University of Zurich^UZH

MASTER THESIS – Communication Systems Group, Prof. Dr. Burkhard Stiller

Design, Implementation, and Analysis of Decentralized Product Passport Systems for Circular Construction

Pascal Emmenegger
Zurich, Switzerland
Student ID: 15-532-302

Supervisor: Daria Schumm, Brandon Byers (ETH Zurich), Prof. Dr. Catherine De Wolf (ETH Zurich), Prof. Dr. Burkhard Stiller
Date of Submission: July 15, 2024

University of Zurich
Department of Informatics (IFI)
Binzmühlestrasse 14, CH-8050 Zürich, Switzerland

ifi

Master Thesis
Communication Systems Group (CSG)
Department of Informatics (IFI)
University of Zurich
Binzmuehlestrasse 14, CH-8050 Zurich, Switzerland
URL: http://www.csg.uzh.ch/

Declaration of Independence

I hereby declare that I have composed this work independently and without using any aids other than those declared (including generative AI such as ChatGPT). I am aware that I take full responsibility for the scientific character of the submitted text myself, even if AI aids were used and declared (after written confirmation by the supervising professor). All passages taken verbatim or in a sense from published or unpublished writings are identified as such. The work has not yet been submitted in the same or similar form or excerpts as part of another examination.

After consulting with my supervisors, I hereby declare that I have used generative AI to improve the writing style of this thesis in terms of readability, conciseness, and clarity. Specifically, the prompt *Improve it* was used with Grammarly AI and *Improve the clarity and conciseness of the following text:* with ChatGPT 4.

Zürich, July 14, 2024

Signature of student

Abstract

The building industry is the most resource-intensive sector in industrialized countries. A shift towards a circular economy is vital to enhance resource efficiency and sustainability. Digital Product Passports (DPPs) are crucial in implementing circular practices by providing essential information. However, integrating DPP systems in the construction sector presents challenges, such as ensuring long-term system and data availability and determining the best method for accessing passport data. These issues will be addressed by designing, implementing, and evaluating a decentralized DPP system prototype with physical components for accessing passport data. The study compares Non-Fungible Tokens (NFTs), Physical Backed Tokens (PBTs), and Decentralized Identifiers (DIDs) for managing product identities and ownership. Additionally, it evaluates the use of QR codes and Hardware-Locked (HaLo) NFC chips for accessing passport data. The evaluation results indicate that while a fully decentralized DPP system design is feasible, implementing a smartphone app as the user interface component depends on centralized services. This raises concerns about the long-term availability of the system. No single digital identifier and data carrier combination excelled in all evaluation criteria. However, HaLo NFC chips were the most tamper-proof option, DID-based passports were more cost-effective, and QR codes offered faster processing.

Zusammenfassung

Die Bauindustrie ist der ressourcenintensivste Sektor in Industrieländern. Der Übergang zu einer Kreislaufwirtschaft ist für die Verbesserung der Ressourceneffizienz und der Nachhaltigkeit unerlässlich. Digitale Produktpässe (DPP) sind für die Umsetzung von Kreislaufwirtschaftspraktiken von entscheidender Bedeutung, da sie wichtige Informationen liefern. Die Integration von DPP-Systemen in den Bausektor ist jedoch mit Herausforderungen verbunden, wie z. B. der Sicherstellung der langfristigen System- und Datenverfügbarkeit und der Bestimmung der besten Methode für den Zugriff auf Passdaten. Diese Probleme werden durch den Entwurf, die Implementierung und die Bewertung eines dezentralen DPP-Systemprototyps mit physischen Komponenten für den Zugriff auf Passdaten angegangen. Die Studie vergleicht Non-Fungible Tokens (NFTs), Physical Backed Tokens (PBTs) und Decentralized Identifiers (DIDs) für die Verwaltung von Produktidentitäten und Eigentumsrechten. Darüber hinaus wird die Verwendung von QR-Codes und Hardware-Locked (HaLo) NFC-Chips für den Zugriff auf Passdaten bewertet. Die Bewertungsergebnisse zeigen, dass ein vollständig dezentralisiertes DPP-Systemdesign zwar machbar ist, die Implementierung einer Smartphone-App als Benutzerschnittstellenkomponente jedoch von zentralisierten Diensten abhängt. Dies wirft Bedenken hinsichtlich der langfristigen Verfügbarkeit des Systems auf. Keine einzige Kombination aus digitalem Identifikator und Datenträger schnitt in allen Bewertungskriterien am besten ab. HaLo NFC-Chips waren jedoch die fälschungssicherste Option, DID-basierte Pässe waren kostengünstiger und QR-Codes boten eine schnellere Verarbeitung.

Acknowledgments

I would like to express my deepest appreciation to my supervisors, Daria Schumm and Brandon Byers of ETH Zurich, for their unwavering support and guidance throughout this Master's Thesis. Their dedication to helping me navigate the complexities of my research, their insightful feedback, and their willingness to engage in meaningful discussions have been pivotal in shaping this work.

I am also sincerely grateful to Prof. Dr. Burkhard Stiller and Prof. Dr. Catherine De Wolf of ETH Zurich for their supervision and enabling collaboration between the Communication Systems Group at the University of Zurich and the Chair of Circular Engineering for Architecture at ETH Zurich. This collaboration was essential for developing and pursuing the topic of this Master's Thesis. Additionally, a huge thank you goes to Arx Research, especially Brent Oshiro, for providing me with a free development kit of HaLo NFC chips.

Finally, I want to extend my heartfelt thanks to my family for their unconditional mental, educational, and financial support during my studies and for always believing in me. My deep gratitude also goes to my close friends, especially my long-term flatmates, Lea Rapp and Antea Busato, who always lent a sympathetic ear and helped me recharge my batteries with their support and distractions.

Contents

Chapter 1

Introduction

The Industrial Revolution in the 18th and 19th centuries fundamentally transformed economic and social structures. The advent of machines and new production technologies significantly boosted productivity and prosperity. Industrialization also led to the emergence of the linear economy, an economic model characterized by the ”take-make-use-waste” sequence. In this system, resources are extracted, used to produce goods, and disposed of when no longer needed. Globalization has reinforced this model as the most profitable for many industries.

However, the long-term negative effects of the linear economy are now evident: resource depletion, increased waste, and greenhouse gas emissions that harm the environment and human health. Researchers agree that the continued use of a linear model threatens the planet’s livability for future generations. The European Commission (EC) acknowledges the need to replace the linear economy with a sustainable model. Recently, the circular economy has gained momentum as a sustainable alternative. The European Green Deal [24], released in 2019, and the new Circular Economy Action Plan (CEAP) [22], published in 2020, aim to implement a circular economy through digitization, achieving climate neutrality in the European Union (EU) by 2050.

A circular economy aims to create a regenerative system that minimizes resource input, waste, emissions, and energy leakage. It transforms the linear ”take-make-use-waste” model into a closed-loop system focused on recycling, returning, repairing, and reusing resources. This approach minimizes waste by keeping products and materials in use for as long as possible, ideally achieving zero waste. Transitioning to a circular economy reduces strain on natural resources, fosters sustainable economic growth, and promotes job creation [21]. However, such a shift requires fundamental changes in product design, manufacturing processes, and consumer behavior. It also demands cooperation among manufacturers, consumers, waste managers, and policymakers [21].

Digitally accessible knowledge of product composition and resource usage throughout the product lifecycle is fundamental for implementing circular economy practices [63]. Effective management of product-related data during manufacturing, use, reuse, and recycling is essential [90]. Today, this information is often inaccessible, hindering the adoption of circular economy practices. Nevertheless, technological advancements and digital transformation promise to create solutions to make this data accessible soon.

1.1 Motivation and Problem Statement

The construction sector is one of the most resource-intensive and environmentally harmful industries. In 2021, it consumed 50% of all raw materials in Europe and produced 36% of Europe's total waste [114]. The United Nations Environment Programme reported that by 2022, the construction sector was responsible for 37% of global greenhouse gas emissions [84].

The industry also lags in digital transformation. The lack of data on buildings and their components, along with poor data exchange among stakeholders, hinders the integration of circular economy principles. Digitizing building information through product passports can simplify data access and transfer, promoting circular construction. Academia and EU agree that digital product passports (DPPs) are one of the key enablers of circular construction [10, 29, 53, 104, 127].

Although the EU has already drafted a DPP regulation [23], there are still many uncertainties and challenges regarding the design and development of a DPP system in the construction industry. This thesis aims to tackle two major problems in this area:

- **Ensuring Long-Term System and Data Availability:** Buildings and their components typically have an average use phase of 60 years [32], with some single elements lasting up to 100 years [103]. Therefore, a passport system for these products must guarantee long-term system and data availability. However, this requirement is novel and unanticipated for software systems, with no best practices or existing examples to follow, leading to uncertainty in how to achieve it.
- **Accessing Passport Data:** Data retrieval is essential for a DPP system, as a system without data access would be ineffective. However, the method of effectively linking passport data to construction products remains unclear. The upcoming EU DPP regulation, expected to be approved in mid-2024, suggests using data carriers such as QR codes, RFID tags, NFC tags, watermarks, or Bluetooth-Low Energy technology. Despite these suggestions, no specific data carrier has been officially recommended for the construction industry.

1.2 Thesis Goals

Advancements in decentralized technologies, such as distributed ledger technologies (DLTs) and decentralized data storage, offer promising opportunities to achieve long-term availability of systems and data. Therefore, this thesis investigates the feasibility of a decentralized DPP system.

Non-Fungible Tokens (NFTs), Physical Backed Tokens (PBTs), and Decentralized Identifiers (DIDs) will be employed to provide a unique and decentralized representation of a product's identity and ownership. The increasing use of QR codes, NFC technology, and smartphones underscores their potential to enable access to passport data. Therefore, this thesis further examines the effectiveness of QR codes and HaLo NFC chips as physical data carriers that connect to their digital identifiers.

The primary goal of this thesis is to provide insights that assist decision-makers in identifying the most suitable technology and architecture for implementing a DPP system in the real world. Thereby, the following research questions will be addressed:

- How can decentralized DPP systems be designed and implemented with physical components for passport data access?
- What are the benefits and drawbacks of using NFTs, PBTs, and DIDs to represent a product's identity and ownership?
- What are the benefits and drawbacks of using QR Codes versus HaLo NFC chips to access passport data?
- What are the comparative advantages and disadvantages of passport implementations using QR Code x NFT, QR Code x DID, HaLo NFC x PBT, and HaLo NFC x DID?

1.3 Methodology

A prototype application will be designed, implemented, and evaluated to achieve the research goals. The design will be informed by theoretical knowledge and an extensive literature review. Requirements will be elicited, a technical architecture will be developed, and suitable technologies will be selected for implementing the architectural components. Given the implementation of the designed prototype, the four passport types and their single components for representing product identity and accessing passport data will be evaluated. Qualitative and quantitative trade-offs will be identified to address the research questions.

1.4 Thesis Outline

In Chapter 2, fundamental theories and knowledge necessary for understanding the thesis context will be introduced. Chapter 3 provides an overview of existing literature related to the thesis, compares research in the construction industry to other fields, and identifies knowledge gaps that this thesis aims to address. Chapter 4 initiates the prototyping work by presenting the design of the DPP system prototype, including its requirements, technical architecture, and technology choices. Chapter 5 details the technical implementation of the prototype. Following this, Chapter 6 offers a comparative evaluation of the technologies used for different passport types. Finally, Chapter 7 interprets and discusses the results from the evaluation, leading to the thesis conclusion in Chapter 8.

Chapter 2

Background

This chapter elaborates on the fundamental concepts and theories necessary to understand this thesis. It begins with defining the circular economy and then describes passport instruments that promote circular construction. Additionally, it delves into the discussion of technologies that have been used for related work identification or have been utilized to design and implement the DPP system prototype.

2.1 Circular Economy

Geissdoerfer et al. [44] define a circular economy as a restorative and regenerative economic model aiming to minimize resource input, waste, emissions, and energy leakage. To reach those objectives, MacArthur [68] outlines five principles as its foundation:

- **Design out waste:** When developing products or services, designers should consider their recyclability or biodegradability. This involves creating products that can be easily disassembled, repaired, and reused. Biological materials should be incorporated to decompose products and return them to the soil. Such a design facilitates the reduction of resource waste.

- **Build resilience through diversity:** In a rapidly changing world, modularity, versatility, and adaptivity are crucial for resilience. Systems with multiple connections and scales are more resilient than those designed for efficiency.

- **Relying on renewable energy:** Fossil fuels are limited in quantity and pollute the environment. Therefore, the circular economy should be powered by renewable energy sources such as wind, solar, hydro, and tidal power. This not only improves energy security but also helps to reduce energy consumption.

- **Think in systems:** This principle refers to the capability of comprehending the interconnectedness of various elements in a system. By examining the relationship between the system and its components over time, one can identify and address the underlying causes of problems instead of just treating their symptoms. This approach can help in regenerating the system more effectively.

- **Waste is food:** By treating waste as a valuable resource, biological materials will be returned to nature, while technical materials will be repurposed to enhance their quality. The goal is to incorporate more natural materials into products, reuse them in various ways, and eventually return their nutrients to the environment as part of a new cycle.

Figure 2.1 compares the resource flow in the linear, recycling, and circular economy. Unlike the linear model, a circular economy decouples economic growth and prosperity from material consumption, carbon emissions, and waste, making it sustainable. It achieves this goal by designing longer-lasting products and repairing, maintaining, and reusing them. Additionally, materials are recycled, refurbished, and remanufactured. In the circular economy, materials are expected to retain their maximum value for as long as possible and to travel in circles within the economy to reduce waste, pollution, and negative environmental effects [21, 61, 68].

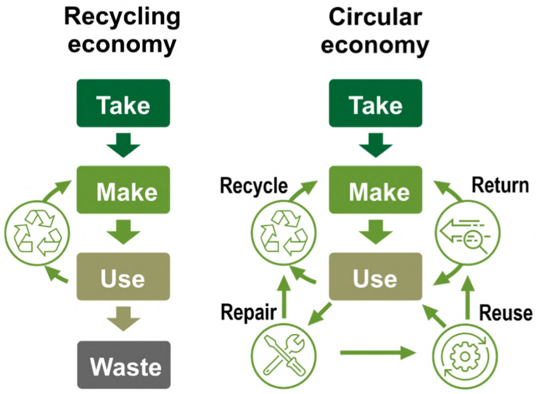


Figure 2.1: Resources Flows in the Linear, Recycling, and Circular Economy [90]

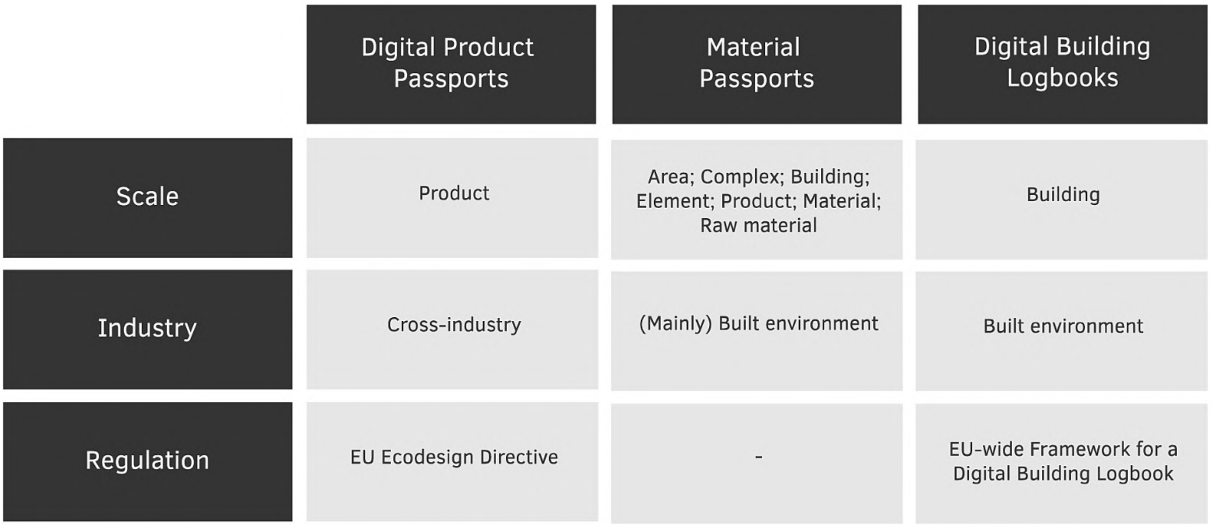
To implement a circular economy, four distinct resource strategies are proposed [62, 127]:

- **Narrow:** Using fewer resources through efficiencies in the production and design process.
- **Slow:** Using and consuming less by ensuring long product life, extending product life, and avoiding unnecessary consumption.
- **Close:** Reusing or recycling materials after use.
- **Regenerate:** Leaving the environment and society in a better state than before, for example, by improving biodiversity.

2.2 Passport Instruments for Circular Construction

A literature review conducted by Van Capelleveen et al. [113] highlights the existence of various alternative terminologies for product passports for circular economy, such as material passport, (digital) product passport, resource passport, recycling passport, or cradle-to-cradle passport. These passport concepts differ in their domain, focus, specificity of attributes, and goals. However, they share some common elements. They are ”(1) digital, (2) act as an interface, (3) create a certified identity, (4) address a single identifiable product, (5) construct this identity via the life cycle registrations of its component tree, and (6) are used for gaining insight into sustainability and circularity characteristics, value estimation and identifying opportunities.”

Considering the built environment, Çetin et al. [128] identified three major passport instruments supported by the EU: Digital Product Passports (DPPs), Material Passports (MPs), and Digital Building Logbooks. Figure 2.2 presents their high-level differences and similarities. While DPP is a more general concept that can be applied to any industry and product, MP and Digital Building Logbook are more specific to buildings and building materials. It is important to note that the MP is not officially acknowledged and supported by an EU regulation, despite being funded by the EU's Horizon 2020 research and innovation programme [14]. Although the three passport concepts differ in their scope and purpose, they share the common goal of providing valuable information that can be used to implement the circular economy's four R cycles (Repair, Reuse, Recycle, and Return), ultimately enabling a circular construction.



	Digital Product Passports	Material Passports	Digital Building Logbooks
Scale	Product	Area; Complex; Building; Element; Product; Material; Raw material	Building
Industry	Cross-industry	(Mainly) Built environment	Built environment
Regulation	EU Ecodesign Directive	-	EU-wide Framework for a Digital Building Logbook

Figure 2.2: Comparison of DPPs, MPs, and Digital Building Logbooks [128]

2.2.1 Digital Product Passport (DPP)

A DPP is a digital document that provides information about a product's lifecycle, materials, and sustainability attributes [48, 101, 118]. This includes comprehensive details about the product's origin, durability, composition, reuse, repair, dismantling options, and disposal methods [2].

DPPs deliver the following core benefits [2, 48, 59]:

- **Traceability, Trust, and Transparency Improvement:** DPPs allow for tracking and tracing products from their beginning to end-of-life. All stakeholders must be able to confirm the authenticity of a product and its compliance with regulations. As a result, supply chain transparency is increased, and the risk of product counterfeiting is reduced, promoting ethical sourcing of the product.

- **Consumer Empowerment:** DPPs can be leveraged to offer personalized product information and customization, enhancing consumer engagement and experience. By sharing information throughout a product's life cycle, customers can access information that enables them to make more informed and sustainable choices.
- **Circular Economy Support:** DPPs facilitate the reuse and recycling of products by providing detailed information on repair, maintenance, and recycling options. This helps minimize waste and resource use, promoting a circular economy. DPPs also encourage innovative thinking on circularity and new practices, which could lead to the development of entirely new business models that support the transition to a circular economy.

The European Commission (EC) is aware of the potential of DPPs in helping to shift towards a circular economy. Hence, in 2022, the EC proposed the Ecodesign for Sustainable Products Regulation, which includes a draft regulation of the EU DPP [23]. The EU DPP is a first-of-its-kind, strong regulatory circularity tool [101].

Figure 2.3 illustrates the timeline for implementing the EU DPP. At the time of writing, the final approval of the EU DPP regulation is still pending. After approval, more details will be provided in delegated acts per product group over the next few years. The EC has identified five prioritized product categories with a high environmental impact and potential for improvement: Electronics & ICT, batteries & vehicles, textiles, plastics, construction & buildings. DPP is required to come into effect for the initial product groups in 2026/7, but these groups are yet to be defined. By 2030, DPPs are expected to be mandatory for most industries [23].

Beanland [10] argues that the implementation timeline remains uncertain beyond these first indications. Götz et al. [48] assume that the EC plans to introduce a generic DPP design for the first product groups, which can later be modified for other product groups through sectoral modulations. However, many uncertainties and technological challenges must be overcome before implementing the EU DPP across various industries [10]. Figure 2.4 explains the scope, technology, and data-related issues that still need to be resolved, using the battery passport as an example.

2.2.2 Material Passport (MP)

The EU Horizon 2020 project Buildings as Material Banks (BAMB) [14] defines MPs as follows:

> *Materials passports (MP) are (digital) sets of data describing defined characteristics of materials and components in products and systems that give them value for present use, recovery, and reuse.*

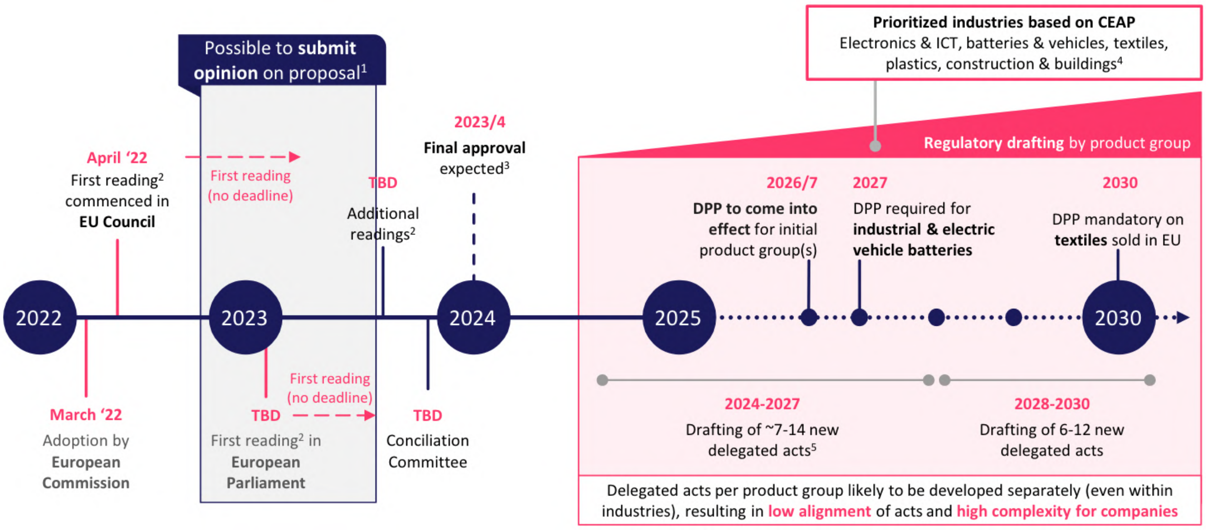
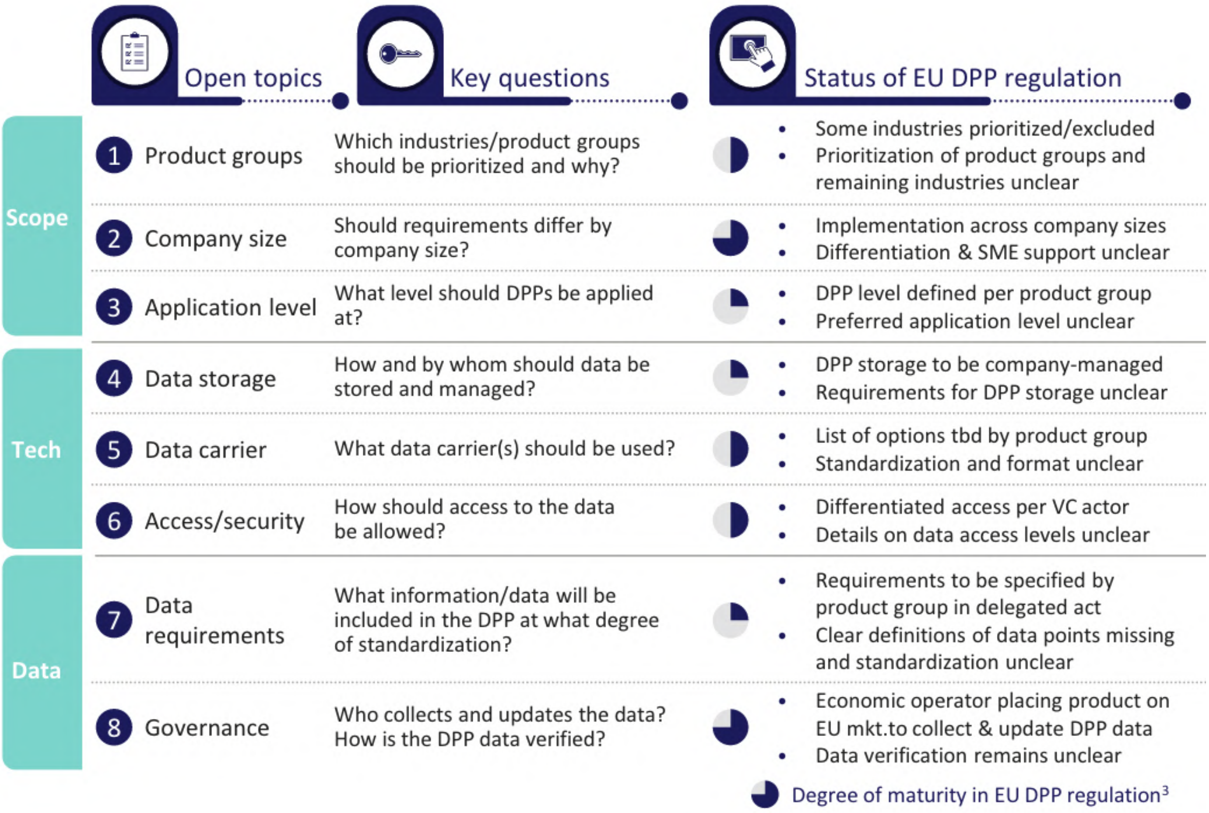

Possible to submit opinion on proposal[1]
Prioritized industries based on CEAP
Electronics & ICT, batteries & vehicles, textiles, plastics, construction & buildings[4]
Regulatory drafting by product group
April '22
First reading[2] commenced in EU Council
First reading (no deadline)
TBD
Additional readings[2]
2023/4
Final approval expected[3]
2026/7
DPP to come into effect for initial product group(s)
2027
DPP required for industrial & electric vehicle batteries
2030
DPP mandatory on textiles sold in EU
2022
2023
2024
2025
2030
March '22
Adoption by European Commission
First reading (no deadline)
TBD
First reading[2] in European Parliament
TBD
Conciliation Committee
2024-2027
Drafting of ~7-14 new delegated acts[5]
2028-2030
Drafting of 6-12 new delegated acts
Delegated acts per product group likely to be developed separately (even within industries), resulting in low alignment of acts and high complexity for companies

Figure 2.3: Timeline for the EU DPP Implementation [101]



	Open topics	Key questions	Status of EU DPP regulation	
Scope	1 Product groups	Which industries/product groups should be prioritized and why?	◐	• Some industries prioritized/excluded • Prioritization of product groups and remaining industries unclear
	2 Company size	Should requirements differ by company size?	◕	• Implementation across company sizes • Differentiation & SME support unclear
	3 Application level	What level should DPPs be applied at?	◔	• DPP level defined per product group • Preferred application level unclear
Tech	4 Data storage	How and by whom should data be stored and managed?	◔	• DPP storage to be company-managed • Requirements for DPP storage unclear
	5 Data carrier	What data carrier(s) should be used?	◐	• List of options tbd by product group • Standardization and format unclear
	6 Access/security	How should access to the data be allowed?	◐	• Differentiated access per VC actor • Details on data access levels unclear
Data	7 Data requirements	What information/data will be included in the DPP at what degree of standardization?	◔	• Requirements to be specified by product group in delegated act • Clear definitions of data points missing and standardization unclear
	8 Governance	Who collects and updates the data? How is the DPP data verified?	◕	• Economic operator placing product on EU mkt.to collect & update DPP data • Data verification remains unclear

◕ Degree of maturity in EU DPP regulation[3]

Figure 2.4: Open Topics in EU DPP Draft Regulation [10]

Like DPPs, MPs offer valuable information on construction products, promoting circular construction. Both aim to simplify value assessment by providing relevant data for a circular economy. DPPs are a broad concept for any product in various industries, while MPs focus on buildings and construction. Despite being funded by BAMB, no regulatory framework exists to standardize different MP approaches [53, 128].

There are various approaches to implementing MPs, considering different granularities, content, and data formats. Research has explored the application of MPs at both the construction component level [15, 16] and the building level, including BIM data [8, 51, 52, 74].

2.2.3 Digital Building Logbooks

In addition to DPPs and MPs, there is another passport instrument called digital building logbooks, specifically designed for buildings. An EU-wide framework supports these logbooks, which are only applied in the construction industry [53, 128].

The framework [39] defines a digital building logbook as a centralized repository for all relevant building data. It aims to enhance transparency, trust, and information sharing among stakeholders in the construction industry. A digital building logbook records changes and major events throughout a building's lifecycle. The logbook can include various types of information, such as plans, land descriptions, technical systems, and data related to the building's surroundings. While some data remain static, others, such as those from smart meters and intelligent devices, are dynamic and require regular updates. Data can be stored directly within the logbook or hosted in a different location, with the logbook acting as a gateway to access this information.

2.3 Automatic Identification and Data Capture (AIDC)

Šeba, Hruška, and Švadlenka [129] describe AIDC technologies as methods for identifying objects, collecting data, and using this data. These technologies aim for fast, easy, and accurate data exchange with devices like computers or smartphones [116]. In this thesis, AIDC technologies enable devices to interact with DPPs. The following sections discuss QR codes, RFID tags, and NFC tags as AIDC technologies.

2.3.1 Quick Response (QR) Code

A QR code is a two-dimensional grid of black-and-white modules arranged to encode information. It was developed to overcome the limited information capacity of traditional barcodes, which can only hold up to 20 alphanumeric characters [106].

QR codes have three main advantages that contribute to their widespread use. First, their orientation and scale do not affect readability; a scanner can detect and read the data matrix from any direction (360°) and different scales. Second, QR codes are resistant to distortion due to their alignment patterns. Those patterns allow them to be read accurately even when the camera is not exactly rectangular oriented to the code. Lastly, QR codes feature error correction capabilities with four levels (7%, 15%, 25%, and 30%), enabling accurate reading even if the code is smudged or damaged. The error correction level can be set when creating the code [97, 106].

Figure 2.5 illustrates an exemplary data exchange using QR codes. The text *Hello World !!!* is first encoded into a QR code using an encoder, producing a QR code symbol. Cameras with QR code reading capabilities, such as cameras on common smartphones, can read this symbol. Once the QR code is captured, the scanner decodes the symbol and returns the plain data to the user.

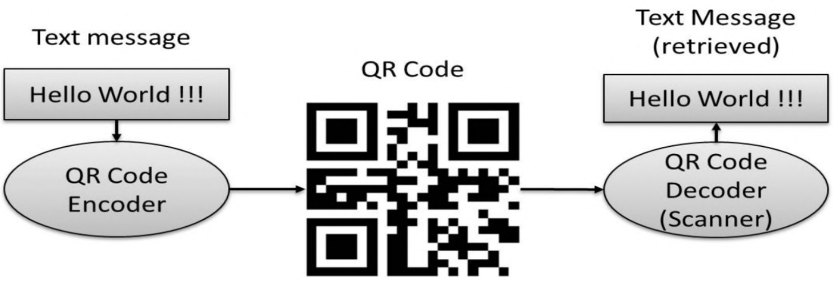


Figure 2.5: Exemplary Data Exchange Using QR Codes [106]

Plain text, URLs, or other data can be encoded as QR code symbols. The more data to be encoded, the more black and white dots are required, making the QR code denser, larger, and more complex. However, there is a maximum amount of data to be encoded, depending on the data format and the error correction level. At the lowest error correction level (7%), a QR code can contain up to 7'089 numeric characters or 4'296 alphanumeric characters. The highest error correction level (30%) can include up to 3'057 numeric characters or 1'852 alphanumeric characters [106, 116].

Figure 2.6 illustrates the structure of a QR code symbol. It comprises a quiet zone, functional patterns, and an encoding region. The quiet zone surrounds the symbol on all four sides, highlighting its borders. Functional patterns are essential for decoding and must be placed in specific areas to ensure the QR code scanner can correctly identify and orient the symbol at any angle and scale. The encoding region contains the data, information about the density and size of the QR code, and details for error correction [73, 106]

2.3.2 Radio Frequency Identification (RFID) Tag

RFID is an AIDC technique that employs radio waves to store and access information from an identification chip, known as an RFID tag. These tags are affixed to items for identification purposes, such as a pallet containing materials [116, 129].

An RFID system generally comprises three primary components [116, 129]:

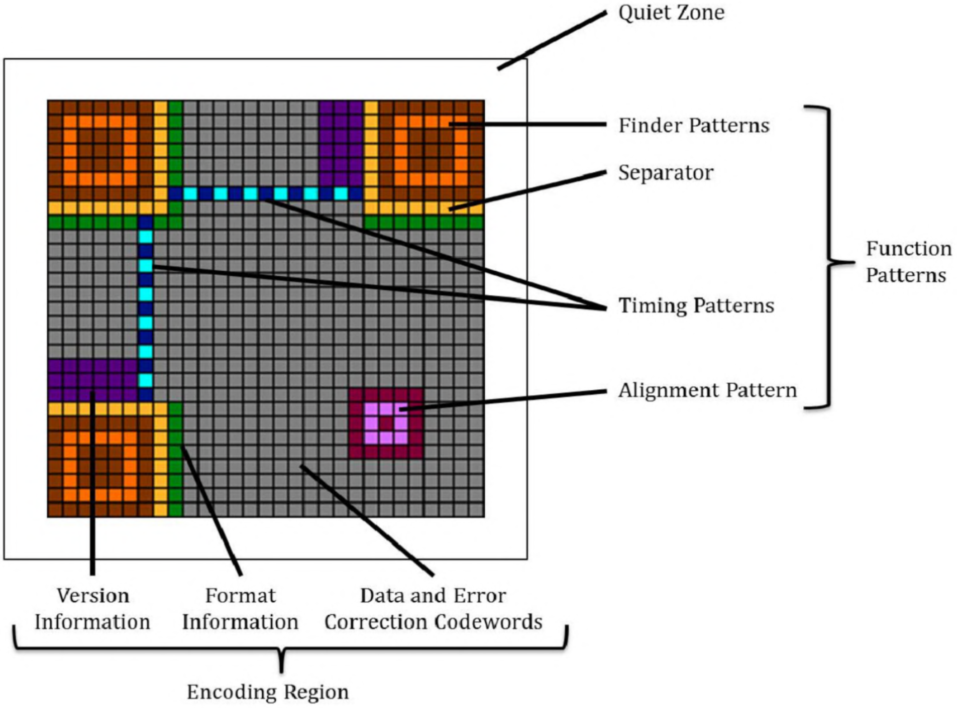


Figure 2.6: Structure of a QR Code Symbol [106]

- **RFID Reader/Writer:** Contains an antenna, transceiver, and decoder. It periodically transmits signals to locate tags, captures signals from tags, and forwards the data to the controller.

- **RFID Tag:** Includes an antenna, radio transceiver, and integrated circuit for information storage and processing. Tags have writable memory ranging from tens to thousands of bytes, depending on the model. They rely on the reader's (electro)magnetic field for data transmission to the controller, with a maximum range of 15 meters.

- **Controller:** Manages the data collected by the RFID reader.

RFID tags are classified into two types: active and passive [27, 122, 129]:

- **Active Tags:** Have their own power supply, such as a battery or solar cell. This internal power supply allows them to operate with a weaker (electro)magnetic field emitted by readers. Consequently, they are typically more reliable than passive tags and can communicate with a reader at longer distances.

- **Passive Tags:** Do not have an internal power supply. They receive energy from the (electro)magnetic field emitted by the reader. Therefore, if the tag is outside the reader's range, it lacks power and cannot send signals. Readers can interact with passive tags from approximately 10 centimeters to a few meters.

2.3.3 Near Field Communication (NFC) Tag

NFC is an AIDC technique similar to RFID. It utilizes short-range, high-frequency radio waves to store and retrieve data from an identification chip known as an NFC tag. NFC allows data exchange within a 10 cm range. While NFC and RFID communicate using radio frequencies, RFID can operate over longer distances, extending beyond a few meters [116].

Modern mobile phones are equipped with NFC technology, enabling them to function as NFC-enabled devices. In read/write mode, these devices can interact with NFC tags and access their memory. NFC-enabled devices connect to only one NFC tag at a time, reducing the risk of accidental transactions. NFC tags are passive and receive power from the NFC reader/writer. When an NFC-enabled device is near a tag, it powers the tag to transfer information to the reader. There are four types of NFC tags (Type 1 to Type 4), each varying in memory capacity, communication speed, and settings for readability, re-writability, or read-only status [3, 27].

Data on NFC tags is exchanged using the NFC Data Exchange Format (NDEF). NDEF is a binary format that encapsulates one or more application-defined payloads into a single message, with linked records to support larger payloads. An NDEF message, illustrated in Figure 2.7, consists of one or more records enclosed by the Message Begin (MB) and Message End (ME) flags. Each record contains the payload length, type, and an optional identifier. The NFC Forum defines specific NDEF record types, including text, image, URI, phone number, and smart poster messages. Smart poster records are common and contain data along with instructions for the device. When an NFC device taps a smart poster tag, it reads and processes the data, triggering actions such as opening a web browser, visiting a website, or sending an SMS to receive a ringtone [27, 116].

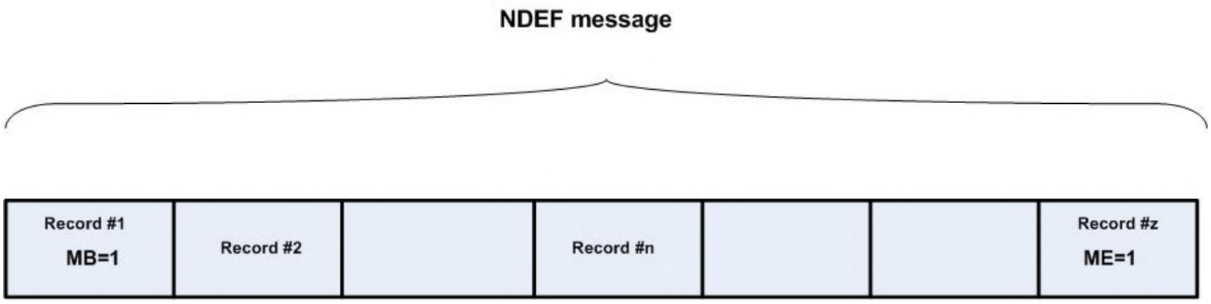


Figure 2.7: Structure of an NDEF Message [116]

2.3.3.1 Hardware-Locked (HaLo) NFC Chip

NFC chips, including HaLo NFC chips manufactured by Arx Research, offer advanced features beyond basic NDEF message reading and writing. Notably, the HaLo chip supports self-certification via asymmetric cryptography, which is a first in the industry. This allows the chip to verify its authenticity autonomously. Each HaLo chip generates a unique asymmetric key pair: a public key, shared as a public identification number, and a private key, stored on the chip for creating unique message signatures. These signatures verify the authenticity and ownership of the public key. Any nearby NFC-enabled device can request authentication signatures from the chip [87, 88].

Figure 2.8 demonstrates the self-certification feature. The HaLo NFC chip uses its private key to sign messages, ensuring authenticity for smart contracts. Since public keys are non-confidential, they can be stored on public DLTs, enabling secure authentication without third-party involvement [88].

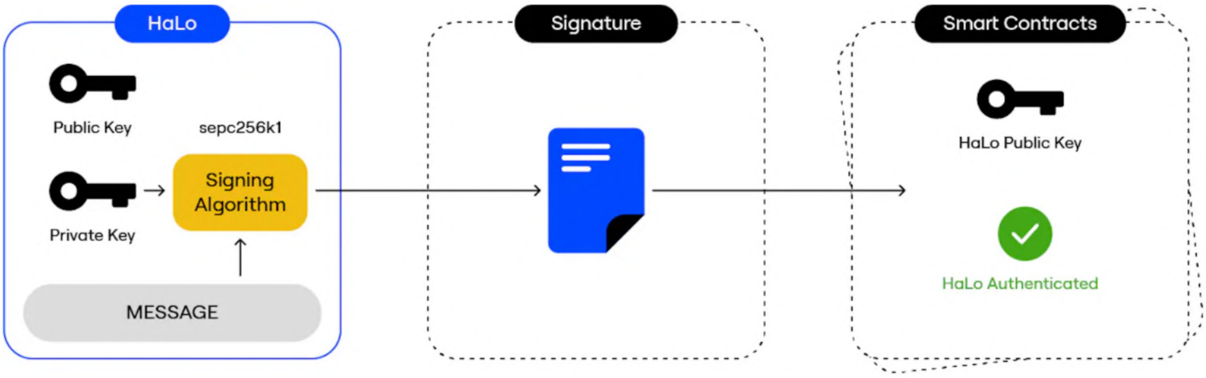


Figure 2.8: Exemplary Application of Self-Certification using HaLo NFC Chips [88]

HaLo NFC chips, readable using the NFC Forum Type 4 Tag Standard, store a URL as an NDEF record. This URL is immutable for security reasons related to self-certification. Below is an example of a URI-type record from a HaLo NFC chip (version c5), including all relevant information and public keys.

```
https://eth.vrfy.ch/?
  [...]
  &pk1=0428C[...]88FE
  &pk2=04052[...]39FF
  [...]
  &rnd=00000[...]D382
  [...]
```

where:

- `pk1` contains the first secp256k1 public key in uncompressed SEC format. This key pair is factory-initialized and can sign any external data [87].
- `pk2` contains the second secp256k1 public key in uncompressed SEC format. Initialized in the factory, pk2 signs a random number (see `rnd`) with each tap [87].
- `rnd` is a Big-endian UInt32 incremental counter that increases by 1 with each tap and includes 23 random bytes generated by the tag for each tap [87].

2.4 Distributed Ledger Technology (DLT)

DLTs are data structures for recording transactions and functions to manipulate them. A primary objective of DLTs is to enable users who do not inherently trust each other to interact without relying on a trusted third party. This is particularly relevant when there is mistrust between participants, such as business partners or anonymous entities. DLTs inherently provide transparency, traceability, and security in such environments [33, 60]

While each DLT employs different data models and technologies, they generally rely on three foundational technologies: public key cryptography, distributed peer-to-peer networks, and consensus mechanisms. Public key cryptography establishes a secure digital identity for every participant, essential for operating in an untrusted environment. Each participant has a pair of keys (one public, one private) to record transactions in the DL. A peer-to-peer network ensures scalability, prevents single points of failure, and avoids control by a single entity or a small group. Consensus protocols allow all participants, or nodes, to agree on a single version of the truth without a trusted third party [33, 60]

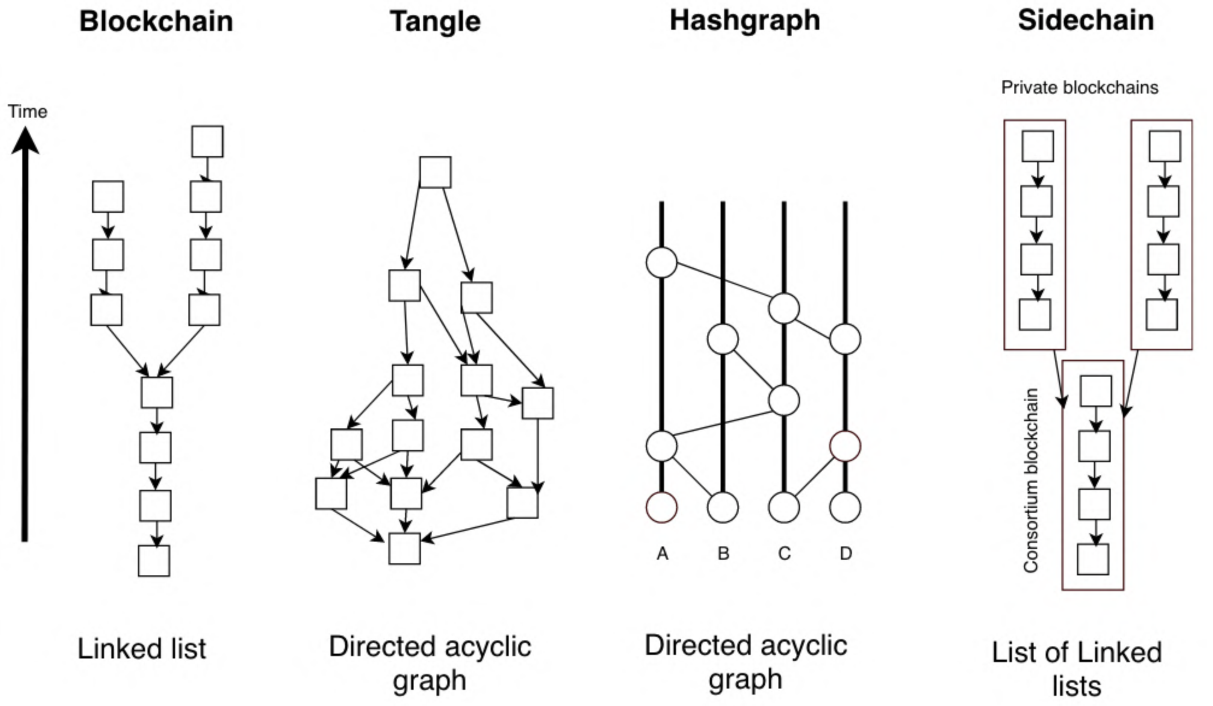


Figure 2.9: Overview of DLT Concepts [33]

El Ioini and Pahl [33] categorize DLTs into four distinct concepts, as illustrated in Figure 2.9:

- **Blockchain:** A blockchain is a distributed, decentralized, and immutable ledger storing transaction histories. It consists of blocks linked by hash codes, each referencing the previous one. This structure ensures tamper resistance, as altering any block changes its hash, invalidating subsequent blocks. Each block consists of transactions representing data modifications. Miners process new transactions into a block and add it to the blockchain. Each transaction requires gas fees to compensate for the costs of their computational effort [33].

- **Tangle:** IOTA's Tangle is a decentralized data storage and consensus protocol based on a Directed Acyclic Graph (DAG). In the DAG, nodes represent transactions, and edges indicate transaction validations. This design allows the Tangle to grow proportionally, enabling more simultaneous transactions than blockchains in a more cost-efficient manner [33].
- **Hashgraph:** Hashgraph uses a DAG for transaction storage, combined with a voting algorithm and gossip protocol to achieve rapid consensus. It emphasizes transactional fairness. Thereby, the concept of ordering ensures that transactions are validated based on their submission order. This contrasts with blockchain, where miners can influence transaction order [33].
- **Sidechain:** This architecture uses a central consortium blockchain to manage access requests and private sidechains for local transactions. Each sidechain maintains its information, sharing only selected data. This approach addresses blockchain security, privacy, and performance limitations by integrating multiple blockchains [33].

2.4.1 Smart Contracts

Smart contracts are immutable programs on DLTs that can manage assets and execute transactions. They contain programmed rules that automatically execute when triggered by DLT participants, such as humans or other smart contracts. Each execution is an immutable transaction. Smart contracts are deterministic, guaranteeing consistent outcomes in identical contexts [64, 126].

