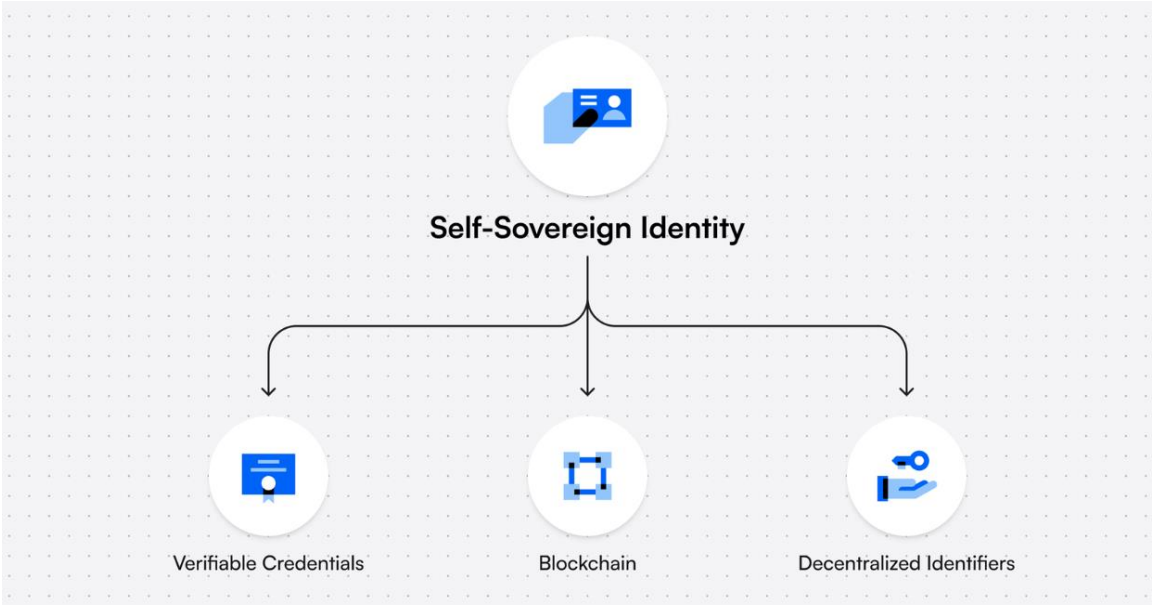
**ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ**
**ΣΧΟΛΗ ΜΗΧΑΝΙΚΩΝ**
**ΤΜΗΜΑ ΗΛΕΚΤΡΟΛΟΓΩΝ & ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ**

