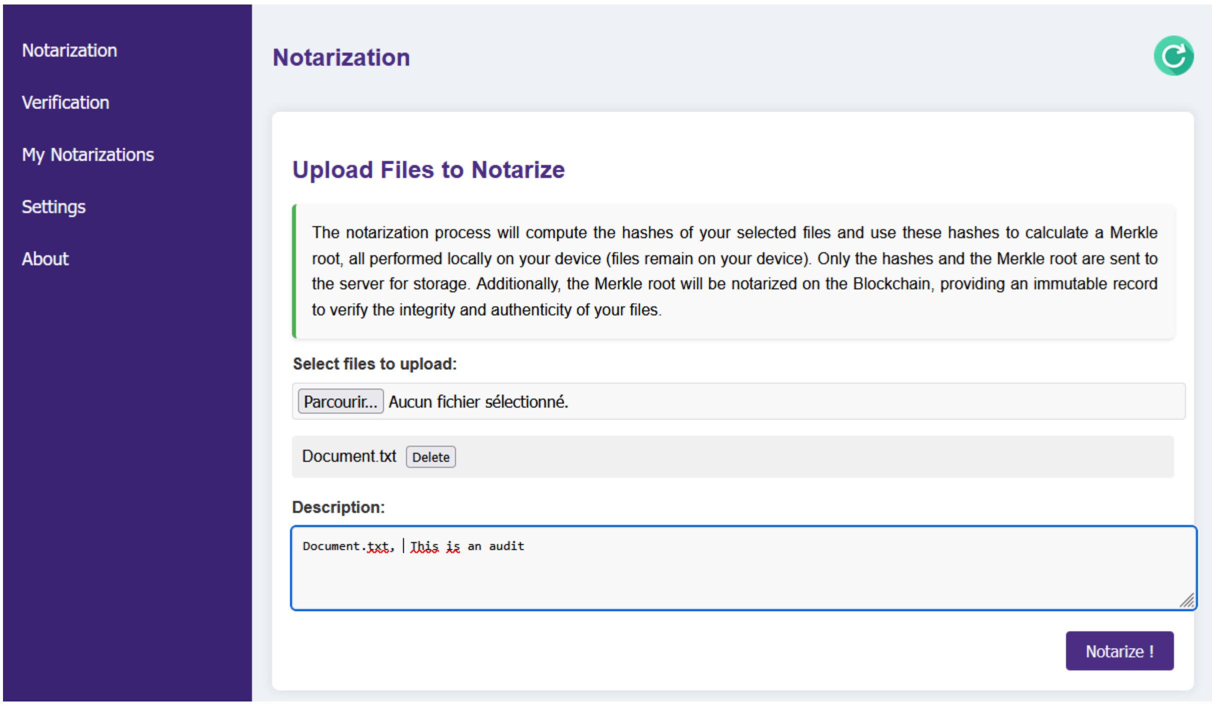

Notarizer
Notara Web App (Server Side)
Blockchain
Notara request
Notara Web page
Choose New Notarization menu
Select Documents from local Storage
Insert Desciprtion
Click on Notarize
Hashes of selected documents are computed locally
Hashes are ordered and Merkle root is computed locally
send (Notarizer address , description, Merkle root)
Notarization is saved via a Smart contract on the Blockchain
send (timestamp and Index of the Notarization)
send (Notarizer address, description, Merkle root, All the hashes of the documents, timestamp, Index of the Notarization)
Generate Proofs for notarized files
Save Notarization details

Figure 5 - Notarization process in Notara (see demo in Deliverable D3.5)

Funded by the European Union



Notarization

Upload Files to Notarize

The notarization process will compute the hashes of your selected files and use these hashes to calculate a Merkle root, all performed locally on your device (files remain on your device). Only the hashes and the Merkle root are sent to the server for storage. Additionally, the Merkle root will be notarized on the Blockchain, providing an immutable record to verify the integrity and authenticity of your files.

Select files to upload: Aucun fichier sélectionné.

Document.txt

Description: Document.txt, This is an audit

Figure 6 - Notara tool interface for notarization

2.2.3.2 Verification process

The verification process ensures that previously notarized files have not been tampered with. The tool offers two verification methods as follows in next subsections.

2.2.3.2.1 Partial File Verification (Server-Based)

Used when the user does not have all notarized files. In this case he cannot compute the Merkle Tree root and check its validity on Blockchain. In this case, we use the server side to get the missing hashes to be able to compute the Merkle root and compare with the one stored on the blockchain.

The process includes:

1. User selects available files and enter the index of the notarization.
2. The tool computes hashes of these files.
3. It checks if the computed hashes match those stored on the server.
4. The tool verifies whether the Merkle root on the server matches the one on the Blockchain.