2.4.2 Ethereum

Ethereum is a public and permissionless blockchain, meaning all transactional data is publicly accessible, and anyone can create an Ethereum address to participate in the network. The native cryptocurrency, Ether, is denominated in units of Gwei (10^9 Gwei = 1 Ether) and Wei (10^{18} Wei = 1 Ether) [60, 123].

Ethereum employs a proof-of-stake mechanism for selecting miners. By staking Ether, miners lock Ether and apply to be selected to validate and add transactions, earning rewards for this operation. Miners are chosen randomly, with higher stakes increasing the odds of selection. This system is considered secure because acquiring Ether requires fiat money. The more money invested, the more reliable a miner is expected to be, as incorrect data processing would decrease trust in Ethereum. A lack of trust would subsequently lower Ether's value and cause significant financial loss to the miner [60, 123].

Ethereum includes Solidity [94] and the Ethereum Virtual Machine (EVM). Solidity is a programming language for developing smart contracts, while the EVM compiles, deploys, and executes smart contract code. Gas fees on Ethereum are primarily determined by the computational effort required by the EVM to execute a smart contract's function. Besides the Ethereum mainnet, there are many other EVM-based or EVM-compatible blockchains, such as Sepolia, Goerli, Polygon, Optimism, and Binance Smart Chain. Thus, smart contracts written in Solidity can be deployed and executed on various blockchains [69, 123].

2.4.3 Non-Fungible Token (NFT)

An NFT is a unique digital identifier representing objects. Each NFT has a distinct serial number, known as the token ID, ensuring its uniqueness. Unlike Ether tokens, which are interchangeable and lack unique identifiers, NFTs are specifically identified by their token ID [18, 19, 121].

On Ethereum, the ERC-721 standard [35] defines NFTs by providing an API interface for implementing smart contracts on the Ethereum blockchain. This standard mandates functionality for transferring tokens between accounts, retrieving a wallet's current balance, and identifying the owner of a specific token [18, 19, 121].

2.4.4 Physical Backed Token (PBT)

A PBT extends the concept of NFTs by linking the unique digital representation to a physical object. A PBT's ownership is tied to that of its physical counterpart. Therefore, creating, modifying, or transferring PBTs requires prior verification of the physical item's authenticity [1, 91].

The ERC-5791 standard [1] on Ethereum defines PBTs and provides an API interface for implementing smart contracts on the Ethereum blockchain. Unlike ERC-721 NFTs, which can be transferred on-chain directly, transferring a PBT requires collecting and inputting verification data from the physical item. The verification occurs on-chain, and the token transfer will not proceed if the verification data is incorrect [1, 91].

2.5 Self-Sovereign Identity (SSI)

Today, identity verification on the internet primarily relies on centralized or federated systems, where a central authority manages authentication. These methods often pose security and privacy risks. SSI offers a new model for managing and verifying digital identities without a central authority, leveraging advances in cryptography, distributed ledgers, and smartphones [83, 95].

Figure 2.10 illustrates how SSI-based identity verification works. Instead of email addresses, individuals or organizations are represented by Decentralized Identifiers (DIDs). Data associated with a DID, such as public keys, is stored on a verifiable data registry, while private keys are stored locally on the holder's device. Credentials are verified using Verifiable Credentials (VCs), which are signed by the issuer's private key and can be checked against the issuer's public key [67, 83]

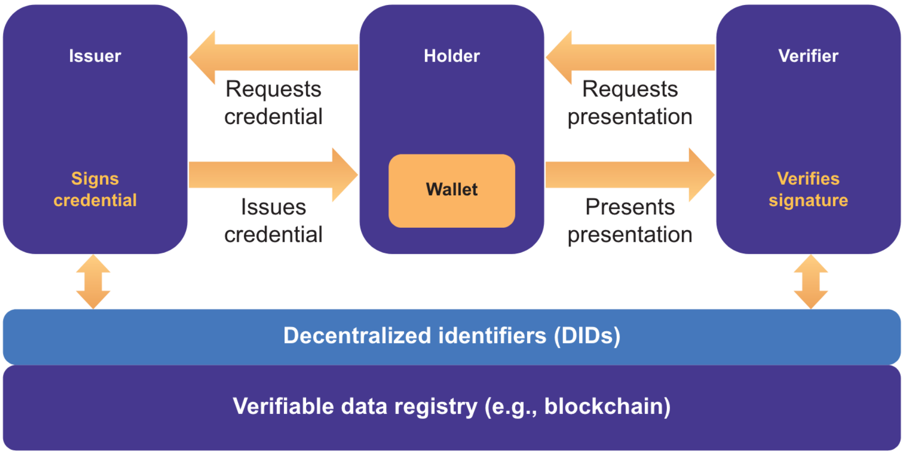


Figure 2.10: Identity Verification using SSI [83]

The process begins when an issuer, such as the Swiss Driver Licensing Agency, issues a VC (e.g., a digital driver's license) to a holder. The holder stores the VC in a digital wallet app. When a verifier, such as the police, requests verification, the holder presents the VC. The verifier uses cryptographic algorithms to check the VC against the Swiss Driver Licensing Agency's public key, available through the verifiable data registry, to confirm its authenticity [67, 83]

2.5.1 Decentralized Identifier (DID)

DIDs, like IP addresses, are globally unique internet identifiers not directly tied to the identity of the person, organization, or entity controlling them. Developed by W3C [98], DIDs aim to enable digital identity verification in a decentralized manner without a central authority. Decentralization here refers to creating, controlling, and managing identities, rather than storage of identity data [83].

Figure 2.11 illustrates the components of a DID infrastructure and their relationships. A DID identifies a subject, such as a person, organization, thing, data model, or abstract entity. Each DID resolves to a DID document describing the subject and providing the necessary information for secure and verifiable interaction. DID existence and document data are recorded on a verifiable data registry, which can be centrally or decentrally managed. The DID controller, typically the subject itself, can transfer control to another entity, such as parents managing their children's DIDs or companies managing product DIDs [98].

Figure 2.12 shows a DID structure and its corresponding DID document. A DID is a simple text string comprising the scheme, the DID method, and the DID method-specific identifier. The scheme value `did` indicates the identifier is a DID. The DID method specifies how to resolve and manage the DID, with various methods available, such as `btcr`

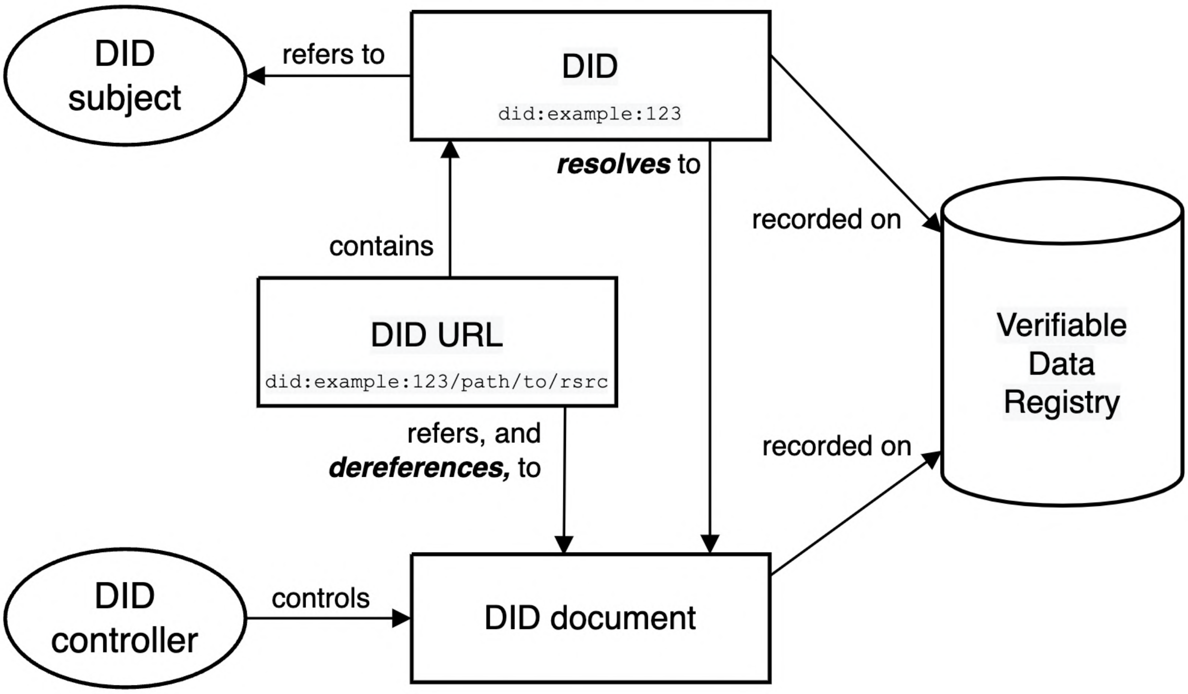
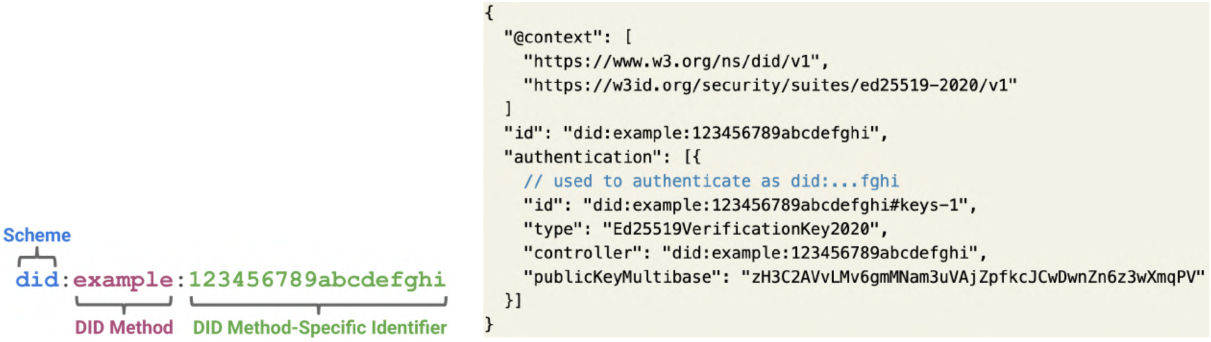


Figure 2.11: Overview of the DID Architecture [98]

(Bitcoin blockchain), `ethr` (Ethereum blockchain), `web` (traditional web infrastructure), and `ipid` (IPFS-based). The method-specific identifier uniquely represents the DID within its method environment [98].


Scheme
did:example:123456789abcdefghi
DID Method
DID Method-Specific Identifier

1. DID Structure

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    // used to authenticate as did:...fghi
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

2. DID Document

Figure 2.12: Example of a DID and DID Document [98]

Using the DID method's technology, a DID can be resolved to its DID document, as visualized in Figure 2.12. The DID document, formatted as JSON-LD, includes the `@context` property for semantic context and the `id` attribute representing the DID. The `authentication` array lists methods for authenticating the DID and its subject. Additionally, the DID document can include various properties such as different verification methods (including cryptographic algorithms and mechanisms), detailed information about the DID's controller, and service endpoints linking to URLs or URIs for interoperability with third-party systems [98]

2.5.2 Verifiable Credentials (VCs)

VCs are digital credentials that validate claims to verifiers without a central authority. Data models for VCs are under development by W3C [99]. A VC comprises a credential identifier, metadata, claims, and the issuer's signature. Figure 2.13 illustrates these components using a driver's license as an example. The credential identifier, such as a driver's license number, is unique. Credential metadata provides details about the credential, like its expiration date. Claims represent the subject of proof, demonstrating that the individual holds a valid driver's license. Lastly, the issuer's signature, typically from the licensing agency, authenticates the credential [83].

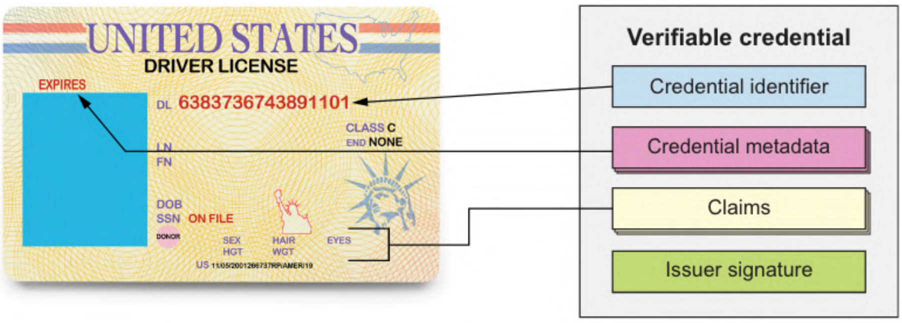


Figure 2.13: VC Components [83]

Chapter 3

Related Work

This chapter presents academic literature that is closely related to this research. It first introduces the methodology for identifying literature. Then, it follows related research regarding the usage of data carriers, digital identifiers, and prototypes of decentralized DPP systems. A discussion of the results and presentation of research gaps concludes this chapter.

3.1 Methodology

This thesis employed boolean search strategies and the snowball method, also known as citation chaining, to identify related literature.

Boolean search is a technique that uses keywords and logical operators (AND, OR, NOT) to filter out irrelevant search results. Enclosing a search term within quotation marks (" "), the results will contain an exact match for that term. Without quotation marks, the search results will contain any word that appears somewhere in the search term. Wildcards are allowed using asterisks (*) and question marks (?). The asterisk represents any number of unknown characters, whereas the question mark represents a single unknown character [25, 37].

Given the difficulty in pinpointing the exact search terms to find relevant studies, the snowball method was adopted. This approach, effectively discovering related works through the references cited in similar studies, involves tracing the citation trail from one work to another [36].

The PRISMA 2020 guideline for systematic literature review was utilized to evaluate the trustworthiness and application of the related work findings. This guideline includes the PRISMA flow diagram to illustrate how the literature review was conducted. There are three phases: Identification, screening, and inclusion. The identification phase indicates where potential literature for review was identified and how many records were found. The screening phase explains why and how many records were excluded. Lastly, the inclusion phase presents relevant literature [81, 89].

The subsequent sections each contain a PRISMA flow diagram depicting the origins of related work presented. During the identification phase, boolean searches were conducted on the 6th of March 2024 across Google Scholar, IEEE Xplore, and ACM Digital Library. Snowballing was utilized to expand the search for relevant records. This involved searching for records based on the titles of the references used in records found through the initial database search. To stay within the scope of this thesis, only references of records that were assessed for eligibility were considered for the snowball method. The figures provide a detailed overview of the search terms and snowballing procedure used for the database searches. Identified records through database search and snowballing were checked for duplicates, and student theses were excluded due to their lack of peer review. In the screening phase, certain records were omitted based on exclusion criteria that will be elaborated upon in each subchapter. Finally, each PRISMA flow diagram showcases the related work after applying the snowballing method and the database results.

This thesis does not specifically target the construction industry but addresses some construction-related challenges. Therefore, related work from other industries was not categorically excluded. However, to manage the limited timeframe, the initial database search concentrated on key terms relevant to the construction industry, such as *Product Passports*, *Material Passports*, and *Building Logbooks* [128]. For each distinctive topic, the search term *"Product Passport*" OR "Material Passport*" OR "Building Logbook*"* was used to identify related work in databases. This approach allowed studies from other industries to appear due to including *"Product Passport*"*. However, because more specific search terms for other industries were not used, those results are indicative rather than comprehensive. Different industries may use their specific terms to describe the concept of a product passport.

3.2 Related Work on Data Carriers

This section focuses on related work that employs tracking technology affixed to an item, acting as a data carrier that can be used for passport data retrieval. The most common types of data carriers discussed in academic discourse are QR codes, RFID tags, and NFC tags [5, 46]. Each of these data carriers will be discussed in the following sections.

3.2.1 QR Code

This chapter presents previous research on QR codes as data carriers for accessing passport information. Figure 3.1 depicts the PRISMA flow diagram communicating how related work was selected.

To identify relevant studies via databases, this thesis utilized the search term *"QR Code*" AND ("Product Passport*" OR "Material Passport*" OR "Building Logbook*")*. Additionally, snowballing was employed by searching for *"QR Code*"* in the titles of references within reports assessed eligible from the initial database search.

During the screening phase, records were excluded that only mentioned QR codes as an example of a data carrier. Similarly, studies investigating QR codes in contexts unrelated to object identification were omitted.

Finally, 9 studies were selected as related work. 8 studies [11, 15–17, 30, 46, 76, 82] were obtained from the database results. 1 study [115] was identified by snowballing. The subsequent paragraphs review these studies and present a summary of their contributions in Table 3.1.

Researchers in the construction industry explore incorporating QR codes into building elements. This includes the attachment of QR codes and the impacts on industry processes.

Byers et al. [16] investigate how engraved QR codes can connect building components with MPs for circular construction. The research first compares asset-tracking technologies such as barcodes, QR codes, RFID, BLE, and NFC based on the requirements for building component tracking systems. Then, it presents a proof of concept where QR codes are laser engraved on structural wooden members such that the QR code is read through the contrast between the engraved and not engraved pixels. QR codes are selected for their low-cost benefits, fast implementation speed, and accessibility (common smartphone cameras can read QR codes out of the box). However, the study identifies some challenges, such as required visual access to materials, difficulties adapting the physical and digital representation when the component is modified, and QR code readability issues caused by material properties, poor environmental lighting, and bad camera quality.

In their subsequent research, Byers and De Wolf [15] use QR code-based MPs to investigate the impact of integrating tracking technology throughout various stages of circular construction. Employing two case studies, their work uses a replicable wooden structure to demonstrate the practical application of MPs in small-scale construction scenarios. Physically, the paper details the use of QR codes during construction stages, emphasizing benefits such as enhanced tracking of components, delivering critical information to users, and aiding in the processes of deconstruction and reconstruction. It also addresses potential challenges, including the risk of QR code damage and aesthetic concerns. Digitally, the research showcases the effectiveness of various platforms and file formats in managing MP data. It features Google Spreadsheets, HTML web pages integrated with CSV files, and software applications that employ JSON files.

Another crucial aspect of research within the built environment focuses on linking QR codes with BIM to improve communication and understanding among construction project participants.

Dervishaj, Hernández Vargas, and Gudmundsson [30] examine the potential of utilizing QR codes, NFC, and BLE tags with BIM to support the reuse of prefabricated concrete components. The study proposes combining the three tracking technologies, a database, and digital models to identify building components and facilitate data exchange throughout the components' life cycle. The paper highlights the benefits and limitations of QR codes for storing unique IDs for each element, enabling easy generation and scanning with smartphones but requiring visual access. Due to the occurrence of NFC, this study will also be covered in Chapter 3.2.3.

Panoti, Abdelhafez, and Ha [82] discuss the potential for reducing carbon emissions in construction projects by reusing precast concrete panels. They propose using BIM as a digital tool to achieve this goal and suggest that QR codes can be used as a data carrier to access BIM. By providing BIM data on a QR code, the structural and geometrical properties of precast concrete panels can be assessed and utilized by practicing designers in new building designs. This availability of data can prove to be a valuable resource for designers in their future projects.

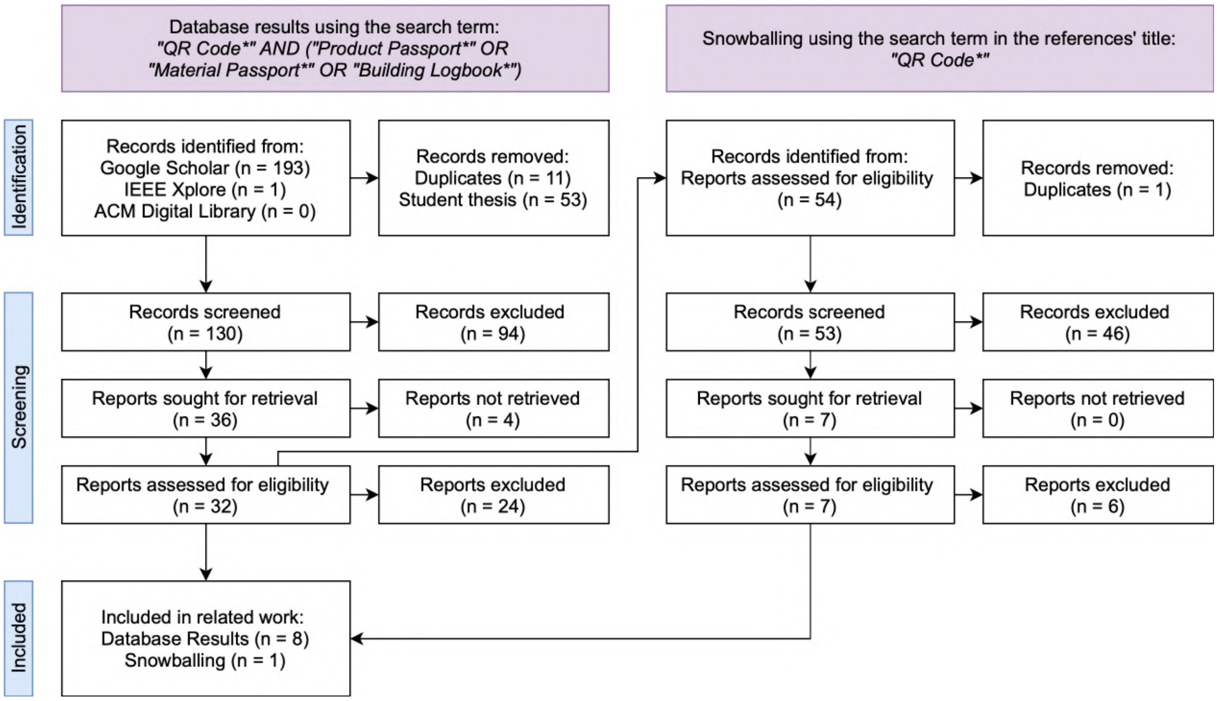


Figure 3.1: PRISMA Flow Diagram for Related Work on QR Codes (adopted from Page et al. [81])

Industry	Reference	Year	Contribution
Construction	Byers and De Wolf [15]	2023	Assessing circular construction's efficiency through QR code-based MPs.
	Byers et al. [16]	2022	Linked building components to MPs using engraved QR codes for circular construction.
	Dervishaj, Hernández Vargas, and Gudmundsson [30]	2023	Connected BIM and prefabricated concrete components for reuse via QR codes.
	Panoti, Abdelhafez, and Ha [82]	2023	Utilized QR Codes for BIM data storage and access to facilitate sustainable design with precast concrete panels.
	Vasilyev et al. [115]	2019	Implemented QR codes for BIM data retrieval via smartphones at the construction site to enhance understanding and communication.
Plastic	Berg et al. [11]	2022	Proposed the integration of QR codes in a DPP system for lifecycle tracking of plastic products.
ICT	Navarro et al. [76]	2022	Utilized QR codes within a DPP prototype for ICT devices to capture device-related data and link it to blockchain transactions for verifiability.
All	Carlsson, Nevzorova, and Vikingsson [17]	2022	Created a digital platform for product information management and sustainability tracking via QR codes.
	Gligoric et al. [46]	2019	Investigated QR code printing inks that respond to changes in temperature and luminosity.

Table 3.1: Summary of Related Work on QR Codes

Vasilyev et al. [115] developed a subsystem that combines BIM and QR codes to improve communication and understanding among participants in construction projects. QR codes are attached to building and equipment elements at the construction site to use the subsystem, and construction workers use a QR code reading device, such as a smartphone, to retrieve BIM-related data. This system enhances staff security, decision-making, and mutual understanding among construction workers regarding the assembly, disassembly, and management of construction components.

Berg et al. [11] discuss how QR codes linked to DPPs can address plastic value chain information deficits. Using DIDs and VCs, stakeholders can create traceable and verifiable product information, enhancing trust and transparency. QR codes link to DPPs, providing access to detailed information about the plastic material, recycling codes, and proof of origin. Through a consistent chain of documentation, products can be traced and tracked reliably, facilitating the reuse of recycled plastics. The paper highlights that QR codes enable a digitally supported circular economy for plastics by providing easy access to essential product information. This study will also be covered in Chapter 3.3.2 on DIDs and VCs.

Navarro et al. [76] examine the digital transformation of the circular economy by implementing DPPs for Information and Communication Technology (ICT) devices. Their research focuses on developing a registry to verify DPPs, identifying devices and their components, and promoting their reuse, recycling, and responsible disposal. To help identify and track devices throughout their lifecycle, QR codes are used as machine-readable elements on physical tags. The researchers integrate QR code scanning in a mobile Android application to capture device-related data and link it to blockchain transactions for verifiability. This approach allows for associating media content with blockchain transactions, enhancing trust and accountability in the traceability of ICT devices within the circular economy. This study is also related to the work on DID with VCs in Chapter 3.3.2 and the prototypes of decentralized DPP systems in Chapter 3.4.

Two papers regarding QR codes were found without a specific industry focus.

Carlsson, Nevzorova, and Vikingsson [17] developed a digital platform, "Certified to LAST," which merges digital information with physical products through QR codes, enhancing the credibility of sustainability claims to consumers. The platform provides comprehensive product information to consumers, including service and spare parts availability. This enables users to make informed decisions on product sustainability, durability, and repairability. By employing QR codes directly on the products, the system offers access to a digital twin of the product, providing general and specific information about the product's sustainability features and lifecycle management options. This initiative aims to address the current market gap by providing a transparent and reliable platform that supports circular economy goals, ensuring that products are designed for durability, maintainability, and sustainability.

Gligoric et al. [46] introduce a new type of contextual QR code that can change its appearance based on the environment. To achieve this, the authors used thermochromic and photochromic inks to print QR codes that can be decoded into different tags depending on their present state, such as temperature or luminosity. This unique technology allows individual items to be identified and their environmental conditions monitored throughout their lifecycle. As a result, a more detailed and dynamic product passport can be created, providing information about the product's usage, condition, and recyclability.

3.2.2 RFID

This chapter presents previous research on RFID tags as data carriers for accessing passport information. Figure 3.2 depicts the PRISMA flow diagram communicating how related work was selected.

To identify relevant studies via databases, this thesis utilized the search term *RFID AND ("Product Passport*" OR "Material Passport*" OR "Building Logbook*").* Additionally, snowballing was employed by searching for *"RFID"* in the titles of references within reports assessed eligible from the initial database search.

During the screening phase, records were excluded that only mentioned RFID tags as an example of a data carrier. Similarly, studies investigating RFID technology in contexts unrelated to object identification were omitted.

Finally, 10 studies were selected as related work. 7 studies [9, 45, 49, 54, 77, 105, 112] were obtained from the database results. 3 studies [26, 75, 102] were identified by snowballing. The subsequent paragraphs review these studies and present a summary of their contributions in Table 3.2.

Similar to QR codes, researchers in the construction industry examine the use of RFID tags to link them with BIM. Additionally, RFID technology is being explored by integrating it with Computer-Aided Design (CAD) modeling or Cloud technology to automate and enhance materials management on construction sites.

Naranje and Swarnalatha [75] propose a system that uses RFID technology to track prefabricated building components. The system aims to enhance efficiency and coordination within the construction industry's supply chain. Prefabricated components are tagged with RFID at the manufacturing unit, enabling their tracking through various stages until assembly at the construction site. This system integrates with BIM through a color-coded CAD model, visually representing the components' current locations in the supply chain. Using a LEGO model to symbolize a construction project with six main components, the researchers demonstrated the system. The demonstration showcased the potential of RFID technology in reducing construction costs and time. Furthermore, it also improves project management and resource flow between different supply chain stages.

Ness et al. [77] present a cyber-physical prototype system that combines RFID, BIM, and a Cloud-based platform to enhance the reuse of building components. This system facilitates the identification, tracking, and management of reusable building components, thereby supporting Product Service System (PSS) relationships between suppliers/providers and users/clients for the reuse of building components. By integrating ICT-based data management and PSS, suppliers can manage reusable building components over an extended life, retain their value, and identify new profit centers. Clients benefit from reused components' assured quality and performance, leading to cost and carbon savings. The paper showcases an example of an internal glazed system, demonstrating the application of this system and its potential for sustainable building practices.

Swift et al. [102] demonstrate the potential benefits of using RFID and BIM technologies in the construction industry. By linking real-world building components with a digital

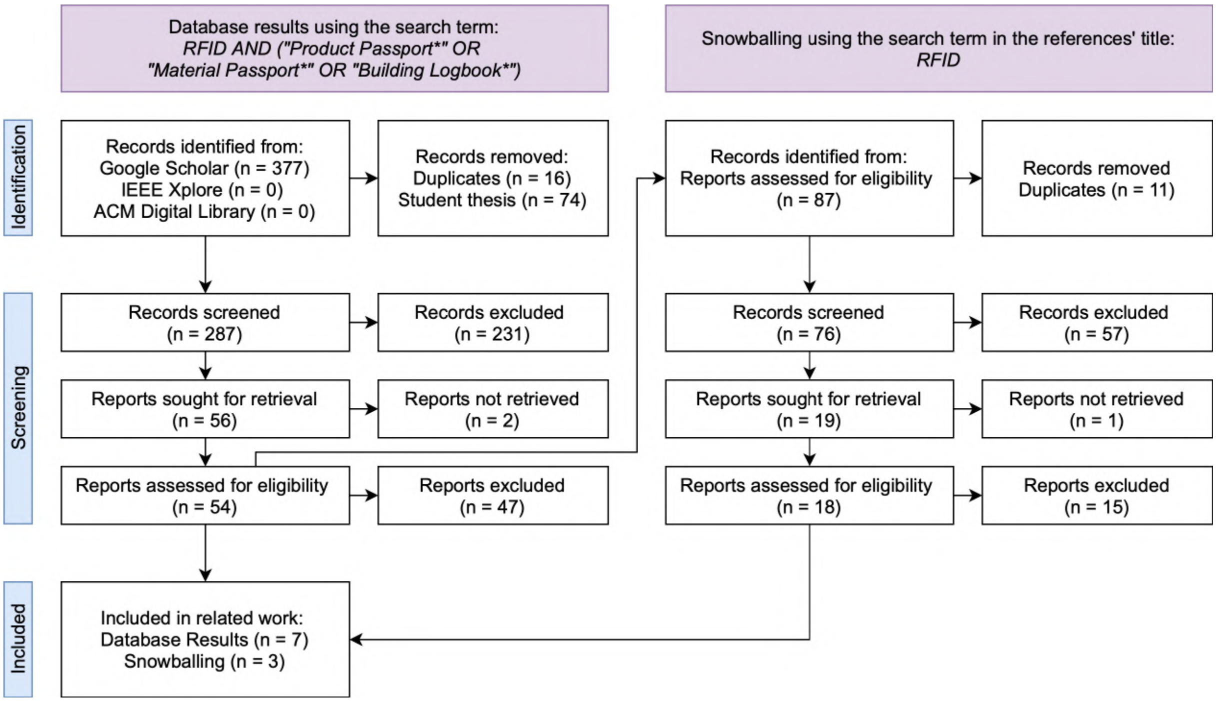

Database results using the search term:
RFID AND ("Product Passport*" OR "Material Passport*" OR "Building Logbook*")
Snowballing using the search term in the references' title: RFID
Identification
Screening
Included
Records identified from:
Google Scholar (n = 377)
IEEE Xplore (n = 0)
ACM Digital Library (n = 0)
Records removed:
Duplicates (n = 16)
Student thesis (n = 74)
Records identified from:
Reports assessed for eligibility (n = 87)
Records removed
Duplicates (n = 11)
Records screened (n = 287)
Records excluded (n = 231)
Records screened (n = 76)
Records excluded (n = 57)
Reports sought for retrieval (n = 56)
Reports not retrieved (n = 2)
Reports sought for retrieval (n = 19)
Reports not retrieved (n = 1)
Reports assessed for eligibility (n = 54)
Reports excluded (n = 47)
Reports assessed for eligibility (n = 18)
Reports excluded (n = 15)
Included in related work:
Database Results (n = 7)
Snowballing (n = 3)

Figure 3.2: PRISMA Flow Diagram for Related Work on RFID (adopted from Page et al. [81])

Industry	Reference	Year	Contribution
Construction	Copeland and Bilec [26]	2020	Explored technologies, including RFID, to link demolition and construction projects to foster the reuse of building elements.
	Giovanardi et al. [45]	2023	Proposed the embedding of RFID tags in facade infrastructure to improve material traceability.
	Hradil, Jaakkola, and Tuominen [54]	2023	Implemented RFID tags in a traceability system for constructional steel reuse.
	Naranje and Swarnalatha [75]	2019	Employed RFID technology and CAD models for tracking prefabricated building components.
	Ness et al. [77]	2019	Introduced a system prototype that combines RFID, BIM, and Cloud technology for identifying, tracking, and managing reusable building components.
	Swift et al. [102]	2017	Connected BIM and building components for enhanced adaptability and reuse via RFID tags.
	Vahidi et al. [112]	2024	Utilized RFID tags in recycled concrete supply chain to enhance sustainability by improving transparency, traceability, and data reliability.
Battery	Bandini et al. [9]	2023	Utilized RFID tags within a DPP system for batteries.
Fashion	Tihon and Weißmann [105]	2023	Implemented RFID technology to digitize fashion industry services.
Packaging	Hakola et al. [49]	2024	Analyzed the durability of RFID tags in washing and heating for reusable packaging.

Table 3.2: Summary of Related Work on RFID

database, companies can track and update information on these components across their entire lifecycle, enhancing their adaptability and potential for reuse. The study highlights the importance of developing new business models that allow for reassigning ownership of movable components, such as walls and doors, to enable their take-back for reuse or remanufacture, promoting a circular economy within the industry. The use of RFID and BIM technologies not only increases building adaptability and component reuse but also contributes to the efficiency of design and construction processes. By enabling real-time data retrieval, these technologies reduce the time delays associated with traditional data acquisition and archiving methods.

Numerous studies in the construction industry investigate the use of RFID in the context of PPs or MPs to track or trace building elements.

Copeland and Bilec [26] explore various technologies, including RFID data tags, to improve the link between demolition and construction projects. They introduce a framework for executing Building as a Material Bank (BAMB) projects to promote the transition to a circular built environment. This framework suggests a systematic assessment of materials retrievable from deconstruction processes for their potential in recycling, upcycling, or direct reuse. It advocates for tagging materials certified for reuse with passive RFID tags. The RFID tag data will be stored on a blockchain and contain information about the material's structural properties, history, and stored location. This ensures data integrity and transparency, enabling construction projects to access data on reclaimed materials.

Giovanardi et al. [45] recommend incorporating RFID technology into facade infrastructure to capture, document, and distribute asset-related information. This proposal is part of a comprehensive framework that leverages the capabilities of the IoT to combine data from physical and digital domains, resulting in the development of an integrated product passport. This framework aims to address the issue of insufficient traceability data related to building materials.

Hradil, Jaakkola, and Tuominen [54] explore developing and implementing an RFID-based traceability system for constructional steel reuse. Attaching RFID tags to steel building components establishes a link to a cloud-based electronic MP and 3D information model obtained through aerial scanning before deconstruction. The system aims to provide complete and accurate information about building components, facilitating more efficient reuse and informed decision-making during deconstruction planning. The technology was successfully demonstrated on a real deconstruction and reuse project of an industrial steel hall in Tampere, Finland.

Vahidi et al. [112] investigate the feasibility of using RFID technology as MP in the circular economy of recycled concrete. The study examines the potential of RFID tags to improve sustainability by ensuring data reliability and transparency throughout the supply chain. The researchers conducted laboratory tests to determine the resilience of RFID tags to mechanical stresses encountered during the supply chain and their ability to maintain readability when embedded in concrete. The tests assessed the impact of various factors, such as water content in concrete, aggregate type, particle size distribution, and proximity to steel rebar, on the performance of RFID tags. The study found that water content significantly affects initial tag readability, though readability improves over time. The findings confirm that an RFID-based system can significantly enhance the management of the recycled concrete supply chain, providing an efficient and scalable method for promoting product sustainability and traceability.

Bandini et al. [9] examine a variety of passive UHF-RFID tags and utilize them to establish battery traceability within a DPP solution for batteries. The authors describe a system architecture that permits the reading and writing vital battery parameters, such as the State of Charge, State of Health, and other significant cell-related events. The research advocates for integrating a Battery Management System that automatically and periodically monitors the battery's condition, recording these parameters onto the RFID tag. Users can then easily access the stored data with an RFID reader, streamlining the battery management process and enhancing traceability. The study highlights the potential of UHF RFID technology in supporting the implementation of a digital battery passport, contributing to the sustainable and circular management of batteries in applications such as electric vehicles.

Tihon and Weißmann [105] discuss a business model for the fashion industry, focusing on using RFID technology to digitize service processes and enhance the sustainability of the fashion lifecycle. By integrating RFIDs, customers can access and manage the entire product development and maintenance process through a personalized login, giving them direct insight into product history, maintenance, and repair services. This approach aims to strengthen the personal connection between consumers and their clothing by offering individualized product development and specialized laundry care services. The authors present a scenario where outdoor jackets are mass-customized and equipped with RFIDs to track and manage individual garment information, promoting sustainable practices through specific laundry care, repair services, and extended product life cycles. Integrating RFID technology in the fashion supply chain offers numerous benefits, including reducing waste, conserving resources, and promoting environmental sustainability. The study suggests that the fashion industry can significantly benefit from digitalization and customer involvement in creating eco-friendly and sustainable product lifecycles.

Hakola et al. [49] investigate the development of smart tags that are sustainable and durable for identity management and condition monitoring in reusable packaging. The study examines four smart tag technologies: laser-engraved 2D barcodes, printed 2D barcodes with temperature indicators, printed NFC tags, and commercial RFID tags. The technologies have been tested for durability against washing and heating, and all have shown excellent durability when protected appropriately. A SWOT analysis has been conducted to evaluate each technology's strengths and weaknesses, considering its use case, technical performance, and recyclability. The research emphasizes the importance of smart tags in facilitating the traceability of items throughout the product lifecycle, which contributes to sustainable packaging solutions. The discussion also addresses the challenges of recycling smart tags, particularly those that contain electronic functionalities or are embedded within packaging materials. This underscores the need for innovative recycling methodologies. The study highlights the potential of smart tags in enabling DPPs for various sectors, which contributes to more sustainable and circular value chains. Due to the occurrence of NFC, this study will also be included in Chapter 3.2.3.

3.2.3 NFC

This chapter presents previous research on NFC tags as data carriers for accessing passport information. Figure 3.3 depicts the PRISMA flow diagram communicating how related work was selected.

To identify relevant studies via databases, this thesis utilized the search term *NFC AND ("Product Passport*" OR "Material Passport*" OR "Building Logbook*").* Additionally, snowballing was employed by searching for *"NFC"* in the titles of references within reports assessed eligible from the initial database search.

During the screening phase, records were excluded that only mentioned NFC tags as an example of a data carrier. Similarly, studies investigating NFC technology in contexts unrelated to object identification were omitted.

Finally, 3 studies were selected as related work. 2 studies [30, 49] were obtained from the database results. 1 study [66] was identified by snowballing. The subsequent paragraphs review these studies and present a summary of their contributions in Table 3.3.

Dervishaj, Hernández Vargas, and Gudmundsson [30] explore how the construction industry can benefit from integrating various tracking technologies such as QR codes, NFC, and Bluetooth Low Energy (BLE) tags with BIM of prefabricated concrete components. This integration can promote the reuse of these components throughout their life cycles. The study identifies NFC as a suitable solution for tagging building components due to its effectiveness in different scenarios, including embedding within concrete at varying depths and attaching to surfaces. NFC offers the ability to store multiple data types, secure communications, low cost, and compatibility with smartphones, making it accessible to many users. Laboratory tests reveal that NFC tags can remain functional under common interior surfaces, indicating their suitability for long-term use in circular construction projects. The research highlights the interoperability of NFC with digital models, enabling the creation of digital twins for precast concrete assets that are updated with new information as needed. Due to the occurrence of QR codes, this study was also covered in Chapter 3.2.1.

Liu and Ma [66] introduce NFC washable labels that allow consumers to access information about their clothes using their smartphones. The labels can store both read-only information manufacturers provide, such as product details and brand stories, and writable information for consumer inputs like clothing evaluations or preferences. After washing, the study tested the labels' durability and readability, confirming their practicality for everyday use and compatibility with current smartphone technology. This innovation opens up exciting possibilities for smart clothing management, offering benefits like personalized clothing care advice, enhanced consumer engagement, and targeted marketing opportunities for brands. The NFC washable labels represent a significant step towards integrating digital technology into textiles, enhancing user experience and operational efficiency in the fashion sector.

Hakola et al. [49] investigate the development of smart tags that are sustainable and durable for identity management and condition monitoring in reusable packaging. The study examines four smart tag technologies: laser-engraved 2D barcodes, printed 2D barcodes with temperature indicators, printed NFC tags, and commercial RFID tags. The technologies have been tested for durability against washing and heating, and all have shown excellent durability when protected appropriately. A SWOT analysis has been conducted to evaluate each technology's strengths and weaknesses, considering its use case, technical performance, and recyclability. The research emphasizes the importance of smart tags in facilitating the traceability of items throughout the product lifecycle,

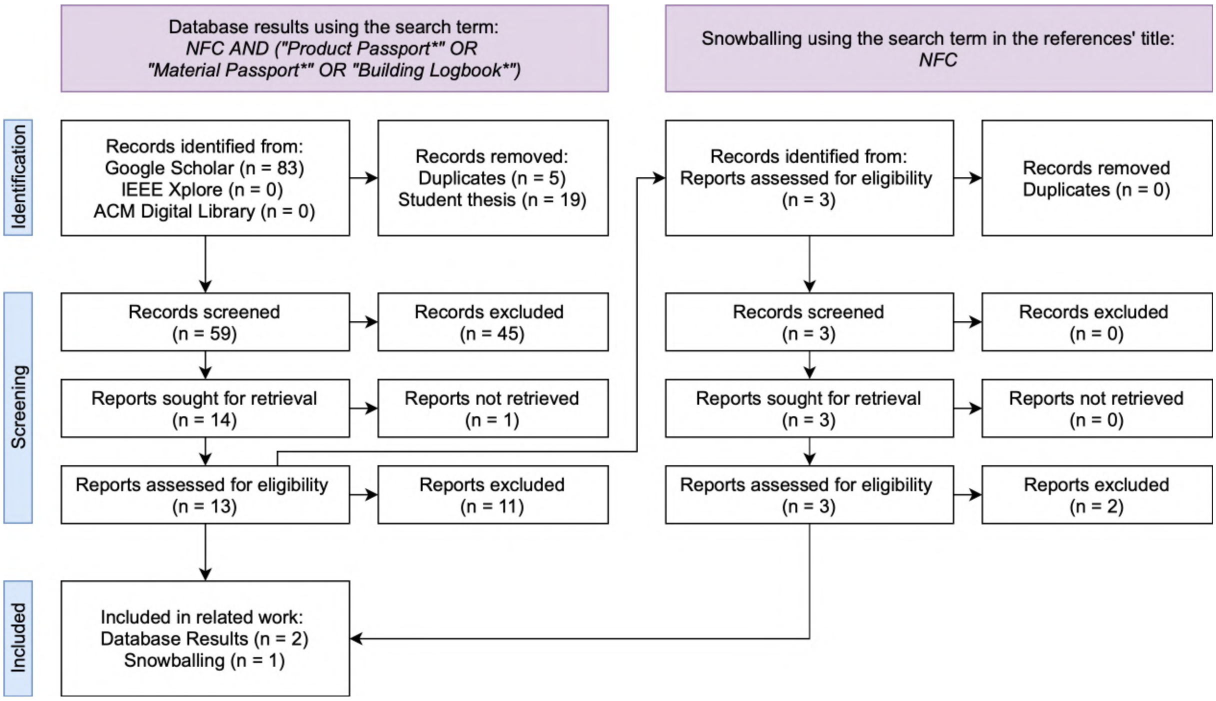


Figure 3.3: PRISMA Flow Diagram for Related Work on NFC (adopted from Page et al. [81])

Industry	**Reference**	**Year**	**Contribution**
Construction	Dervishaj, Hernández Vargas, and Gudmundsson [30]	2023	Utilized NFC tags for BIM integration to facilitate reuse of prefabricated concrete.
Fashion	Liu and Ma [66]	2018	Embedded NFC in clothing labels for accessible wash and care instructions.
Packaging	Hakola et al. [49]	2024	Analyzed the durability of NFC chips in washing and heating for reusable packaging.

Table 3.3: Summary of Related Work on NFC

which contributes to sustainable packaging solutions. The discussion also addresses the challenges of recycling smart tags, particularly those that contain electronic functionalities or are embedded within packaging materials. This underscores the need for innovative recycling methodologies. The study highlights the potential of smart tags in enabling DPPs for various sectors, which contributes to more sustainable and circular value chains. Due to the occurrence of RFID, this study was also covered in Chapter 3.2.2.

3.3 Related Work on Digital Identifiers

This thesis explores the potential of using NFTs, PBTs, and DIDs as digital identifiers for managing passport data and product ownership in a decentralized DPP system. The following chapters will discuss related studies on NFTs and DIDs in conjunction with VCs. Due to the novelty of PBTs, no related studies are available.

3.3.1 NFT

This chapter presents previous research on NFTs as a decentralized object identity and ownership model. Figure 3.4 depicts the PRISMA flow diagram communicating how related work was selected.

To identify relevant studies via databases, this thesis utilized the search term *("Non?Fungible Token" OR "NFT") AND ("Product Passport*" OR "Material Passport*" OR "Building Logbook*")*. Additionally, snowballing was employed by searching for *"Non?Fungible Token"* in the titles of references within reports assessed eligible from the initial database search.

During the screening phase, records were excluded that only mentioned NFTs to implement ownership. Similarly, studies investigating NFTs in contexts unrelated to data access or ownership management were omitted.

Finally, 5 studies were selected as related work. 4 studies [31, 43, 55, 124] were obtained from the database results. 1 study [28] was identified by snowballing. The subsequent paragraphs review these studies and present a summary of their contributions in Table 3.4.

For the construction industry, three related studies were identified. All of them use NFTs within a prototype. Therefore, they will also be covered in Chapter 3.4.