**Διπλωματική Εργασία**

# Αξιολόγηση και χαρακτηριστικά των προτύπων υλοποίησης αποκεντρωμένων χαρακτηριστικών




**Φοιτητής: Χρήστος Τσίλης**
**ΑΜ: 18387100**

**Επιβλέπων Καθηγητής**

**Κόγιας Δημήτριος**
**Ακαδημαϊκός Υπότροφος / Εντεταλμένος Διδάσκων**

**ΑΘΗΝΑ-ΑΙΓΑΛΕΩ, ΜΑΡΤΙΟΣ 2024**

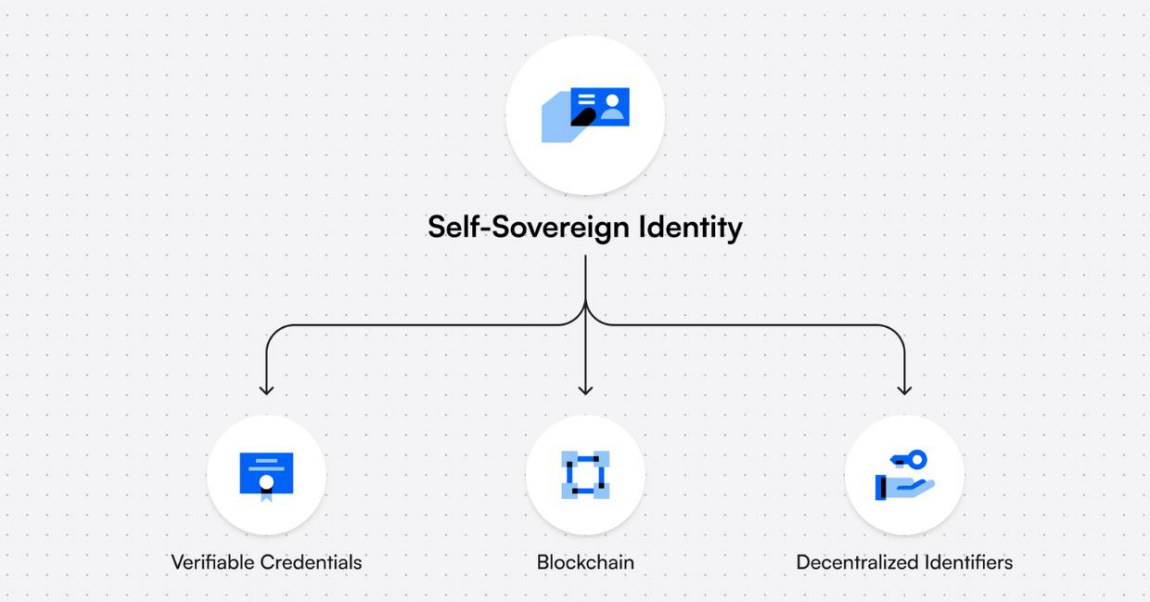
**UNIVERSITY OF WEST ATTICA**

**FACULTY OF ENGINEERING**

**DEPARTMENT OF ELECTRICAL & ELECTRONICS ENGINEERING**

# Diploma Thesis

# Evaluation and characteristics of the development standards for Decentralized Identities (DIDs)




**Student: Christos Tsilis**
**Registration Number: 18387100**

**Supervisor**

**Kogias Dimitris**
**Adjunct Academic Staff**

**ATHENS-EGALEO, MARCH 2024**

Η Διπλωματική Εργασία έγινε αποδεκτή και βαθμολογήθηκε από την εξής τριμελή επιτροπή:

| Κόγιας Δημήτριος,<br>Εντεταλμένος Διδάσκων | Πατρικάκης Χαράλαμπος,<br>Καθηγητής | Παπαδόπουλος Περικλής,<br>Καθηγητής |
|---|---|---|
| Dimitrios Kogias<br>Digitally signed by Dimitrios Kogias<br>Date: 2024.04.10 16:44:40 +03'00'<br>(Υπογραφή) | Digitally signed by Charalampos Patrikakis<br>Date: 2024.04.15 11:52:22 +03'00'<br>(Υπογραφή) | Periklis Papadopoulos<br>Digitally signed by Periklis Papadopoulos<br>Date: 2024.04.13 14:52:10 +03'00'<br>(Υπογραφή) |

**ΠΑΝΕΠΙΣΤΗΜΙΟ ΔΥΤΙΚΗΣ ΑΤΤΙΚΗΣ**
**Χρήστος Τσίλης, Μάρτιος, 2024**



## ΔΗΛΩΣΗ ΣΥΓΓΡΑΦΕΑ ΔΙΠΛΩΜΑΤΙΚΗΣ ΕΡΓΑΣΙΑΣ

Ο κάτωθι υπογεγραμμένος Χρήστος Τσίλης του Βασιλείου, με αριθμό μητρώου 18387100 φοιτητής του Πανεπιστημίου Δυτικής Αττικής της Σχολής ΜΗΧΑΝΙΚΩΝ του Τμήματος ΗΛΕΚΤΡΟΛΟΓΩΝ ΚΑΙ ΗΛΕΚΤΡΟΝΙΚΩΝ ΜΗΧΑΝΙΚΩΝ,