Funded by the European Union

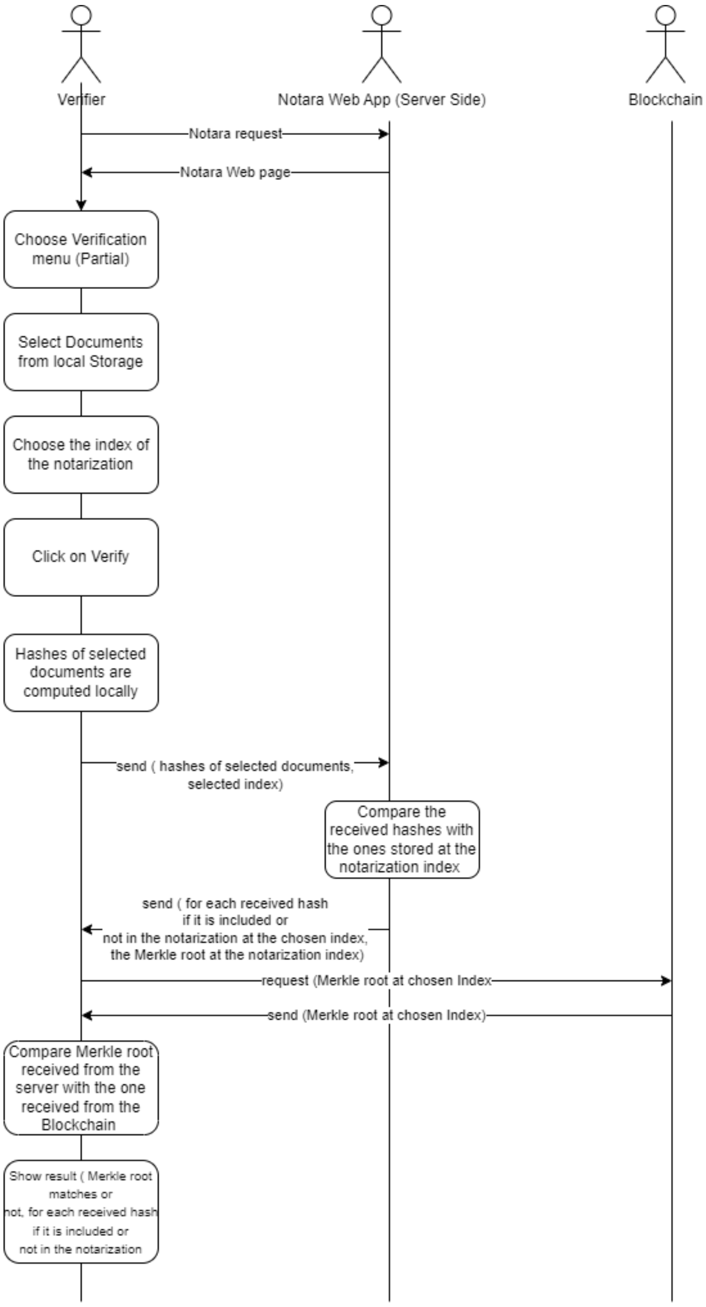

Verifier
Notara Web App (Server Side)
Blockchain
Notara request
Notara Web page
Choose Verification menu (Partial)
Select Documents from local Storage
Choose the index of the notarization
Click on Verify
Hashes of selected documents are computed locally
send (hashes of selected documents, selected index)
Compare the received hashes with the ones stored at the notarization index
send (for each received hash if it is included or not in the notarization at the chosen index, the Merkle root at the notarization index)
request (Merkle root at chosen Index
send (Merkle root at chosen Index)
Compare Merkle root received from the server with the one received from the Blockchain
Show result (Merkle root matches or not, for each received hash if it is included or not in the notarization

Figure 7 - Partial verification process

2.2.3.2.2 Full File Verification (Blockchain-Based)

Used when the user has all notarized files. The process includes:

1. User selects all notarized files.
2. The tool computes the hashes and reconstructs the Merkle tree.
3. The tool compares the computed Merkle root with the one stored on the Blockchain.