Dounas, Jabi, and Lombardi [31] develop a prototype for applying NFTs to building components for a circular economy in the construction industry. Using blockchain technology, the study proposes a digital infrastructure layer that enables the creation, storage, and management of digital twins for building components, allowing for their tracking, reuse, or recycling. NFTs serve as unique digital identifiers for each building component, linked to their material, structural, and provenance data stored on the blockchain. This information is immutable, secure, and accessible throughout the building components' lifecycle. By embedding carbon performance and supply chain data into the design process through digital twins and NFTs, the study suggests a transformative strategy for achieving sustainability and efficiency in the built environment. The authors claim that

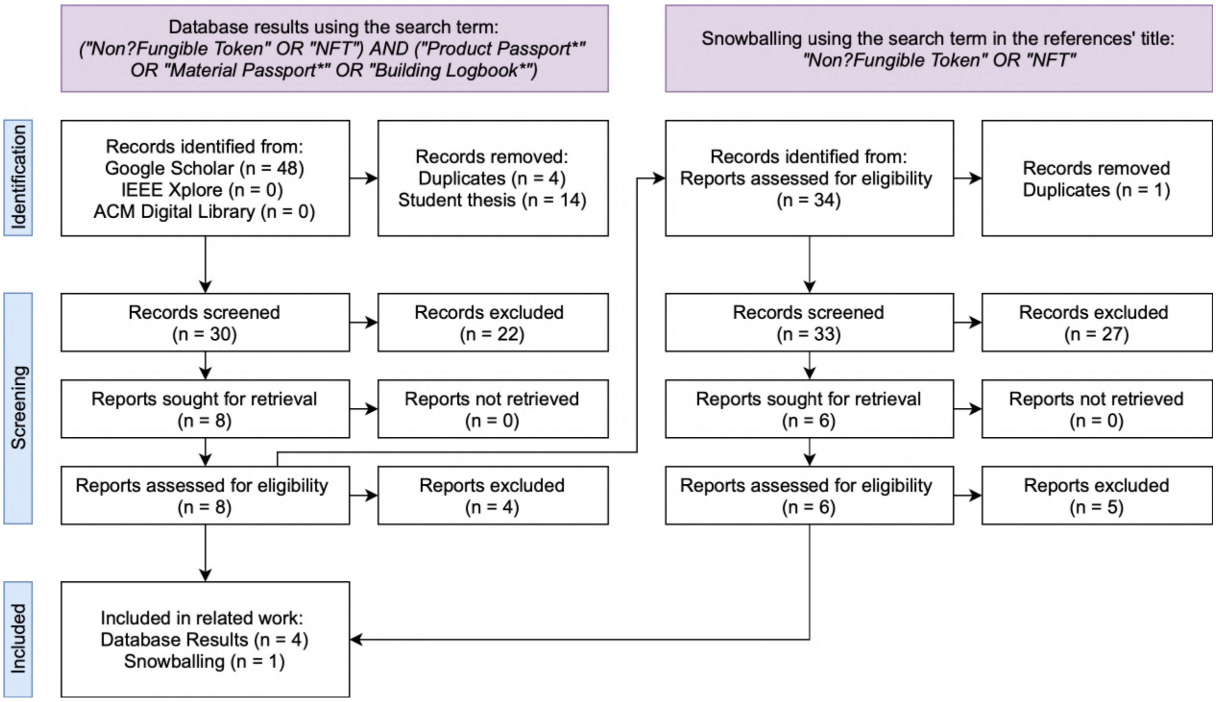


Figure 3.4: PRISMA Flow Diagram for Related Work on NFT (adopted from Page et al. [81])

Industry	Reference	Year	Contribution
Construction	Dounas, Jabi, and Lombardi [31]	2021	Employed NFTs for lifecycle tracking of building components, digitizing ownership, and supporting sustainable practices.
	Hunhevicz et al. [55]	2023	Leveraged NFTs for ownership modeling and token-based MP data access control.
	Wu et al. [124]	2023	Developed NFT-enabled passports for construction waste materials to digitize ownership, facilitate trading, and prevent issue duplication.
Medicine	Gebreab et al. [43]	2022	Utilized NFTs for medical device traceability and ownership management.
All	Davies et al. [28]	2024	Explored NFTs to represent ownership of digital and physical items to enhance sustainable supply chain management.

Table 3.4: Summary of Related Work on NFTs

their digital infrastructure has the potential to create a transparent and global registry for MPs and building components.

Hunhevicz et al. [55] evaluate the potential of Web3 technologies in the construction industry for managing and accessing lifecycle data of building materials. Specifically, the study focuses on MPs and compares the current centralized Web2 approaches to a decentralized Web3 model. The research examines two Web3 access control mechanisms: role-based and token-based, implemented on the Stacks blockchain and Gaia decentralized storage. NFTs were utilized to implement token-based MP access control. The findings suggest that token-based access is more scalable and flexible than role-based access, particularly for the fragmented Architecture, Engineering, and Construction (AEC) industry. However, the study also highlights challenges such as system design, private key management, and industry requirements for data management and calls for further research in this area.

Wu et al. [124] introduce a framework that uses blockchain technology and NFTs to create 'passports' for construction waste materials (CWMs). These passports enable cross-jurisdictional trading of CWMs by providing a unique identification system for each material. The authors developed a prototype of their framework using the permissioned blockchain Hyperledger Fabric. This enables sub-member registration through certificates to control system access and the creation of NFTs as MPs. All trading transactions and MP NFTs, including metadata, are stored on the blockchain. This framework aims to digitize CWMs, increase information transparency, and improve trading efficiency. Additionally, it secures transaction records through the use of blockchain technology. This prototype demonstrates the feasibility and effectiveness of using blockchain and NFTs to support sustainable development and circular economy principles in the construction industry.

Gebreab et al. [43] present an NFT-based system to enhance traceability and ownership management of medical devices. By representing each medical device as a unique digital twin through NFTs, the system provides a reliable method to track the lifecycle of each device, from production and manufacturing to distribution, use, and ownership. The system ensures authenticity and compliance with regulatory standards, using Ethereum smart contracts to verify and authenticate medical devices and mechanisms for issuing certificates of authenticity. It aims to tackle counterfeiting and improve transparency and security in the medical device supply chain. The study concludes by comparing the NFT-based solution with traditional blockchain and tokenless systems, highlighting its cost efficiency, user-friendliness, and adaptability for broader applications beyond medical devices.

Davies et al. [28] assess the potential of NFTs in improving sustainability within supply chains, specifically in the realm of the evolving metaverse. The research examined NFTs through the Technology-Organization-Environment (TOE) framework and highlighted how they could help overcome barriers to blockchain technology adoption in sustainable supply chain management (SSCM). As NFTs can represent ownership of digital and physical items, they provide a new approach to creating "phygital" products. The authors propose that NFTs can incentivize stakeholders to adopt sustainable practices, increase consumer willingness to pay for sustainable products, offer anti-counterfeit measures, and support the growth of circular business models. They introduced the concept of a "Mint-to-Order" production strategy that leverages NFTs for demand-driven manufacturing, reducing waste and overproduction. Finally, the study suggests that NFTs' unique characteristics, such as their ability to verify authenticity and provenance, make them valuable for achieving sustainability goals in supply chains.

3.3.2 DID with VCs

This chapter presents previous research on DIDs with VCs as a decentralized object identity and ownership model. Figure 3.5 depicts the PRISMA flow diagram communicating how related work was selected.

To identify relevant studies via databases, this thesis utilized the search term *("Self? Sovereign Identity" OR "Decentrali?ed Identifier*" OR "Verifiable Credentials") AND (" Product Passport*" OR "Material Passport*")*. Additionally, snowballing was employed by searching for *"Self?Sovereign Identity" OR "Decentrali?ed Identifier*" OR "Verifiable Credentials"* in the titles of references within reports assessed eligible from the initial database search.

During the screening phase, records that only mentioned DIDs or VCs to implement ownership were excluded. Similarly, studies investigating DIDs or VCs in contexts unrelated to data access or ownership management were omitted.

Finally, 2 studies were selected as related work. Both studies [11, 76] were obtained from the database results. The subsequent paragraphs review these studies and present a summary of their contributions in Table 3.5.

Berg et al. [11] discuss how DIDs and VCs can be employed within a DPP for plastic products. The authors propose linking QR codes to digital DIDs and VCs to provide reliable recycling information for individual products. This technology addresses the information gaps and discrepancies in the circular plastics economy. By creating digital twins of physical products through DIDs and improving traceability with VCs, the authors suggest that their proposed system could significantly enhance recycling rates and the sustainability of plastic materials. Due to the use of QR codes, this study is also discussed in Chapter 3.2.1 about QR codes.

Navarro et al. [76] examine the digital transformation of the circular economy by implementing DPPs for ICT devices. Their research focuses on developing a registry to verify DPPs, identifying devices and their components, and promoting their reuse, recycling, and responsible disposal. To ensure transparency, verifiability, and accountability of DPPs for ICT products, DIDs with VCs are used. DIDs uniquely identify ICT devices and link them to their corresponding DPP on a verifiable data registry deployed on a permissioned ledger. VCs are employed to issue and verify credentials related to device actions, proofs, and reports, enabling stakeholders to assert ownership or access rights to specific data within the registry. This study is also related to QR codes in Chapter 3.2.1 and the prototypes of decentralized DPP systems in Chapter 3.4.

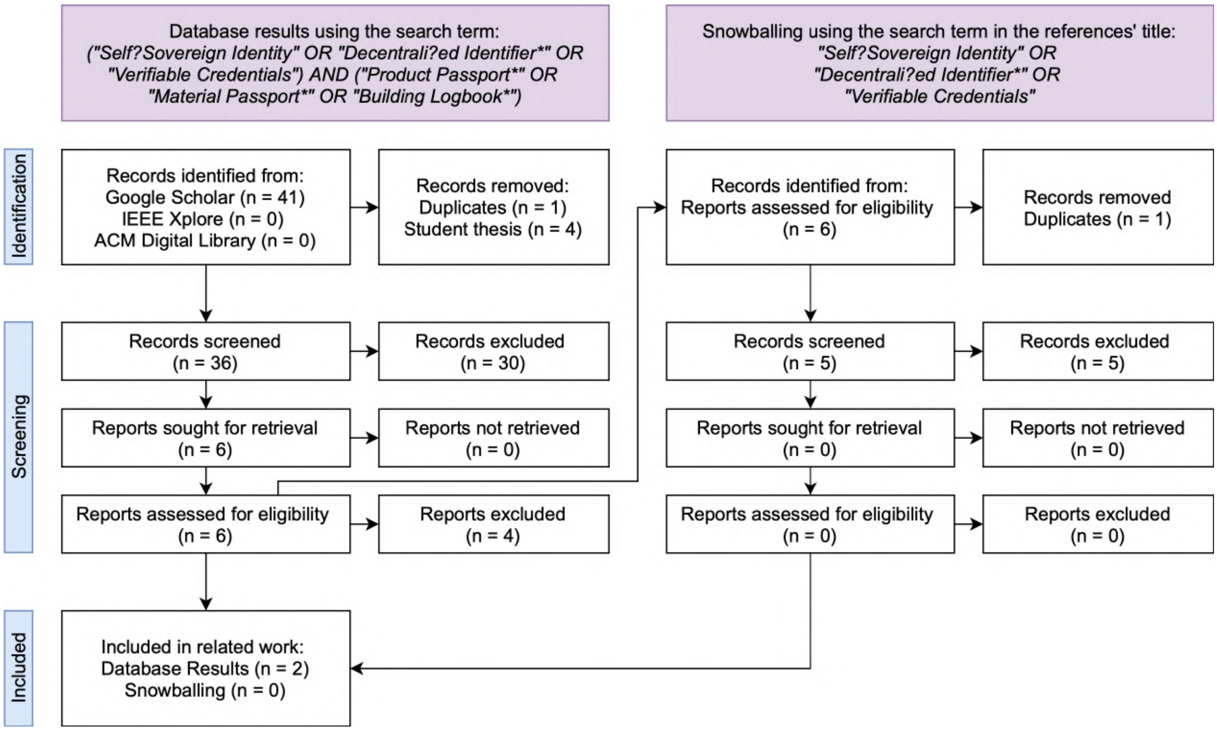

Database results using the search term:
("Self?Sovereign Identity" OR "Decentrali?ed Identifier*" OR "Verifiable Credentials") AND ("Product Passport*" OR "Material Passport*" OR "Building Logbook*")
Snowballing using the search term in the references' title:
"Self?Sovereign Identity" OR "Decentrali?ed Identifier*" OR "Verifiable Credentials"
Identification
Screening
Included
Records identified from:
Google Scholar (n = 41)
IEEE Xplore (n = 0)
ACM Digital Library (n = 0)
Records removed:
Duplicates (n = 1)
Student thesis (n = 4)
Records identified from:
Reports assessed for eligibility
(n = 6)
Records removed
Duplicates (n = 1)
Records screened
(n = 36)
Records excluded
(n = 30)
Records screened
(n = 5)
Records excluded
(n = 5)
Reports sought for retrieval
(n = 6)
Reports not retrieved
(n = 0)
Reports sought for retrieval
(n = 0)
Reports not retrieved
(n = 0)
Reports assessed for eligibility
(n = 6)
Reports excluded
(n = 4)
Reports assessed for eligibility
(n = 0)
Reports excluded
(n = 0)
Included in related work:
Databse Results (n = 2)
Snowballing (n = 0)

Figure 3.5: PRISMA Flow Diagram for Related Work on DID with VCs (adopted from Page et al. [81])

Industry	Reference	Year	Contribution
Plastic	Berg et al. [11]	2022	Suggested using DIDs and VCs to establish DPP ownership for plastic products.
ICT	Navarro et al. [76]	2022	Utilized DIDs and VCs for ICT device DPPs to digitize ownership and access, ensuring transparency, verifiability, and accountability.

Table 3.5: Summary of Related Work on DID with VCs

3.4 Prototypes of Decentralized DPP Systems

This chapter is dedicated to related studies on prototypes of decentralized DPP systems. Figure 3.6 depicts the PRISMA flow diagram communicating how related work was selected.

To identify relevant studies via databases, this thesis utilized the search term *Prototype AND ("Blockchain" OR "Decentrali?ed" OR "Distributed*File*") AND ("Product Passport*" OR "Material Passport*" OR "Building Logbook*").* Additionally, snowballing was employed by searching for *Prototype AND ("Blockchain" OR "Decentrali?ed" OR "Distributed*File*")* in the titles of references within reports assessed eligible from the initial database search.

During the screening phase, records showing prototypes in contexts unrelated to decentralized DPP systems were excluded.

Finally, 5 studies were selected as related work. All 5 studies [31, 55, 76, 79, 124] were obtained from the database results. The subsequent paragraphs review these studies and present a summary of their contributions in Table 3.6.

For the construction industry, three related studies were identified. They all include NFTs and were therefore covered in Chapter 3.3.1.

Dounas, Jabi, and Lombardi [31] introduce a prototype for applying NFTs to building components for a circular economy in the construction industry. It uses a combination of Topologic, a topology software library, the Ethereum blockchain for smart contracts, and the IPFS for storing additional metadata. The prototype translates building components into a digital format that can be securely and immutably recorded on the blockchain, facilitating the reuse and tracking of materials. It demonstrates the process using a simple house model, highlighting the potential for creating a transparent, global registry for MPs and building components to support sustainable development and circular economy practices in architecture and construction.

Hunhevicz et al. [55] developed a prototype implementation that showcased the use of Web3 technology to manage data access in the construction industry, focusing on an MP use case. The prototype utilized Stacks blockchain smart contracts and Gaia as decentralized data storage, providing decentralized access control. The results revealed that token-based access is more scalable and flexible than role-based access, making it advantageous for the fragmented AEC industry. The prototype enables the creation of access tokens without assigning specific roles to stakeholders, which has the potential to facilitate a decentralized marketplace for data access. The study also identified challenges such as system design, private key management, and industry requirements for data management, highlighting the need for further research in this area.

Wu et al. [124] introduce a framework that uses blockchain technology and NFTs to create 'passports' for construction waste materials (CWMs). These passports enable cross-jurisdictional trading of CWMs by providing a unique identification system for each material. The authors developed a prototype of their framework using the permissioned blockchain Hyperledger Fabric. This enables sub-member registration through certificates to control system access and the creation of NFTs as MPs. All trading transactions and MP NFTs, including metadata, are stored on the blockchain. This framework aims to digitize CWMs, increase information transparency, and improve trading efficiency. Additionally, it secures transaction records through the use of blockchain technology. This

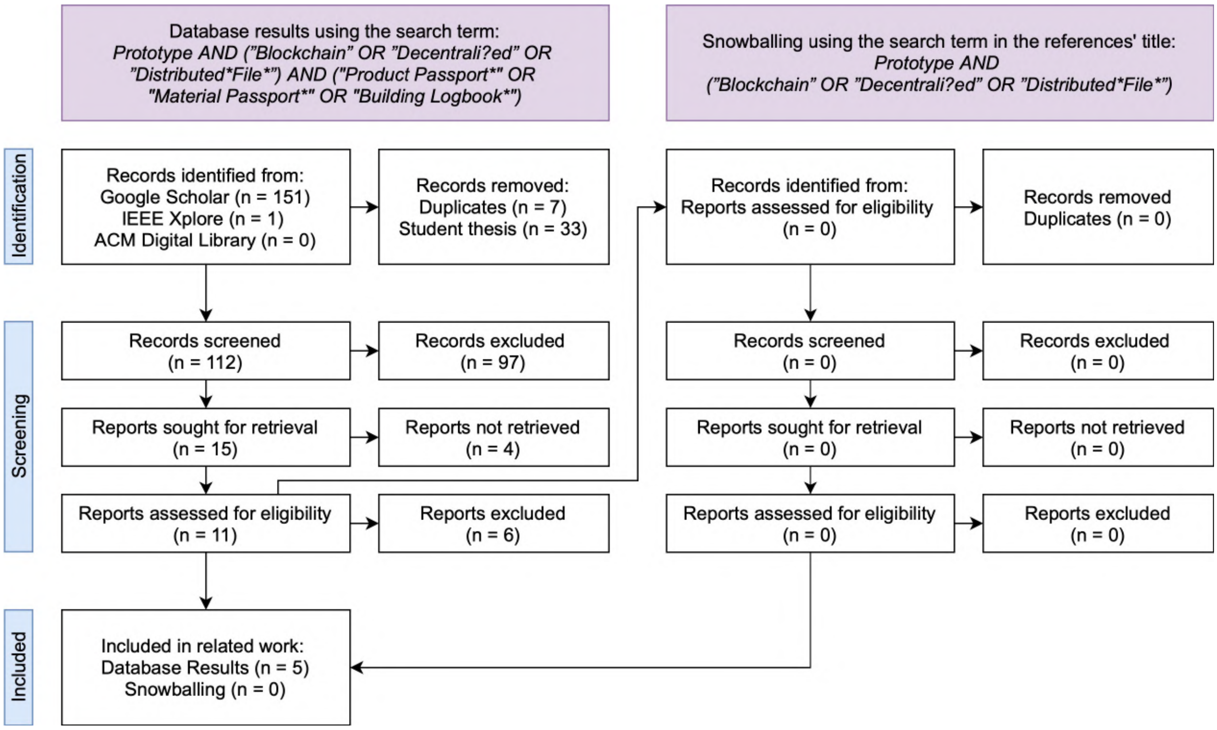

Database results using the search term:
Prototype AND ("Blockchain" OR "Decentrali?ed" OR "Distributed*File*") AND ("Product Passport*" OR "Material Passport*" OR "Building Logbook*")
Snowballing using the search term in the references' title:
Prototype AND ("Blockchain" OR "Decentrali?ed" OR "Distributed*File*")
Identification
Screening
Included
Records identified from: Google Scholar (n = 151) IEEE Xplore (n = 1) ACM Digital Library (n = 0)
Records removed: Duplicates (n = 7) Student thesis (n = 33)
Records screened (n = 112)
Records excluded (n = 97)
Reports sought for retrieval (n = 15)
Reports not retrieved (n = 4)
Reports assessed for eligibility (n = 11)
Reports excluded (n = 6)
Records identified from: Reports assessed for eligibility (n = 0)
Records removed Duplicates (n = 0)
Records screened (n = 0)
Records excluded (n = 0)
Reports sought for retrieval (n = 0)
Reports not retrieved (n = 0)
Reports assessed for eligibility (n = 0)
Reports excluded (n = 0)
Included in related work: Database Results (n = 5) Snowballing (n = 0)

Figure 3.6: PRISMA Flow Diagram for Related Work on Prototypes of Decentralized DPP Systems (adopted from Page et al. [81])

Industry	**Reference**	**Year**	**Contribution**
Construction	Dounas, Jabi, and Lombardi [31]	2021	Introduced a prototype for a topology data MP using Topologic, Ethereum smart contracts and NFTs, and the IPFS for storing NFT metadata.
	Hunhevicz et al. [55]	2023	Presented a prototype for Web3-based data access in building MPs, employing Stacks smart contracts and Gaia decentralized storage.
	Wu et al. [124]	2023	Developed an NFT-enabled prototype for creating 'passports' for construction waste material using Hyperledger Fabric and on-chain metadata storage.
ICT	Navarro et al. [76]	2022	Created a DPP prototype including a mobile Android application as client software, a verifiable registry API provider as the backend, and a permissioned DLT that handles verification.
All	Nowacki, Sisik, and Angelopoulos [79]	2023	Proposed a framework and technical prototype architecture for DPPs utilizing IOTA as DLT and IOTA Smart Contracts.

Table 3.6: Summary of Related Work on Prototypes of Decentralized DPP Systems

prototype demonstrates the feasibility and effectiveness of using blockchain and NFTs to support sustainable development and circular economy principles in the construction industry.

Navarro et al. [76] examine the digital transformation of the circular economy by implementing DPPs for ICT devices. Their research focuses on developing a registry to verify DPPs, identifying devices and their components, and promoting their reuse, recycling, and responsible disposal. To achieve this, they have created a prototype that includes registering ICT devices, generating and verifying DPPs, and producing verifiable ICT device reports. The system comprises a mobile Android application as client software, a verifiable registry API provider as the backend, and a permissioned DLT that handles verification. By scanning a QR code on the ICT device, the client software sends a proof request to the backend to verify the device and retrieve its hardware details. The backend provides a set of operations that interact with the smart contracts running on a permissioned DLT. The authors propose running DLT nodes based on Ethereum Geth or Hyperledger Besu on a local standalone setup or as part of the Alastria network. The initiative aims to improve sustainability by enabling better tracking and managing ICT devices throughout their lifecycle. This study is also related to the work on QR codes in Chapter 3.2.1 and DID with VCs in Chapter 3.3.2.

Nowacki, Sisik, and Angelopoulos [79] present a system architecture for DPPs integrating IoT devices, IOTA as DLT, and Smart Contracts. It aims to address the challenges of standardizing DPP systems across various market sectors, facilitating the transition to a circular economy. The authors have also developed a working prototype for this architecture. After a unique identifier is generated, the data from IoT devices associated with the identifier is saved to the IOTA network. Users can access the DPPs through frontend applications or services powered by Python backend and cache servers. The backend services provide further authorization, data processing, and a gateway to update or generate functionality for authorized personnel. Meanwhile, cache services reduce calls to IOTA nodes and provide faster data to frontend applications or services. The research demonstrates the potential for DPPs to enhance sustainability and regulatory compliance in manufacturing and supply chains. However, the authors also mention privacy and authentication as potential weaknesses to be addressed.

3.5 Discussion on Related Work

The previous chapters reviewed academic literature related to this thesis. Figure 3.7 presents a Venn diagram summarizing related work within the construction industry. It depicts the distribution and overlap among selected topics. Figure 3.8 shows the same information for industries outside of construction.

Related studies outside the construction industry are only related to the term *Product Passport*. Notably, the amount of those studies is well-balanced compared to the construction industry. Research on QR codes and RFID tags is significantly more advanced in the construction industry than NFC chips. It is also important to note the absence of

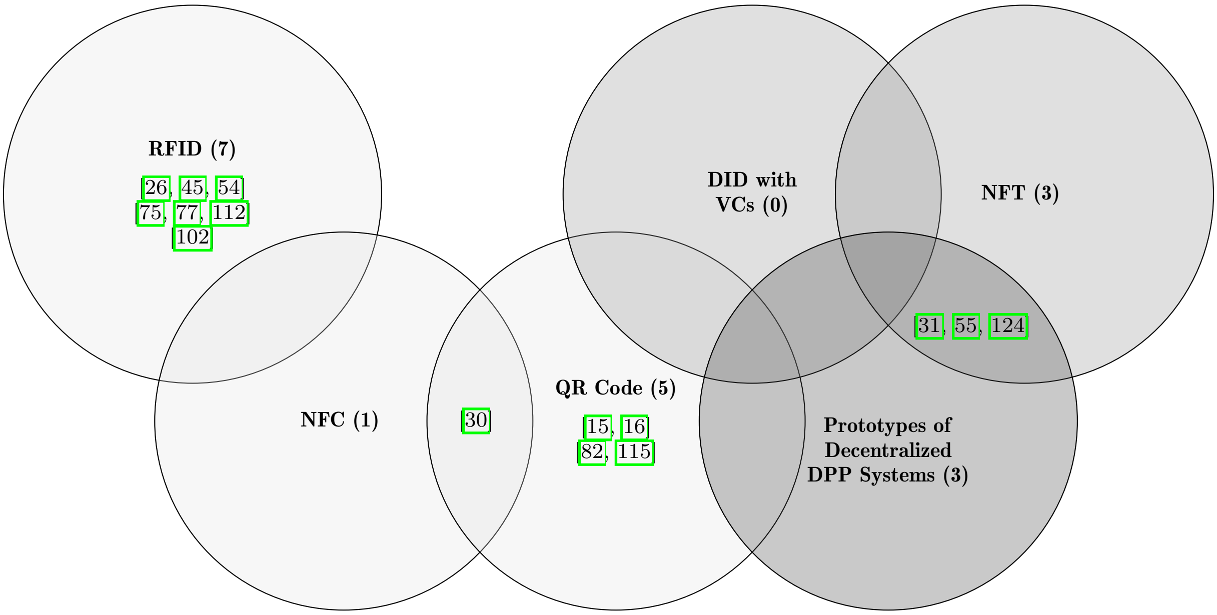


Figure 3.7: Distribution of Related Work By Topics in Construction Industry

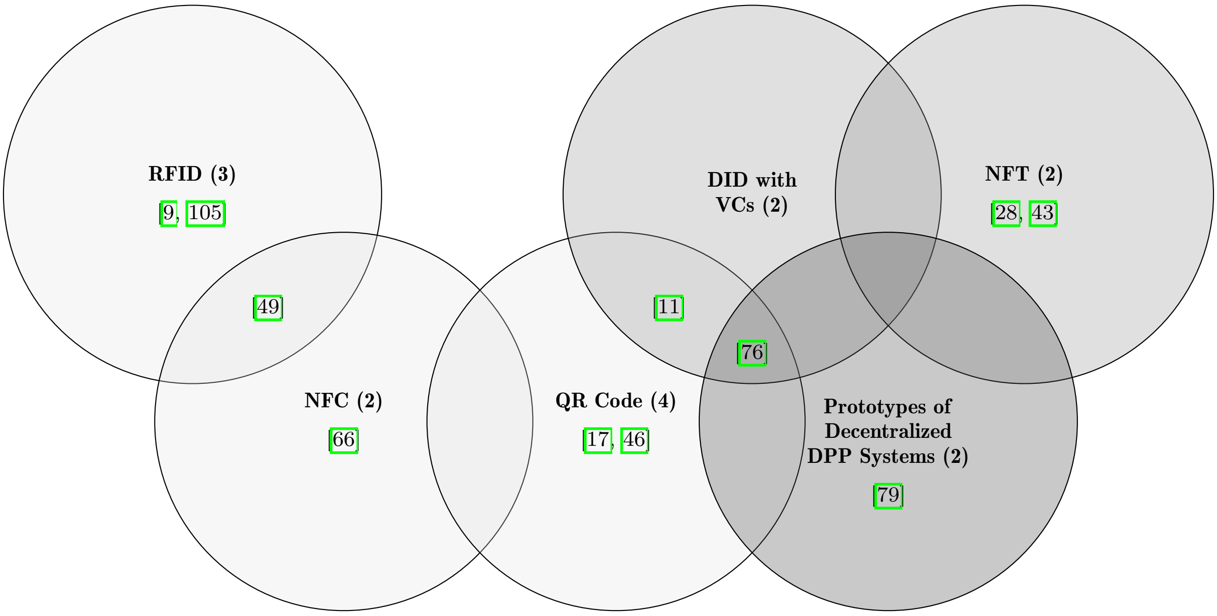


Figure 3.8: Distribution of Related Work by Topics in Non-Construction Industries

studies related to DID with VCs and prototypes of decentralized DPP systems that utilize a data carrier. However, NFTs combined with decentralized DPP system prototypes appear promising and have already begun to be explored.

The following research gaps were identified, which this thesis aims to address:

- **Unexplored Design and Implementation of Decentralized DPP Systems Integrating Data Carriers:** Nowacki, Sisik, and Angelopoulos [79] only propose a theoretical framework and technical architecture, while the other papers also include prototype implementation of decentralized DPP systems. Three studies use NFTs [31, 55, 124], and one uses DIDs and VCs [76]. However, none incorporate data carriers for passport data access in their design or implementation.

- **Lack of Comparative Analysis of NFTs, PBTs and DIDs as Digital Identifiers in a DPP System:** PBTs are a new concept, with no studies exploring their potential as digital identifiers within a DPP system. NFTs have been investigated in five studies: three in the construction industry [31, 55, 124] and two outside it [28, 43]. For DIDs, two studies outside the construction sector examine their use in a DPP context [11, 76]. Thus, while individual digital identifiers have been explored to some extent, no comparative analysis presents their relative benefits and drawbacks for managing passport data and product ownership.

- **Lack of Comparative Analysis of QR Codes and NFC Chips for Accessing Passport Data in a DPP System:** NFC chips are underexplored, with only three studies investigating them, compared to 10 studies on RFID tags and 9 on QR codes. Comparative analyses between these data carriers are scarce. Hakola et al. [49] compared NFC and RFID technology for identity management and condition monitoring of reusable packages, focusing on durability and recyclability. Only one study by Dervishaj, Hernández Vargas, and Gudmundsson [30] compares QR codes and NFC for tracking and tracing construction products. Thus, a clear research gap exists in comparing QR codes and NFC chips for accessing DPP data within a DPP system.

Chapter 4

Design

This chapter outlines the decentralized DPP system prototype design in three sections. First, it delves into the prototype's requirement elicitation. Second, it describes the prototype's architecture, including the necessary components and their interactions. Finally, it explains the workflows, illustrating the theoretical implementation of functional requirements within the architecture using UML sequence diagrams. This prototype is called *PermaPass* to emphasize the essential need for permanent passports in circular construction.

4.1 Requirements

This section consists of theoretical DPP system requirements and the prototype requirements. As no related work on decentralized DPP system prototypes included a requirement analysis, the prototype requirements were derived from theoretical DPP system requirements.

4.1.1 DPP System Requirements

The presented requirements in this section are primarily based on the structured study by Jansen et al. [59], which identified requirements based on stakeholder involvement and current literature from science and industry. These requirements were categorized according to the ISO/IEC 25010:2011 [58] regarding system and software quality requirements and assessment, as summarized in Table 4.1. Although these requirements are identified at a general level for DPP systems across any industry, they can be applied to the construction industry. Construction-related literature has supported and elaborated on these requirements, with almost all requirements backed by a construction-related study conducted by Buchholz and Lützkendorf [13]. Individual requirements were supported by specific research in the built environment.

Category	Requirement	Sources
Accessibility	R1 – Enable users to access passport information. R2 – Define and enforce access control rules. R3 – Allow system use without extra technical setups.	[13, 53] [13, 47] [47, 59]
Availability	R4 – Provide timely access to passport data. R5 – Guarantee long-term data and system access.	[13, 59] [48, 55]
Security	R6 – Secure data storage and exchange. R7 – Verify passport information authenticity.	[11, 13, 47, 59] [11, 13, 47, 48, 59, 124]
Interoperability and Portability	R8 – Use standardized or agreed-upon data schemas and data carriers. R9 – Offer APIs for data transferability. R10 – Allow data carriers to connect to various data source systems.	[11, 13, 53, 59] [11, 13, 48, 53, 59] [11, 13, 48, 53, 59]
Modularity and Modifiability	R11 – Support user and passport creation, update, and removal. R12 – Facilitate system expansion for international adaptation.	[13, 47, 59] [11, 59]
Legal Obligation	R13 – Comply with ESPR and GDPR.	[59]

Table 4.1: Summary of DPP System Requirements

4.1.1.1 Accessibility

Accessibility refers to the extent to which individuals with diverse characteristics and abilities can utilize a system to achieve a specific goal in a specific use context [58, 59].

To achieve accessibility, the system must provide permanent access to passport data [13, 53].

The composition and supply chain of a construction product can be a closely guarded company secret and competitive advantage of a company. Therefore, access control mechanisms are a requirement such that members of the DPP system must only have access to the information they need, resulting in appropriate access authorizations [13, 47].

The system must be accessible without requiring additional technical infrastructure to include all economic actors. In many countries, small and medium-sized companies operate with smartphones instead of having an internal information system. Therefore, implementing DPP systems accessible only via systems interfaces is not a feasible option [47, 59].

4.1.1.2 Availability

Availability refers to the extent to which individuals can access specific information or resources provided by a system under certain conditions [59].

First, the system must provide timely access to passport data, offering real-time or up-to-date information as required by the user's needs [13, 59].

The construction industry is known for its long-lasting nature; buildings and their components typically have an average use phase of 60 years [32], with some individual elements lasting up to 100 years [103]. Therefore, DPP systems for circular construction must ensure long-term system and data availability [48, 55].

4.1.1.3 Security

Security refers to the extent to which a system protects information to ensure appropriate access based on authorization levels. [58].

The secure storage of data and the protected exchange of data among the members of a construction product's value chain are crucial functions of a DPP system for safeguarding intellectual property [11, 13, 47, 59].

Since digital data can be easily copied and modified, a DPP system must ensure the authenticity of passport information. Authentic data is complete, accurate, and trustworthy. To implement accuracy and completeness Buchholz and Lützkendorf [13] suggest regularly conducted quality controls as a requirement. To implement trustworthiness, it is necessary to record and track data changes to verify the data, prevent users from denying transactions, and ensure that data cannot be modified without detection [11, 13, 47, 48, 59, 124].

4.1.1.4 Interoperability and Portability

Interoperability refers to the extent to which two or more systems can exchange information and use the exchanged information [58]. Portability refers to the extent to which a system can be effectively and efficiently transferred from one piece of hardware, software, or other IT system to another [58]. Whereas interoperability concerns the exchange of information between different systems, portability concerns the future replacement of a system or its parts. Portability is hardly distinguishable from interoperability in purely DPP systems, as transferring passport information is the main concern. However, portability becomes crucial for cyber-physical DPP systems that utilize physical identifiers linked to digital product information. This is because the transfer of information needs to include the physical identifiers and the links to product information [59].

Shared semantics are crucial for ensuring a clear understanding of the system's functionality, facilitating smoother interactions, and enhancing system transferability. To achieve this, passport data schemas must be standardized or widely accepted, which helps organize data more coherently. Specifically, adopting standardized physical identifiers in cyber-physical DPP systems is imperative. These identifiers should be consistently referenced and harmonized across the EU to ensure seamless integration and interoperability [11, 13, 53, 59].

Offering an API for data provision and requests is essential for promoting interoperability and enhancing portability. With an API, passport information can be seamlessly exchanged among various systems of different stakeholders [11, 13, 48, 53, 59].

When developing cyber-physical DPP systems, ensuring that product identifiers are compatible with various digital platforms is pivotal. Consequently, these identifiers must be designed to function with multiple independent systems that store and provide passport information [11, 13, 48, 53, 59].

4.1.1.5 Modularity and Modifiability

Modularity and modifiability refer to the extent to which a system is structured into distinct components, such that a change to one component has minimal impact on other components. Modifiability focuses on organizing the system into separately manageable units, while modifiability concerns the ease with which the system can be changed. A thoughtfully designed modular system generally promotes easier modification [58, 59].

The built environment is characterized by many actors who frequently change in an extremely fragmented supply chain. The relevant attributes of construction products delivered by the passport constantly evolve. Therefore, DPP systems require the flexibility to create, update, and remove users, passports for construction products, and passport data [13, 47, 59].

DPP systems designed for circular construction must be easily expandable and prepared for broader international use. Implementing these systems as modular frameworks allows for seamless adjustments, accommodating a growing number of users and passports efficiently [11, 59].

4.1.1.6 Legal Obligations

A circular construction DPP system must comply with existing and emerging regulations and standards [59]. This includes the EC's "Proposal for the new Ecodesign for Sustainable Products Regulation" (ESPR) [23] introduced in March 2022. This document outlines mandatory and voluntary information requirements for DPPs. Furthermore, the General Data Protection Regulation (GDPR), effective May 2018, governs data privacy and the handling of personal data within the EU, impacting DPP systems that process personal information.

4.1.2 Prototype Requirements

This section discusses the functional and non-functional requirements for *PermaPass*. These requirements were derived from the DPP systems' requirements presented in the previous chapter. Initially, all requirements were assessed for feasibility and relevance within the context of this thesis. The following requirements were excluded due to infeasibility or irrelevance:

- **R4 – Provide timely access to passport data:** The lack of standardized data schemas for construction products creates uncertainties about the timeliness of data access. Defining real-time or up-to-date data, identifying who needs access, and specifying these terms would be time-consuming. While data availability remains essential, the immediacy of data will not be considered for *PermaPass*.

- **R6 – Secure data storage and exchange:** Since *PermaPass* is a proof-of-concept rather than a production system, this security feature is irrelevant.

- **R8 – Use standardized or agreed-upon data schemas and data carriers:** Currently, no standardized data schema exists, so an assumed data schema will include the necessary construction product properties.
- **R9 – Offer APIs for data transferability:** Providing APIs for data transferability is not the purpose of this prototype, as it is not intended to be a production system.
- **R10 – Allow data carriers to connect to various data source systems:** Integrating multiple data source systems without a common data schema is impractical and subject to change, making this requirement overly time-consuming.
- **R12 – Facilitate system expansion for international adaptation:** This requirement is beyond the prototype's scope, suggesting future projects might explore this expansion.
- **R13 – Comply with ESPR and GDPR regulations:** Compliance with these legal requirements demands legal expertise outside the scope of this thesis.

Consequently, the remaining requirements (R1, R2, R3, R7, R5, R8, and R11) were refined into specific functional and non-functional requirements, as presented in the following sections.

4.1.2.1 Functional Prototype Requirements

Functional requirements specify what a system should do. They describe the various interactions between the system and its users or other systems, detailing its behavior in particular situations. They refer to the system's functions or features.

The following DPP system requirements were used to specify functional requirements for *PermaPass*:

- **R1 – Enable users to access passport information:** Implement functionality to read passports.
- **R2 – Define and enforce access control rules:** Provide functionality for passport owners to control reading access, allowing owners to grant or revoke access. Access control can also mean that update or deletion functionalities should be restricted. For *PermaPass*, it was assumed that only the passport owners should be authorized to update or delete their passports. Due to time constraints, implementing control over passport read access was deemed excessively time-consuming and was not included in this prototype.
- **R7 – Verify passport information authenticity:** Allow users to verify passport authenticity by showing passport modification history.
- **R11 – Support user and passport creation, update, and removal:** Allow users to independently manage access to the system and provide the functionality to create, update, or delete passports.

Table 4.2 summarizes the functional prototype requirements and origins from Table 4.1.

Functional Requirement	Origin
Allow users to read passports.	R1
Allow users to read passport modification history.	R7
Allow users to create passports.	R11
Allow passport owners to update their passports.	R2, R11
Allow passport owners to delete their passports.	R2, R11

Table 4.2: Functional Requirements of *PermaPass*

4.1.2.2 Non-Functional Prototype Requirements

Non-functional requirements describe how systems execute functionality. They specify criteria that can be used to judge the operation of a system rather than specific behaviors. These requirements refer to the system's quality attributes or characteristics.

The following DPP system requirements were used to specify non-functional requirements for *PermaPass*:

- **R3 – Allow system use without extra technical setups:** The system must be accessible via common smartphones, which are widespread and capable of reading HaLo NFC chips and QR codes.
- **R5 – Guarantee long-term data and system access:** Since individual building elements can last up to 100 years [103], *PermaPass* must ensure data availability for that duration.
- **R8 – Use standardized or agreed-upon data schemas and data carriers:** HaLo NFC chips and QR codes are standardized data carriers. This requirement will be implicitly fulfilled.

Table 4.3 summarizes the non-functional prototype requirements and origins from Table 4.1.

Non-Functional Requirement	Origin
The system must be accessible via common smartphones.	R3
The system and its data must be available for at least 100 years.	R5
The system must incorporate HaLo NFC chips and QR codes linking to passports.	R8

Table 4.3: Non-Functional Requirements of *PermaPass*

4.2 Architecture

This chapter details the architecture of *PermaPass*, which comprises six main components: users, data carriers, a user interface, a wallet app, a distributed ledger, and a decentralized storage provider.

Due to the objectives of this thesis, the following components are inherently given:

- **Users:** *PermaPass* is designed to manage and interact with construction product passports for users such as building owners, manufacturers, or architects.
- **Data Carriers:** To explore the potential of QR codes and HaLo NFC chips for linking to construction passports, those data carriers must be incorporated.
- **Distributed Ledger:** NFTs, PBTs, and DIDs are used as digital identifiers for construction products, with a requirement for data availability for at least 100 years. Therefore, *PermaPass* must include DLT, which these identifiers rely on.

However, these three components alone are insufficient. The following additional components are required to meet all *PermaPass* requirements:

- **User Interface:** A user interface is necessary for users to access *PermaPass*, with a requirement for smartphone accessibility.
- **Software Wallet App:** Transactions on distributed ledgers that change data and state require a wallet address signature to confirm gas fee payment. Creating, updating, and deleting passports are examples of state-changing transactions that need this signature. Implementing this functionality is beyond the scope of this thesis, so the architecture of *PermaPass* relies on existing software wallet apps. These apps can manage wallet addresses, securely store private keys, and sign distributed ledger transactions.
- **Decentralized Storage Provider:** Storing passport data as QR codes or on HaLo NFC chips is impractical due to their limited data capacity. This approach would only allow minimal passport data to be linked and completely detaches the data carrier from the product's digital identifier. Instead, the data carrier will store a pointer linking to passport metadata. This metadata contains the passport type (NFT, PBT, DID) and instructions on retrieving the digital identifier from a distributed ledger. Passport data, such as product name, manufacturer, and warranty, can be retrieved via digital identifier.

  Storing passport data on a digital identifier is impractical. NFTs, PBTs, and DIDs are designed to model unique and verifiable identifiers, not to store extensive data. For example, the ERC-721 standard for NFTs on Ethereum [35] recommends using third-party services to store attached data. Additionally, blockchains are expensive, slow, and limited in the data types they can store (e.g., Ethereum cannot store images). Therefore, *PermaPass* connects digital identifiers to passport data using a pointer to the passport data storage location.

  Consequently, passport metadata and data must be stored on a separate component. To meet the requirement of data accessibility for at least 100 years, a decentralized storage provider is essential, as centralized providers like centralized databases or cloud providers such as AWS or Microsoft Azure do not guarantee such long-term accessibility.

Figure 4.1 summarizes the architecture and interaction of these six components, along with the technologies chosen for the user interface, DLT, wallet app, and decentralized storage provider. The following paragraphs will explain the reasons behind each technology choice.

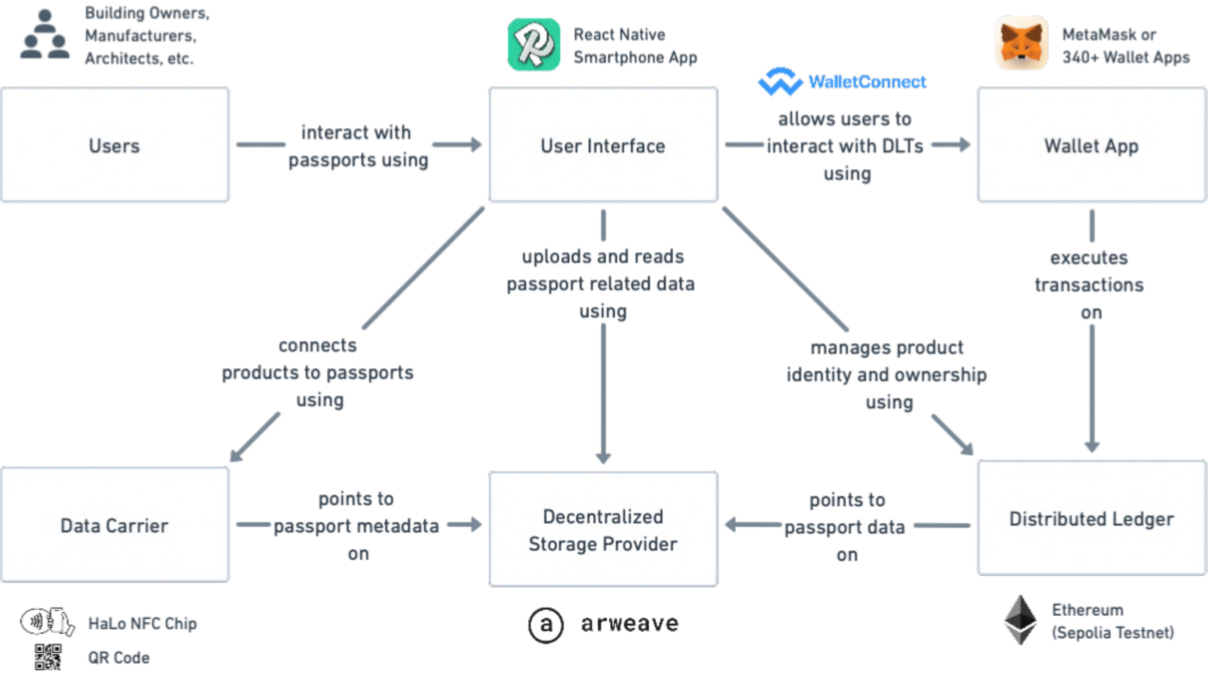

Building Owners, Manufacturers, Architects, etc.
React Native Smartphone App
MetaMask or 340+ Wallet Apps
WalletConnect
Users
interact with passports using
User Interface
allows users to interact with DLTs using
Wallet App
uploads and reads passport related data using
executes transactions on
connects products to passports using
manages product identity and ownership using
Data Carrier
points to passport metadata on
Decentralized Storage Provider
points to passport data on
Distributed Ledger
HaLo NFC Chip
QR Code
arweave
Ethereum (Sepolia Testnet)

Figure 4.1: Architecture and Technology Choices of *PermaPass*

4.2.1 User Interface – React Native Smartphone App

To meet the non-functional requirement that *PermaPass* must be accessible via a common smartphone, there are two options: developing a website or a native smartphone app. As shown in Figure 4.1, the user interface interacts with data carriers (QR codes and HaLo NFC chips), the decentralized storage provider, the distributed ledger, and a wallet app. Code libraries can be included in websites and native apps to connect to decentralized storage providers or distributed ledgers. However, the interaction with wallet apps and data carriers differs between these options.

Integrating wallet apps with websites is complicated and user-unfriendly. Standard browser apps on iOS and Android cannot connect to native wallet apps on the same device. Users must first open the wallet app and then visit the website within the wallet app's built-in browser, which is highly unintuitive. Conversely, a native smartphone app can directly request a connection to the wallet app.

Interacting with data carriers like QR codes and NFC chips is also more straightforward with native apps. Using a website, accessing the camera to read QR codes is more time-consuming to implement, and interacting with NFC chips is not supported by all browsers (e.g., iOS Safari). Native apps, however, can easily access the camera and NFC functionality on all common smartphones.

In conclusion, using a website as the user interface is less user-friendly, more complex, and impractical for NFC chip interactions. Therefore, the decision was made to develop a native smartphone app. The author's familiarity with React and the ability to use a single codebase to generate both iOS and Android apps led to the choice of React Native for implementation.

4.2.2 Distributed Ledger – Ethereum (Sepolia Testnet)

In the architecture of *PermaPass*, a distributed ledger manages product identities and ownerships using smart contracts. Hence, the ledger must support writing and deploying customized smart contracts to implement this functionality.

The Ethereum ecosystem was chosen because it includes the Solidity programming language [94]. This language facilitates customized smart contract coding, and various utility libraries expedite development.

Furthermore, the Ethereum ecosystem uniquely defines a smart contract standard, ERC-5791, for PBTs [1]. NFTs also adhere to an established standard, ERC-721, for EVM chains [35]. These standards ensure interoperability and simplify the implementation of PBTs and NFTs. Libraries providing basic implementations of the PBT [65] and NFT [80] standards accelerate development and offer guidance on their implementation.

Additionally, EVM-compatible chains are advantageous because Veramo (formerly uPort) maintains a DID method specification [109]. Veramo's Ethr-DID Library [111] enables using Ethereum addresses as fully self-managed DIDs, facilitating the creation and updating of Ethr-DIDs. This specification and library significantly support the implementation of *PermaPass*.