**δηλώνω υπεύθυνα ότι:**

«Είμαι συγγραφέας αυτής της διπλωματικής εργασίας και ότι κάθε βοήθεια την οποία είχα για την προετοιμασία της είναι πλήρως αναγνωρισμένη και αναφέρεται στην εργασία. Επίσης, οι όποιες πηγές από τις οποίες έκανα χρήση δεδομένων, ιδεών ή λέξεων, είτε ακριβώς είτε παραφρασμένες, αναφέρονται στο σύνολό τους, με πλήρη αναφορά στους συγγραφείς, τον εκδοτικό οίκο ή το περιοδικό, συμπεριλαμβανομένων και των πηγών που ενδεχομένως χρησιμοποιήθηκαν από το διαδίκτυο. Επίσης, βεβαιώνω ότι αυτή η εργασία έχει συγγραφεί από μένα αποκλειστικά και αποτελεί προϊόν πνευματικής ιδιοκτησίας τόσο δικής μου, όσο και του Ιδρύματος.
Παράβαση της ανωτέρω ακαδημαϊκής μου ευθύνης αποτελεί ουσιώδη λόγο για την ανάκληση του διπλώματός μου.
Επιθυμώ την απαγόρευση πρόσβασης στο πλήρες κείμενο της εργασίας μου μέχρι 8/04/2024 και έπειτα από αίτησή μου στη Βιβλιοθήκη και έγκριση του επιβλέποντος καθηγητή.»

Ο Δηλών
Χρήστος Τσίλης

Αφιερωμένη στην οικογένειά μου
και στους φίλους μου.

# Ευχαριστίες

Θα ήθελα να ευχαριστήσω τους γονείς μου για όλη την συμπαράσταση και υπομονή που μου έχουν δείξει και την αδερφή μου που πίστευε πάντα σε μένα.

Επιπλέον, θα ήθελα να ευχαριστήσω όλους τους φίλους που μου στάθηκαν όλα αυτά τα χρόνια.

Τέλος, θέλω να δώσω ιδιαίτερες ευχαριστίες στους φίλους και συναδέλφους Χένρι και Βασίλη που έπαιξαν καθοριστικό ρόλο στην πορεία μου.

# Περίληψη

Στο εξελισσόμενο τοπίο της ψηφιακής τεχνολογίας, η έννοια της επαλήθευσης και διαχείρισης ταυτότητας έχει γίνει αναπόσπαστο κομμάτι των διαδικτυακών αλληλεπιδράσεων και συναλλαγών. Αυτή η διπλωματική εργασία εμβαθύνει στο μετασχηματιστικό δυναμικό των Αποκεντρωμένων Ταυτοτήτων (DID) στην αναμόρφωση της ψηφιακής ταυτοποίησης, με ιδιαίτερη έμφαση στην υποκείμενη τεχνολογία του Blockchain που μας επιτρέπει αυτή την υλοποίηση. Η μελέτη στοχεύει να αξιολογήσει τα πρότυπα ανάπτυξης των DIDs και την αποτελεσματικότητά τους στην αντιμετώπιση των εγγενών προβλημάτων των παραδοσιακών μεθόδων ψηφιακής ταυτοποίησης.

Το πρώτο κεφάλαιο θέτει τη θεμελιώδη κατανόηση της τεχνολογίας του blockchain, διευκρινίζοντας τον κεντρικό ρόλο της στον τομέα της ψηφιακής ταυτοποίησης. Παρέχει μια ολοκληρωμένη επισκόπηση των θεμελιωδών στοιχείων του blockchain και εξηγεί πώς αυτά τα στοιχεία είναι ζωτικής σημασίας στο πλαίσιο των DIDs. Το κεφάλαιο διερευνά, περαιτέρω, το τρέχον τοπίο της ψηφιακής ταυτοποίησης, επισημαίνοντας τους περιορισμούς και τις ευπάθειες των υφιστάμενων συστημάτων, όπως ο κεντρικός έλεγχος δεδομένων, οι ανησυχίες για το προσωπικό απόρρητο και η ευπάθεια στην απάτη.