Funded by the European Union

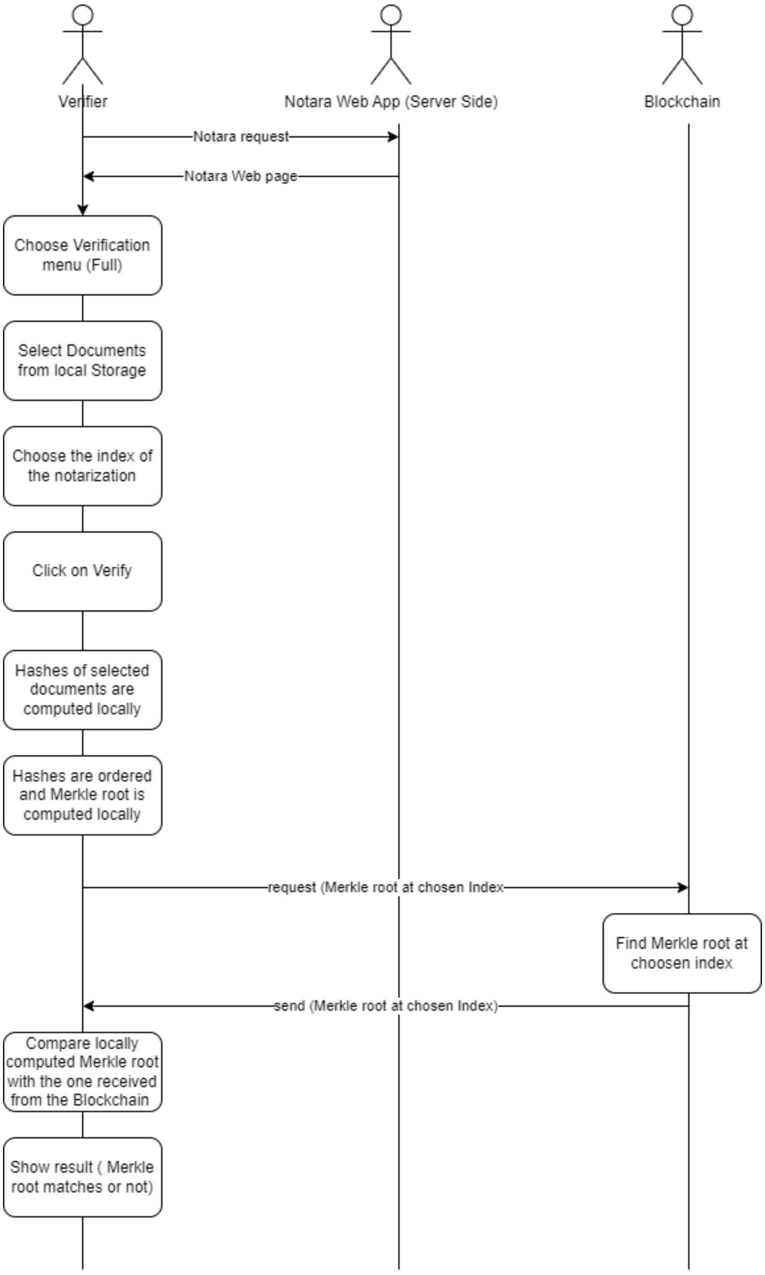

Verifier
Notara Web App (Server Side)
Blockchain
Notara request
Notara Web page
Choose Verification menu (Full)
Select Documents from local Storage
Choose the index of the notarization
Click on Verify
Hashes of selected documents are computed locally
Hashes are ordered and Merkle root is computed locally
request (Merkle root at chosen Index
Find Merkle root at choosen index
send (Merkle root at chosen Index)
Compare locally computed Merkle root with the one received from the Blockchain
Show result (Merkle root matches or not)

Figure 8 – Full File verification process in Notara tool (check demo in D3.5)

2.2.3.3 Account Notarization Verification

The tool also allows users to check their notarization history, either from the server or the Blockchain.

2.2.3.3.1 Server-Based Account Verification

The tool queries the server for notarized file records associated with the user's account.

Funded by the European Union

The server returns stored hashes and Merkle roots.

2.2.3.3.2 Blockchain-Based Account Verification

The tool queries the Blockchain for notarized Merkle roots linked to the user’s account.

It verifies that the recorded Merkle root exists on the Blockchain.

2.2.3.4 Security Considerations

2.2.3.4.1 Privacy

The notarization process is designed to preserve user privacy. Files never leave the user's device; instead, only their cryptographic hashes are generated and stored. These hashes serve as digital fingerprints, and their registration on the blockchain ensures a tamper-proof, immutable record without exposing the original content.

2.2.3.4.2 Integrity

File integrity is guaranteed through the use of hash functions, which generate unique digital fingerprints for each file. To further strengthen integrity verification, these hashes are structured into a Merkle tree, allowing efficient and scalable validation of individual files or entire datasets based on the root hash.

2.2.3.4.3 Authentication

The system authenticates notarized data by verifying that the Merkle root derived from user files exists on the blockchain. This mechanism enables users to prove the authenticity and integrity of their documents without disclosing the content itself, ensuring secure and private validation.