The choice of the specific EVM-compatible blockchain was critical. Given that the productive version of *PermaPass* is most likely intended for the Ethereum mainnet, a blockchain closely simulating such an environment was necessary for meaningful evaluation without investing fiat money to pay for gas fees. The Sepolia Testnet was chosen as it closely mimics the Ethereum mainnet, allowing developers to test applications and smart contracts in a risk-free environment before mainnet deployment. Sepolia ETH, the native cryptocurrency, is used to pay for transactions, similar to how ETH is used on the Ethereum mainnet. Every 24 hours, a limited amount of Sepolia ETH can be freely obtained by Sepolia faucets [4].

4.2.3 Software Wallet App – WalletConnect

Many software wallet apps, such as MetaMask [71], Trust [107], and Rainbow Wallet [85], are available for smartphones. WalletConnect [120] provides developers with tools to facilitate wallet connections, allowing users to connect to approximately 340 wallet apps. This makes it a popular choice for modern applications to connect with users' software wallet apps.

WalletConnect offers a software development kit in React Native [119], which will be used to implement the user interface. This choice simplifies wallet connections and allows users to connect to their preferred wallet app, which may already be installed on their smartphone.

4.2.4 Decentralized Storage Provider – Arweave

In recent years, the Interplanetary File System (IPFS) [56] has become a popular choice for storing NFT metadata decentralized. Alongside IPFS, various DLTs have been developed to efficiently store large amounts of data files in a decentralized manner. Arweave [6], Filecoin [42], Storj [100], Sia [93], and BitTorrent [12] are among the most popular and established decentralized ledgers that focus on providing decentralized storage [72, 92].

After comparing the available options, Arweave was selected for its focus on permanent data storage, aiming to meet data availability requirements for at least 100 years. Arweave offers sustainable storage for any file type, guaranteeing storage for at least 200 years. It compensates individuals with the Arweave Token (AR) for hosting data on their blockweave network to incentivize long-term storage. Users pay a one-time fee in AR to store their files permanently, covering initial storage costs for 200 years and contributing to an endowment for future storage. Despite historical data storage costs falling by an average of 30.5% per year, Arweave conservatively assumes a decline rate of just 0.5% annually. This conservative estimate and the endowment system ensure the network's economic viability for centuries [6, 96].

4.3 Workflows

Given the prototype architecture, this section suggests workflows to implement the functional prototype requirements. First, common sequences for various passport actions will be outlined, followed by detailed workflows for each functional requirement.

4.3.1 Shared Sequences

The processes for creating, reading, updating, and deleting passports rely on shared sequences: wallet connection establishment, blockchain transaction execution, and HaLo NFC chip signature creation. To enhance readability, these common sequences are described here and will not be repeated in subsequent sections.

Figure 4.2 illustrates the sequence for connecting a wallet to the *PermaPass* App. The process begins with the user initiating a wallet connection request via the *PermaPass* App. This request is forwarded to the user's Wallet App through the WalletConnect interface. The Wallet App prompts the user to approve or reject the connection request. If approved, the Wallet App acts as the signer within the *PermaPass* App, confirming the wallet connection and displaying a success message to the user. If rejected, the Wallet

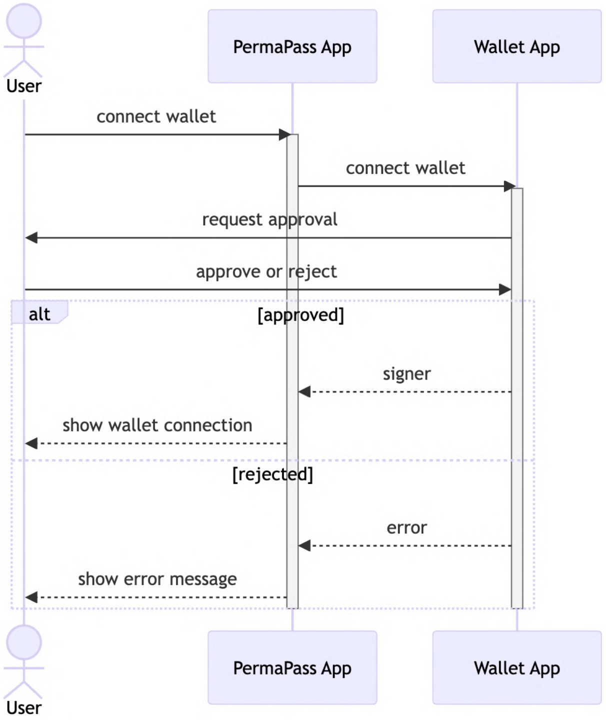


Figure 4.2: UML Sequence Diagram of Wallet Connection Establishments

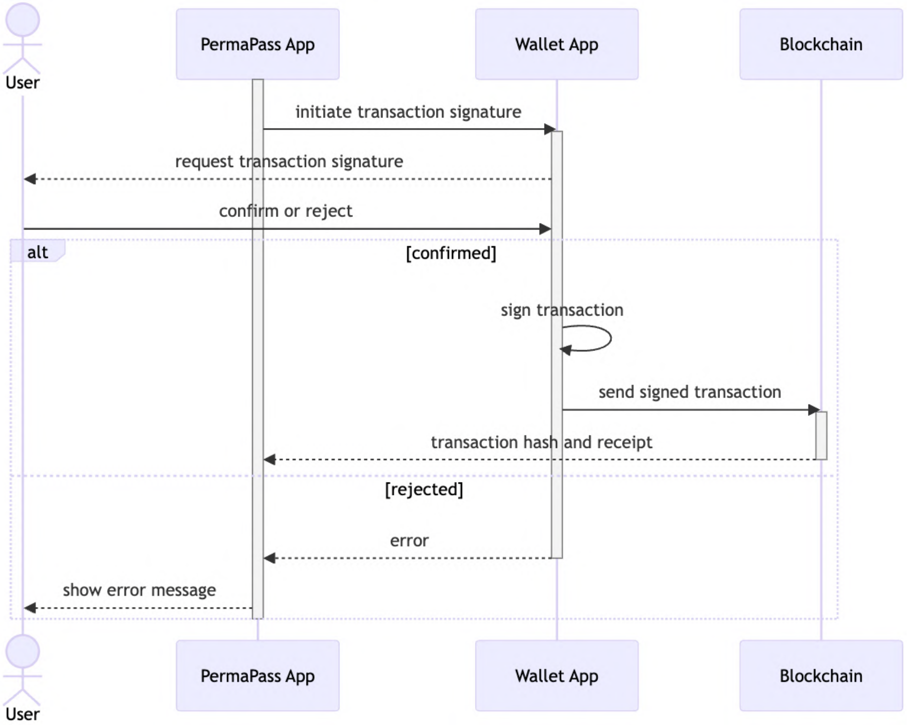


Figure 4.3: UML Sequence Diagram of Blockchain Transaction Executions

App returns an error message to the *PermaPass* App, notifying the user of the unsuccessful connection. A successful wallet connection enables the user to execute blockchain transactions initiated by the *PermaPass* App.

Before executing a blockchain transaction, a successful wallet connection is required. Figure 4.3 depicts the workflow for executing a blockchain transaction initiated by the *PermaPass* App. The process starts with the *PermaPass* App initiating a transaction signature request to the Wallet App, which prompts the user to confirm or reject the transaction. If confirmed, the Wallet App signs the transaction with its private key and sends it to the blockchain for processing. The blockchain generates a transaction hash and receipt, which the *PermaPass* App fetches to notify the user of the successful transaction. If the user rejects the transaction, the Wallet App sends an error message back to the *PermaPass* App, which informs the user that the transaction was not processed. This sequence is used whenever a user needs to change the state of a passport on the blockchain, such as for creating, updating, or deleting passports.

A signature by the HaLo NFC chip is involved when reading or creating HaLo NFC-based passports. Figure 4.4 visualizes the sequence for creating such a signature. First, the *PermaPass* App requests users to tap the HaLo NFC chip with their smartphones. If the user taps the chip, the *PermaPass* App requests a signature from the HaLo NFC chip, which responds with a signature using the private key stored on the chip. This signature is returned to the *PermaPass* App. If the user rejects the request to tap the chip, the *PermaPass* App displays an error message indicating that the action was not completed.

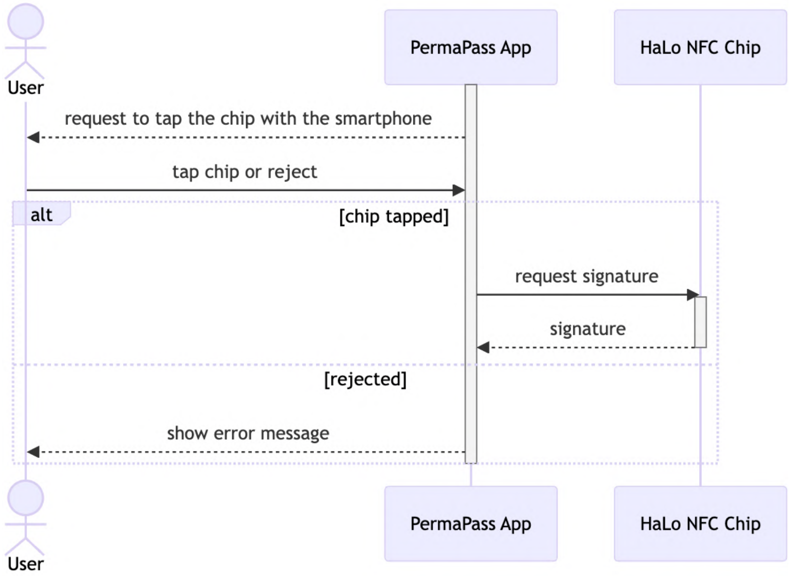


Figure 4.4: UML Sequence Diagram of HaLo NFC Chip Signature Creations

4.3.2 Passport Creation

The passport creation sequence shows how *PermaPass* processes the creation of passports. Due to the complexity, this workflow is divided into three subsequences for clarity. A successful wallet connection is a prerequisite since passport creation requires state changes on the blockchain.

Figure 4.5 shows the first step of the creation sequence, which involves the user entering the necessary data to create a passport. This includes uploading a JSON document with product details such as product name, manufacturer, warranty, and other relevant properties. The user then selects the passport's data carrier (QR code or HaLo NFC chip) and chooses a digital identifier (NFT, PBT, or DID) based on the previous selection. With all required data inputted, the user can initiate the creation process.

The second creation sequence will be triggered once the user starts the creation process in the first sequence. This sequence is depicted in Figure 4.6 and manages the creation of the digital identifier on the blockchain. Initially, the *PermaPass* App uploads the passport data to Arweave and generates a `passportURI` from the transaction ID. The `passportURI` is an identifier pointing to the passport data stored on Arweave. The blockchain's creation process is initiated depending on the selected digital identifier.

For NFTs, the process involves executing the Blockchain Transaction Sequence (BTS) to mint the NFT. For PBTs, a HaLo NFC chip signature is required before initiating the transaction on the PBTRegistry smart contract to mint the PBT. According to the smart contract standards of NFTs and PBTs, while minting them, the owner address and `passportURI` can be passed and set in one blockchain transaction.

For DIDs, the *PermaPass* App first creates an Ethereum account for the product. According to the Ethr DID method specification [109], every Ethereum address is implicitly an identity that can be used as Ethereum DID. Thus, there is no blockchain transaction to register the address as a DID on the blockchain. Contrary to NFTs and PBTs, changing the ownership and linking the `passportURI` to the identifier must be executed in two separate transactions. First, the product's DID ownership will be changed to the wallet address using a signature by the product account's private key. Finally, a DID service called `ProductPassport` containing the `passportURI` will be attached to the product's DID.

Finally, the digital identifier for the product has been created and is owned by the user's wallet address.

The final step, shown in Figure 4.7, involves linking the passport metadata to the selected data carrier. First, the *PermaPass* App creates a JSON document with the passport metadata and uploads it to Arweave, generating a `metadataURI`. This `metadataURI` points to the metadata stored on Arweave.

For QR codes, this `metadataURI` and additional details on how to open read a passport using the *PermaPass* App will be merged to a `QRCodeURI`, which is then encoded as QR code and displayed to the user.

For HaLo NFC chips, the process involves linking the `metadataURI` to the chip address using the chip signature on the HaLoNFCMetadataRegistry smart contract. This external metadata linking is needed since the chip's NDEF tag is immutable. For a DID-based passport, such a signature needs first to be created. For a PBT-based passport, the previously generated signature will be reused.

Upon success, the *PermaPass* App confirms the passport creation to the user.

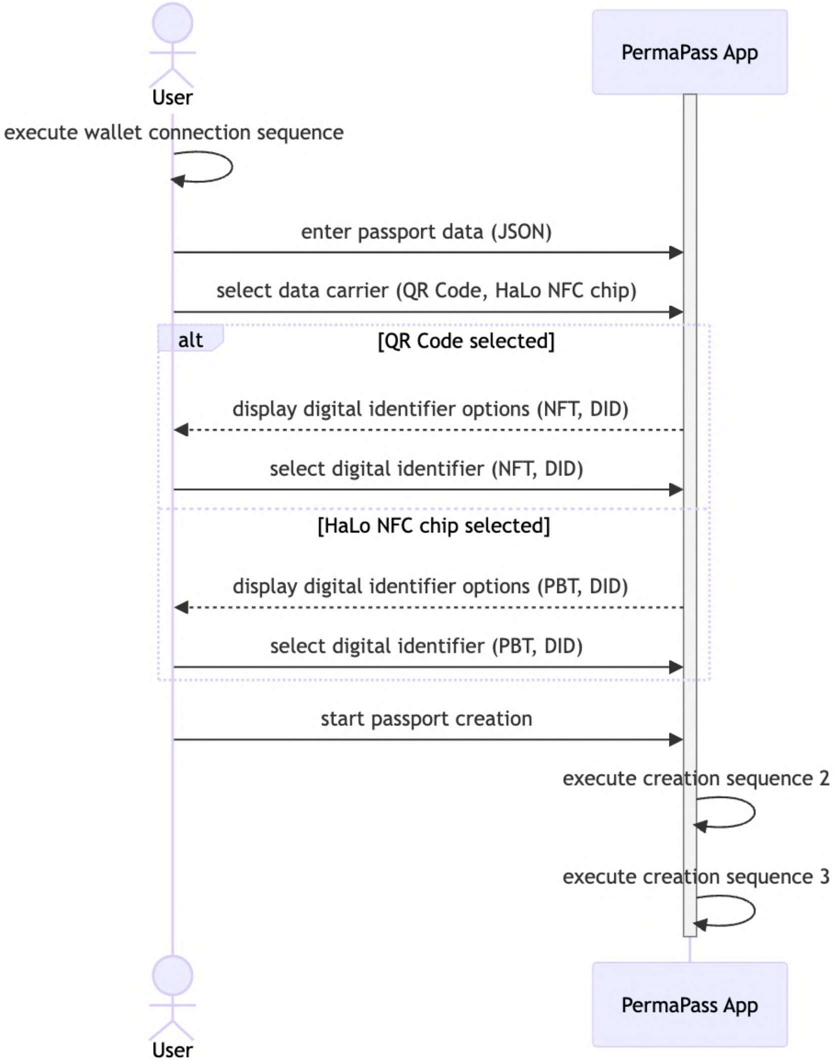

User
PermaPass App
execute wallet connection sequence
enter passport data (JSON)
select data carrier (QR Code, HaLo NFC chip)
alt
[QR Code selected]
display digital identifier options (NFT, DID)
select digital identifier (NFT, DID)
[HaLo NFC chip selected]
display digital identifier options (PBT, DID)
select digital identifier (PBT, DID)
start passport creation
execute creation sequence 2
execute creation sequence 3
User
PermaPass App

Figure 4.5: UML Sequence Diagram of Passport Creation 1/3: Setting Creation Data

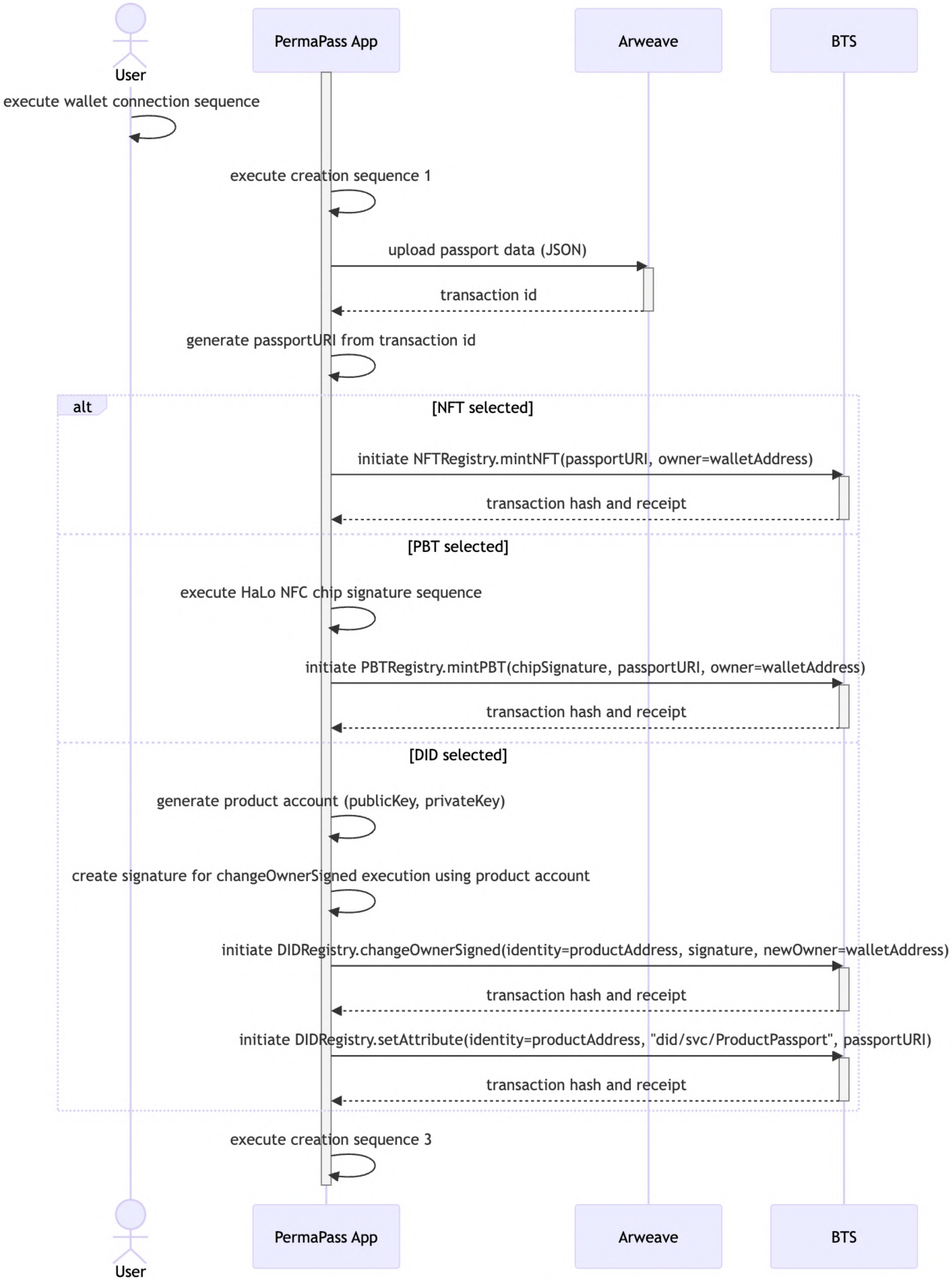

User
PermaPass App
Arweave
BTS
execute wallet connection sequence
execute creation sequence 1
upload passport data (JSON)
transaction id
generate passportURI from transaction id
alt
[NFT selected]
initiate NFTRegistry.mintNFT(passportURI, owner=walletAddress)
transaction hash and receipt
[PBT selected]
execute HaLo NFC chip signature sequence
initiate PBTRegistry.mintPBT(chipSignature, passportURI, owner=walletAddress)
transaction hash and receipt
[DID selected]
generate product account (publicKey, privateKey)
create signature for changeOwnerSigned execution using product account
initiate DIDRegistry.changeOwnerSigned(identity=productAddress, signature, newOwner=walletAddress)
transaction hash and receipt
initiate DIDRegistry.setAttribute(identity=productAddress, "did/svc/ProductPassport", passportURI)
transaction hash and receipt
execute creation sequence 3
User
PermaPass App
Arweave
BTS

Figure 4.6: UML Sequence Diagram of Passport Creation 2/3: Creating Digital Identifiers

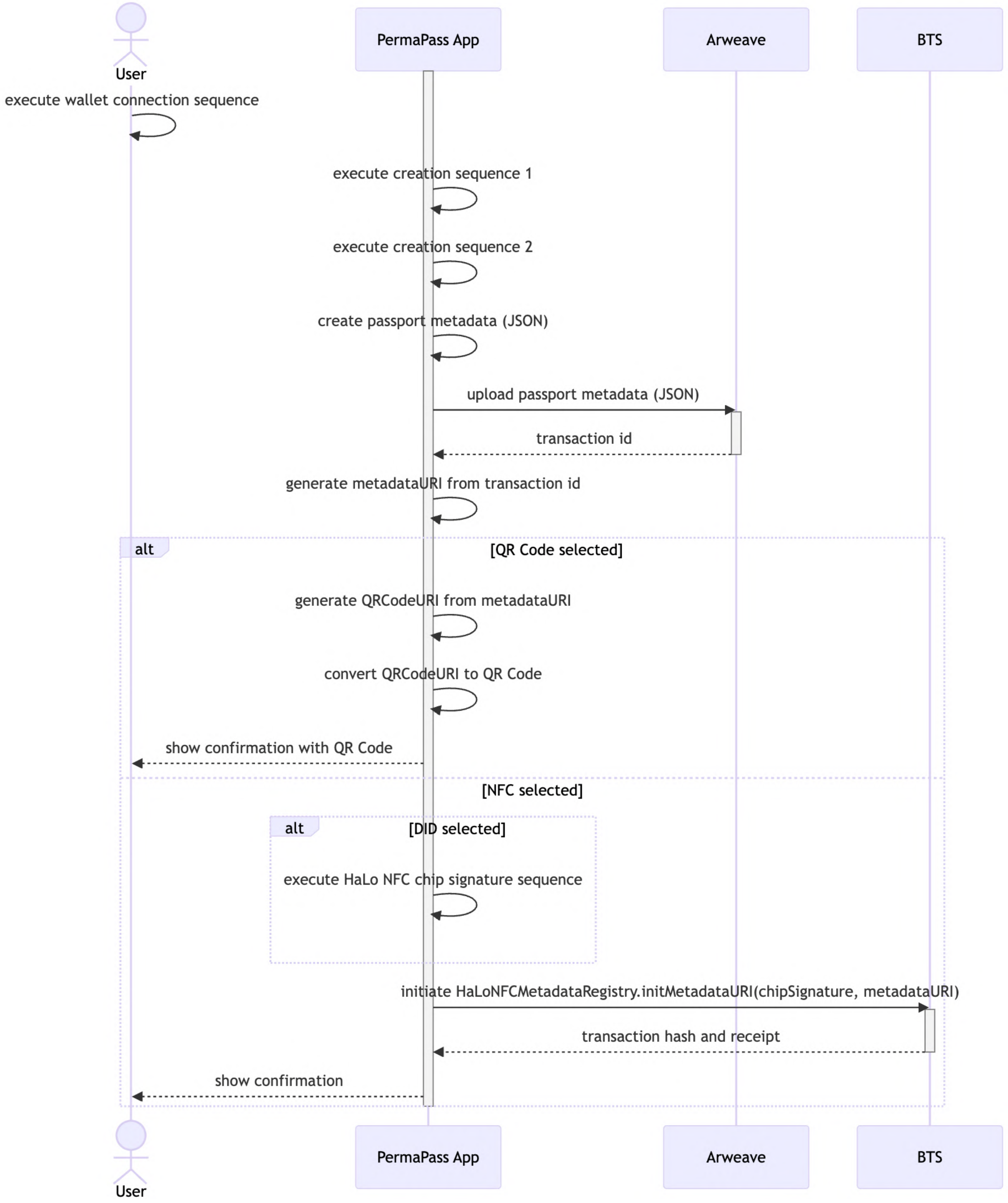

User
PermaPass App
Arweave
BTS
execute wallet connection sequence
execute creation sequence 1
execute creation sequence 2
create passport metadata (JSON)
upload passport metadata (JSON)
transaction id
generate metadataURI from transaction id
alt
[QR Code selected]
generate QRCodeURI from metadataURI
convert QRCodeURI to QR Code
show confirmation with QR Code
[NFC selected]
alt
[DID selected]
execute HaLo NFC chip signature sequence
initiate HaLoNFCMetadataRegistry.initMetadataURI(chipSignature, metadataURI)
transaction hash and receipt
show confirmation
User
PermaPass App
Arweave
BTS

Figure 4.7: UML Sequence Diagram of Passport Creation 3/3: Linking Passport Metadata to Data Carrier

4.3.3 Passport Reading

Figure 4.8 illustrates the sequence of reading and verifying a passport. For this sequence, users are not required to be connected to their wallets because no state-changing blockchain transaction is involved.

The process begins with the user requesting a QR code or HaLo NFC chip passport reading via the *PermaPass* App. If the QR code method is selected, the camera will be opened so the user can scan the QR code. The `metadataURI` will be extracted from this QR code. If the HaLo NFC chip reading method is selected, the *PermaPass* App first requests a chip signature from the HaLo NFC chip. The chip signature is then used to extract the chip address and read the `metadataURI` from the HaLoNFCMetadataRegistry.

Next, the `metadataURI` is converted into a `metadataURL`, which is then fetched to retrieve the passport metadata in JSON format. The *PermaPass* App extracts the passport type from the metadata. Depending on this type (NFT, PBT, or DID), the *PermaPass* App reads past modification events from the respective registry contract (NFTRegistry, PBTRegistry, or DIDRegistry) such that the passport's history can be composed. These events are then processed to extract and sort `passportURIs`, which are converted into `passportURLs`.

The final step involves fetching the `passportURLs` to retrieve the complete passport data, including its history, and displaying this information to the user within the *PermaPass* App.

4.3.4 Passport Update

Figure 4.9 visualizes the passport update process. Since updating a passport requires a blockchain state change, users must be connected to their wallets to execute the BTS. The update process builds on the passport reading sequence, so the passport must be read first.

The process starts with the user requesting an update for the previously read passport. If the connected wallet address is not the passport owner, the process terminates with an error. If the wallet address is verified, the *PermaPass* App uploads the new passport data to Arweave, receiving a transaction ID. From this ID, the `newPassportURI` will be generated. The sequence then follows different paths to update the passport data on the respective registry contract based on the passport type (NFT, PBT, or DID).

For an NFT or PBT-based passport, the app extracts the registry contract details and the `tokenId` from the passport metadata. Using this information, a blockchain transaction will be initiated to update the token URI of the corresponding NFT or PBT. For a DID-based passport, in addition to the DIDRegistry details, the `productAddress` will be extracted from the DID received within the passport metadata. Next, the `newPassportURI` will be set as new service attribute of the DID.

Finally, the *PermaPass* App then shows a confirmation to the user, completing the update process.

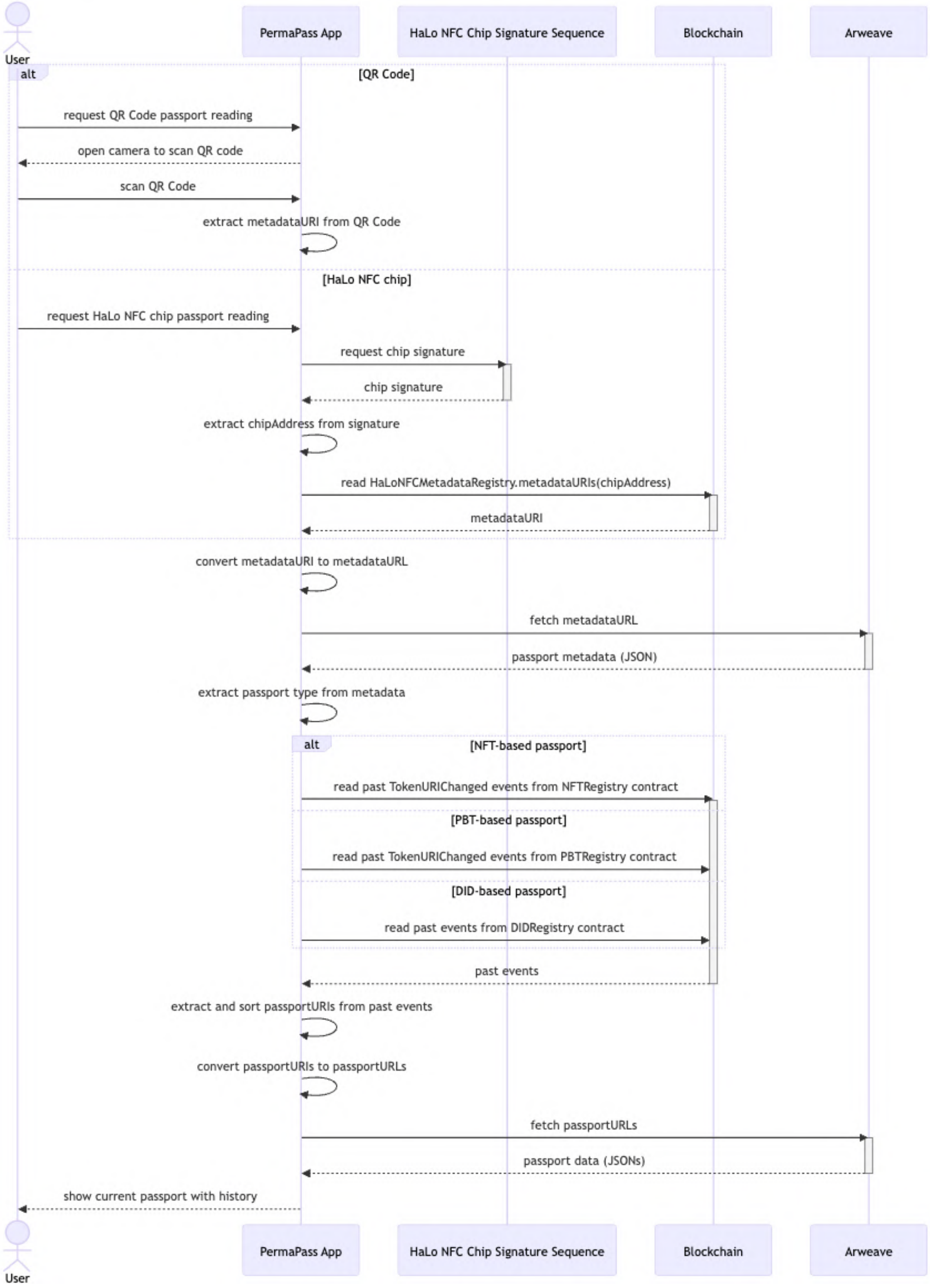

User
PermaPass App
HaLo NFC Chip Signature Sequence
Blockchain
Arweave
alt
[QR Code]
request QR Code passport reading
open camera to scan QR code
scan QR Code
extract metadataURI from QR Code
[HaLo NFC chip]
request HaLo NFC chip passport reading
request chip signature
chip signature
extract chipAddress from signature
read HaLoNFCMetadataRegistry.metadataURIs(chipAddress)
metadataURI
convert metadataURI to metadataURL
fetch metadataURL
passport metadata (JSON)
extract passport type from metadata
alt
[NFT-based passport]
read past TokenURIChanged events from NFTRegistry contract
[PBT-based passport]
read past TokenURIChanged events from PBTRegistry contract
[DID-based passport]
read past events from DIDRegistry contract
past events
extract and sort passportURIs from past events
convert passportURIs to passportURLs
fetch passportURLs
passport data (JSONs)
show current passport with history
User
PermaPass App
HaLo NFC Chip Signature Sequence
Blockchain
Arweave

Figure 4.8: UML Sequence Diagram of Passport Reading

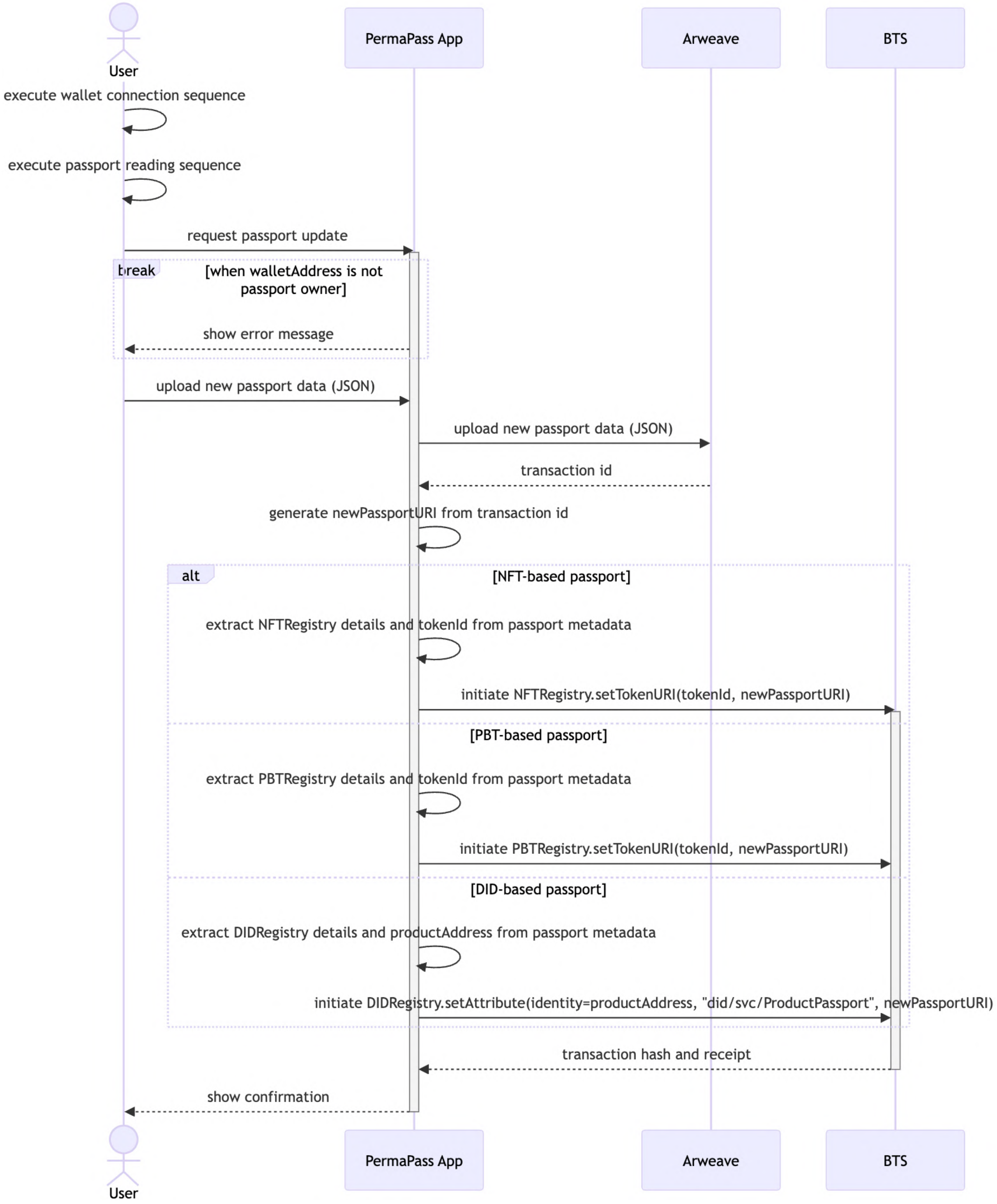

User
PermaPass App
Arweave
BTS
execute wallet connection sequence
execute passport reading sequence
request passport update
break
[when walletAddress is not passport owner]
show error message
upload new passport data (JSON)
upload new passport data (JSON)
transaction id
generate newPassportURI from transaction id
alt
[NFT-based passport]
extract NFTRegistry details and tokenId from passport metadata
initiate NFTRegistry.setTokenURI(tokenId, newPassportURI)
[PBT-based passport]
extract PBTRegistry details and tokenId from passport metadata
initiate PBTRegistry.setTokenURI(tokenId, newPassportURI)
[DID-based passport]
extract DIDRegistry details and productAddress from passport metadata
initiate DIDRegistry.setAttribute(identity=productAddress, "did/svc/ProductPassport", newPassportURI)
transaction hash and receipt
show confirmation
User
PermaPass App
Arweave
BTS

Figure 4.9: UML Sequence Diagram of Passport Update

4.3.5 Passport Deletion

Figure 4.10 details the passport deletion process. The initial steps, such as deletion request, verifying the wallet address, and extracting smart contract details, `tokenId`, and `productAddress` from the read passport data, are similar to the passport update sequence. However, different blockchain transactions execute the deletion. Passport deletion in *PermaPass* means archiving, as blockchain records cannot be deleted.

For NFT and PBT-based passports, the token is burned by transferring it to the zero address. The product's DID ownership is transferred to the zero address for DID-based passports. Thus, the passport can still be read but not updated. After these operations, the corresponding registry contract processes the deletion request and returns a transaction hash and receipt to confirm the successful deletion. The *PermaPass* App then shows a confirmation to the user, indicating the passport has been successfully deleted.

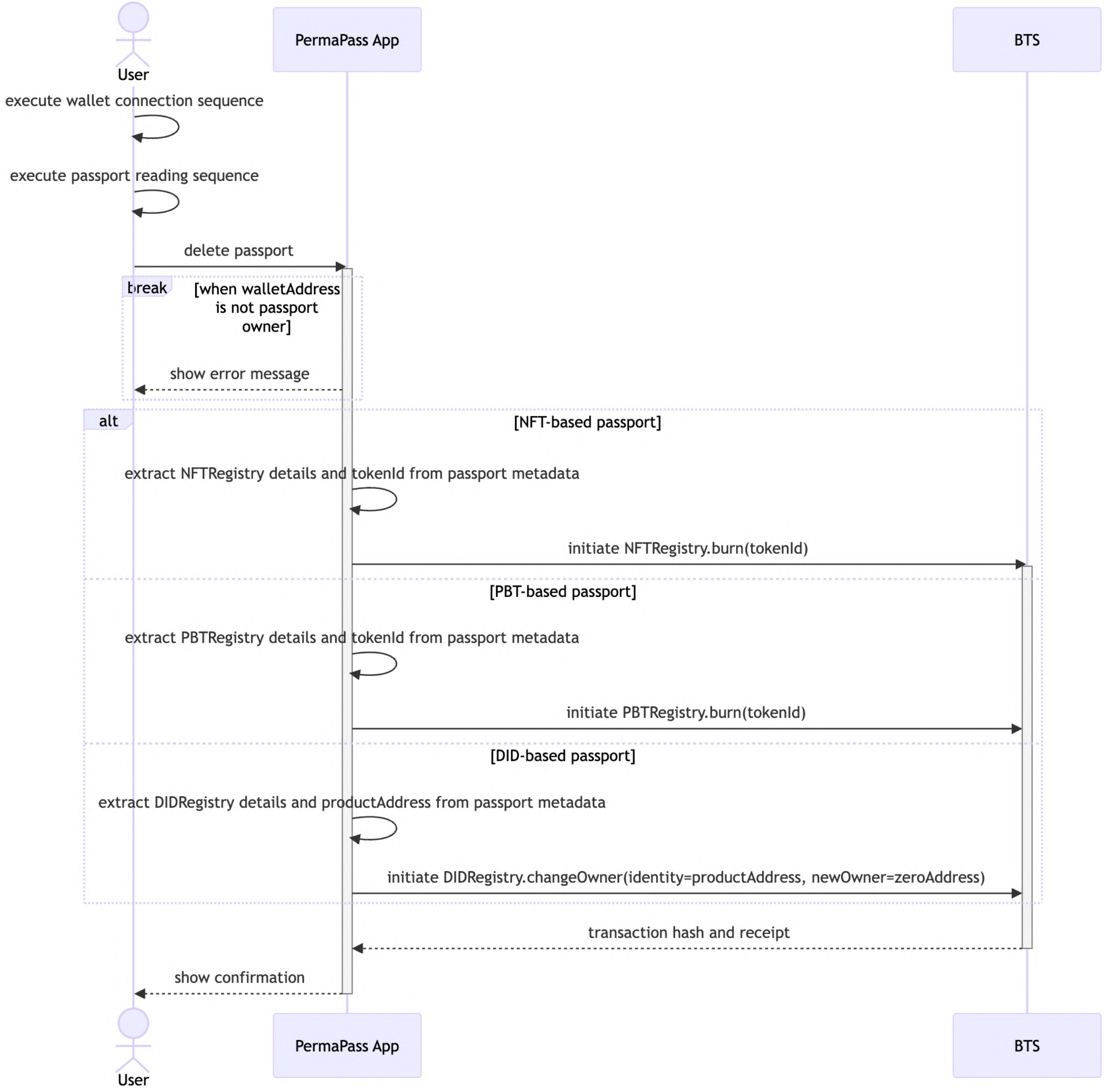

User
PermaPass App
BTS
execute wallet connection sequence
execute passport reading sequence
delete passport
break
[when walletAddress is not passport owner]
show error message
alt
[NFT-based passport]
extract NFTRegistry details and tokenId from passport metadata
initiate NFTRegistry.burn(tokenId)
[PBT-based passport]
extract PBTRegistry details and tokenId from passport metadata
initiate PBTRegistry.burn(tokenId)
[DID-based passport]
extract DIDRegistry details and productAddress from passport metadata
initiate DIDRegistry.changeOwner(identity=productAddress, newOwner=zeroAddress)
transaction hash and receipt
show confirmation
User
PermaPass App
BTS

Figure 4.10: UML Sequence Diagram of Passport Deletion

Chapter 5

Implementation

This chapter delves into the implementation of *PermaPass*, focusing on the user interface and distributed ledger component as proposed in the previous chapter. The entire codebase has been uploaded to a public GitHub repository [34]. Table 5.1 summarizes the code repository structure and its components.

Architecture Component	**Directory Path**	**Description**
User Interface	`./dapp`	React Native smartphone app enabling interactions with data carriers and their digital identifiers stored on an EVM-compatible blockchain. It is considered a decentralized application (dapp) as its main purpose is interacting with a distributed ledger.
	`./web-api`	An API that supports the `./dapp` with functionalities that were required but not supported by React Native.
Distributed Ledger	`./ethereum`	Smart contract implementations.

Table 5.1: Structure of the *PermaPass* Code Repository [34]

5.1 User Interface

The *PermaPass* code repository includes two directories for the user interface development: `./dapp` and `./web-api`. During the development of the React Native smartphone app, considered a decentralized application and therefore located in `./dapp`, it was discovered that certain dependency packages required to interact with the other architectural components were either incompatible with each other or lacked support for React Native. Consequently, a Web API located in `./web-api` was created to provide functionalities that could not be implemented directly in the app. The following sections detail the development of the React Native smartphone app, called *PermaPass* App, and the Web API.

5.1.1 PermaPass App

To develop the *PermaPass* App and its interactions with other architectural components, the following technologies were employed:

- **React Native:** A framework that compiles JavaScript or TypeScript code into native iOS and Android code, allowing developers to maintain a single codebase for both platforms. Released by Meta in 2015, it continues to be actively maintained [70].
- **Expo:** A framework that simplifies the development of React Native apps by providing tools to facilitate and accelerate the process. Apps utilizing these tools are known as Expo apps [40].
- **TypeScript:** A strongly typed programming language that enhances JavaScript by providing better tooling and early error detection through a type system, making the code more reliable [108].
- **Yarn:** A fast, reliable, and secure package manager for managing node modules, supporting the app's development [125].
- **WalletConnect + Wagmi:** WalletConnect [119] is an open-source protocol for securely connecting mobile wallets to decentralized applications and facilitating transactions. WalletConnect must be configured with an appropriate library to interact with the Ethereum blockchain. For React Native, WalletConnect recommends using Wagmi [117] due to its built-in TypeScript support and high performance.

The source code for the *PermaPass* App is located in the `./dapp` directory of the *PermaPass* code repository [34]. Table 5.2 provides an overview of the main files and folders in this directory:

Directory Path	**Description**
`./app`	Contains the app screens, with `index.tsx` as the starting screen. A `_layout.tsx` file defines the basic layout for each screen in the same subdirectory.
`./context`	Holds React Native context providers for managing global state during runtime. For example, `CreationContext.tsx` manages inputted creation data, while `ModalContext.tsx` controls the display of a modal component.
`./hooks`	Contains custom React Native hooks used in the app.
`./lib`	Contains configuration properties, utility functions, and the API client for communicating with the Web API.
`app.json`	Configuration file for the Expo app.

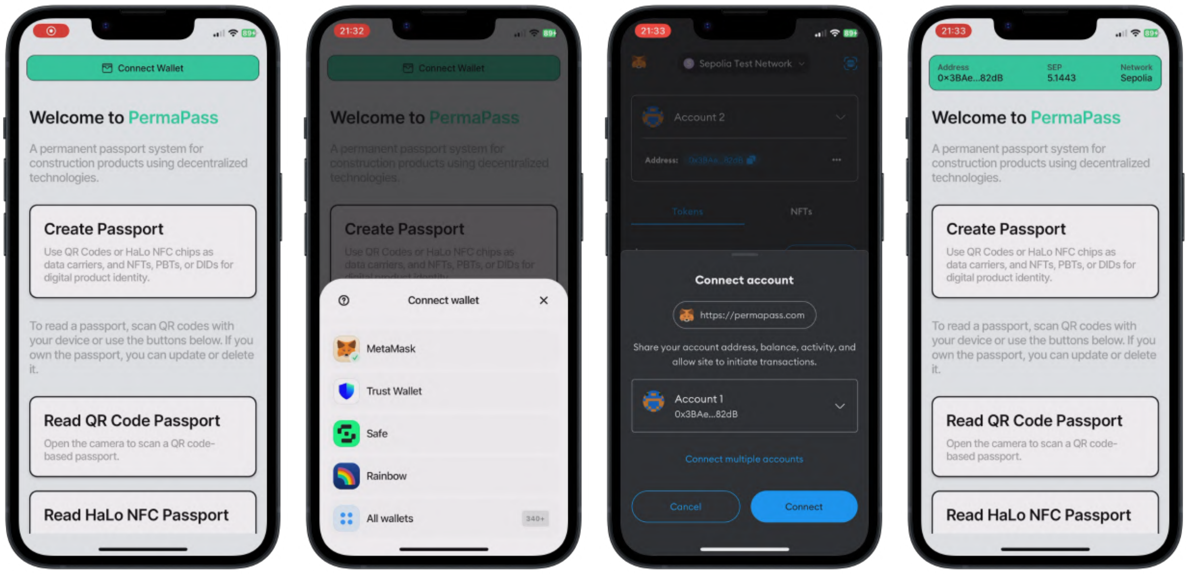
Table 5.2: Structure of *PermaPass* App Directory [34]

The data structures for passport metadata and passport data are in Appendix B, including example files for both.

The following paragraphs describe how the designed workflows presented in Chapter 4.3 have been developed in the *PermaPass* App.

5.1.1.1 Shared Sequences

Figure 5.1 outlines the steps to connect a wallet to the *PermaPass* App. The first screenshot displays the home screen without a connected wallet. Clicking the ”Connect Wallet”



Welcome to PermaPass

A permanent passport system for construction products using decentralized technologies.

Create Passport

Use QR Codes or HaLo NFC chips as data carriers, and NFTs, PBTs, or DIDs for digital product identity.

To read a passport, scan QR codes with your device or use the buttons below. If you own the passport, you can update or delete it.

Read QR Code Passport

Open the camera to scan a QR code-based passport.

Read HaLo NFC Passport

Connect account

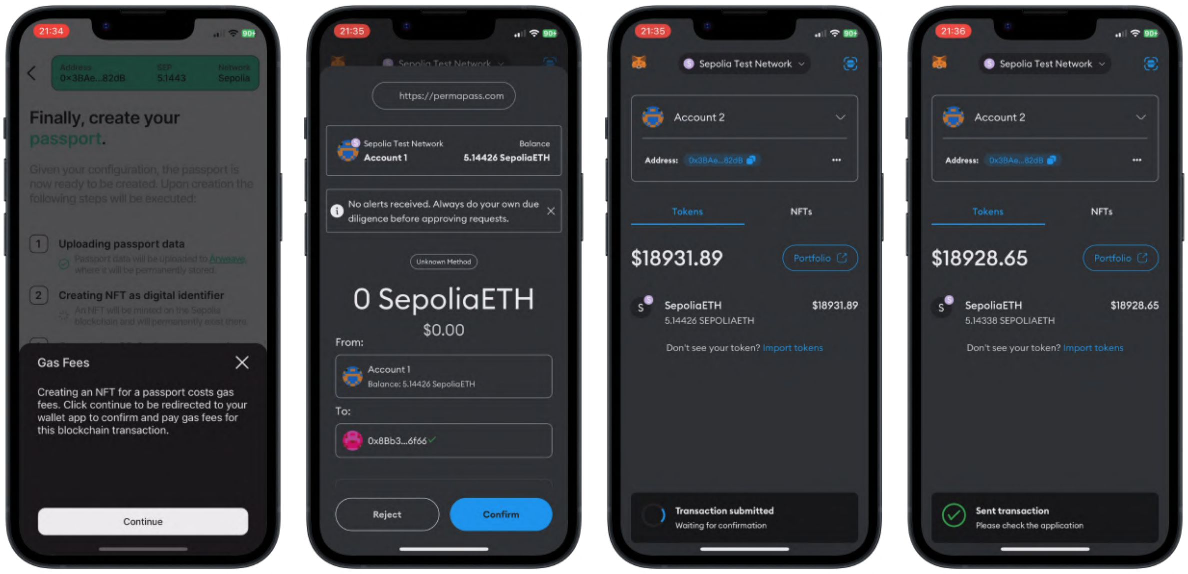
Share your account address, balance, activity, and allow site to initiate transactions.

Account 1
0x3BAe...82dB

Address 0×3BAe...82dB | SEP 5.1443 | Network Sepolia

1. Wallet Disconnected 2. Connect Wallet 3. Confirm Connection 4. Wallet Connected

Figure 5.1: User Interfaces for Connecting Wallet Apps



Address 0×3BAe...82dB | SEP 5.1443 | Network Sepolia

Finally, create your passport.

Given your configuration, the passport is now ready to be created. Upon creation the following steps will be executed:

1 Uploading passport data

Passport data will be uploaded to Arweave, where it will be permanently stored.

2 Creating NFT as digital identifier

An NFT will be minted on the Sepolia blockchain and will permanently exist there.

Gas Fees

Creating an NFT for a passport costs gas fees. Click continue to be redirected to your wallet app to confirm and pay gas fees for this blockchain transaction.

Sepolia Test Network — Account 1 — Balance 5.14426 SepoliaETH

No alerts received. Always do your own due diligence before approving requests.

0 SepoliaETH
$0.00

From: Account 1 — Balance: 5.14426 SepoliaETH

To: 0x8Bb3...6f66

$18931.89

SepoliaETH $18931.89
5.14426 SEPOLIAETH

Don't see your token? Import tokens

Transaction submitted
Waiting for confirmation

$18928.65

SepoliaETH $18928.65
5.14338 SEPOLIAETH

Don't see your token? Import tokens

Sent transaction
Please check the application

1. Gas Fees Information 2. Confirm Transaction 3. Transaction Submitted 4. Transaction Successful

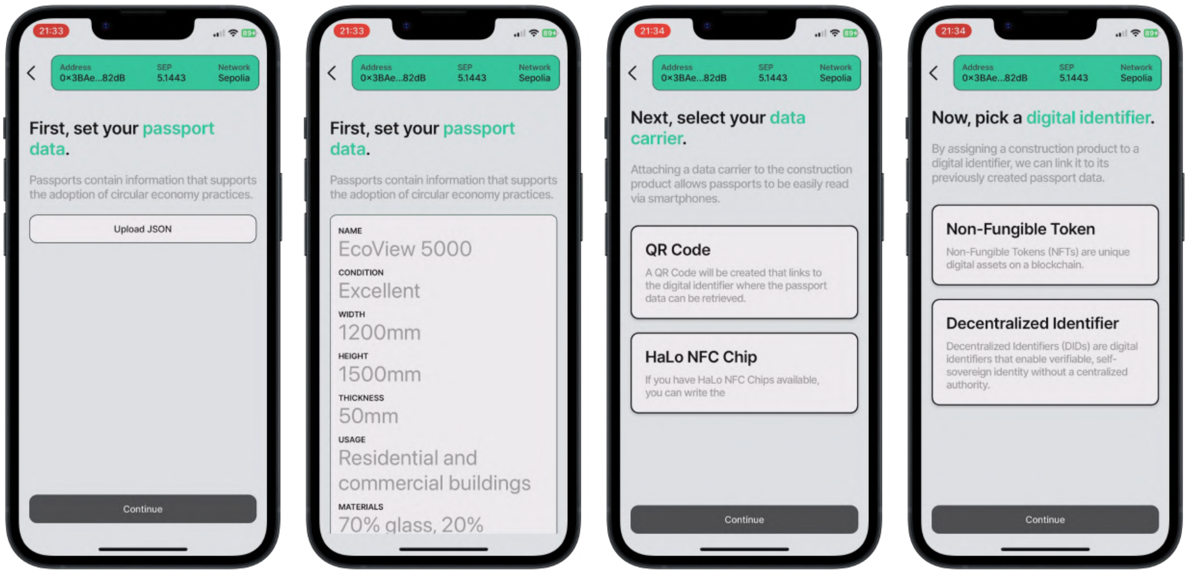
Figure 5.2: User Interfaces for Executing Blockchain Transactions

button leads to the second screenshot, where users can choose from various wallet apps via the Web3Modal component provided by WalletConnect. The MetaMask wallet app has been selected in this example, shown in the third screenshot confirming the connection. Finally, the home screen shows a successful connection by displaying the connected wallet's address, network, and balance. After successfully connecting the wallet, transactions on EVM-compatible chains can be executed. The *PermaPass* App supports only the Sepolia or a locally run Hardhat network.

Figure 5.2 outlines the steps to execute a blockchain transaction. First, a modal will inform users about gas fees when initiating a transaction. Upon continuing, the connected wallet app will open for the user to confirm and sign the transaction, covering the gas fees. The wallet app then submits the transaction, and a message confirms its successful execution. The user can then return to the *PermaPass* App.

5.1.1.2 Passport Creation

Figure 5.3 illustrates the implementation of the first creation sequence, focusing on setting passport creation data. The process begins with uploading a JSON file containing the data. Next, the user selects the data carrier. If a QR code is chosen, the user can select an NFT or DID as a digital identifier on the next screen. Otherwise, they can select PBT or DID.



First, set your passport data.

Passports contain information that supports the adoption of circular economy practices.

1. Upload Passport Data

First, set your passport data.

Passports contain information that supports the adoption of circular economy practices.

NAME
EcoView 5000
CONDITION
Excellent
WIDTH
1200mm
HEIGHT
1500mm
THICKNESS
50mm
USAGE
Residential and commercial buildings
MATERIALS
70% glass, 20%

2. Passport Data Uploaded

Next, select your data carrier.

Attaching a data carrier to the construction product allows passports to be easily read via smartphones.

QR Code
A QR Code will be created that links to the digital identifier where the passport data can be retrieved.

HaLo NFC Chip
If you have HaLo NFC Chips available, you can write the

3. Choose Data Carrier

Now, pick a digital identifier.

By assigning a construction product to a digital identifier, we can link it to its previously created passport data.

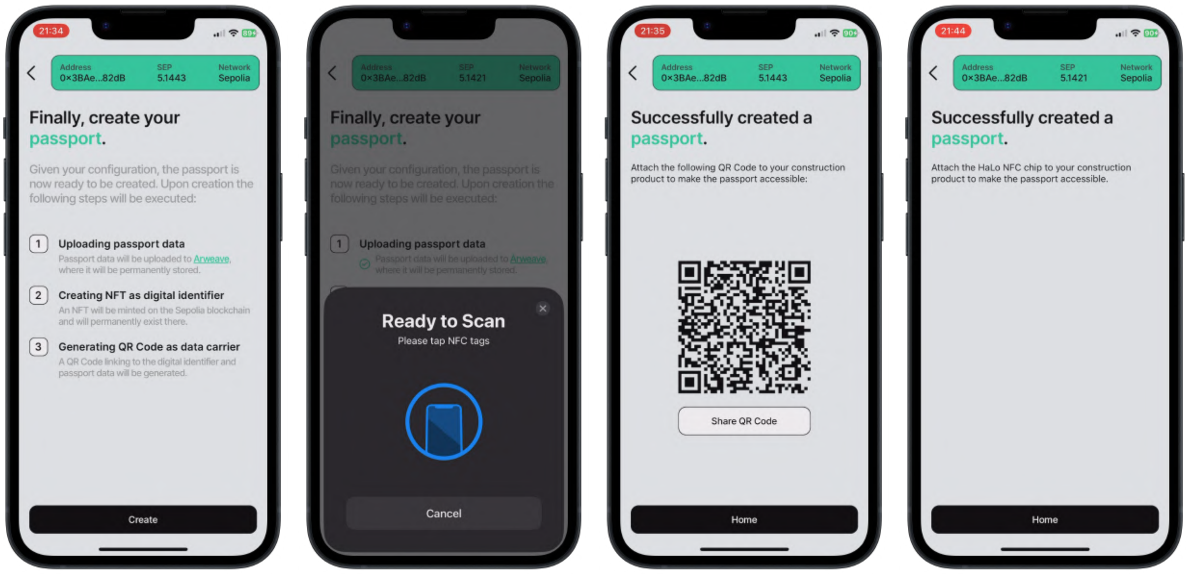
Non-Fungible Token
Non-Fungible Tokens (NFTs) are unique digital assets on a blockchain.

Decentralized Identifier
Decentralized Identifiers (DIDs) are digital identifiers that enable verifiable, self-sovereign identity without a centralized authority.

4. Choose Digital Identifier

Figure 5.3: User Interfaces for Setting Passport Creation Data

Figure 5.4 shows the screens visible during the passport creation process, as proposed in the second and third creation sequences. Initially, an overview screen outlines the steps needed to create the passport. Upon starting the creation process, blockchain transactions are initiated, prompting the user to the connected wallet app to pay gas fees. If the HaLo NFC chip is selected as the data carrier, the user is prompted to tap the NFC chip to create the required chip signature, as shown in the second screenshot. After successfully creating the passport, the confirmation screen appears. If the QR code is selected as the data carrier, the QR code will be displayed. Otherwise, a text message confirming the success will be shown.



Finally, create your passport.

Given your configuration, the passport is now ready to be created. Upon creation the following steps will be executed:

1 Uploading passport data
Passport data will be uploaded to Arweave, where it will be permanently stored.

2 Creating NFT as digital identifier
An NFT will be minted on the Sepolia blockchain and will permanently exist there.

3 Generating QR Code as data carrier
A QR Code linking to the digital identifier and passport data will be generated.

Finally, create your passport.

Given your configuration, the passport is now ready to be created. Upon creation the following steps will be executed:

1 Uploading passport data
Passport data will be uploaded to Arweave, where it will be permanently stored.

Ready to Scan

Please tap NFC tags

Successfully created a passport.

Attach the following QR Code to your construction product to make the passport accessible:

Successfully created a passport.

Attach the HaLo NFC chip to your construction product to make the passport accessible.

1. Creation Overview 2. HaLo NFC Chip Signature 3. QR Code Successful 4. NFC-Passport Successful

Figure 5.4: User Interfaces for Passport Creation

5.1.1.3 Passport Reading

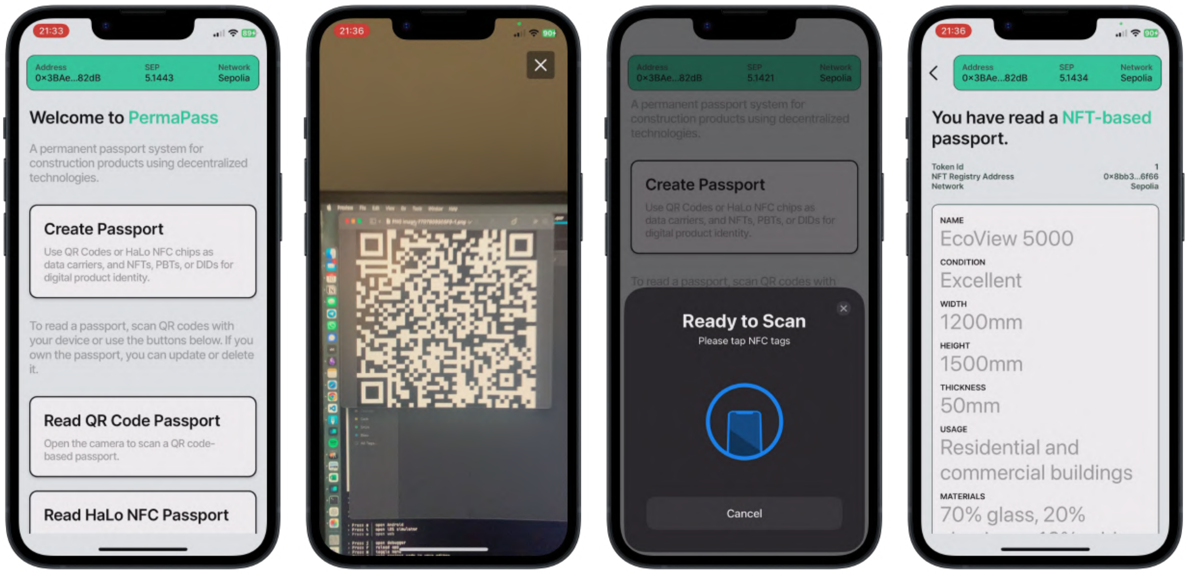
Users start at the home screen to read a passport and its history, as shown in Figure 5.5. Pressing the ”Read QR Code Passport” button opens the camera, as seen in the second screenshot. In contrast, clicking the ”Read HaLo NFC Passport” button prompts users to tap the NFC chip with their smartphone. The final screenshot shows the passport data. Users are automatically redirected to this screen once the QR code or HaLo NFC chip is read.

5.1.1.4 Passport Update

Figure 5.6 illustrates the user interface for updating a passport. To perform this operation, the user must first read a passport. The update button in the first screenshot will only be visible if the connected wallet address is the passport owner. After clicking it, the user must upload new passport data as a JSON file. Since updating the passport changes the blockchain state, the user is prompted to confirm the blockchain transaction. Upon successful execution, a screen displays the updated passport properties.

5.1.1.5 Passport Deletion

Figure 5.7 portrays the user interface for passport deletions. Similarly to passport updates, the deletion button does not appear if the connected wallet address is not the passport



21:33

Address 0×3BAe...82dB | SEP 5.1443 | Network Sepolia

Welcome to PermaPass

A permanent passport system for construction products using decentralized technologies.

Create Passport

Use QR Codes or HaLo NFC chips as data carriers, and NFTs, PBTs, or DIDs for digital product identity.

To read a passport, scan QR codes with your device or use the buttons below. If you own the passport, you can update or delete it.

Read QR Code Passport

Open the camera to scan a QR code-based passport.

Read HaLo NFC Passport

1. Home Screen

21:36

2. Read QR Code

Address 0×3BAe...82dB | SEP 5.1421 | Network Sepolia

A permanent passport system for construction products using decentralized technologies.

Create Passport

Use QR Codes or HaLo NFC chips as data carriers, and NFTs, PBTs, or DIDs for digital product identity.

To read a passport, scan QR codes with

Ready to Scan

Please tap NFC tags

Cancel

3. Read NFC Chip

21:36

Address 0×3BAe...82dB | SEP 5.1434 | Network Sepolia

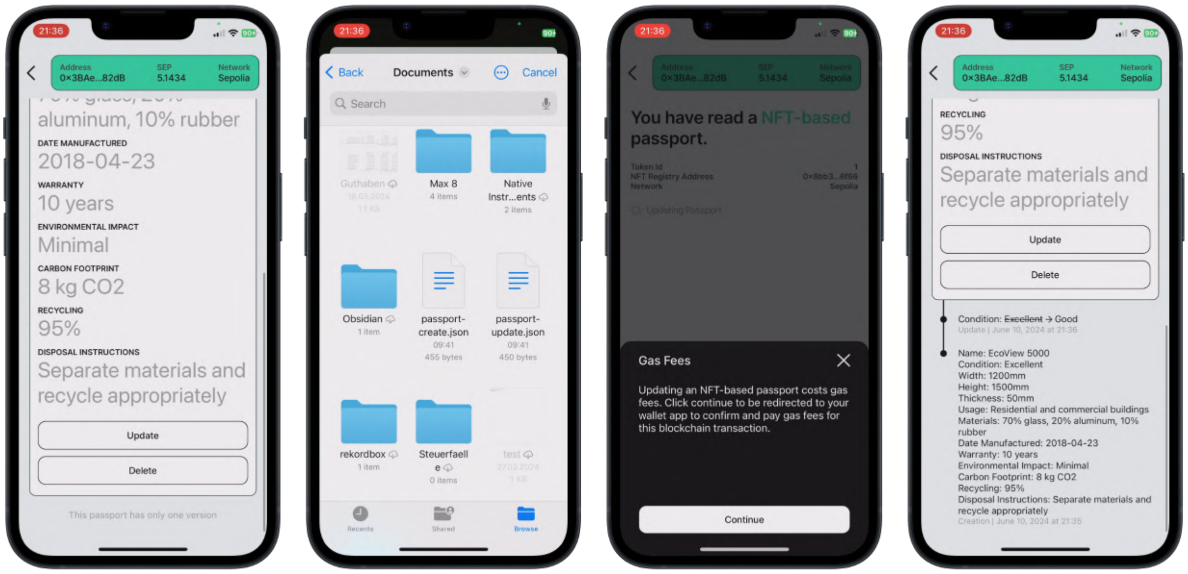
You have read a NFT-based passport.

Token Id 1
NFT Registry Address 0×8bb3...6f66
Network Sepolia

NAME
EcoView 5000
CONDITION
Excellent
WIDTH
1200mm
HEIGHT
1500mm
THICKNESS
50mm
USAGE
Residential and commercial buildings
MATERIALS
70% glass, 20%

4. Passport Read

Figure 5.5: User Interfaces for Passport Reading



21:36

Address 0×3BAe...82dB | SEP 5.1434 | Network Sepolia

aluminum, 10% rubber
DATE MANUFACTURED
2018-04-23
WARRANTY
10 years
ENVIRONMENTAL IMPACT
Minimal
CARBON FOOTPRINT
8 kg CO2
RECYCLING
95%
DISPOSAL INSTRUCTIONS
Separate materials and recycle appropriately

Update

Delete

This passport has only one version

1. Passport Read

21:36

Back | Documents | Cancel

Search

Guthaben 18.03.2024 11 KB
Max 8 4 items
Native Instr...ents 2 items
Obsidian 1 item
passport-create.json 09:41 455 bytes
passport-update.json 09:41 450 bytes
rekordbox 1 item
Steuerfaelle 0 items
test 27.02.2024 1 KB

Recents | Shared | Browse

2. Upload Passport Data

21:36

Address 0×3BAe...82dB | SEP 5.1434 | Network Sepolia

You have read a NFT-based passport.

Token Id 1
NFT Registry Address 0×8bb3...6f66
Network Sepolia

Updating Passport

Gas Fees

Updating an NFT-based passport costs gas fees. Click continue to be redirected to your wallet app to confirm and pay gas fees for this blockchain transaction.

Continue

3. Confirm Transaction

21:36

Address 0×3BAe...82dB | SEP 5.1434 | Network Sepolia

RECYCLING
95%
DISPOSAL INSTRUCTIONS
Separate materials and recycle appropriately

Update

Delete

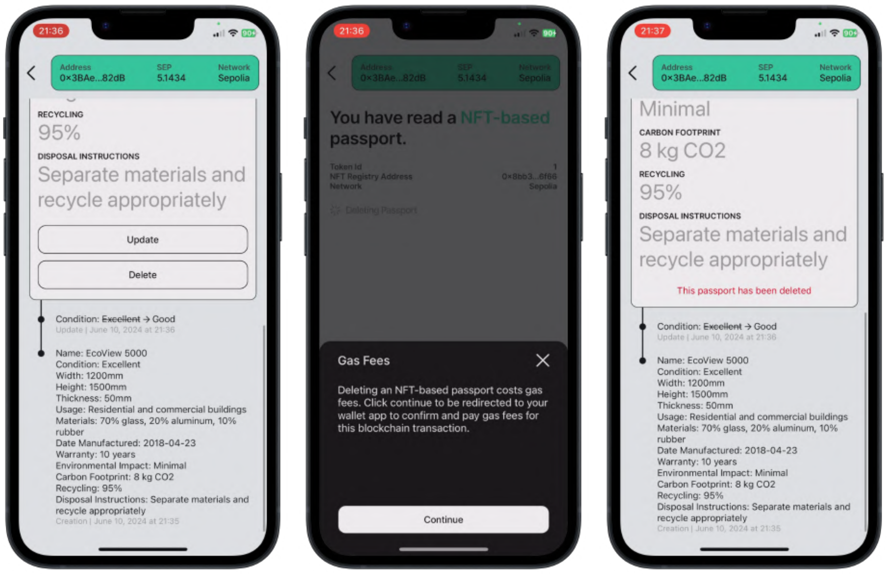
Condition: ~~Excellent~~ → Good
Update | June 10, 2024 at 21:36

Name: EcoView 5000
Condition: Excellent
Width: 1200mm
Height: 1500mm
Thickness: 50mm
Usage: Residential and commercial buildings
Materials: 70% glass, 20% aluminum, 10% rubber
Date Manufactured: 2018-04-23
Warranty: 10 years
Environmental Impact: Minimal
Carbon Footprint: 8 kg CO2
Recycling: 95%
Disposal Instructions: Separate materials and recycle appropriately
Creation | June 10, 2024 at 21:35

4. Update Successful

Figure 5.6: User Interfaces for Passport Update

owner. After clicking the button, the user must confirm the deletion transaction on the blockchain. Once the transaction is successfully executed, the user interface marks the passport as deleted.



21:36

Address 0×3BAe...82dB SEP 5.1434 Network Sepolia

RECYCLING
95%
DISPOSAL INSTRUCTIONS
Separate materials and recycle appropriately

Condition: ~~Excellent~~ → Good
Update | June 10, 2024 at 21:36

Name: EcoView 5000
Condition: Excellent
Width: 1200mm
Height: 1500mm
Thickness: 50mm
Usage: Residential and commercial buildings
Materials: 70% glass, 20% aluminum, 10% rubber
Date Manufactured: 2018-04-23
Warranty: 10 years
Environmental Impact: Minimal
Carbon Footprint: 8 kg CO2
Recycling: 95%
Disposal Instructions: Separate materials and recycle appropriately
Creation | June 10, 2024 at 21:35

21:36

Address 0×3BAe...82dB SEP 5.1434 Network Sepolia

You have read a NFT-based passport.

Token Id	1
NFT Registry Address	0×8bb3...6f66
Network	Sepolia

Deleting Passport

Gas Fees

Deleting an NFT-based passport costs gas fees. Click continue to be redirected to your wallet app to confirm and pay gas fees for this blockchain transaction.

21:37

Address 0×3BAe...82dB SEP 5.1434 Network Sepolia

Minimal
CARBON FOOTPRINT
8 kg CO2
RECYCLING
95%
DISPOSAL INSTRUCTIONS
Separate materials and recycle appropriately

This passport has been deleted

Condition: ~~Excellent~~ → Good
Update | June 10, 2024 at 21:36

Name: EcoView 5000
Condition: Excellent
Width: 1200mm
Height: 1500mm
Thickness: 50mm
Usage: Residential and commercial buildings
Materials: 70% glass, 20% aluminum, 10% rubber
Date Manufactured: 2018-04-23
Warranty: 10 years
Environmental Impact: Minimal
Carbon Footprint: 8 kg CO2
Recycling: 95%
Disposal Instructions: Separate materials and recycle appropriately
Creation | June 10, 2024 at 21:35

1. Passport Read 2. Confirm Transaction 3. Deletion Successful

Figure 5.7: User Interfaces for Passport Deletion

5.1.2 Web API

To implement the Web API, the following technologies were utilized:

- **Express.js:** A fast, minimalist web framework for Node.js [41, 78], providing HTTP utility methods to create a robust API quickly.
- **Yarn:** A fast, reliable, and secure package manager for managing node modules, facilitating the API's development [125].

Listing 5.1 demonstrates the Web API programming. The API includes two endpoints: a GET endpoint to resolve a DID document and a POST endpoint to upload data to the Arweave mainnet.

To resolve a DID document, the GET endpoint requires the didUrl and the registryAddress (the address where the DIDRegistry contract is deployed) as query parameters. The Veramo DID resolver packages use the URL to detect the network the DID resides on and resolve the DID from the provided registry address. Finally, this endpoint returns the DID document.

To upload data to the Arweave mainnet, the Irys Node 2 is used. This allows free data uploads under 100 KiB, with a limit of 600 transactions per minute [7, 57]. Initially, an object to interact with the node is instantiated. The *PermaPass* App can then pass JSON data to the Arweave POST endpoint, which uploads the data to the Arweave mainnet using the Irys Node 2 and returns the transaction ID from Arweave, provided there are no errors.

```
import express from "express";
import Irys from "@irys/sdk";
import { DIDResolverPlugin } from "@veramo/did-resolver";
import { getResolver as ethrDidResolver } from "ethr-did-resolver";

// init irys node 2
const irys = new Irys({
  network: "mainnet",
  token: "arweave",
  key: [...]
});

[...]

/**
 * @endpoint GET /did
 * @description Resolve a DID to retrieve its DID Document. Supports ’
    sepolia’ and ’hardhat’ networks.
 * @query {string} didUrl - The DID URL to resolve (e.g., did:ethr:
    sepolia:0x123...).
 * @query {string} registryAddress - Address of the DIDRegistry contract
    .
 * @example
 * curl -X GET "http://localhost:3000/did?didUrl=did:ethr:sepolia:0x123
    ...&registryAddress=0xabc..."
 */
app.get("/did", async (req, res) => {
  const { didUrl, registryAddress } = req.query;

  [...]

  const networks = [
    {
      name: "sepolia",
      provider: new ethers.JsonRpcProvider(...),
      registry: registryAddress,
      chainId: 11155111,
    },
    {
      name: "hardhat",
      provider: new ethers.JsonRpcProvider(...),
      registry: registryAddress,
      chainId: 31337,
    },
  ];

  const resolver = new DIDResolverPlugin({
    ...ethrDidResolver({ networks }),
  });
  const doc = await resolver.resolveDid({ didUrl });

  res.json(doc.didDocument);
});

/**
 * @endpoint POST /arweave
 * @description Upload data to Arweave mainnet using the Irys Node 2.
 * @body {object} - JSON body with the data to be uploaded.
 * @example
 * curl -X POST .../arweave -H "Content-Type: application/json" -d '{"
   data": "your data here"}'
 */
app.post("/arweave", async (req, res) => {
  [...]
  const receipt = await irys.upload(Buffer.from(JSON.stringify(req.body)
     ));
  if (!receipt.id) throw new Error();
  res.json({ txid: receipt.id });
});
```

Listing 5.1: Excerpt of ./web-api/api/index.mjs

5.2 Distributed Ledger

To implement and deploy smart contracts on EVM-compatible blockchains, the following technologies were used:

- **Solidity:** An object-oriented, high-level programming language for developing smart contracts on EVM-compatible blockchains. All smart contracts were written in Solidity [94].
- **Hardhat:** A development environment used to build, test, and deploy smart contracts on various networks. It offers scripts for task automation and a local network for contract testing [50].
- **Yarn:** A fast, reliable, and secure package manager for managing node modules, assisting in smart contract development [125].

Four smart contracts — the NFT Registry, PBT Registry, DID Registry, and HaLo NFC Metadata Registry — were developed to implement the prototype's functionalities. The source code is available in ./ethereum/contracts/. UML class diagrams were created for each contract to provide a visual overview of the contracts' structures, variables, functions, and other features. These diagrams can be found in Appendix C for quick reference. The following sections describe the development of the main functionalities of each contract.

5.2.1 NFT Registry Contract

The NFT Registry contract allows NFTs to be created, read, updated, and deleted. It uses the ERC-721 standard [35], which defines a common interface for NFT contracts on EVM-compatible blockchains. To implement this interface, the NFT Registry extends OpenZeppelin's ERC721URIStorage contract [80]. This contract provides core NFT functionalities, such as minting and burning, and allows attaching a URI to a token. For

PermaPass, such a URI attachment is essential to link passport data stored on Arweave to a product's token.

When creating NFT-based passports, an NFT must be minted. Listing 5.2 demonstrates this process. Since the NFT Registry contract manages multiple tokens, each token requires a unique ID. First, such a unique ID is generated for the new token. Using this token ID, the ERC721URIStorage contract's safe mint function is executed to mint the token and set the owner to the sender's wallet address. Then, a Minted event is emitted to notify the *PermaPass* App of the successful minting and the new token ID. Finally, the URI pointing to the passport data on Arweave is set for this token.

```
[...]

contract NFTRegistry is ERC721URIStorage {
    uint256 private _nextTokenId;

    [...]

    function mintNFT(address to, string memory uri) external {
        // get next token ID
        uint256 tokenId = ++_nextTokenId;

        // mint token
        _safeMint(to, tokenId);
        emit Minted(to, uri, tokenId);

        // set token URI
        setTokenURI(tokenId, uri);
    }

    [...]
}
```

Listing 5.2: Implementation of the NFT Registry's `mintNFT` function

Listing 5.3 details setting the token URI. This function is crucial for creating and updating tokens, which involves changing the passport data. Only the token owner can execute this function to align with the requirements. It first sets the token URI using OpenZeppelin's ERC721URIStorage contract. Next, it emits an event indicating the token URI has changed and records the current block number. These two steps allow a user interface to track and display the history of changes to a product's passport data.

```
[...]

contract NFTRegistry is ERC721URIStorage {
    [...]
    mapping(uint256 => uint256) public changed;

    [...]

    function setTokenURI(
        uint256 tokenId,
        string memory uri
    ) public onlyTokenOwner(tokenId) {
        _setTokenURI(tokenId, uri);
        emit TokenURIChanged(tokenId, msg.sender, uri, changed[tokenId])
            ;
        changed[tokenId] = block.number;
    }

    [...]
}
```

Listing 5.3: Implementation of the NFT Registry's `setTokenURI` function

The NFT Registry contract also includes a function to burn tokens, setting the token's owner to the zero address. This ensures the data remains on the blockchain but cannot be modified. This burning function utilizes OpenZeppelin's ERC721URIStorage implementation without any custom adjustments.

5.2.2 PBT Registry Contract

The PBT Registry contract manages PBTs using the ERC-5791 standard [1], an extension of ERC-721 [35], designed for EVM-compatible blockchains. To implement the required interface, it builds upon Chiru Labs's PBTSimple contract [65]. This contract offers core functionalities such as seeding an NFC chip, minting tokens, and verifying chip signatures. Since PBTSimple does not support attaching a URI to a token, the contract incorporates functionality from OpenZeppelin's ERC721URIStorage contract to attach passport data on Arweave.

A PBT must be minted for a HaLo NFC chip to create PBT-based passports, as shown in Listing 5.4. First, the chip address is checked to ensure it has not been minted. Once verified, a new token ID is generated, following the same process as the NFT Registry contract. The HaLo NFC chip is seeded and registered to be linked to a PBT. After seeding, a token can be minted with the chip. This seeding and minting process occurs on the underlying PBTSimple contract, where the chip signature is verified for authenticity. Finally, the passport data URI is set on the token.

```
[...]

contract PBTRegistry is PBTSimple {
    [...]
    uint256 private _nextTokenId;

    [...]

    function mintPBT(
        address chipAddress,
        bytes calldata signatureFromChip,
        uint256 blockNumberUsedInSig,
        string memory _tokenURI
    ) external {
        // Revert if the chip has already been seeded and minted
        if (_tokenDatas[chipAddress].set) {
            revert AlreadyMinted();
        }
        // get next token ID
        uint256 tokenId = ++_nextTokenId;

        // seed chip to token mapping, i.e. register chip
        address[] memory chipAddresses = new address[](1);
        uint256[] memory tokenIds = new uint256[](1);
        chipAddresses[0] = chipAddress;
        tokenIds[0] = tokenId;
        _seedChipToTokenMapping(chipAddresses, tokenIds);

        // mint token with chip, i.e. mint PBT
        _mintTokenWithChip(signatureFromChip, blockNumberUsedInSig);

        // set token URI
        setTokenURI(tokenId, _tokenURI);
    }

    [...]
}
```

Listing 5.4: Implementation of the PBT Registry's `mintPBT` function

Listing 5.5 shows how to set the token URI. This function is similar to setting the token URI in the NFT registry contract. The main difference is that the code for storing the token URI, originally from OpenZeppelin's URIStorage contract, has been integrated into this contract. This integration is necessary because the PBTSimple contract extends another contract that does not include URI storage functionality.

```
[...]

contract PBTRegistry is PBTSimple {
    mapping(uint256 => string) private _tokenURIs;
    [...]
    mapping(uint256 => uint256) public changed;

    [...]

    function setTokenURI(
        uint256 tokenId,
        string memory _tokenURI
    ) public onlyTokenOwner(tokenId) {
        [...]
        _tokenURIs[tokenId] = _tokenURI;
        emit TokenURIChanged(tokenId, msg.sender, _tokenURI, changed[
            tokenId]);
        changed[tokenId] = block.number;
    }

    [...]
}
```

Listing 5.5: Implementation of the PBT Registry's `setTokenURI` function

Similar to the NFT Registry contract, the PBT Registry contract also burns a token.

This function is used to delete a passport. It simply forwards the call to OpenZeppelin's underlying ERC-721 implementation.

5.2.3 DID Registry Contract

The DID Registry contract manages DIDs on EVM-compatible blockchains. It is a copy of Veramo's EthereumDIDRegistry contract [110], adhering to the Ethereum DID specification [109]. Consequently, it works with Veramo's ETHR DID Resolver package to resolve DID documents from Ethereum DIDs.

Listing 5.6 shows how to change a DID's owner, thereby altering its controller. This function is crucial for creating passports, as it transfers the newly created Ethereum addresses for construction products to the creator's wallet. The changeOwnerSigned function enables this transfer, with the transaction executed from the user's wallet to cover gas fees and change the owner from the construction product's wallet. The provided signature allows the user's wallet to perform this function on behalf of the construction product's wallet. The *PermaPass* App generates this signature, creating the Ethereum account for the construction product and holding its private key. After verifying the signature, the owner is updated in the owners mapping. Additionally, the DIDOwnerChanged event is emitted, and the current block number is recorded. These last two actions, similar to the NFT Registry contract, are necessary for tracking the history of DID changes in the user interface.

```
[...]

contract DIDRegistry {
    mapping(address => address) public owners;
    [...]
    mapping(address => uint) public changed;

    [...]

    function checkSignature(
        address identity,
        uint8 sigV,
        bytes32 sigR,
        bytes32 sigS,
        bytes32 hash
    ) internal returns (address) {
        address signer = ecrecover(hash, sigV, sigR, sigS);
        require(signer == identityOwner(identity), "bad_signature");
        nonce[signer]++;
        return signer;
    }

    [...]

    function changeOwner(
        address identity,
        address actor,
        address newOwner
    ) internal onlyOwner(identity, actor) {
        owners[identity] = newOwner;
        emit DIDOwnerChanged(identity, newOwner, changed[identity]);
        changed[identity] = block.number;
    }

    function changeOwner(address identity, address newOwner) public {
        changeOwner(identity, msg.sender, newOwner);
    }

    function changeOwnerSigned(
        address identity,
        uint8 sigV,
        bytes32 sigR,
        bytes32 sigS,
        address newOwner
    ) public {
        bytes32 hash = keccak256(
            abi.encodePacked(
                bytes1(0x19),
                bytes1(0),
                this,
                nonce[identityOwner(identity)],
                identity,
                "changeOwner",
                newOwner
            )
        );
        changeOwner(
            identity,
            checkSignature(identity, sigV, sigR, sigS, hash),
            newOwner
        );
    }

    [...]

}
```

Listing 5.6: Implementation of the DID Registry's `changeOwnerSigned` function

Listing 5.7 illustrates the process of setting DID attributes. This functionality allows the owner of a DID to add passport data URIs to the DID services. Since DID services are not stored on the blockchain, the emitted event DIDAttributeChanged and the recording of the current block number in a mapping enable a user interface to resolve a DID document. This can be achieved by recursively fetching all past events because ever event refers to its predecessor. Veramo argues that this implementation reduces the gas fees required for changing attributes.

```
[...]

contract DIDRegistry {
    [...]
    mapping(address => uint) public changed;
    [...]

    function setAttribute(
        address identity,
        address actor,
        bytes32 name,
        bytes memory value,
        uint validity
    ) internal onlyOwner(identity, actor) {
        emit DIDAttributeChanged(
            identity,
            name,
            value,
            block.timestamp + validity,
            changed[identity]
        );
        changed[identity] = block.number;
    }

    [...]
}
```

Listing 5.7: Implementation of the DID Registry's `setAttribute` function

To delete a passport using the DID Registry contract, the changeOwner must be called using the zero address as the new owner. This is similar to the process used in the NFT and PBT Registry.

5.2.4 HaLo NFC Metadata Registry Contract

The HaLo NFC Metadata Registry contract maps chip addresses to their passport metadata URIs. This contract is necessary because the HaLo NFC chip's NDEF tag is immutable, preventing direct writing of metadata URIs to the chip. However, the chip address is inherently available on the chip. This chip address will, therefore, be used to link metadata URIs to chips.

Listing 5.8 shows the implementation of the HaLo NFC Metadata Registry contract. The metadataURIs mapping associates chip addresses with their passport metadata URIs. The initMetadataURI function writes a metadata URI to this mapping, giving it a chip address and signature. It first checks if the metadata URI has not been set and then verifies the provided chip signature. If the signature is correct, the metadata URI is set in the mapping and can be accessed via the user interface. This code was adapted from the PBTSimple contract.

```
[...]

contract HaLoNFCMetadataRegistry {
    [...]
    mapping(address => string) public metadataURIs;

    function initMetadataURI(
        address chipAddress,
        bytes calldata signatureFromChip,
        uint256 blockNumberUsedInSig,
        string memory metadataURI
    ) external {
        // Revert if the metadataURI has already been set
        if (bytes(metadataURIs[chipAddress]).length > 0) {
            revert AlreadySet();
        }

        // The blockNumberUsedInSig must be in a previous block because
           the blockhash of the current
        // block does not exist yet.
        if (block.number <= blockNumberUsedInSig) {
            revert InvalidBlockNumber();
        }

        unchecked {
            if (block.number - blockNumberUsedInSig > 100) {
                revert BlockNumberTooOld();
            }
        }

        bytes32 blockHash = blockhash(blockNumberUsedInSig);
        bytes32 signedHash = keccak256(abi.encodePacked(msg.sender,
           blockHash))
            .toEthSignedMessageHash();
        address chipAddr = signedHash.recover(signatureFromChip);

        // Revert if the chip addresses does not match
        if (chipAddr != chipAddress) {
            revert InvalidSignature();
        }


        metadataURIs[chipAddr] = metadataURI;
    }
}
```

Listing 5.8: Implementation of the HaLo NFC Metadata Registry

Chapter 6

Evaluation

This chapter evaluates the passport types QR Code x NFT, QR Code x DID, HaLo NFC x PBT, and HaLo NFC x DID based on their implementation within *PermaPass*. It begins by comparing the performance and costs of passport operations for each type. It further provides a comparative theoretical analysis of each passport type's scalability, interoperability, security, and privacy.

6.1 Experimental Analysis of Performance and Costs

Performance refers to the duration of operations throughout a passport's lifecycle, while costs pertain to the expenses incurred during these operations. The core functions of *PermaPass* include creating, reading, updating, and deleting passports. As a result, the performance and costs of these actions and infrastructure deployment for each passport type were measured and compared. This analysis focused on Sepolia transactions and Arweave interactions.

6.1.1 Experimental Setup

For performance analysis, the time taken for blockchain transactions was recorded, including deploying smart contracts and executing their create, read, update, and delete functions. Similarly, the time for uploading (create, update) and reading data from Arweave was measured. Thereby, the following performance metrics were recorded:

- **durationInMs:** The operation's duration in milliseconds.
- **startTimestamp:** The Unix timestamp at the operation's start.
- **endTimestamp:** The Unix timestamp at the operation's end.

For costs, Arweave operations are free due to *PermaPass* using Irys Node 2. Hence, costs only refer to gas fees for blockchain transactions. For those transactions, the following cost metrics were recorded:

- **functionName:** The type of smart contract function executed.
- **gasUsed:** Amount of gas units consumed by the blockchain transaction. This value represents how much computational power it requires to execute the transaction on the blockchain.
- **effectiveGasPriceInWei:** The gas price in Wei must be paid for one gas unit at the execution time. This is calculated based on the base fee of the block and the inclusion fee (tip) provided by the user. This value can fluctuate based on network state and congestion.
- **gasCostsInWei:** The effective transaction cost in Wei, calculated by multiplying `gasUsed` and `effectiveGasPriceInWei`.

Two individual evaluation scripts were developed to record performance and cost metrics: the blockchain script and the Arweave script. The blockchain script was executed using Sepolia to simulate the Ethereum mainnet environment. Performance and costs in Sepolia ETH may vary due to network conditions. Similarly, the performance of Arweave operations can be affected by the status of Irys Node 2. Therefore, the scripts were run multiple times within a specific time to capture fluctuations, identify outliers, and collect meaningful data. Due to the limited free Sepolia ETH available for each address, the interval was set to 1 hour, with scripts executed every 5 minutes, totaling 12 executions. All smart contracts and Arweave operations were evaluated simultaneously to prevent varying conditions from impacting the results. Table 6.1 summarizes the details of the evaluation script executions.

Parameter	**Details**
Hardware	Apple MacBook Air (2022, M2) 24 GB RAM
Internet Connection	25-30 Mbps upload/download speed
Date	2024-06-14
Interval	Every 5 minutes from 17:00 to 18:00 CEST Total of 12 times
Executed Scripts	Blockchain Script using Sepolia Testnet Arweave Script on Arweave Mainnet using Irys Node 2 for Uploads
Blockchain Script Details	Script Path: `./ethereum/scripts/evaluate.ts` Results Path: `./evaluation/data/contracts/*`
Arweave Script Details	Script Path: `./web-api/evaluate.mjs` Results Path: `./evaluation/data/Arweave.json`

Table 6.1: Evaluation Script Execution Details

6.1.2 Results

The plots and results presented in the following sections consider the mean values of all 12 script executions. Detailed visualizations of individual runs, showing fluctuations over time, can be found in Appendix D.1 for performance and Appendix D.2 for costs. Performance metrics are displayed in seconds, and costs are shown in Sepolia ETH. As Sepolia ETH has no real value, it was converted to USD based on the Ethereum mainnet rate of USD 3'481.87 on 2024-06-14 at 17:08:41 CEST [20] for reference.

6.1.2.1 Infrastructure Deployment

Depending on the digital identifier, every passport type relies on the NFT, PBT, or DID Registry contract as infrastructure. Hence, this contract must first be deployed on the blockchain. When using HaLo NFC chips, the HaLo NFC Metadata Registry contract must also be deployed to remember passport metadata URIs.

Figure 6.1 shows the infrastructure deployment times for each passport type. On Sepolia, all contracts took about 16 seconds to deploy. The QR code x DID and HaLo NFC x DID passport types performed similarly for this step because both rely on the DID Registry contract. In total, passport types using the HaLo NFC chip took nearly twice as long due to the additional HaLo NFC Metadata Registry contract deployment.

Figure 6.2 compares the gas costs for deploying the contracts needed for each passport type. The DID Registry contract was significantly cheaper to deploy than the NFT and PBT Registry contracts. The PBT contract was slightly more expensive because it extended the NFT contract with additional functionalities. The HaLo NFC Metadata Registry contract was the cheapest to deploy, as it only manages metadata URIs. The QR Code x DID passport type was the most cost-effective at around 8 USD, followed by the QR Code x NFT and HaLo NFC x DID passport types at around 12 USD. The HaLo NFC x PBT passport type was the most expensive and cost twice as much as the cheapest option.

6.1.2.2 Passport Creation

Considering only Sepolia transactions and Arweave interactions, the passport creation process involves four steps. First, passport data is uploaded to Arweave. Second, a digital identifier is created on the blockchain using the passport data URI. Third, the *PermaPass* App automatically creates and uploads the passport metadata to Arweave. This metadata URI can then be encoded into a QR code. For HaLo NFC chip passports, the metadata URI must be linked to the chip's address on the HaLo NFC Metadata Registry contract as the fourth step.