Funded by
the European Union

3 Existing DPP Projects and Technology Choices

As part of the platform selection process, Deliverable D3.2 presents an analytical overview of existing Digital Product Passport (DPP) solutions, based on data from the EU-funded CIRPASS project. This study examined 28 DPP initiatives in the battery sector—one of the first sectors to mandate DPPs under EU regulation.

The results, summarized in Figure 6, show that 41% of the analysed projects integrate blockchain technology, with Ethereum-based solutions leading at 37%, followed by IOTA and Hyperledger Fabric, each representing 18%. This highlights a strong trend toward decentralized approaches, though with varying architectural and governance models. These findings offer a foundational perspective for selecting appropriate platforms in MaDiTraCe. Further technical evaluation criteria and recommendations for blockchain choice will be provided in Deliverable D3.7.

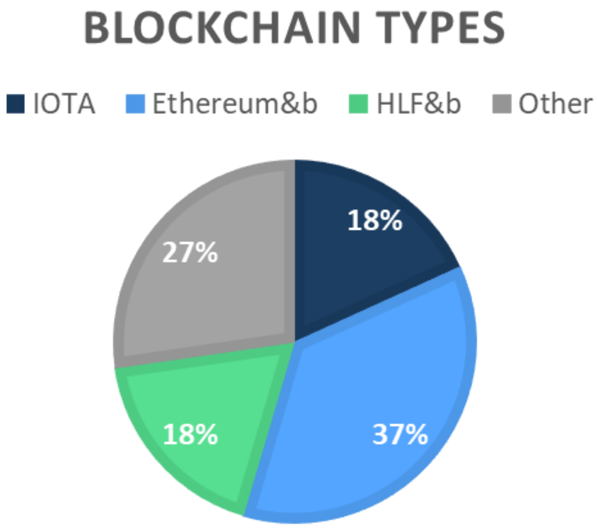


Figure 9 – Analysis of 28 existing battery DPP solution

4 Conclusions

This document outlines a concrete and modular approach for implementing digital traceability in the raw materials supply chain, leveraging emerging standards in Digital Product Passports, Decentralized Identity (DID), and Blockchain Notarization. By combining regulatory compliance requirements with verifiable data exchange, the methodology supports both technical interoperability and organizational accountability.

The inclusion of practical components—such as the Postman-based DPP generation workflow and a blockchain-powered notarization tool—illustrates how the proposed architecture can be operationalized. These tools empower stakeholders to implement secure and auditable DPPs, thus enabling a trustworthy digital infrastructure for certification and sustainability in the CRM sector. The guidelines provided in this deliverable form the basis for future integrations, testing, and refinement as the MaDiTraCe platform evolves.

Finally we note that, while the overall architecture and technical building blocks (such as notarization mechanisms, identity management, and data exchange protocols,...) are designed to be reusable across various DPP systems, the main specificities of the MaDiTraCe implementation lie in the data model tailored for raw materials and in the integration logic of the fingerprint verification service. This will be detailed in the Deliverable D3.6.

5 References

[1] Guth-Orlowski, S. (2023). Implementing Digital Product Passports using decentralized identity standards. Spherity GmbH. Retrieved from https://medium.com/spherity/implementing-digital-product-passports-using-decentralized-identity-standards-f1102c452020

[2] European Commission, Proposal for a Regulation on Batteries and Waste Batteries (Batteries Regulation), COM/2020/798 final, Article 14(1).

[3] Maditrace D3.4: Architecture definitions for POC implementation – Intermediate Report. Internal Project Deliverable.

[4] W3C CCG. (2020). A Primer for Decentralized Identifiers. Retrieved from https://w3c-ccg.github.io/did-primer/

[5] W3C. (2022). Decentralized Identifiers (DIDs) v1.0. Retrieved from https://www.w3.org/TR/did-core/

[6] W3C. (2023). Verifiable Credentials Data Model v2.0. Retrieved from https://www.w3.org/TR/vc-data-model-2.0/

[7] Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*.

Funded by the European Union

[8] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). *An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends*. In 2017 IEEE International Congress on Big Data.

[9] Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In 2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE) (pp. 1-6). IEEE.

[10] Szabo, N. (1997). Formalizing and securing relationships on public networks. First Monday

[11] Buterin, V. (2014). A next-generation smart contract and decentralized application platform. white paper, 3(37), 2-1.

[12] Merkle, R. C. (2019). Protocols for public key cryptosystems. In Secure communications and asymmetric cryptosystems (pp. 73-104). Routledge.

[13] Stamp, M. (2011). Information security: principles and practice. John Wiley & Sons.