Figure 6.3 illustrates the time required for each operation during passport creation. Uploading data to Arweave, whether metadata or passport data, takes approximately 330

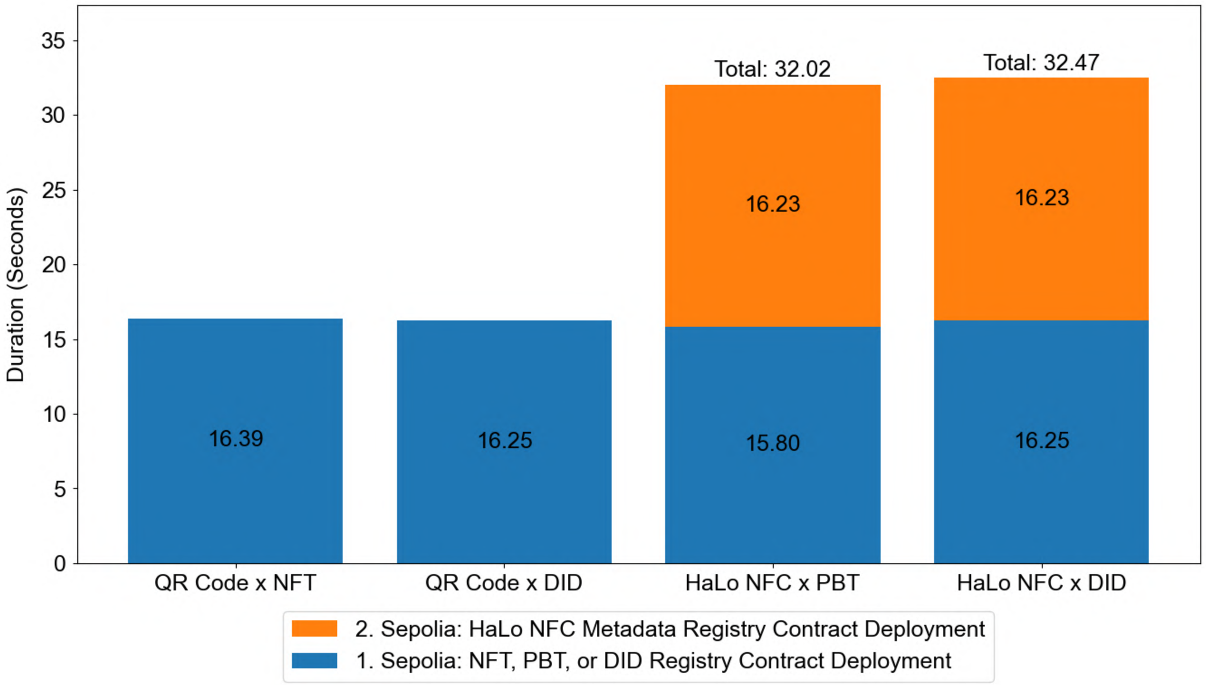


Figure 6.1: Performance of Infrastructure Deployment by Passport Types

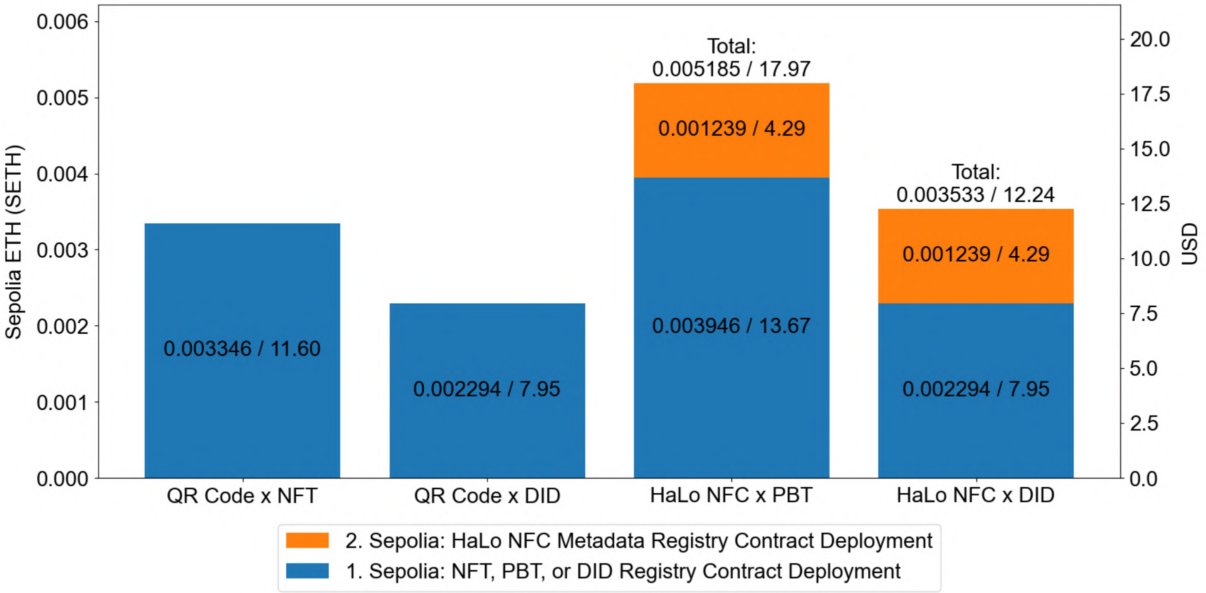


Figure 6.2: Gas Costs for Infrastructure Deployment by Passport Types

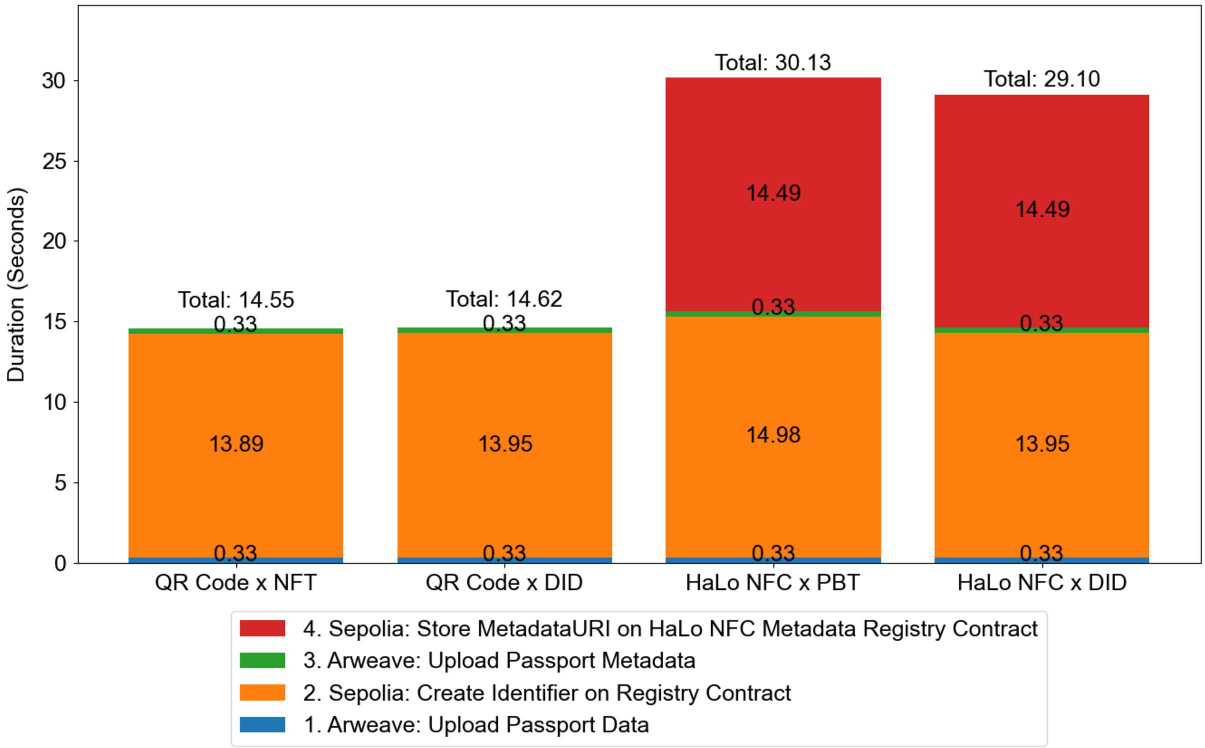


Figure 6.3: Performance of Passport Creation by Passport Types

milliseconds on average. Blockchain transactions on Sepolia take around 14 seconds. Consequently, creating passports using HaLo NFC chips, which requires two Sepolia transactions, takes twice as long as those using a QR code.

Figure 6.4 compares the costs for passport creations. The costs for uploading data to Arweave were not tracked because *PermaPass* uses Irys Node 2 for free uploads. Blockchain transactions incur gas costs. The DID Registry was the most cost-effective, followed by the NFT and PBT registries. Thus, the QR Code x DID passport type was the cheapest to create, costing 0.28 USD on average. Despite requiring an additional Sepolia transaction to store the metadata URI, the HaLo NFC chip x DID passport, costing around 1 USD, was still significantly cheaper than the QR Code x NFT, costing around 1.50 USD. This is due to the low costs of 0.28 USD for creating a DID. However, the HaLo NFC x PBT passport type was the most expensive due to the highest Sepolia transaction costs for creating the digital identifier and storing the metadata URI.

6.1.2.3 Passport Reading

Given a metadata URI, the reading process consists of multiple sequential steps. First, the metadata is read from Arweave. Then, using this metadata, the passport data URI can be retrieved from the NFT, PBT, or DID Registry contract. Finally, this URI is used to fetch Arweave's passport data. If the metadata URI is not stored directly on the data carrier (e.g., a QR code), it must be read from the blockchain, as with the HaLo NFC chip. Since reading data from Arweave and EVM-compatible blockchains is free, there are no costs associated with reading a passport.

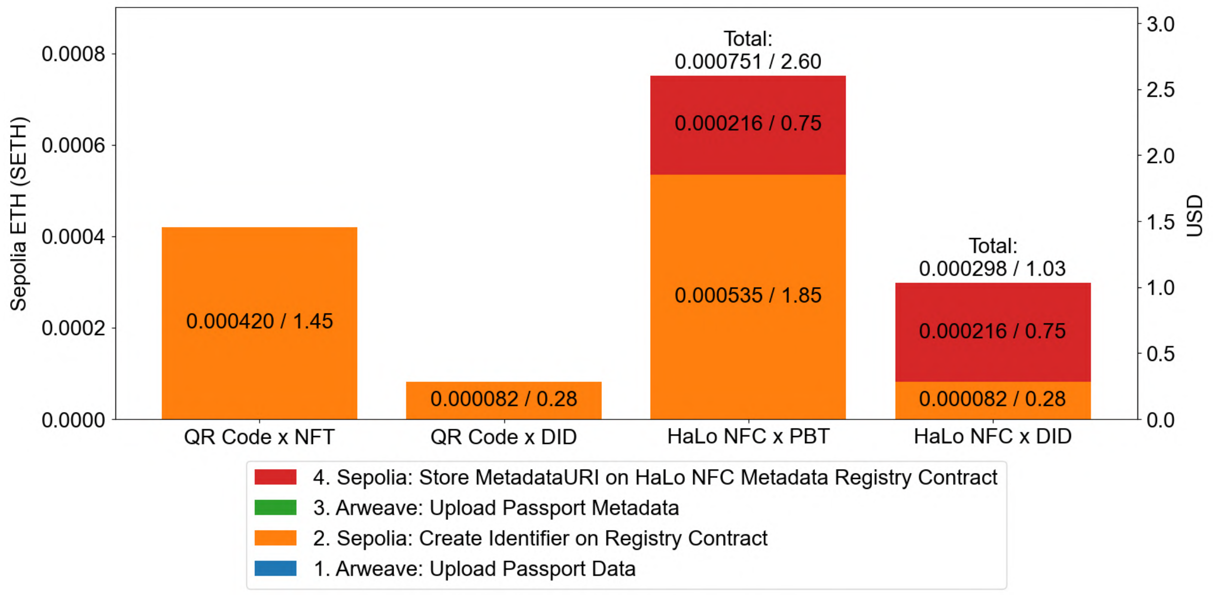


Figure 6.4: Gas Costs for Passport Creation by Passport Types

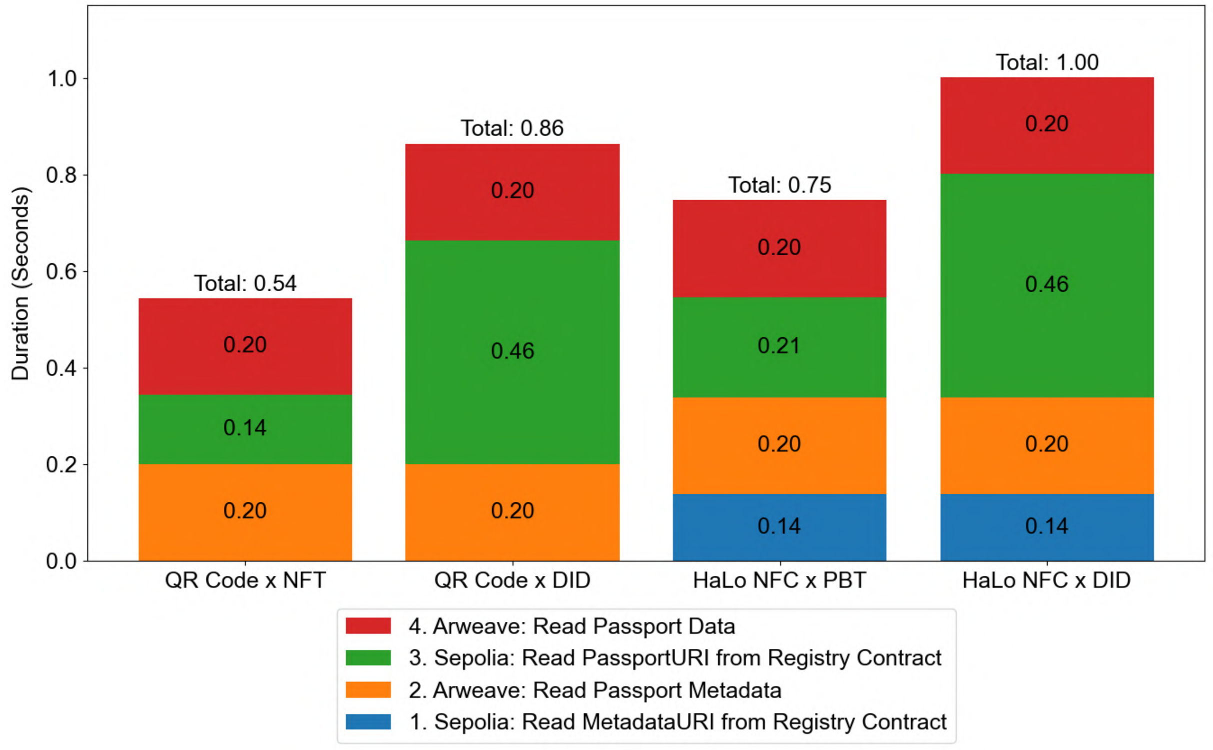


Figure 6.5: Performance of Passport Reading by Passport Types

Figure 6.5 compares the time required for each of these four steps across different passport types. Reading data from Arweave took approximately 0.2 seconds on average. Retrieving passport data URIs from the NFT and PBT Registry contracts also took about 0.2 seconds, whereas using the DID Registry contract took about 0.4 seconds. This is because the DID Registry requires recursively reading all past events, unlike the NFT and PBT registries, which only need a single function call. As a result, passports using DIDs are slower to read than those using NFTs or PBTs.

6.1.2.4 Passport Update

The passport update process involves two main steps: uploading new passport data to Arweave and updating the digital identifier on the blockchain.

Figure 6.6 shows the duration of each operation during the passport update. Uploading passport data to Arweave took approximately 400 milliseconds for all passport types. Updating the digital identifier on registry contracts took about 13 seconds.

Figure 6.7 illustrates the costs for each operation during the passport update. The costs for uploading data to Arweave were not tracked because *PermaPass* uses Irys Node 2 for free uploads. However, Sepolia transactions do incur gas costs. Similar to passport creation, updating a DID on the DID Registry contract was the most cost-effective, costing only USD 0.28. In contrast, updates on the NFT and PBT registries were the most expensive, averaging USD 0.33.

6.1.2.5 Passport Deletion

To delete a passport, its digital identifier must be deleted on the PBT, NFT, or DID Registry contract. Since data cannot be deleted from a blockchain, this process resembles archiving. The owner is changed to the zero address, making the data accessible but unmodifiable.

Figure 6.8 shows the time to delete a digital identifier for each passport type. NFT and PBT registries were the quickest, each taking around 13 seconds. The DID Registry took 17.45 seconds.

Figure 6.9 illustrates the cost of deleting a digital identifier for each passport type. The PBT Registry was the most cost-effective at USD 0.25, followed closely by the DID Registry at USD 0.27. Deleting an NFT was the most expensive, averaging USD 0.35.

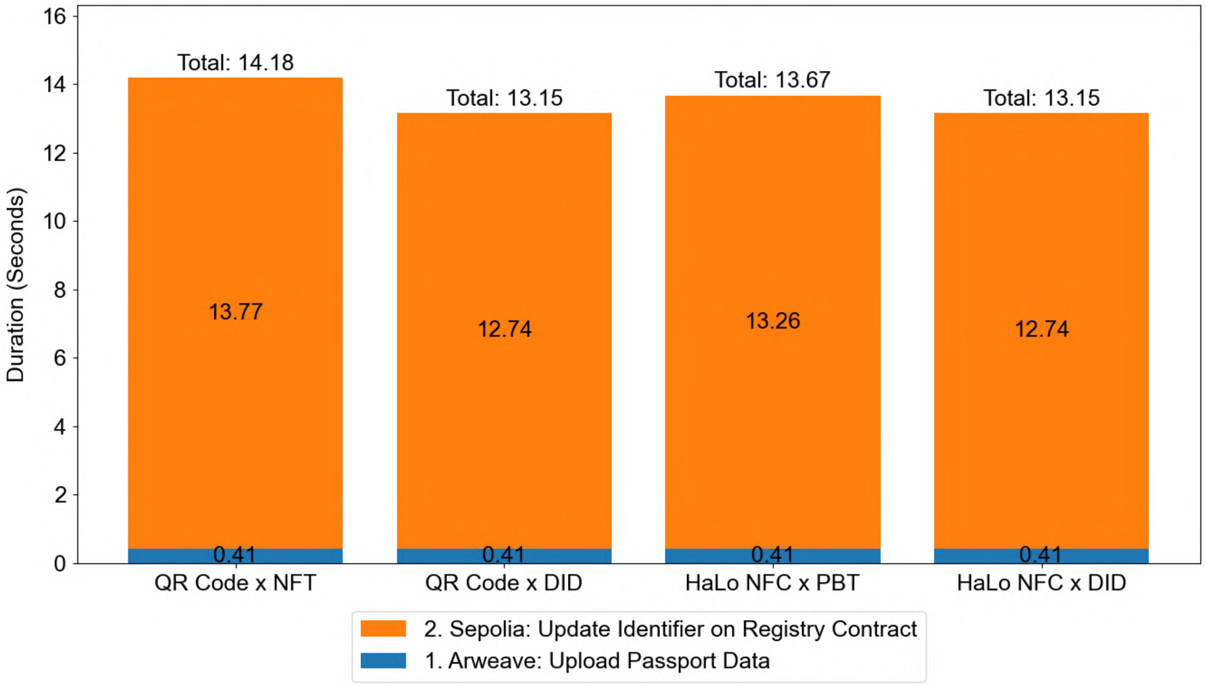


Figure 6.6: Performance of Passport Update by Passport Types

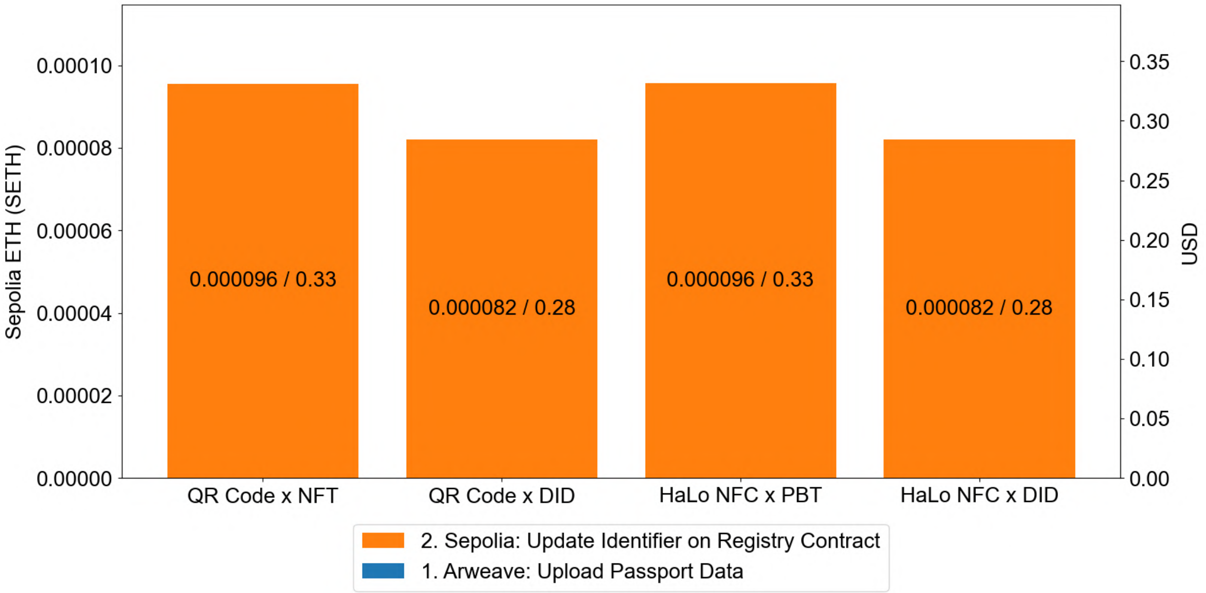


Figure 6.7: Gas Costs for Passport Update by Passport Types

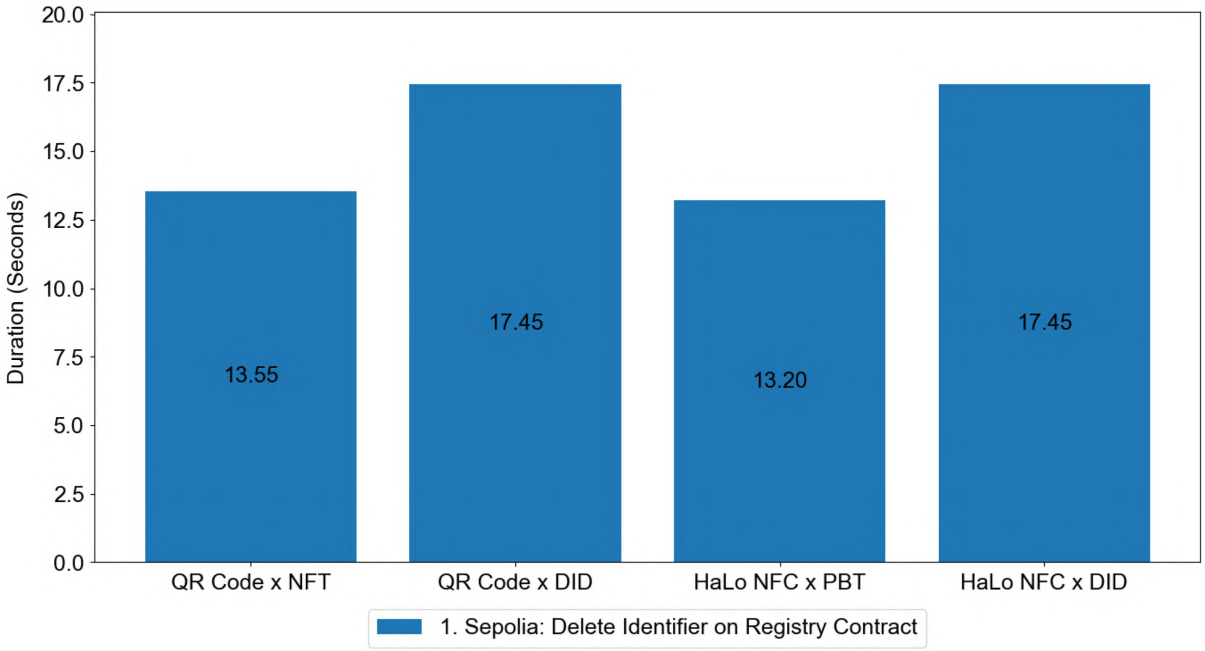


Figure 6.8: Performance of Passport Deletion by Passport Types

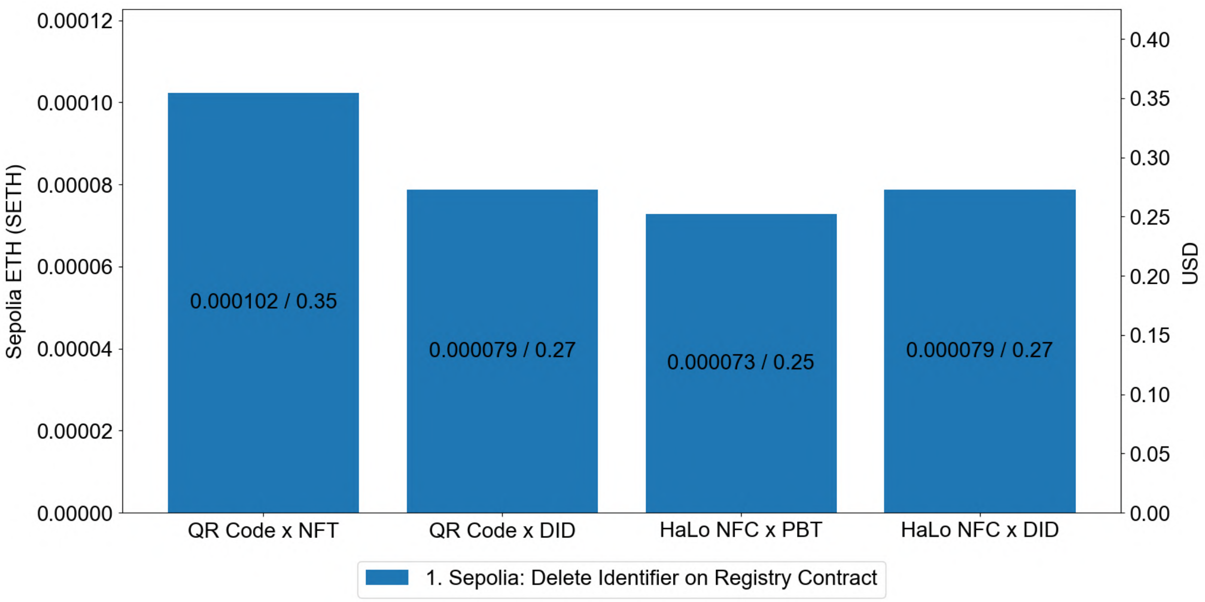


Figure 6.9: Gas Costs for Passport Deletion by Passport Types

6.2 Theoretical Analysis

This chapter provides a theoretical analysis of each passport type's scalability, interoperability, security, and privacy. These evaluation criteria are chosen for their importance in real-world applications of product passport systems, as discussed in Chapter 4.1.1.

6.2.1 Scalability

This section examines the scalability of each passport type. Scalability is considered as the ability to handle an increasing number of passports.

Blockchains are inherently scalable, supporting increasing transactions and data entries. Since all passport types (NFT, PBT, or DID) use the same blockchain, Sepolia, their scalability uniformly depends on Sepolia's capacity to manage extensive data and transactional loads.

The primary scalability differences arise with the data carriers. QR codes can be generated indefinitely. Once created, they can be printed or engraved onto construction products. In contrast, HaLo NFC chips are hardware components requiring specific materials and manufacturing processes. Their production depends on material availability and manufacturing capacity, making them vulnerable to supply chain limitations and bottlenecks.

To conclude, NFTs, PBTs, and DIDs share equal scalability due to their reliance on the same blockchain. However, due to the production dependencies of HaLo NFC chips, QR codes are considered a more scalable data carrier.

6.2.2 Interoperability

This evaluation will assess interoperability by examining how easily other systems can access or modify information within *PermaPass*. The integration of external information into *PermaPass* is not analyzed due to the absence of comparable DPP systems.

Relevant information to exchange with other systems includes passport metadata, passport data (and its modifications), and ownership data.

By design, passport metadata and all versions of the passport data are stored on Arweave as JSON files. Any user interface or computer can access this data using the Arweave URI. The JSON format, being a common and machine-readable standard, supports interoperability.

Passport metadata can be accessed via standardized data carriers such as QR codes and HaLo NFC chips, readable by common smartphones and interfaces. However, ease of access varies. A QR code encodes a URI linking to the *PermaPass* App's reading screen with the metadata URI, for example:

```
com.permapass.app://read?metadataURI=ar://9oHw...9fB0
```

where:

- `com.permapass.app://` denotes the protocol and app schema.
- `read` specifies the location within the app.
- `?metadataURI=ar://9oHw...9fB0` indicates query parameters for the app page.

This standardized format allows third-party systems to parse and use the metadata URI. In contrast, retrieving the metadata URI from a HaLo NFC chip requires fetching it from the blockchain, necessitating prior knowledge of the HaLo NFC Metadata Registry contract address and network.

Once the metadata URI is known, data can be fetched to enable third-party systems to interact with the product's digital identifier. This includes the identifier type (NFT, PBT, or DID), the registry contract's address, the network, and contract interaction data. The metadata structure is detailed in Appendix B. At this point, only the contract's ABI is missing to interact with the contract. Given the network and contract address from the metadata, the contract's ABI can be retrieved from a block explorer like Etherscan for Sepolia [38]. With this information, the blockchain functions as an API with publicly accessible endpoints to retrieve passport data, including modifications and ownership details. Smart contract functions serve as endpoints, and the ABI or contract code acts as documentation.

In summary, using HaLo NFC chips to exchange passport metadata presents more challenges and requires greater effort than QR codes, reducing interoperability. On the other hand, making passport data and ownership information accessible to other systems is equally straightforward for all digital identifiers.

6.2.3 Security

This chapter compares the security of each passport type. Since the prototype's data is stored and secured by Arweave without protected data access to be examined, the security analysis focuses on the authenticity of passport information. For this proof-of-concept system, assessing authenticity based on data completeness and accuracy is impractical. Therefore, the focus is on the trustworthiness of the passport information, specifically the tamper-proof nature of each passport type and its information.

Manipulating passport data in *PermaPass* involves setting a new Arweave URI with manipulated data. For NFTs and PBT, this is done by setting a new token URI on the registry contract. For DIDs, a new service attribute with the new URI can be added. These functions can only be executed when the caller owns the product's digital identifier. This makes the passport data consistent and equally trustworthy across all types.

However, significant differences in trustworthiness arise when linking DPP data to physical products. QR codes can be copied and attached to counterfeit products, risking multiple products linking to the same digital identifier. If not engraved, QR codes can be stolen and transferred to fake products. Additionally, attackers can manipulate QR codes to link products to incorrect passports. Conversely, the HaLo NFC chip is more resistant to modification and duplication because it has a unique chip address and a private key for signing messages to verify authenticity. According to the manufacturer, this data cannot be altered as it is securely and immutably stored on the chip. Duplicating a HaLo NFC chip-based passport would involve linking a new chip to existing passport information, requiring the purchase of a new HaLo NFC chip, and extracting metadata from an existing passport. Using HaLo NFC chips with a DID could allow for passport duplication, as the chip signature is only necessary to link passport metadata to a chip. However, with a PBT, duplication is not feasible. Each operation with the PBT requires the chip to provide a signature to ensure authenticity. This direct connection between the chip and digital identifier prevents a new chip from interacting with an existing PBT, as the generated signature would be incorrect. Nevertheless, stealing the HaLo NFC chip and attaching it to a counterfeit product remains risky.

In conclusion, the trustworthiness of passport information depends on the choice of data carrier. Passports using QR codes are less trustworthy due to their susceptibility to copying. HaLo NFC chips with a DID offer more security by complicating passport duplication efforts. Since the combination of HaLo NFC chips and PBTs is not duplicatable, it is the most secure option, ensuring the highest trustworthiness of passport information.

6.2.4 Privacy

This chapter assesses the ability of all passport types to protect information privacy. It will examine differences in safeguarding personal data from unauthorized access or disclosure.

For *PermaPass*, personal data encompasses activity and passport data. Activity data comprises information about who performs specific operations and at what time, which is considered private and is expected only to be shared with the individual's consent. Passport data may include business secrets and competitive advantages of manufacturers, which are considered confidential and controlled by the data owner.

Typical EVM blockchains, such as Sepolia, are public blockchains where all transactions are visible to anyone. Transactions reveal which addresses perform which operations. Although blockchain addresses are pseudonymous, sophisticated analysis can often link them to real-world individuals. This poses a significant privacy concern for *PermaPass* as activity data becomes publicly accessible without consent.

In *PermaPass*, no restrictions on reading access were implemented. Thus, anyone with physical access to the QR code or HaLo NFC chip is allowed to read passport data. The privacy of passport data is further compromised by its plain text storage on Arweave. Anyone with the Arweave URI can access this unencrypted data. These URIs can be identified by analyzing Sepolia transactions associated with known NFT, PBT, and DID Registry contract addresses. Since Sepolia transactions are publicly accessible, privacy concerns are reinforced.

In summary, privacy concerns arise because *PermaPass* was not designed to prioritize privacy. These concerns include the plain text storage of passport data on Arweave and the public nature of Sepolia transactions. However, these privacy issues are inherent to the design of *PermaPass*. Consequently, all passport types are equally affected, whether they use NFTs, PBTs, DIDs, QR codes, or HaLo NFC chips.

Chapter 7

Discussion

This chapter reviews the findings of this thesis, offering a summary and interpretation of key insights related to the research goals. Additionally, it acknowledges the study's limitations and discusses their potential impact on the findings.

7.1 Summary and Interpretation of Findings

This thesis aims to provide insights into achieving long-term system and data availability and determining the best methods for accessing passport data. The following sections summarize and interpret the findings in the context of these two issues.

7.1.1 Long-Term System and Data Availability

Chapter 4 outlines a prototype design for a decentralized DPP system, including the data carriers for accessing passport information. Chapter 5 details the implementation process. As noted in Chapter 3, this design and implementation are novel. The following insights address critical points regarding the long-term system and data availability of the prototype:

- **System Availability Concerns Due to Centralized User Interface and Sepolia Testnet:** Despite the decentralized nature of the system's core elements, the *PermaPass* user interface relies on centralized technologies. This is due to the dependence of iOS and Android smartphone apps on the services provided by Apple and Google, which are centrally managed. Consequently, this prototype is not built thoroughly decentralized, raising concerns about long-term system availability. Additionally, since the prototype was tested on Sepolia, a testnet not intended for long-term use, its durability is uncertain. Deploying the prototype on the Ethereum mainnet would likely enhance its long-term availability.

- **Data Availability Concerns Due to Arweave Promise:** Long-term data availability depends on Arweave, the decentralized data storage provider used in *PermaPass*. While Arweave claims data will be stored for at least 200 years, this assertion cannot be verified, leading to potential doubts about long-term data availability.

7.1.2 Comparative Benefits and Drawbacks of Passport Types

Chapter 6 details the performances and costs for each operation by passport type. This section summarizes, compares, and interprets those results.

7.1.2.1 Performance

Figure 7.1 compares passport creation, reading, update, and deletion duration for all passport types. Figure 7.2 highlights the relative performance differences among passport types for each evaluation criterion, with coloring to emphasize the differences. The latter additionally includes the duration of the deployment of the passport infrastructure.

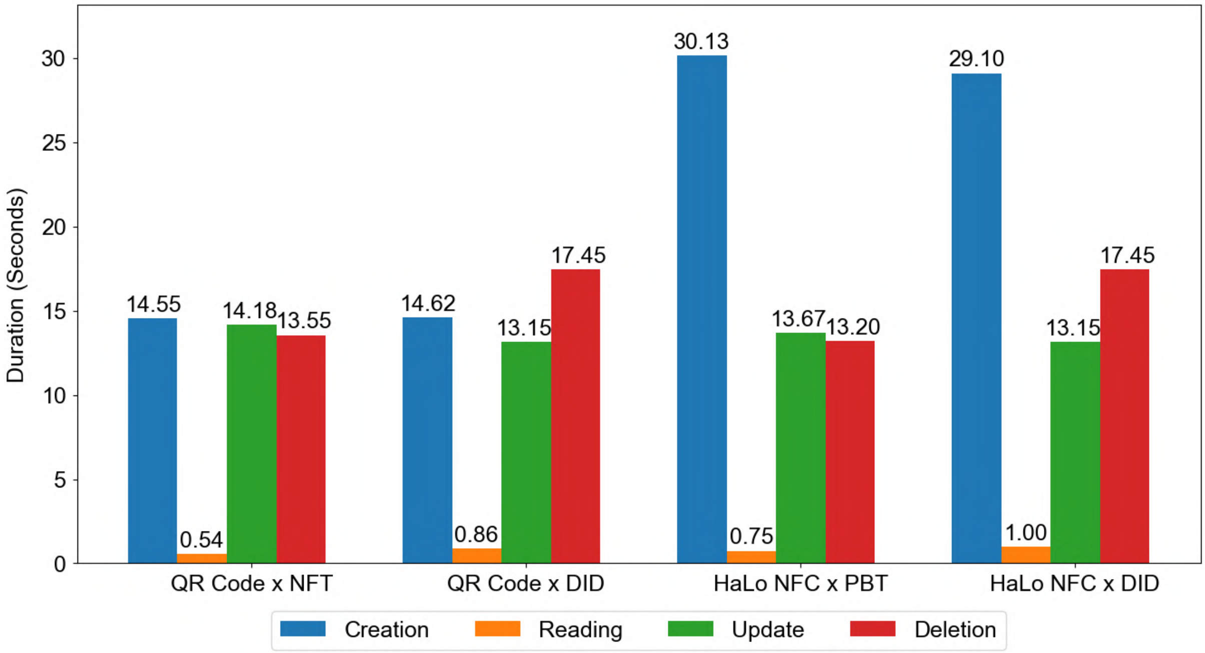


Figure 7.1: Performance of Passport Types Across Passport Actions

Passport reading times ranged from 0.5 to 1 second, approximately 10 times faster than the next quickest passport action. Processing updates and deletions for NFT or PBT types took around 13-14 seconds. In contrast, DID-based passport updates took 13.15 seconds, and deletions took 17.45 seconds, 1.5 times longer. HaLo NFC-based passport creation and infrastructure deployment took significantly longer than QR Code-based passports.

Based on those results, several key insights have been identified:

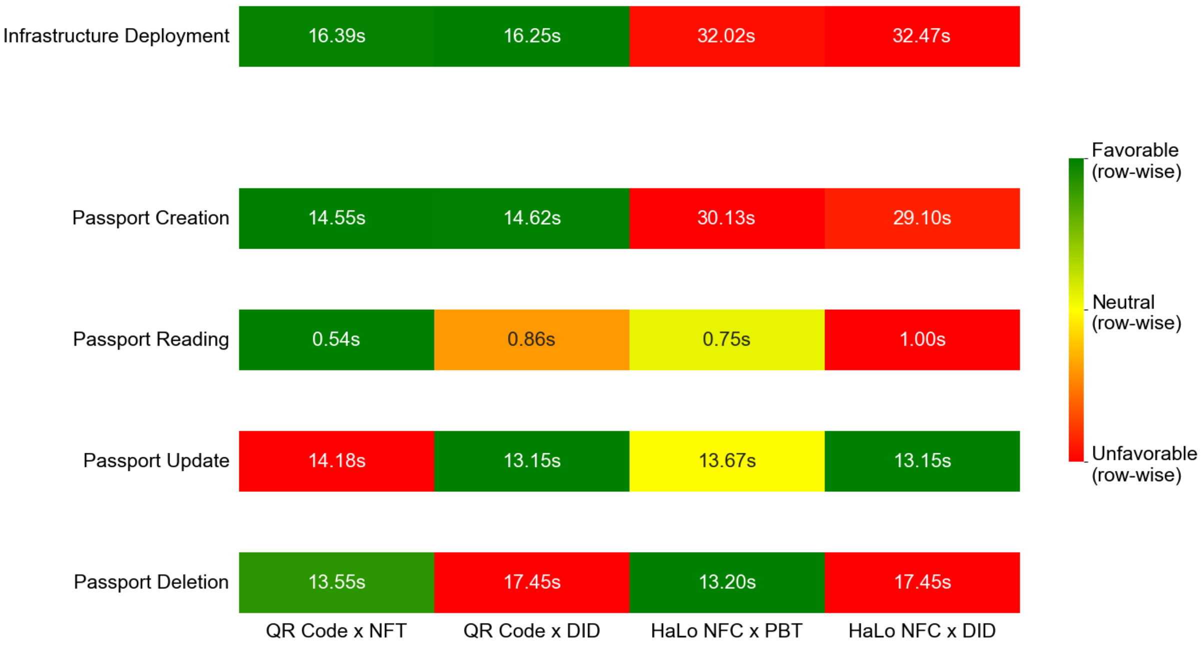


Figure 7.2: Relative Performance Differences of Passport Types by Evaluation Criterion

- **QR Code-Based Passports Offer Faster Infrastructure Deployment and Creation:** QR Code-based passports enable infrastructure deployment and creation almost twice as fast as HaLo NFC chip-based passports. This is because HaLo NFC passports require the deployment and use of the HaLo NFC Metadata Registry contract during creation. This process involves an additional Sepolia transaction, which typically takes 13-16 seconds, significantly contributing to the delay.

- **QR Code x NFT Passports Are the Fastest for Reading:** The duration of passport reading depends on the combination of digital identifier and data carrier. Among digital identifiers, NFTs are the quickest to read, followed closely by PBTs, with a significant lag for DIDs. This discrepancy arises from the DID Registry contract's structure, which necessitates crawling blockchain events to extract the passport URI. In contrast, QR codes outperform HaLo NFC chips, as the latter necessitates an additional blockchain read for the passport's metadata URI.

- **DID-Based Passports Are Faster for Updates:** While DID-based passports are the quickest to update, the performance difference is marginal, less than 10%, providing a slight advantage.

- **NFT and PBT-Based Passports Are Faster for Deletion:** NFTs and PBTs enable faster passport deletion compared to DID-based passports.

7.1.2.2 Costs

Figure 7.3 illustrates the costs for passport creation, update, and deletion for all passport types. Figure 7.4 highlights the relative cost differences among passport types for each evaluation criterion, with coloring to emphasize the differences. The latter additionally includes costs for the deployment of the passport infrastructure.

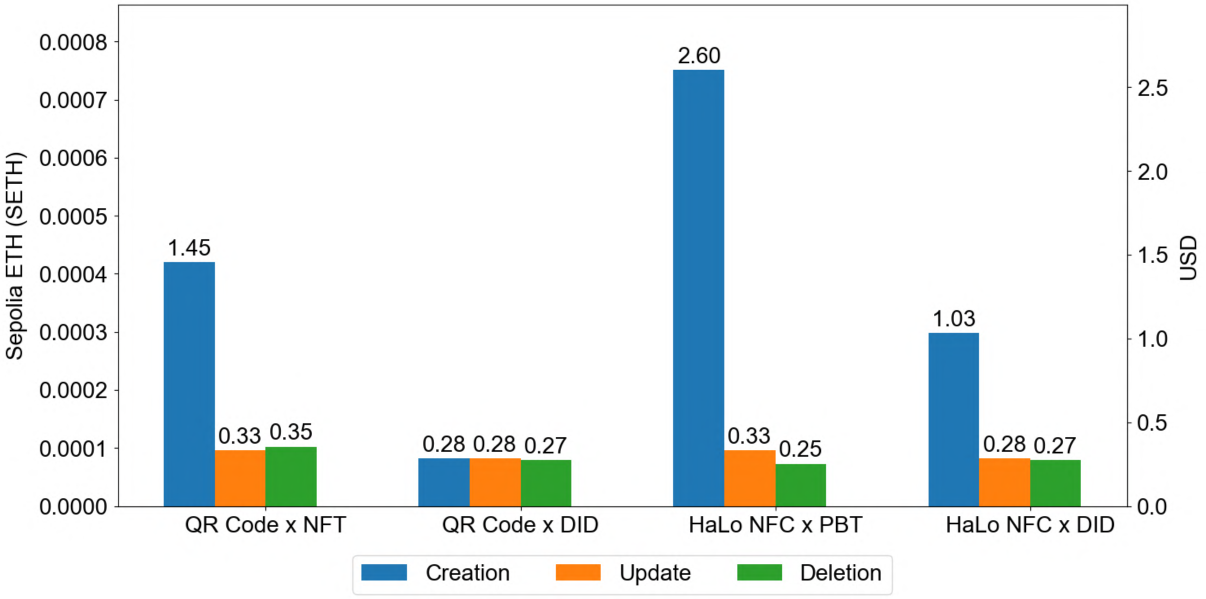
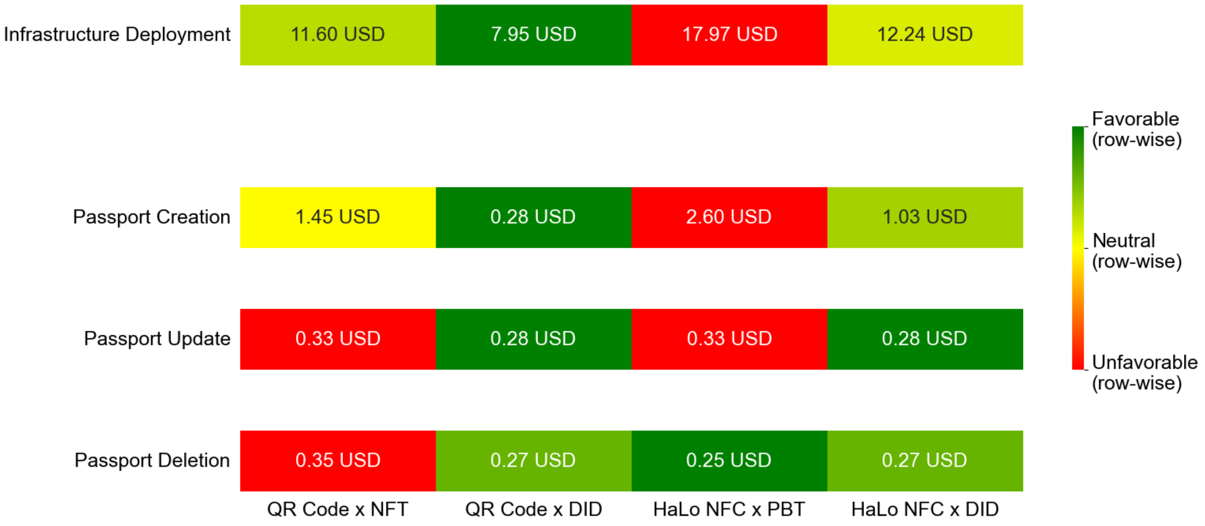


Figure 7.3: Costs of Passport Types Across Passport Actions



	QR Code x NFT	QR Code x DID	HaLo NFC x PBT	HaLo NFC x DID
Infrastructure Deployment	11.60 USD	7.95 USD	17.97 USD	12.24 USD
Passport Creation	1.45 USD	0.28 USD	2.60 USD	1.03 USD
Passport Update	0.33 USD	0.28 USD	0.33 USD	0.28 USD
Passport Deletion	0.35 USD	0.27 USD	0.25 USD	0.27 USD

Figure 7.4: Relative Cost Differences of Passport Types by Evaluation Criterion

The costs for updates and deletions are nearly identical regardless of the passport type. However, passport creation costs vary significantly, with QR Code x DID passports having low costs and HaLo NFC x PBT passports having nearly ten times higher costs. Passport infrastructure deployment is generally ten times more expensive than the next costly operation, such as passport creation, with a significant gap between QR Code x DID and HaLo NFC x PBT passports.

Based on those results, several key insights have been identified:

- **Generally, QR Code x DID Passports Are the Most Cost-Efficient:** Except for deletion, the QR Code x DID passport is the most cost-efficient for any passport operation. This efficiency is due to the cost-effective structure of the DID Registry contract, which was developed by Veramo. Regarding data carriers, HaLo NFC-based passports charge more gas costs for infrastructure deployment and passport creation because of the additional blockchain transactions used to manage passport metadata URIs on the blockchain.

- **PBT-Based Passports Are More Cost-Efficient for Deletion:** The previously introduced cost pattern changes for passport deletion. PBTs are slightly more cost-efficient than DIDs, with NFTs being the most expensive. The higher cost for NFT deletion stems from the additional step of deleting the token URI from the contract's storage. However, given the relatively low absolute cost of around USD 0.30 for a single deletion, the expense is not critical.

7.1.2.3 Scalability, Interoperability and Security

Figure 7.5 highlights the relative differences between passport types based on theoretical analysis results. The analysis reveals that QR Code-based passports are more scalable, as they do not require hardware. They also offer greater interoperability, enabling easier metadata exchange with third-party systems. However, in terms of security, HaLo NFC chip-based passports perform better. The HaLo NFC x DID passport is moderately tamper-proof due to the chip's signature required for metadata reading. The HaLo NFC x PBT passport is the most tamper-proof, securing passport duplication with a chip's signature for both metadata reading and interaction with the digital identifier.

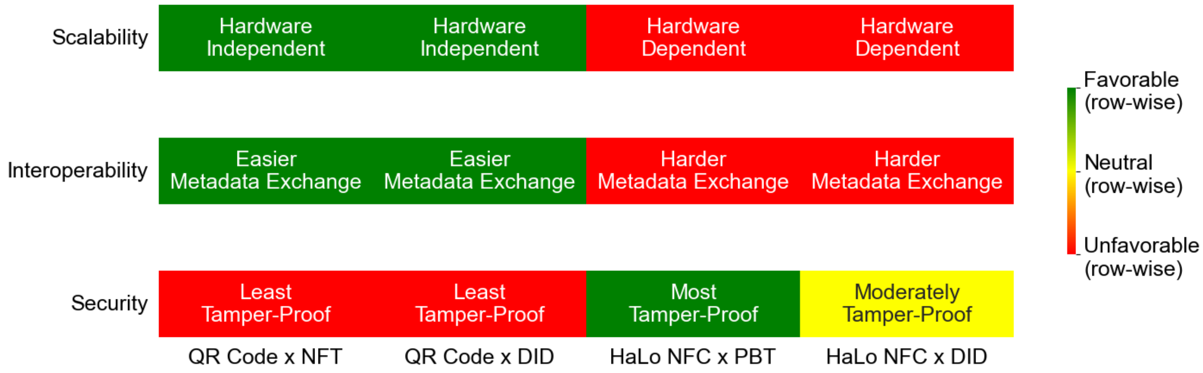
Based on those results, several key insights have been identified:

- **Data Carrier Selection Balances Scalability and Interoperability Against Security:** HaLo NFC-based passports offer better tamper resistance due to their chip address and message signing capabilities. However, since the usage of HaLo NFC chips depends on its production and the improved security hinders easier data passport metadata exchange, the QR code-based passports are more scalable and interoperable.

7.2 Limitations

This research acknowledges several limitations in the evaluation of each passport type, which may influence the findings and their interpretations:

- **Experiment Focused on Sepolia and Arweave Interactions:** The experiment to gather performance and cost data of each passport type focused exclusively on Sepolia transactions and Arweave interactions. The hardware cost of HaLo NFC chips for passport creation was not considered. Additionally, the performance and costs



	QR Code x NFT	QR Code x DID	HaLo NFC x PBT	HaLo NFC x DID
Scalability	🟩 Hardware Independent	🟩 Hardware Independent	🟥 Hardware Dependent	🟥 Hardware Dependent
Interoperability	🟩 Easier Metadata Exchange	🟩 Easier Metadata Exchange	🟥 Harder Metadata Exchange	🟥 Harder Metadata Exchange
Security	🟥 Least Tamper-Proof	🟥 Least Tamper-Proof	🟩 Most Tamper-Proof	🟨 Moderately Tamper-Proof

Figure 7.5: Relative Result Differences of Passport Types by Scalability, Interoperability, and Security

of printing, engraving, or attaching a QR code or HaLo NFC chip to a construction product were not evaluated. For passport reading, the reading time of each data carrier was excluded from the evaluation. Including the performance and costs of purchasing and attaching data carriers could significantly affect the findings. However, including data carrier reading performance is not expected to have a notable impact, as the differences are comparatively small. On a broader level, costs and performance for the entire passport system, including the infrastructure deployment and operation of a user interface, were also not analyzed, which would be useful for comparing the decentralized system to a similar centralized approach.

- **Limited Results for Sepolia Transactions and Arweave Interactions:** The performance and cost data for blockchain transactions on Sepolia and Arweave interactions were based on the average of 12 executions over one hour. This short data collection period does not adequately account for long-term fluctuations in gas costs and performance caused by network state and congestion at the time of execution on Sepolia, as well as the network performance of Arweave. Therefore, the absolute results for performance and costs may vary depending on the future execution time. While the exact values are subject to change, the relative differences in performance and costs are likely to remain consistent, reflecting proportional fluctuations over time.

- **Approximate USD Cost Conversion:** Blockchain transaction costs are paid in the blockchain's native cryptocurrency. Sepolia ETH gas costs were converted to USD using the June 14, 2024 conversion rate. These USD values must be considered reference points due to cryptocurrency volatility, which can significantly affect the results. However, the relative cost differences are likely to remain unchanged.

Chapter 8

Conclusion and Future Work

This chapter presents the conclusion, summarizing key findings and offering recommendations. It further suggests potential future research topics.

8.1 Conclusion

This thesis aims to advance DPP systems development by addressing two key challenges in the built environment: ensuring long-term system and data availability and determining the best method for passport data access. Valuable insights were gained through the design, implementation, and evaluation of a decentralized DPP system prototype called *PermaPass*.

The *PermaPass* prototype illustrated how decentralized technologies and physical components can enhance long-term system and data availability. However, Chapter 7.1.1 identified several issues with this approach.

The most notable finding is the infeasibility of running a smartphone app in a decentralized manner. This limitation hinders the development of a fully decentralized DPP system. Future advancements in technology and devices may enable decentralized user interfaces, improving long-term system availability.

During implementation, several technical challenges were encountered. No packages were available to interact with Arweave for React Native apps. Dependencies for interacting with HaLo NFC chips and using Veramo's services for DIDs on Ethereum were also incompatible. As a result, a Web API was necessary, raising concerns about long-term system availability.

The evaluation, discussed in Chapter 7.1.2, compared NFTs, PBTs, and DIDs for managing product identity and ownership, and QR codes and HaLo NFC chips for passport data access.

DIDs generally offer faster passport updates, while NFTs and PBTs are quicker for passport creation, reading, and deletion. QR codes outperform HaLo NFC chips in overall speed for all actions. Regarding costs, DIDs are the most cost-efficient for passport creation, updates, and deletion. HaLo NFC chip passports are more tamper-proof, while

QR code passports provide better scalability and interoperability.

No single passport type excels in all criteria. HaLo NFC chips are recommended for counterfeit protection. DID-based passports for cost-efficiency, and QR codes for fast processing. However, these recommendations are based on limited experimental data involving Sepolia and Arweave interactions. The analysis did not account for the hardware costs of HaLo NFC chips or the performance and costs associated with attaching QR codes and HaLo NFC chips to construction products, which could significantly affect the results.

8.2 Future Work

Given this research's limitations and general considerations, the following future work is recommended:

- **Comparing Evaluation Results with Centralized Systems:** This thesis evaluates the advantages and drawbacks of different passport types within a decentralized DPP system. Comparing these results with centralized systems can be insightful, particularly if the centralized systems are designed to ensure long-term system and data availability.

- **In-Depth Research on Performance Fluctuations and Gas Fees Across EVM Chains:** The prototype design in this thesis relies on blockchain for managing product passports, making blockchain transactions essential. Future work should investigate the fluctuations in transaction execution speed and gas costs more extensively and derive their impacts. Additionally, this analysis should expand to several productive EVM-compatible blockchains to highlight the trade-offs between different blockchain usages.

- **Usability Study of Decentralized DPP Applications:** Most smartphone apps and software today are based on centralized technologies managed by central companies. In contrast, decentralized applications present a completely new user experience. In centralized applications, user accounts are managed by the companies, while decentralized applications use self-custodial wallets. Operations in centralized systems typically involve entering a user account password and are free when changing data. However, in decentralized systems, operations require transaction confirmations using a wallet application and incur gas fees when changing data. Despite the potential benefits of decentralized DPP systems, user acceptance cannot be assumed due to these significant changes in system interactions. Therefore, a usability study is necessary to explore this issue, providing insights and suggesting design improvements to enhance user-friendliness and acceptance of decentralized systems.

- **Investigate Solutions to Exchange Defective Halo NFC Chips:** HaLo NFC chips are designed to last about 10 years, according to the manufacturer [86]. However, being hardware, they can potentially fail at any time. Even with a system that ensures long-term data availability, access to passport data via HaLo NFC chips cannot be guaranteed indefinitely. The prototype in this thesis does not address replacing data carriers for passport data. Exploring methods to replace defective HaLo NFC chips is recommended to ensure long-term access to passport data.

Bibliography

[1] 2pmflow et al. *ERC-5791: Physical Backed Tokens*. Oct. 2022. URL: https://eips.ethereum.org/EIPS/eip-5791 (visited on July 12, 2024).

[2] Thomas Adisorn, Lena Tholen, and Thomas Götz. “Towards a Digital Product Passport Fit for Contributing to a Circular Economy”. In: *Energies* 14.8 (Apr. 2021), p. 2289.

[3] Hussein Ahmad Al-Ofeishat and Mohammad AA Al Rababah. “Near Field Communication (NFC)”. In: *International Journal of Computer Science and Network Security (IJCSNS)* 12.2 (2012), p. 93.

[4] Alchemy. *What is the Sepolia testnet?* Mar. 2023. URL: https://www.alchemy.com/overviews/sepolia-testnet (visited on June 21, 2024).

[5] Luís Alves et al. “A Traceability Platform for Monitoring Environmental and Social Sustainability in the Textile and Clothing Value Chain: Towards a Digital Passport for Textiles and Clothing”. In: *Sustainability* 16.1 (Dec. 2023), p. 82.

[6] Arweave. *Arweave - A community-driven ecosystem*. URL: https://www.arweave.org/ (visited on Apr. 4, 2024).

[7] Arweave. *Posting Transactions using Irys (Previously Bundlr) | Cooking with the Permaweb*. URL: https://cookbook.arweave.dev/guides/posting-transactions/irys.html (visited on June 24, 2024).

[8] Islam Atta, Emad S. Bakhoum, and Mohamed M. Marzouk. “Digitizing material passport for sustainable construction projects using BIM”. In: *Journal of Building Engineering* 43 (Nov. 2021), p. 103233.

[9] Gabriele Bandini et al. “An RFID System Enabling Battery Lifecycle Traceability”. In: *2023 IEEE International Workshop on Metrology for Automotive (MetroAutomotive)*. June 2023, pp. 46–50.

[10] Andrew Beanland. *The EU Digital Product Passport shapes the future of value chains: What it is and how to prepare now*. 2023.

[11] Holger Berg et al. “Overcoming Information Asymmetry in the Plastics Value Chain with Digital Product Passports”. In: *Wuppertal Institut für Klima, Umwelt, Energie: Wuppertal, Germany* (2022).

[12] BitTorrent. *BitTorrent File System (BTFS) | Scalable Decentralized File Storage*. URL: https://www.bittorrent.com/token/bittorrent-file-system/ (visited on Apr. 4, 2024).

[13] M Buchholz and T Lützkendorf. “Building passports and material inventories – concepts, trends, job sharing”. In: *IOP Conference Series: Earth and Environmental Science* 1122.1 (Dec. 2022), p. 012038.

[14] EPEA Nederland BV and SundaHus i Linkoping AB. *Framework for Materials Passports*. 2017. URL: https://www.bamb2020.eu/wp-content/uploads/2018/01/Framework-for-Materials-Passports-for-the-webb.pdf (visited on Feb. 6, 2024).

[15] Brandon S. Byers and Catherine De Wolf. "QR Code-Based Material Passports for Component Reuse Across Life Cycle Stages in Small-Scale Construction". In: *Circular Economy* 1.2 (July 2023), pp. 1–16.

[16] Brandon S. Byers et al. "Using engraved QR codes to connect building components to materials passports for circular construction". In: *2022 European Conference on Computing in Construction*. July 2022.

[17] Raul Carlsson, Tatiana Nevzorova, and Karolina Vikingsson. "Long-Lived Sustainable Products through Digital Innovation". In: *Sustainability* 14.21 (Nov. 2022), p. 14364.

[18] S. Casale-Brunet et al. *Networks of Ethereum Non-Fungible Tokens: A graph-based analysis of the ERC-721 ecosystem*. Oct. 2021. URL: http://arxiv.org/abs/2110.12545 (visited on July 12, 2024).

[19] Usman W. Chohan. "Non-Fungible Tokens: Blockchains, Scarcity, and Value". In: *SSRN Electronic Journal* (2021).

[20] CoinGecko. *Ethereum Price: ETH Live Price Chart, Market Cap & News Today*. June 2024. URL: https://www.coingecko.com/en/coins/ethereum (visited on June 25, 2024).

[21] European Commission. *Circular economy*. Mar. 2024. URL: https://environment.ec.europa.eu/topics/circular-economy_en (visited on Mar. 14, 2024).

[22] European Commission. *Circular Economy Action Plan: The European Green Deal*. 2020.

[23] European Commission. *Proposal for a Regulation of the European Parliament and of the Council Establishing a Framework for Setting Ecodesign Requirements for Sustainable Products and Repealing Directive 2009/125/EC*. 2022.

[24] European Commission. *The European Green Deal*. 2019.

[25] Association for Computing Machinery. *Advanced Search*. URL: https://dl.acm.org/search/advanced (visited on Mar. 5, 2024).

[26] Samuel Copeland and Melissa Bilec. "Buildings as material banks using RFID and building information modeling in a circular economy". In: *Procedia CIRP* 90 (2020), pp. 143–147.

[27] Vedat Coskun, Kerem Ok, and Busra Ozdenizci. *Near Field Communication (NFC): From Theory to Practice*. Dec. 2011.

[28] Jennifer Davies et al. "Non-fungible tokens: The missing ingredient for sustainable supply chains in the metaverse age?" In: *Transportation Research Part E: Logistics and Transportation Review* 182 (Feb. 2024), p. 103412.

[29] Catherine De Wolf, Sultan Çetin, and Nancy M. P. Bocken, eds. *A Circular Built Environment in the Digital Age*. Circular Economy and Sustainability. 2024.

[30] Arlind Dervishaj, José Hernández Vargas, and Kjartan Gudmundsson. "Enabling reuse of prefabricated concrete components through multiple tracking technologies and digital twins". In: *2023 European Conference on Computing in Construction and the 40th International CIB W78 Conference*. July 2023.

[31] Theodoros Dounas, Wassim Jabi, and Davide Lombardi. “Non-Fungible Building Components: Using Smart Contracts for a Circular Economy in the Built Environment”. In: *Blucher Design Proceedings*. Dec. 2021, pp. 1189–1198.

[32] Luay N. Dwaikat and Kherun N. Ali. “Green buildings life cycle cost analysis and life cycle budget development: Practical applications”. In: *Journal of Building Engineering* 18 (July 2018), pp. 303–311.

[33] Nabil El Ioini and Claus Pahl. “A Review of Distributed Ledger Technologies”. In: *On the Move to Meaningful Internet Systems. OTM 2018 Conferences*. Ed. by Hervé Panetto et al. Vol. 11230. 2018, pp. 277–288.

[34] Pascal Emmenegger. *PermaPass*. URL: https://github.com/pemmenegger/permapass (visited on June 23, 2024).

[35] William Entriken et al. *ERC-721: Non-Fungible Token Standard*. Jan. 2018. URL: https://eips.ethereum.org/EIPS/eip-721 (visited on July 12, 2024).

[36] Erasmus Universiteit Rotterdam. *Search methods & techniques: Search methods*. URL: https://libguides.eur.nl/informationskillssearchmethods/methods (visited on Feb. 14, 2024).

[37] Erasmus Universiteit Rotterdam. *Search methods & techniques: Search techniques*. URL: https://libguides.eur.nl/informationskillssearchmethods/techniques (visited on Feb. 14, 2024).

[38] etherscan.io. *Sepolia (ETH) Blockchain Explorer*. URL: https://sepolia.etherscan.io/ (visited on July 7, 2024).

[39] European Commission. *Definition of the digital building logbook – Report 1 of the study on the development of a European Union framework for buildings’ digital logbook*. 2020.

[40] Expo. *Expo Documentation*. URL: https://docs.expo.dev/get-started/introduction/ (visited on June 23, 2024).

[41] Express.js. *Express - Node.js web application framework*. URL: https://expressjs.com/ (visited on June 24, 2024).

[42] Filecoin. *Filecoin*. URL: https://filecoin.io/ (visited on Apr. 4, 2024).

[43] Senay A. Gebreab et al. “NFT-Based Traceability and Ownership Management of Medical Devices”. In: *IEEE Access* 10 (2022), pp. 126394–126411.

[44] Martin Geissdoerfer et al. “The Circular Economy – A new sustainability paradigm?” In: *Journal of Cleaner Production* 143 (Feb. 2017), pp. 757–768.

[45] Matteo Giovanardi et al. “Internet of Things for building façade traceability: A theoretical framework to enable circular economy through life-cycle information flows”. In: *Journal of Cleaner Production* 382 (Jan. 2023), p. 135261.

[46] Nenad Gligoric et al. “SmartTags: IoT Product Passport for Circular Economy Based on Printed Sensors and Unique Item-Level Identifiers”. In: *Sensors* 19.3 (Jan. 2019), p. 586.

[47] Dr Susanne Guth-Orlowski. *The digital product passport and its technical implementation*. Oct. 2021. URL: https://medium.com/@susi.guth/the-digital-product-passport-and-its-technical-implementation-efdd09a4ed75 (visited on Mar. 21, 2024).

[48] Thomas Götz et al. *Digital Product Passport: the ticket to achieving a climate neutral and circular European economy?* 2022.

[49] Liisa Hakola et al. “Durable and sustainable smart tags for identity management and condition monitoring: Case study for reusable packaging and recyclable data carriers”. In: *Packaging Technology and Science* 37.2 (Feb. 2024), pp. 107–121.

[50] Hardhat. *Hardhat | Ethereum development environment for professionals by Nomic Foundation*. URL: https://hardhat.org/ (visited on June 24, 2024).

[51] M Honic, I Kovacic, and H Rechberger. “Concept for a BIM-based Material Passport for buildings”. In: *IOP Conference Series: Earth and Environmental Science* 225 (Feb. 2019), p. 012073.

[52] Meliha Honic, Iva Kovacic, and Helmut Rechberger. “BIM-Based Material Passport (MP) as an Optimization Tool for Increasing the Recyclability of Buildings”. In: *Applied Mechanics and Materials* 887 (Jan. 2019), pp. 327–334.

[53] Meliha Honic, Pedro Meda Magalhães, and Pablo Van Den Bosch. “From Data Templates to Material Passports and Digital Product Passports”. In: *A Circular Built Environment in the Digital Age*. Ed. by Catherine De Wolf, Sultan Çetin, and Nancy M. P. Bocken. 2024, pp. 79–94.

[54] P. Hradil, K. Jaakkola, and K. Tuominen. “RFID-based traceability system for constructional steel reuse”. In: *Life-Cycle of Structures and Infrastructure Systems*. 1st ed. June 2023, pp. 1295–1302.

[55] Jens J Hunhevicz et al. “Web3-based role and token data access: the case of building material passports”. In: *2023 European Conference on Computing in Construction and the 40th International CIB W78 Conference*. July 2023.

[56] IPFS. *IPFS: An open system to manage data without a central server*. URL: https://ipfs.tech (visited on Apr. 4, 2024).

[57] Irys. *Irys | Fees*. Apr. 2024. URL: https://docs.irys.xyz (visited on June 24, 2024).

[58] ISO/IEC. *ISO/IEC 25010:2011 Systems and software engineering — Systems and software Quality Requirements and Evaluation (SQuaRE) — System and software quality models*. 2011.

[59] Maike Jansen et al. “Stop Guessing in the Dark: Identified Requirements for Digital Product Passport Systems”. In: *Systems* 11.3 (Feb. 2023), p. 123.

[60] Niclas Kannengießer et al. “Trade-offs between Distributed Ledger Technology Characteristics”. In: *ACM Computing Surveys* 53.2 (Mar. 2021), pp. 1–37.

[61] Julian Kirchherr, Denise Reike, and Marko Hekkert. “Conceptualizing the circular economy: An analysis of 114 definitions”. In: *Resources, Conservation and Recycling* 127 (Dec. 2017), pp. 221–232.

[62] Jan Konietzko, Nancy Bocken, and Erik Jan Hultink. “A Tool to Analyze, Ideate and Develop Circular Innovation Ecosystems”. In: *Sustainability* 12.1 (Jan. 2020), p. 417.

[63] Mahtab Kouhizadeh, Qingyun Zhu, and Joseph Sarkis. “Blockchain and the circular economy: potential tensions and critical reflections from practice”. In: *Production Planning & Control* 31.11-12 (2020), pp. 950–966.

[64] Merit Kõlvart, Margus Poola, and Addi Rull. “Smart Contracts”. In: *The Future of Law and eTechnologies*. Ed. by Tanel Kerikmäe and Addi Rull. 2016, pp. 133–147.

[65] Chiru Labs. *PBT (Physical Backed Token)*. URL: https://github.com/chiru-labs/PBT (visited on June 21, 2024).

[66] Zhengdong Liu and Tianyu Ma. “The design of clothing washable labels based on NFC”. In: *ITM Web of Conferences* 17 (2018). Ed. by Kei Eguchi and Tong Chen, p. 03024.

[67] Marcos Allende López. *Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain.* 2020.

[68] Ellen MacArthur. “Towards the circular economy”. In: *Journal of Industrial Ecology* 2.1 (2013), pp. 23–44.

[69] Lodovica Marchesi et al. “Design Patterns for Gas Optimization in Ethereum”. In: *2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE).* Feb. 2020, pp. 9–15.

[70] Meta. *React Native · Learn once, write anywhere.* URL: `https://reactnative.dev/` (visited on June 23, 2024).

[71] MetaMask. *The Ultimate Crypto Wallet for DeFi, Web3 Apps, and NFTs | MetaMask.* URL: `https://metamask.io/` (visited on June 22, 2024).

[72] Finn Miller. *Top 6 Decentralized Storage Platforms for Storing Data on the Blockchain.* Sept. 2023. URL: `https://dailycoin.com/decentralized-data-storage-networks-top-alternatives-to-consider/` (visited on Apr. 4, 2024).

[73] Aayushi Mishra and Manish Mathuria. “A Review on QR Code”. In: *International Journal of Computer Applications* 164.9 (Apr. 2017), pp. 17–19.

[74] M R Munaro et al. “Proposal of a building material passport and its application feasibility to the wood frame constructive system in Brazil”. In: *IOP Conference Series: Earth and Environmental Science* 225 (Feb. 2019), p. 012018.

[75] Vishal Naranje and Rajguru Swarnalatha. “Design of Tracking System for Prefabricated Building Components using RFID Technology and CAD Model”. In: *Procedia Manufacturing* 32 (2019), pp. 928–935.

[76] Leandro Navarro et al. “Digital transformation of the circular economy: Digital product passports for transparency, verifiability, accountability.” 2022.

[77] D. Ness et al. “An ICT-enabled Product Service System for Reuse of Building Components”. In: *IFAC-PapersOnLine* 52.13 (2019), pp. 761–766.

[78] Node.js. *Node.js — Run JavaScript Everywhere.* URL: `https://nodejs.org/en` (visited on June 24, 2024).

[79] Szymon Nowacki, Gokay Meric Sisik, and Constantinos Marios Angelopoulos. “Digital Product Passports: Use Cases Framework and Technical Architecture Using DLT and Smart Contracts”. In: *2023 19th International Conference on Distributed Computing in Smart Systems and the Internet of Things (DCOSS-IoT).* June 2023, pp. 373–380.

[80] OpenZeppelin. *OpenZeppelin Contracts.* URL: `https://github.com/OpenZeppelin/openzeppelin-contracts` (visited on June 21, 2024).

[81] Matthew J Page et al. “PRISMA 2020 explanation and elaboration: updated guidance and exemplars for reporting systematic reviews”. In: *BMJ* (Mar. 2021), n160.

[82] Qirjako Panoti, Radwa Abdelhafez, and Seongho Ha. “Reuse of existing precast panels as a low carbon alternative - Design proposals through the use of digital tools”. In: *Construction & Robotics : Research Driven Project / Sigrid Brell-Cokcan.* 2023, pages 34–56.

[83] Alex Preukschat and Drummond Reed. *Self-Sovereign Identity.* 2021.

[84] United Nations Environment Programme. *2022 Global Status Report for Buildings and Construction: Towards a Zero-emission, Efficient and Resilient Buildings and Construction Sector*. Tech. rep. 2022.

[85] Rainbow. *Rainbow | Fun, powerful, and secure crypto wallets*. URL: https://rainbow.me/ (visited on June 22, 2024).

[86] ARX Research. *Arx Documentation*. URL: https://docs.arx.org/ (visited on July 11, 2024).

[87] ARX Research. *Arx Website*. URL: https://arx.org/ (visited on Jan. 19, 2024).

[88] ARX Research. *The Hidden Expiration Date in NFC Chipped Goods*. Aug. 2023. URL: https://mirror.xyz/arx-research.eth/jgJG3vygw9GbwZtpnxeXE1toZQq4nIjCfCJink55u-c (visited on Jan. 19, 2024).

[89] Melissa L. Rethlefsen and Matthew J. Page. "PRISMA 2020 and PRISMA-S: common questions on tracking records and the flow diagram". In: *Journal of the Medical Library Association* 110.2 (Nov. 2021).

[90] Leila Saari et al. *Digital product passport promotes sustainable manufacturing: Whitepaper*. 2022.

[91] Ethereum Reality Service. *What is a PBT? – ERS Documentation*. Oct. 2023. URL: https://docs.ers.to/overview/concepts/pbt (visited on July 12, 2024).

[92] Robert Sheldon and Brien Posey. *7 decentralized data storage networks compared*. 2023. URL: https://www.techtarget.com/searchstorage/tip/Comparing-4-decentralized-data-storage-offerings (visited on Apr. 4, 2024).

[93] Sia. *Sia - Decentralized data storage*. URL: https://sia.tech/ (visited on Apr. 4, 2024).

[94] Solidity. *Solidity Programming Language*. URL: https://soliditylang.org/ (visited on June 24, 2024).

[95] Reza Soltani, Uyen Trang Nguyen, and Aijun An. "A Survey of Self-Sovereign Identity Ecosystem". In: *Security and Communication Networks* 2021 (July 2021). Ed. by Clemente Galdi, pp. 1–26.

[96] Permanent Data Solutions. *What is Arweave?* Nov. 2023. URL: https://medium.com/ar-io/what-is-arweave-e9ce6920418f (visited on Apr. 4, 2024).

[97] Tan Jin Soon. "QR code". In: *Synthesis Journal* (2008).

[98] Manu Sporny et al. *Decentralized Identifiers (DIDs) v1.0*. July 2022. URL: https://www.w3.org/TR/did-core/ (visited on Apr. 3, 2024).

[99] Manu Sporny et al. *Verifiable Credentials Data Model v1.1*. Mar. 2022. URL: https://www.w3.org/TR/vc-data-model/ (visited on July 12, 2024).

[100] Storj. *Storj*. URL: https://www.storj.io/ (visited on Apr. 4, 2024).

[101] World Business Council for Sustainable Development. *Enabling circularity through transparency: Introducing the EU Digital Product Passport*. Jan. 2023. URL: https://www.wbcsd.org/contentwbc/download/15585/226483/1 (visited on Feb. 6, 2024).

[102] John Swift et al. "Towards Adaptable and Reusable Building Elements: Harnessing the Versatility of the Construction Database Through RFID and BIM". In: *Proceedings of the UIA Seoul World Architects Congress*. 2017.

[103] Swisslife. *What is the lifespan of a house?* Aug. 2017. URL: https://www.swisslife.com/en/home/blog/what-is-the-lifespan-of-a-house.html (visited on Mar. 22, 2024).

[104] Anuja Talla and Stephen McIlwaine. "Industry 4.0 and the circular economy: using design-stage digital technology to reduce construction waste". In: *Smart and Sustainable Built Environment* 13.1 (Jan. 2024), pp. 179–198.

[105] Laura Tihon and Lisa Weißmann. "Mass-Customised Fashion in a Smart Holistic Wear-Care Business Model". In: *ECP 2023*. May 2023, p. 8.

[106] Sumit Tiwari. "An Introduction to QR Code Technology". In: *2016 International Conference on Information Technology (ICIT)*. Dec. 2016, pp. 39–44.

[107] TrustWallet. *Best Crypto Wallet for Web3, NFTs and DeFi | Trust*. URL: `https://trustwallet.com/` (visited on June 22, 2024).

[108] TypeScript. *JavaScript With Syntax For Types*. URL: `https://www.typescriptlang.org/` (visited on June 23, 2024).

[109] Veramo (formerly uPort). *ETHR DID Method Specification*. URL: `https://github.com/decentralized-identity/ethr-did-resolver/blob/master/doc/did-method-spec.md` (visited on June 21, 2024).

[110] Veramo (formerly uPort). *ethr-did-registry/contracts/EthereumDIDRegistry.sol at master · uport-project/ethr-did-registry*. URL: `https://github.com/uport-project/ethr-did-registry/blob/master/contracts/EthereumDIDRegistry.sol` (visited on June 24, 2024).

[111] Veramo (formerly uPort). *uport-project/ethr-did*. Mar. 2024. URL: `https://github.com/uport-project/ethr-did` (visited on Apr. 3, 2024).

[112] Ali Vahidi et al. "RFID-based material passport system in a recycled concrete circular chain". In: *Journal of Cleaner Production* 442 (Feb. 2024), p. 140973.

[113] Guido Van Capelleveen et al. "The anatomy of a passport for the circular economy: a conceptual definition, vision and structured literature review". In: *Resources, Conservation & Recycling Advances* 17 (May 2023), p. 200131.

[114] Freek Van Eijk et al. *Circular buildings and infrastructure - State of play report ECESP Leadership Group on Buildings and Infrastructure 2021*. 2022. URL: `https://rgdoi.net/10.13140/RG.2.2.19196.41609` (visited on July 11, 2024).

[115] R S Vasilyev et al. "BIM and QR-codes interaction on a construction site". In: *Journal of Physics: Conference Series* 1425.1 (Dec. 2019), p. 012089.

[116] Mabel Vazquez-Briseno et al. "Using RFID/NFC and QR-Code in Mobile Phones to Link the Physical and the Digital World". In: *Interactive Multimedia*. Ed. by Ioannis Deliyannis. Mar. 2012.

[117] Wagmi. *Wagmi | Reactivity for Ethereum apps*. URL: `https://wagmi.sh` (visited on June 24, 2024).

[118] Joerg Walden, Angelika Steinbrecher, and Maroye Marinkovic. "Digital Product Passports as Enabler of the Circular Economy". In: *Chemie Ingenieur Technik* 93.11 (Nov. 2021), pp. 1717–1727.

[119] WalletConnect. *The UX Platform for The New Internet | WalletConnect*. URL: `https://walletconnect.com/` (visited on June 22, 2024).

[120] WalletConnect. *WalletConnect Docs | React Native*. URL: `https://docs.walletconnect.com/appkit/react-native/core/installation` (visited on June 22, 2024).

[121] Qin Wang et al. *Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges*. Oct. 2021. URL: `http://arxiv.org/abs/2105.07447` (visited on July 12, 2024).

[122] Roy Want. “An introduction to RFID technology”. In: *IEEE pervasive computing* 5.1 (2006), pp. 25–33.

[123] Dr Gavin Wood. “Ethereum: A Secure Decentralised Generalised Transaction Ledger”. In: *Ethereum Project Yellow Paper* 151 (2014), pp. 1–32.

[124] Liupengfei Wu et al. “A blockchain non-fungible token-enabled ‘passport’ for construction waste material cross-jurisdictional trading”. In: *Automation in Construction* 149 (May 2023), p. 104783.

[125] Yarn. *Home page | Yarn.* URL: https://yarnpkg.com/ (visited on June 23, 2024).

[126] Zibin Zheng et al. “An Overview on Smart Contracts: Challenges, Advances and Platforms”. In: *Future Generation Computer Systems* 105 (Apr. 2020), pp. 475–491.

[127] Sultan Çetin, Catherine De Wolf, and Nancy Bocken. “Circular Digital Built Environment: An Emerging Framework”. In: *Sustainability* 13.11 (June 2021), p. 6348.

[128] Sultan Çetin et al. “Data requirements and availabilities for material passports: A digitally enabled framework for improving the circularity of existing buildings”. In: *Sustainable Production and Consumption* 40 (Sept. 2023), pp. 422–437.

[129] Jiří Šeba, Roman Hruška, and Libor Švadlenka. “Analysis of automatic identification and data capture systems use in logistics”. In: *LOGI Scientific Journal on Transport and Logistics* 7.1 (2016).

Abbreviations

ABI	Application Binary Interface
AIDC	Automatic Identification and Data Capture
API	Application Programming Interface
BIM	Building Information Modeling
BLE	Bluetooth Low Energy
CAD	Computer-Aided Design
DID	Decentralized Identifier
DLT	Distributed Ledger Technology
DPP	Digital Product Passport
EC	European Commission
ETH	Ether (Cryptocurrency)
EU	European Union
EVM	Ethereum Virtual Machine
GDPR	General Data Protection Regulation
HaLo	Hardware-Locked
ICT	Information and Communications Technology
IPFS	Inter Planetary File System
IoT	Internet of Things
MP	Material Passport
NDEF	NFC Data Exchange Format
NFC	Near-Field Communication
NFT	Non-Fungible Token
PP	Product Passport
PBT	Physical Backed Token
QR	Quick Response
RFID	Radio Frequency Identification
SSI	Self-Sovereign Identity
UML	Unified Modeling Language
VC	Verifiable Credential

List of Figures

List of Tables

Listings

Appendix A

Installation Guidelines

This section outlines installing and running *PermaPass* on an Apple smartphone using iOS. Refer to the README.md files in the code repository [34] for more detailed instructions.

Ensure you have the latest versions of Node.js and yarn installed on your local machine. Follow these steps to set up and run *PermaPass* locally:

1. Navigate to the `./web-api` directory and install dependencies:

   ```
   npm install
   ```

2. Start the Web API locally:

   ```
   npm run start
   ```

3. Navigate to the `./ethereum` directory and add environment variables as described in the README.md file.

4. Install dependencies:

   ```
   npm install
   ```

5. Run a local Hardhat node:

   ```
   npm run node
   ```

6. Deploy all smart contracts to the local Hardhat node:

```
npx hardhat run scripts/deploy.ts --network localhost
```

7. Navigate to the `./dapp` directory and add environment variables as described in the README.md file.

8. Install dependencies:

```
npm install
```

9. Connect your iPhone to the computer with a cable.

10. Start the Expo app on the iPhone:

```
npm run ios:device
```

Appendix B

PermaPass App

This appendix includes the data structure used for the *PermaPass* app and examples of passport metadata and passport data.

B.1 Data Structures

```
import { Address } from "viem";

export type PassportMetadata = NFTPassportMetadata | DIDPassportMetadata
    | PBTPassportMetadata;

export type PBTPassportMetadata = {
  type: "pbt";
  chainId: number;
  address: string;
  tokenId: bigint;
};

export type NFTPassportMetadata = {
  type: "nft";
  chainId: number;
  address: string;
  tokenId: bigint;
};

export type DIDPassportMetadata = {
  type: "did";
  chainId: number;
  address: string;
  did: string;
  serviceType: string;
};

export interface PassportCreate {
  name: string;
  condition: string;
  width: string;
  height: string;
  thickness: string;
  usage: string;
  materials: string;
  dateManufactured: string;
  warranty: string;
  environmentalImpact: string;
  carbonFootprint: string;
  recycling: string;
  disposalInstructions: string;
}

export interface PassportReadDetails {
  uri: ArweaveURI;
  blockTimestamp: bigint;
}

export interface PassportRead {
  data: PassportCreate;
  details: PassportReadDetails;
}

export type PassportHistory = {
  entries: PassportRead[];
  ownerAddress: Address;
};

export type DataCarrier = "qr" | "nfc";

export type DigitalIdentifier = "nft" | "pbt" | "did";

export type ArweaveURI = ‘ar://${string}‘;

export type ArweaveURL = ‘https://arweave.net/${string}‘;

[...]
```

Listing B.1: Excerpt of ./dapp/types/index.ts

B.2 Passport Metadata Example

```
{
  "type": "nft";
  "chainId": 11155111;
  "address": "0xebf4455180945bc730363fa01cb39a4a54666439";
  "tokenId": 3;
}
```

Listing B.2: Example of Passport Metadata

B.3 Passport Data Example

```
{
  "name": "EcoView 5000",
  "condition": "Excellent",
  "width": "1200mm",
  "height": "1500mm",
  "thickness": "50mm",
  "usage": "Residential and commercial buildings",
  "materials": "70% glass, 20% aluminum, 10% rubber",
  "dateManufactured": "2018-04-23",
  "warranty": "10 years",
  "environmentalImpact": "Minimal",
  "carbonFootprint": "8 kg CO2",
  "recycling": "95%",
  "disposalInstructions": "Separate materials and recycle appropriately"
}
```

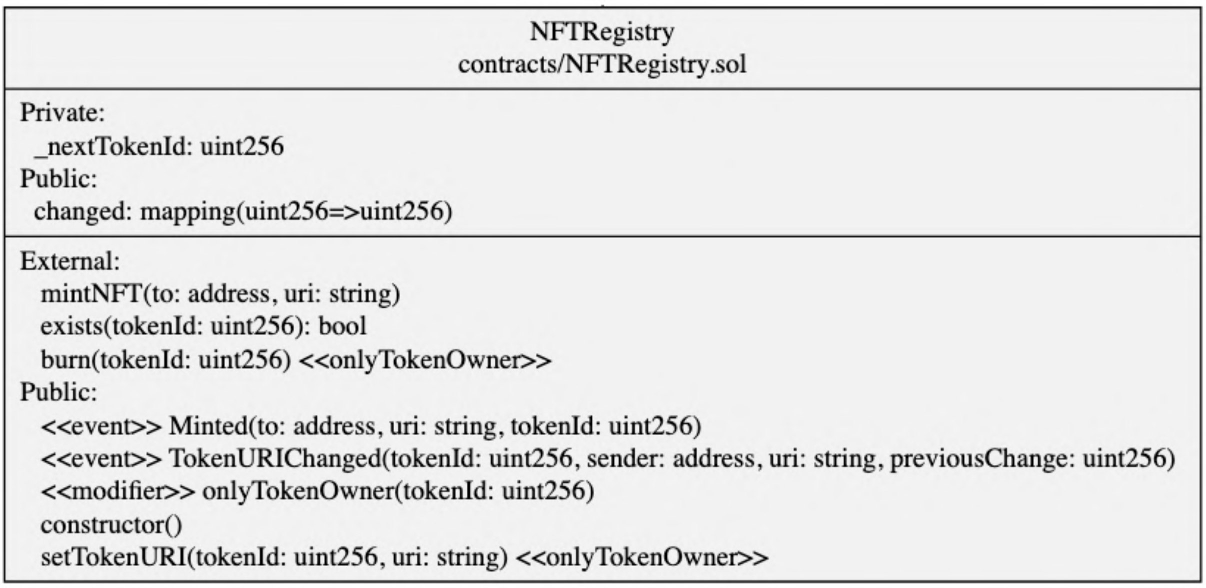
Listing B.3: Example of Passport Data

Appendix C

Ethereum

This appendix contains the UML Class Diagrams of all smart contracts implemented for *PermaPass*.

C.1 UML Class Diagrams for NFT Registry



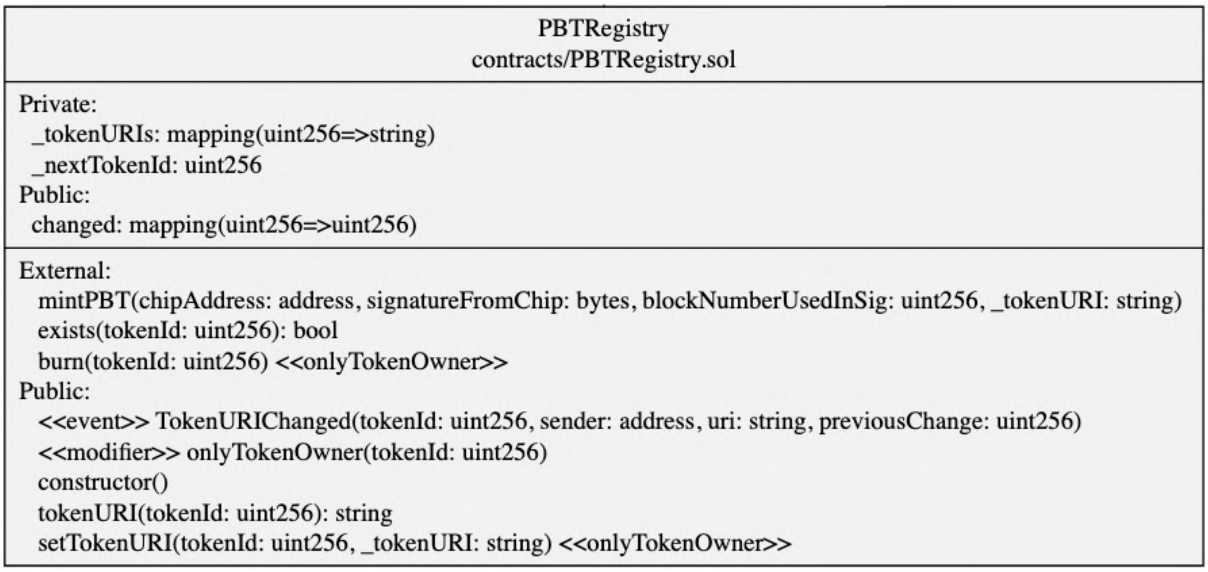
```
NFTRegistry
contracts/NFTRegistry.sol

Private:
  _nextTokenId: uint256
Public:
  changed: mapping(uint256=>uint256)

External:
   mintNFT(to: address, uri: string)
   exists(tokenId: uint256): bool
   burn(tokenId: uint256) <<onlyTokenOwner>>
Public:
   <<event>> Minted(to: address, uri: string, tokenId: uint256)
   <<event>> TokenURIChanged(tokenId: uint256, sender: address, uri: string, previousChange: uint256)
   <<modifier>> onlyTokenOwner(tokenId: uint256)
   constructor()
   setTokenURI(tokenId: uint256, uri: string) <<onlyTokenOwner>>
```

Figure C.1: UML Class Diagram for NFTRegistry.sol

C.2 UML Class Diagrams for PBT Registry



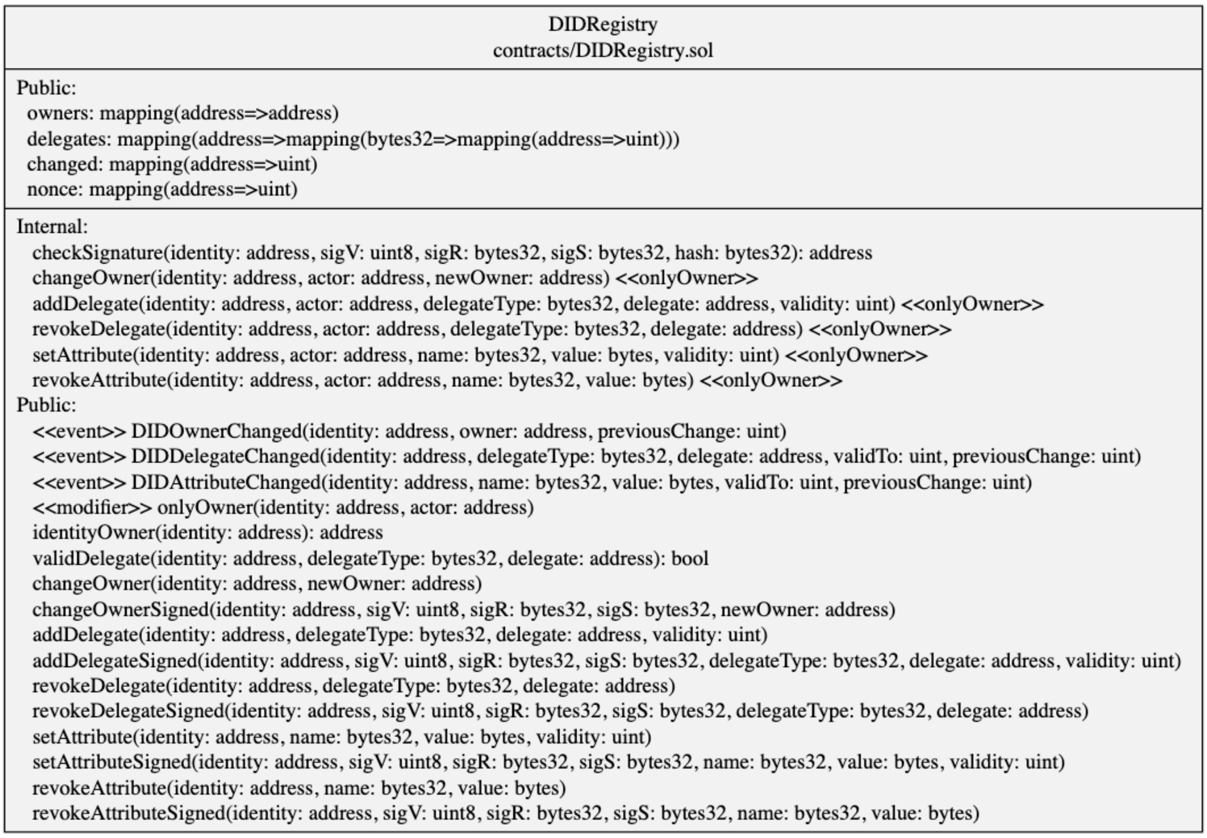
```
PBTRegistry
contracts/PBTRegistry.sol

Private:
  _tokenURIs: mapping(uint256=>string)
  _nextTokenId: uint256
Public:
  changed: mapping(uint256=>uint256)

External:
   mintPBT(chipAddress: address, signatureFromChip: bytes, blockNumberUsedInSig: uint256, _tokenURI: string)
   exists(tokenId: uint256): bool
   burn(tokenId: uint256) <<onlyTokenOwner>>
Public:
   <<event>> TokenURIChanged(tokenId: uint256, sender: address, uri: string, previousChange: uint256)
   <<modifier>> onlyTokenOwner(tokenId: uint256)
   constructor()
   tokenURI(tokenId: uint256): string
   setTokenURI(tokenId: uint256, _tokenURI: string) <<onlyTokenOwner>>
```

Figure C.2: UML Class Diagram for PBTRegistry.sol

C.3 UML Class Diagrams for DID Registry



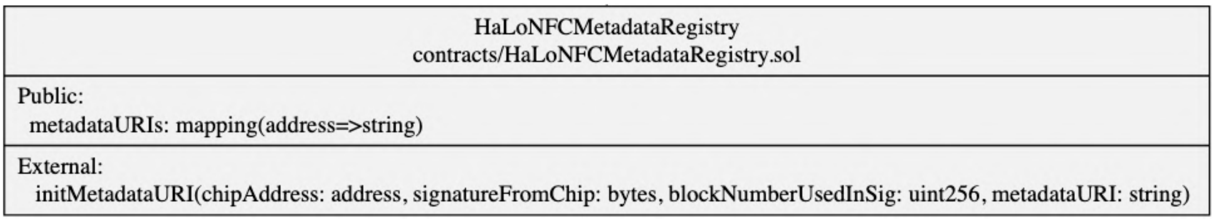
```
DIDRegistry
contracts/DIDRegistry.sol

Public:
  owners: mapping(address=>address)
  delegates: mapping(address=>mapping(bytes32=>mapping(address=>uint)))
  changed: mapping(address=>uint)
  nonce: mapping(address=>uint)

Internal:
   checkSignature(identity: address, sigV: uint8, sigR: bytes32, sigS: bytes32, hash: bytes32): address
   changeOwner(identity: address, actor: address, newOwner: address) <<onlyOwner>>
   addDelegate(identity: address, actor: address, delegateType: bytes32, delegate: address, validity: uint) <<onlyOwner>>
   revokeDelegate(identity: address, actor: address, delegateType: bytes32, delegate: address) <<onlyOwner>>
   setAttribute(identity: address, actor: address, name: bytes32, value: bytes, validity: uint) <<onlyOwner>>
   revokeAttribute(identity: address, actor: address, name: bytes32, value: bytes) <<onlyOwner>>
Public:
   <<event>> DIDOwnerChanged(identity: address, owner: address, previousChange: uint)
   <<event>> DIDDelegateChanged(identity: address, delegateType: bytes32, delegate: address, validTo: uint, previousChange: uint)
   <<event>> DIDAttributeChanged(identity: address, name: bytes32, value: bytes, validTo: uint, previousChange: uint)
   <<modifier>> onlyOwner(identity: address, actor: address)
   identityOwner(identity: address): address
   validDelegate(identity: address, delegateType: bytes32, delegate: address): bool
   changeOwner(identity: address, newOwner: address)
   changeOwnerSigned(identity: address, sigV: uint8, sigR: bytes32, sigS: bytes32, newOwner: address)
   addDelegate(identity: address, delegateType: bytes32, delegate: address, validity: uint)
   addDelegateSigned(identity: address, sigV: uint8, sigR: bytes32, sigS: bytes32, delegateType: bytes32, delegate: address, validity: uint)
   revokeDelegate(identity: address, delegateType: bytes32, delegate: address)
   revokeDelegateSigned(identity: address, sigV: uint8, sigR: bytes32, sigS: bytes32, delegateType: bytes32, delegate: address)
   setAttribute(identity: address, name: bytes32, value: bytes, validity: uint)
   setAttributeSigned(identity: address, sigV: uint8, sigR: bytes32, sigS: bytes32, name: bytes32, value: bytes, validity: uint)
   revokeAttribute(identity: address, name: bytes32, value: bytes)
   revokeAttributeSigned(identity: address, sigV: uint8, sigR: bytes32, sigS: bytes32, name: bytes32, value: bytes)
```

Figure C.3: UML Class Diagram for DIDRegistry.sol

C.4 UML Class Diagrams for HaLo NFC Metadata Registry



HaLoNFCMetadataRegistry
contracts/HaLoNFCMetadataRegistry.sol

Public:
metadataURIs: mapping(address=>string)

External:
initMetadataURI(chipAddress: address, signatureFromChip: bytes, blockNumberUsedInSig: uint256, metadataURI: string)

Figure C.4: UML Class Diagram for HaLoNFCMetadataRegistry.sol

Appendix D

Evaluation

This appendix includes additional plots that detail all data recorded by the experiments, not just the mean values presented in the thesis. It displays every data point for every run and operation recorded by the evaluation scripts. The appendix is divided into visualizations of performance data and cost data.

D.1 Visualizations of Performance

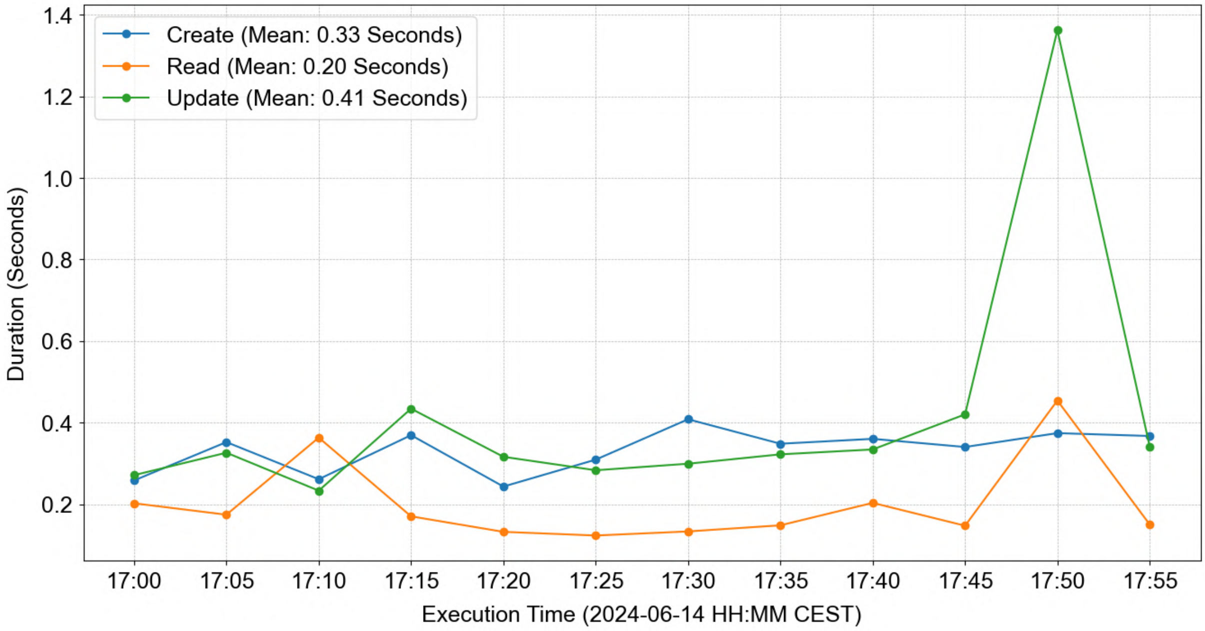


Figure D.1: Performance of Arweave Interactions using Irys Node 2

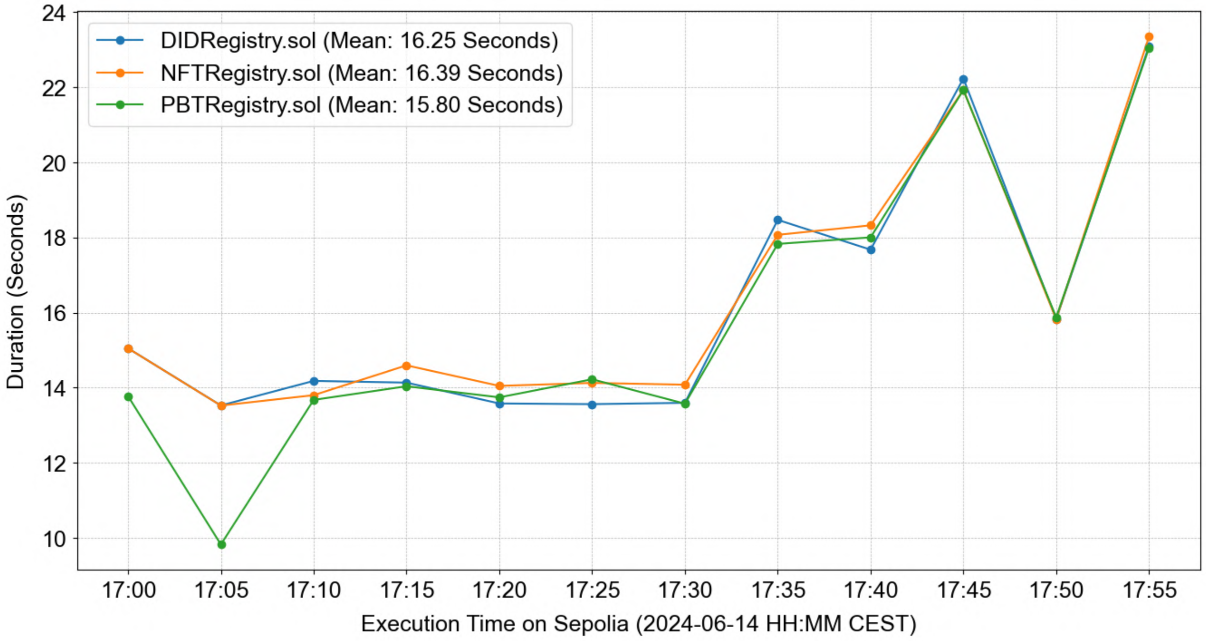


Figure D.2: Performance of Contract Deployment by Registry Contracts

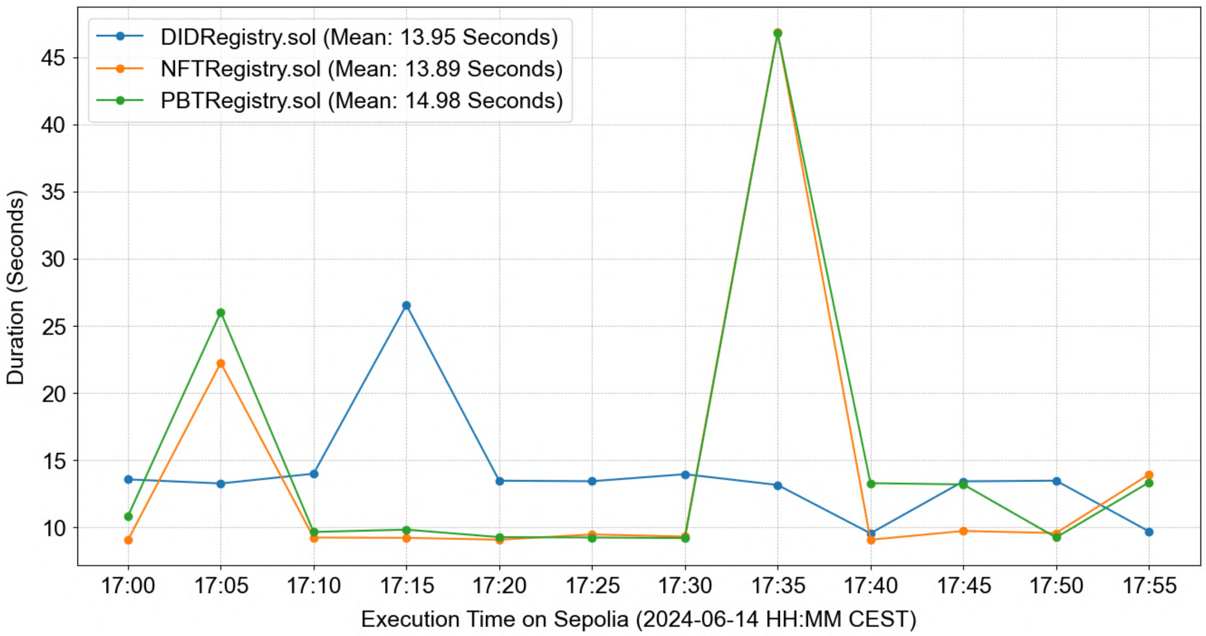


Figure D.3: Performance of Passport Creation by Registry Contracts

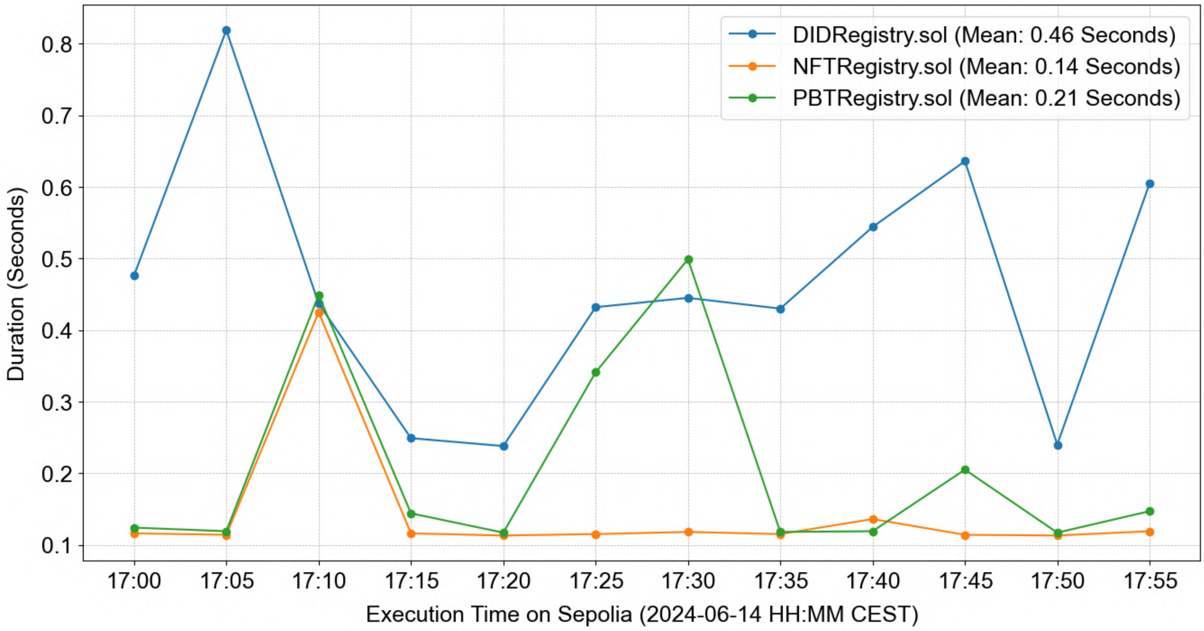


Figure D.4: Performance of Passport Reading by Registry Contracts

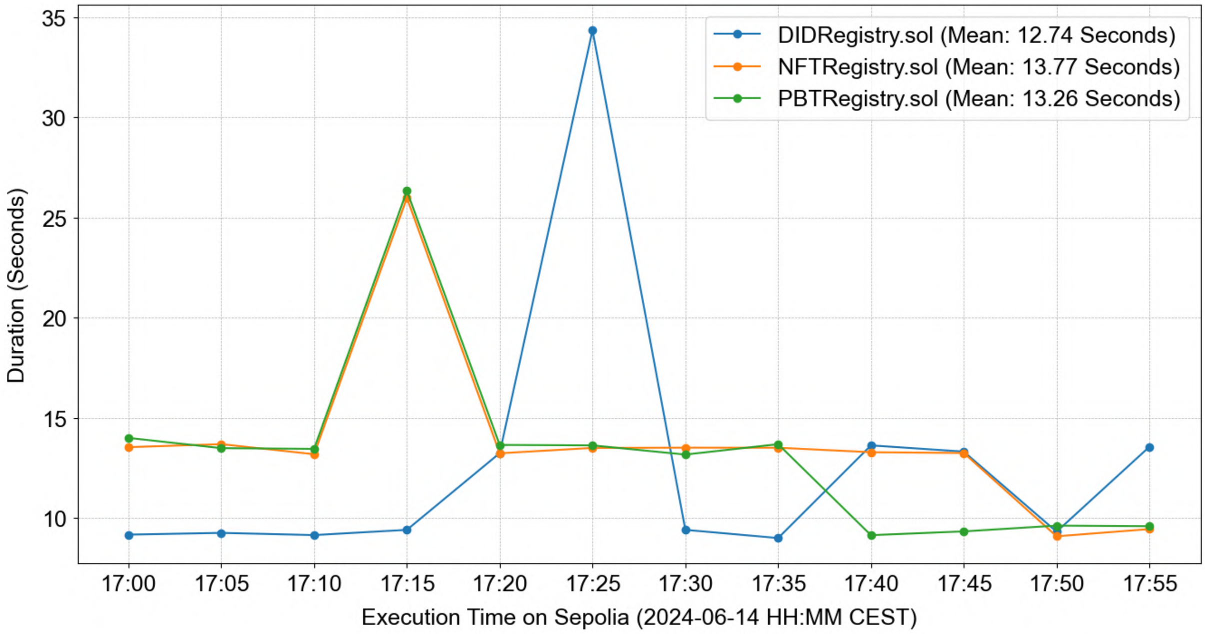


Figure D.5: Performance of Passport Update by Registry Contracts

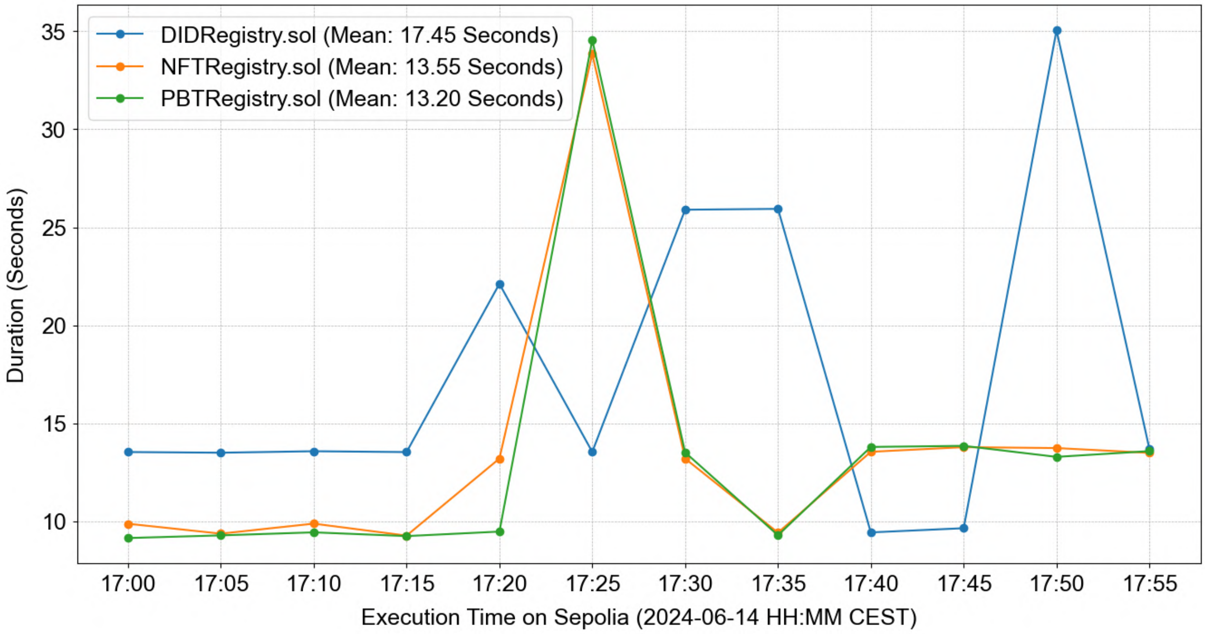


Figure D.6: Performance by Passport Deletion by Registry Contracts

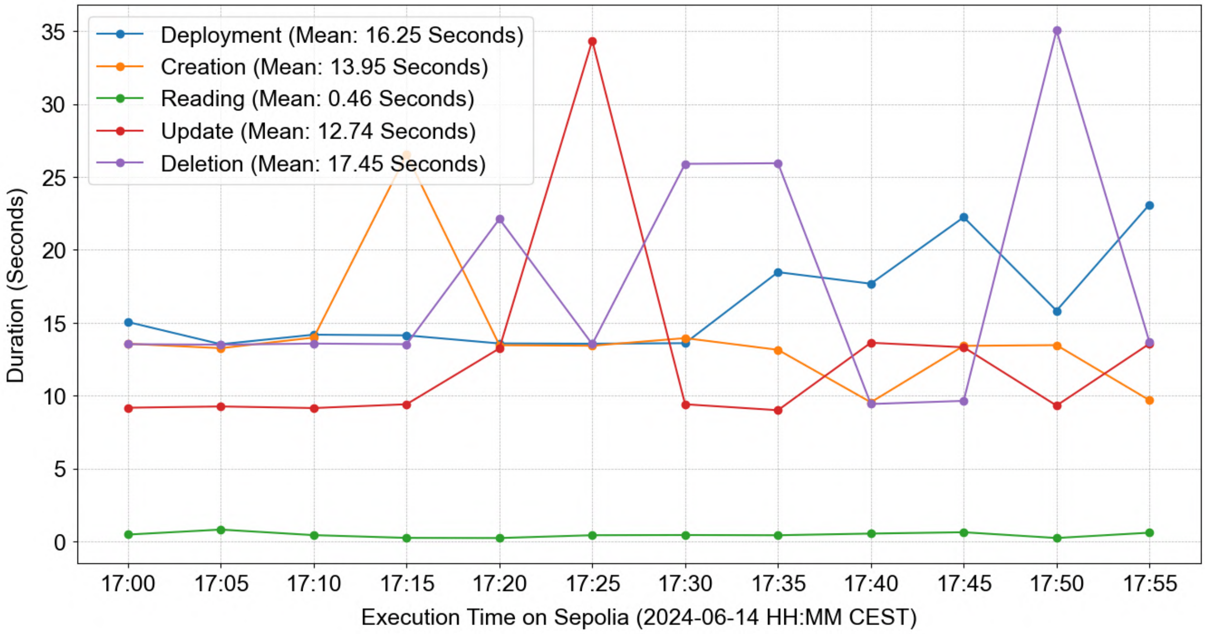


Figure D.7: Performance of DIDRegistry.sol

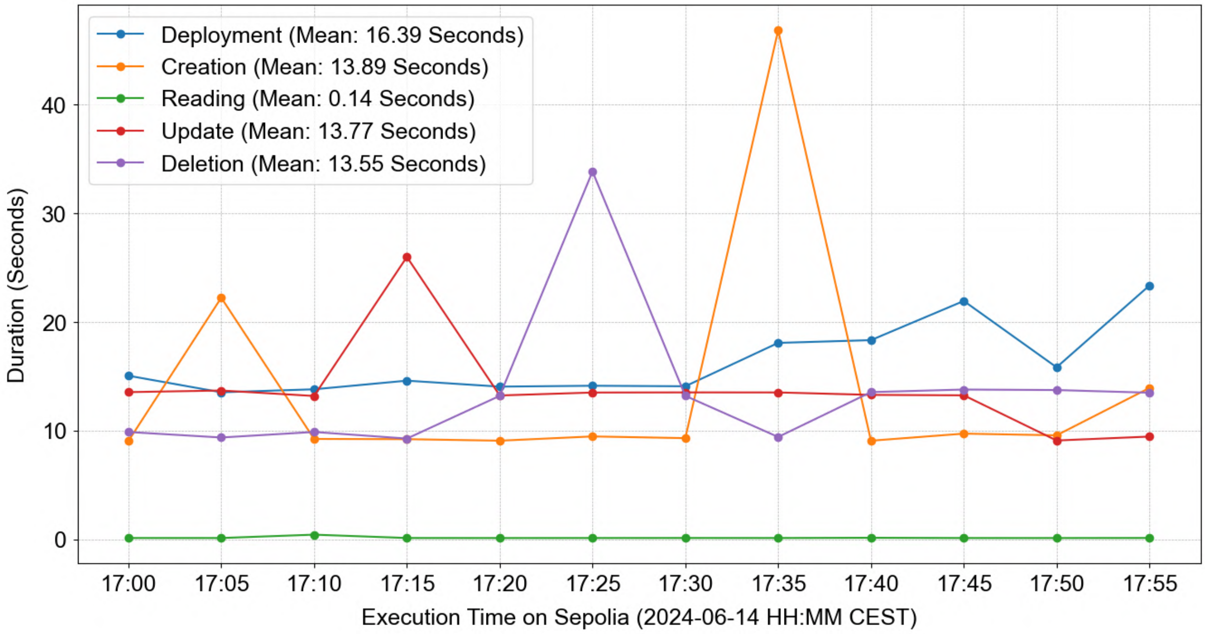


Figure D.8: Performance of NFTRegistry.sol

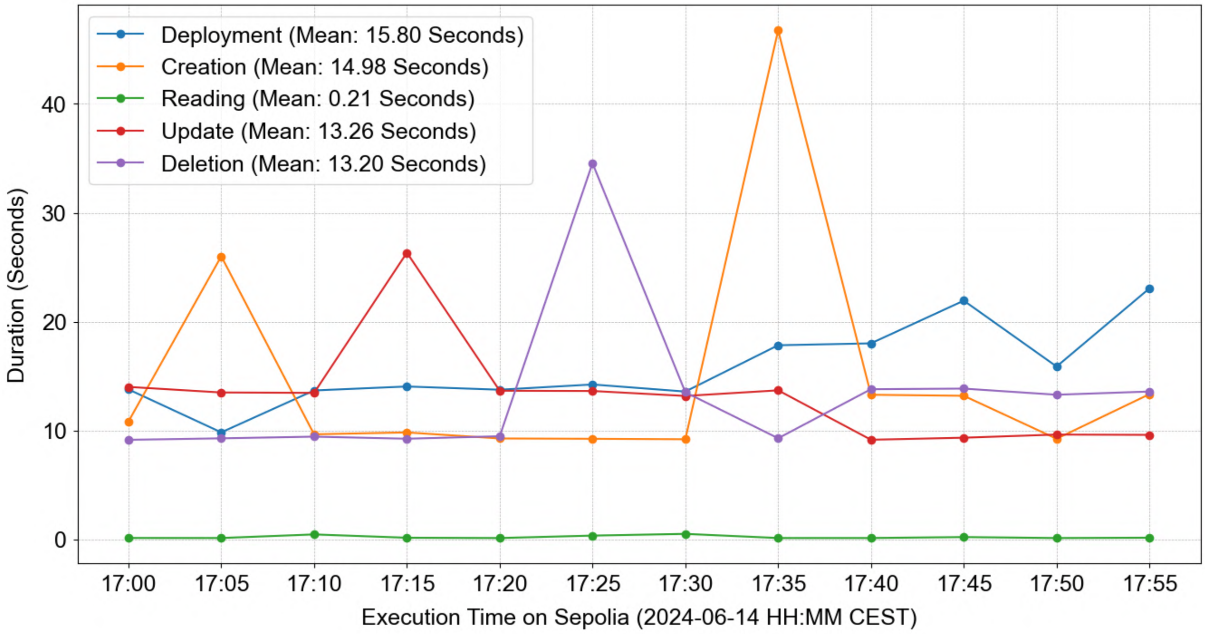


Figure D.9: Performance of PBTRegistry.sol

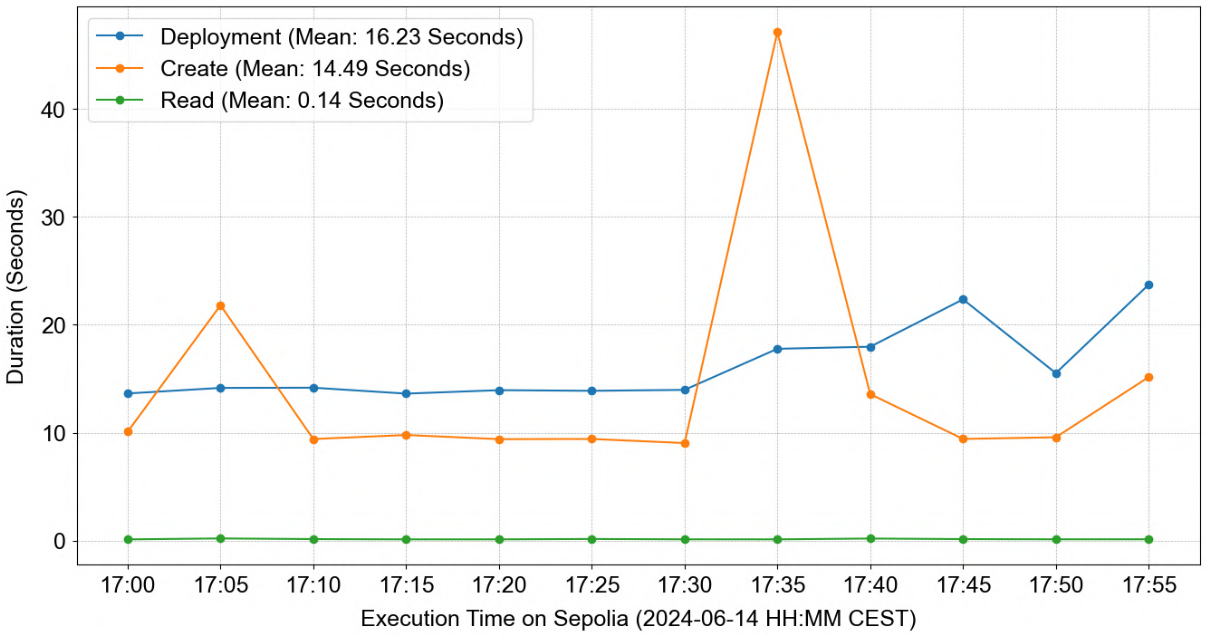


Figure D.10: Performance of HaLoNFCMetadataRegistry.sol

D.2 Evaluation: Visualizations of Costs

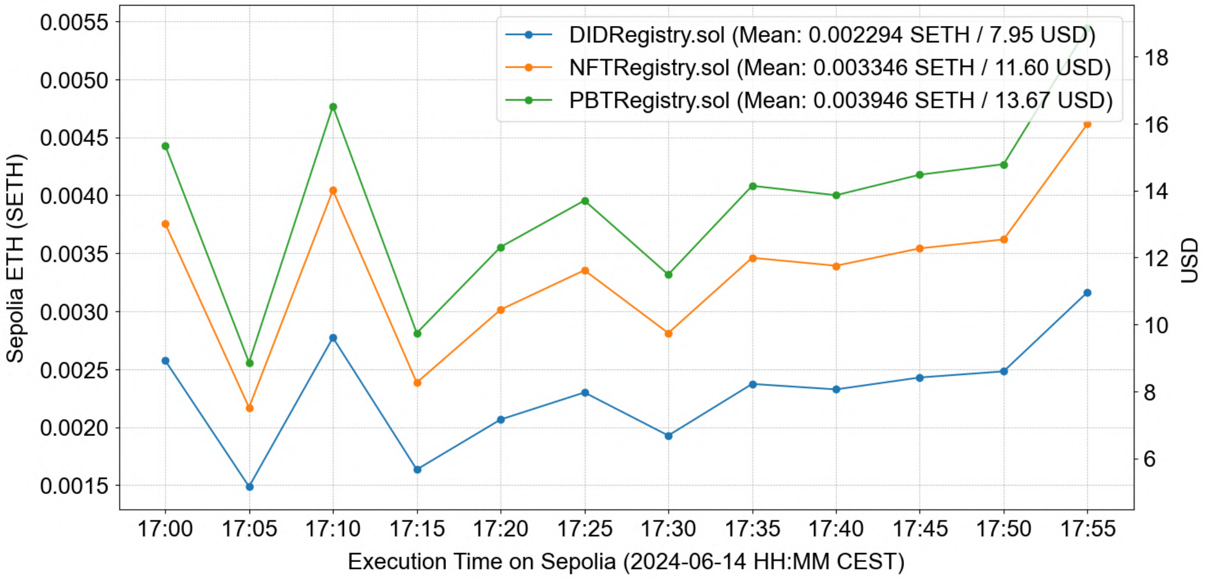


Figure D.11: Gas Costs for Contract Deployment by Registry Contracts

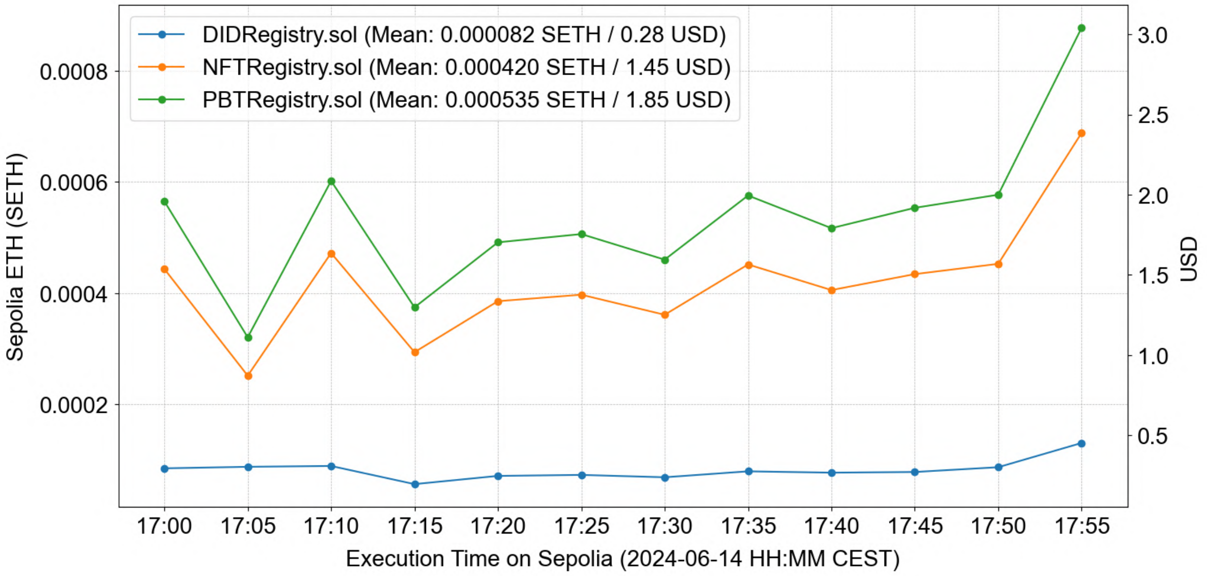


Figure D.12: Gas Costs for Passport Creation by Registry Contracts

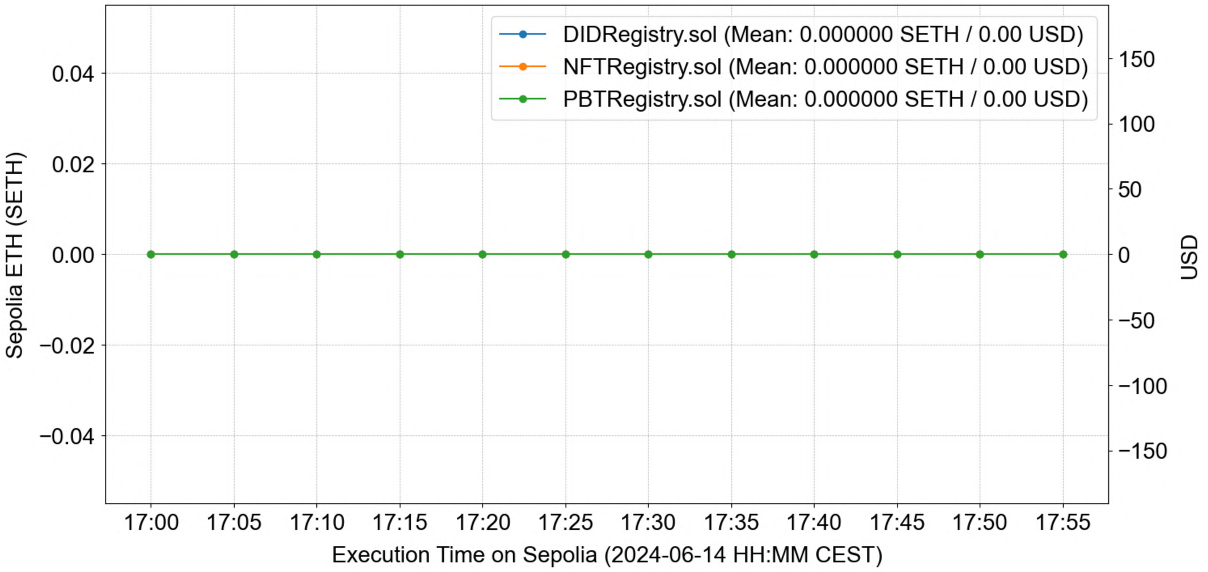


Figure D.13: Gas Costs for Passport Reading by Registry Contracts

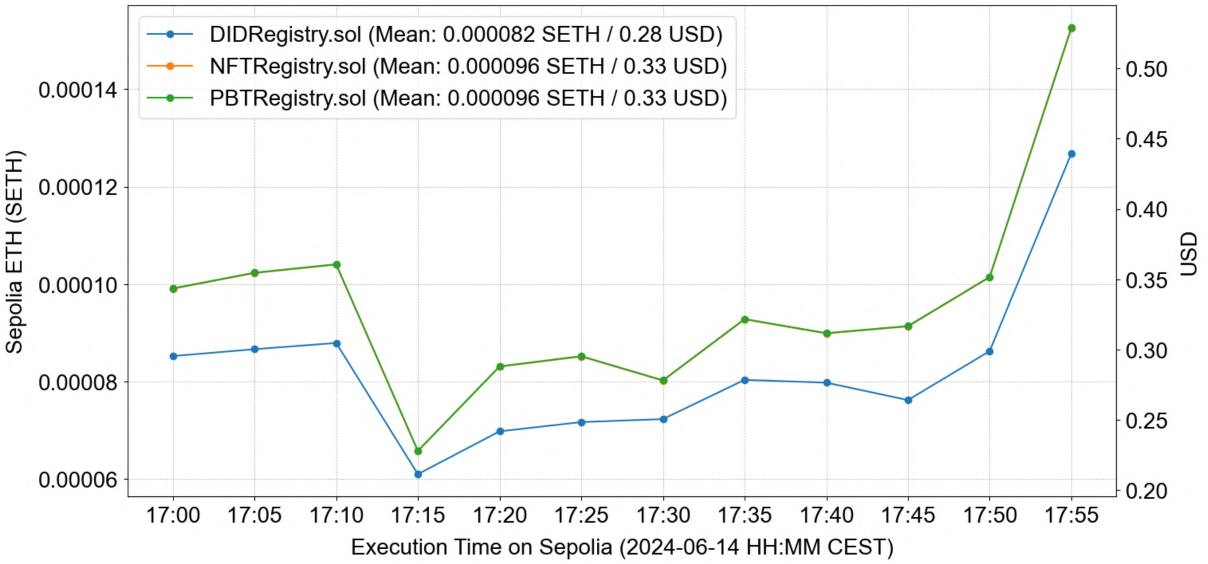


Figure D.14: Gas Costs for Passport Update by Registry Contracts

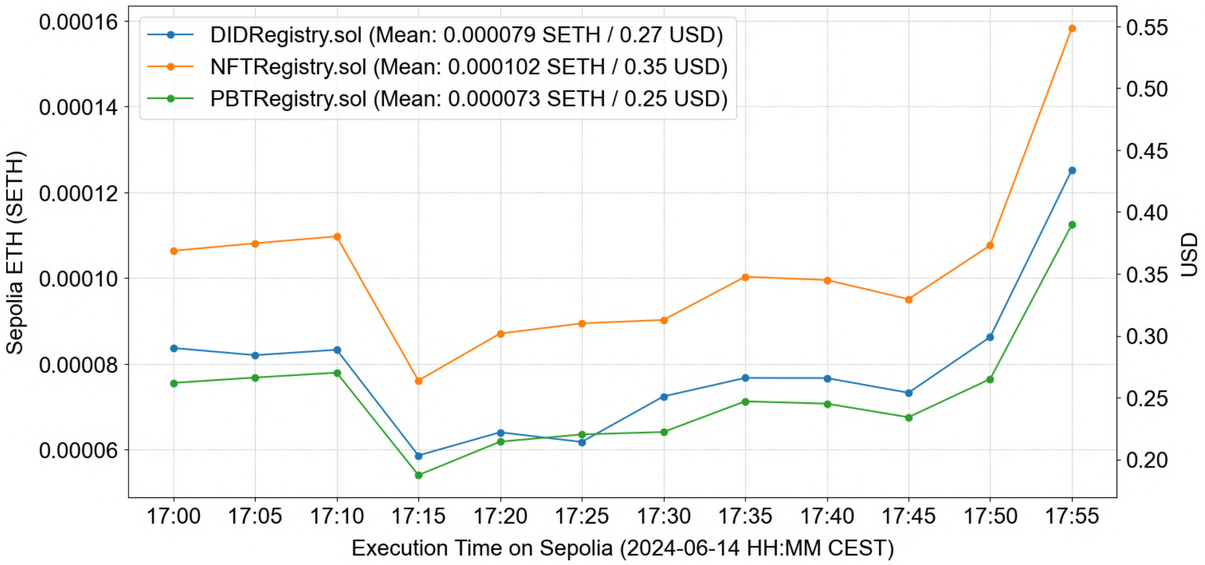


Figure D.15: Gas Costs for Passport Deletion by Registry Contracts

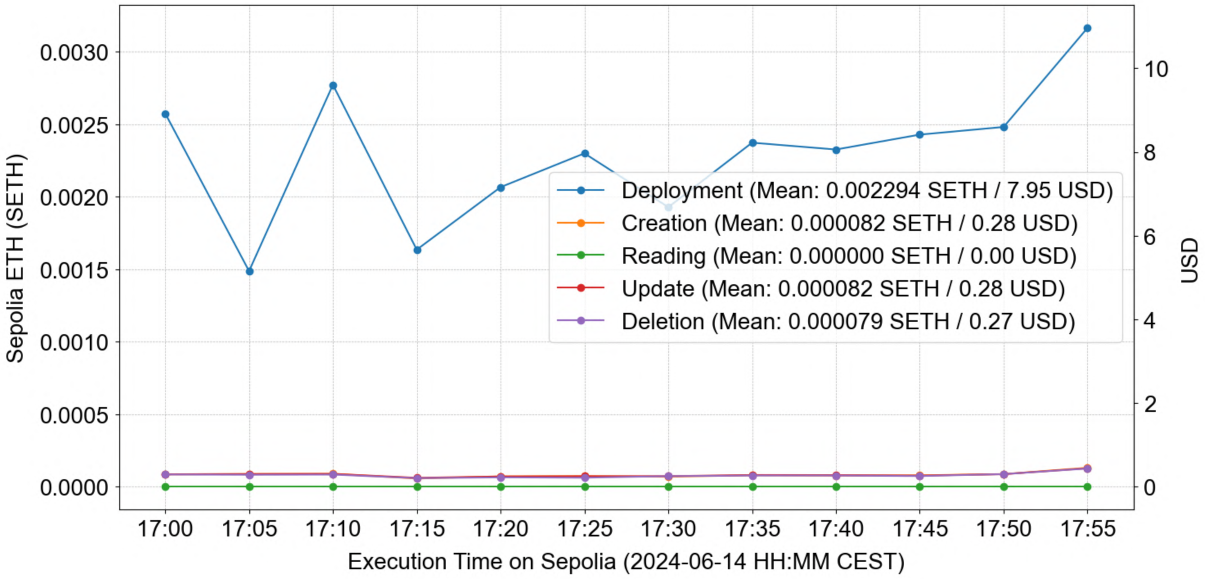


Figure D.16: Gas Costs of DIDRegistry.sol

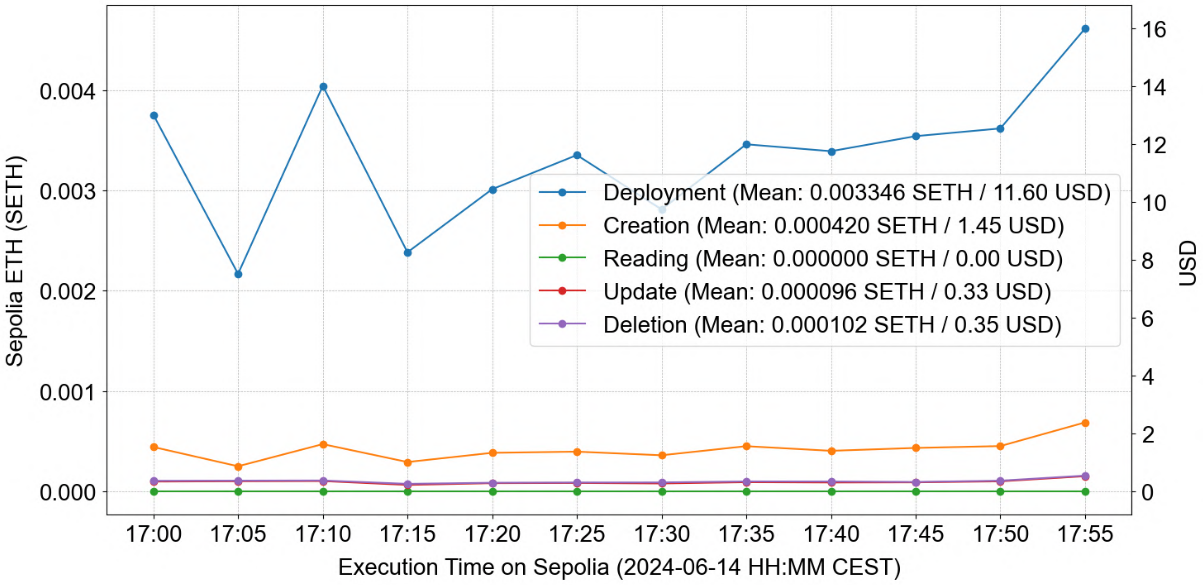


Figure D.17: Gas Costs of NFTRegistry.sol

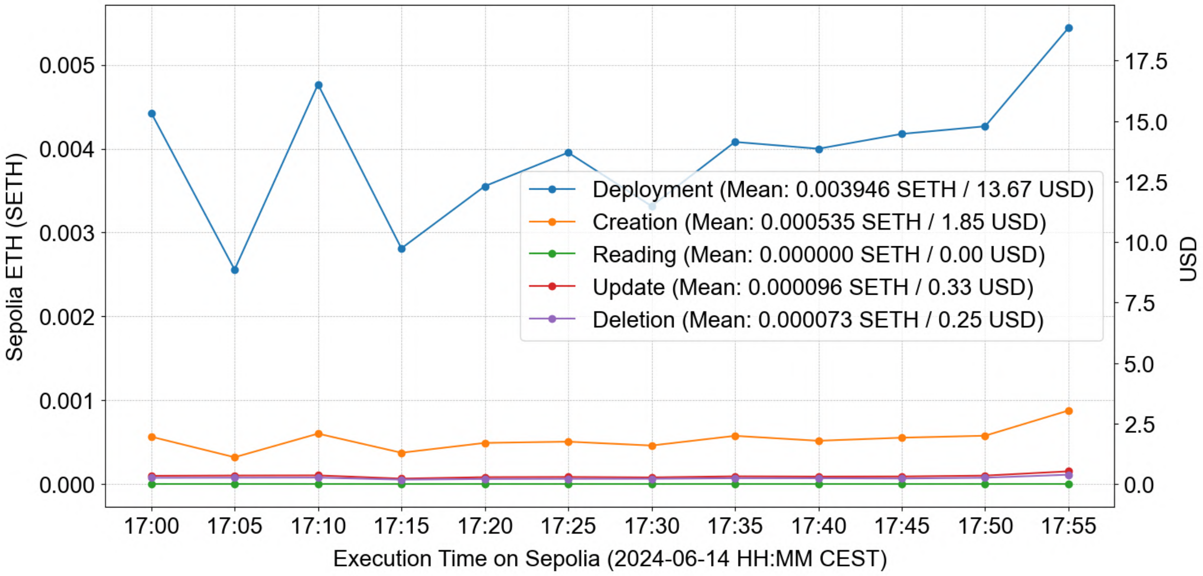


Figure D.18: Gas Costs of PBTRegistry.sol

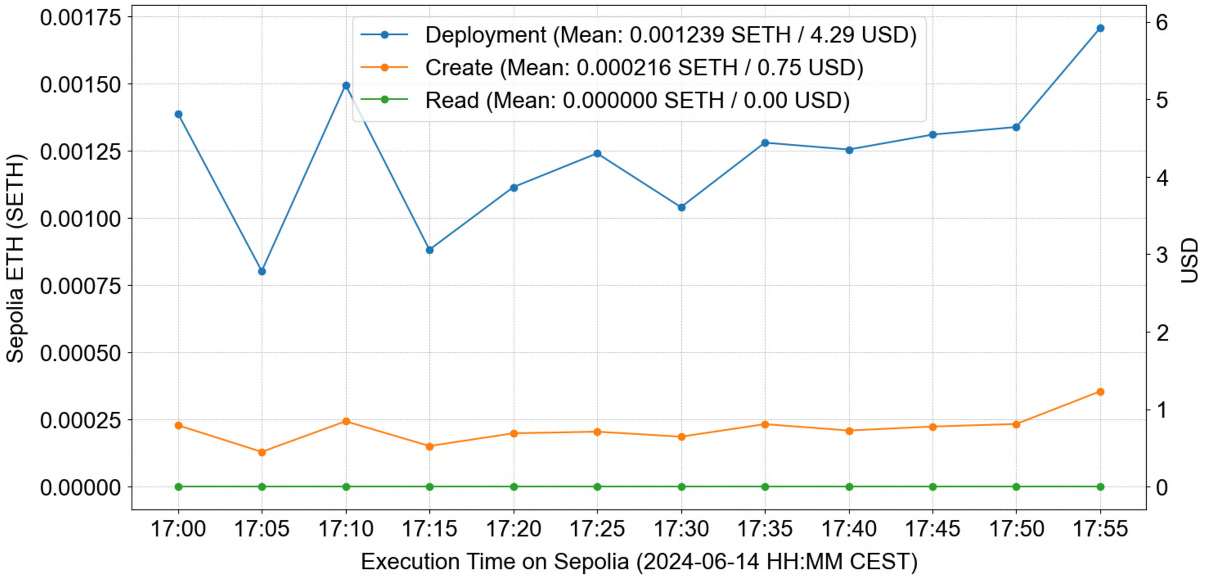


Figure D.19: Gas Costs of HaLoNFCMetadataRegistry.sol