Στο δεύτερο κεφάλαιο, η εργασία εστιάζει στις ίδιες τις Αποκεντρωμένες Ταυτότητες. Ξεκινά με τον ορισμό των DIDs και την πορεία της εξέλιξής τους από μια αυθαίρετη έννοια στην τρέχουσα αναπτυξιακή τους κατάσταση. Αυτή η ενότητα εξετάζει σε βάθος το τεχνικό πλαίσιο και τα πρότυπα που διέπουν τα DIDs, προσφέροντας πληροφορίες για το πώς υπόσχονται ενισχυμένη ασφάλεια, αυτονομία χρήστη και ιδιωτικότητα στις ψηφιακές αλληλεπιδράσεις. Το κεφάλαιο αντιπαραβάλλει επίσης τα DIDs με τις παραδοσιακές μεθόδους αναγνώρισης, επιδεικνύοντας την ανωτερότητά τους στην αντιμετώπιση ζητημάτων όπως παραβιάσεις δεδομένων και κλοπή ταυτότητας.

Το τρίτο κεφάλαιο παρουσιάζει μια πρακτική ματιά μέσα από περιπτωσιολογικές μελέτες στον πραγματικό κόσμο. Εξετάζει τρεις διαφορετικές εφαρμογές των DIDs σε διάφορους τομείς, συμπεριλαμβανομένων της υγειονομικής περίθαλψης, της κυβέρνησης και του Διαδικτύου των Πραγμάτων (IoT). Κάθε μελέτη παρέχει εμπειρικά στοιχεία για τον τρόπο με τον οποίο εφαρμόζονται τα DIDs και τον αντίκτυπο που έχουν σε αυτούς τους τομείς. Αυτή η ενότητα όχι μόνο υπογραμμίζει την ευελιξία και την προσαρμοστικότητα των DIDs αλλά επίσης συζητά τις προκλήσεις και τις μελλοντικές προοπτικές στην ευρύτερη εφαρμογή τους.

Συμπερασματικά, αυτή η διατριβή υπογραμμίζει τις μετασχηματιστικές δυνατότητες των DIDs στην επανάσταση στην ψηφιακή ταυτοποίηση. Αξιοποιώντας την τεχνολογία του blockchain, τα DIDs προσφέρουν μια πιο ασφαλή, αποτελεσματική και με επίκεντρο τον χρήστη προσέγγιση για τη διαχείριση της ταυτότητας. Τα ευρήματα από τις περιπτωσιολογικές μελέτες υποδηλώνουν μια αυξανόμενη τάση προς την υιοθέτηση των DIDs, υποδεικνύοντας τον κεντρικό ρόλο τους στο μέλλον των ψηφιακών αλληλεπιδράσεων. Η διατριβή ολοκληρώνεται δίνοντας έμφαση στην ανάγκη για συνεχή έρευνα και ανάπτυξη σε αυτόν τον τομέα για την πλήρη αξιοποίηση των δυνατοτήτων των DIDs στην προώθηση ενός πιο ασφαλούς και δίκαιου ψηφιακού κόσμου.

## Λέξεις – κλειδιά

Αποκεντρωμένα αναγνωριστικά, DIDs, επαληθεύσιμα διαπιστευτήρια, W3C, τεχνολογία Blockchain, Κρυπτογραφία, Ψηφιακή Ταυτότητα, Ασφάλεια, Απόρρητο, Διαλειτουργικότητα, Διαχείριση ταυτότητας

## Abstract

In the evolving landscape of digital technology, the concept of identity verification and management has become a cornerstone of online interactions and transactions. This thesis delves into the transformative potential of Decentralized Identifiers (DIDs) in reshaping the digital identification paradigm, with a particular focus on the underlying blockchain technology that facilitates this shift. The study aims to evaluate the development standards of DIDs and their efficacy in addressing the inherent challenges of traditional digital identification methods.

The first chapter lays the foundational understanding of blockchain technology, elucidating its pivotal role in the realm of digital identification. It provides a comprehensive overview of blockchain's fundamental components and explains how these elements are crucial in the context of DIDs. The chapter further explores the current landscape of digital identification, highlighting the limitations and vulnerabilities of existing systems, such as centralized data control, privacy concerns, and susceptibility to fraud.

In the second chapter, the thesis shifts its focus to Decentralized Identities themselves. It begins by defining DIDs and tracing their evolution from a conceptual standpoint to their current developmental state. This section critically examines the technical framework and standards governing DIDs, offering insights into how they promise enhanced security, user autonomy, and privacy in digital interactions. The chapter also contrasts DIDs with traditional identification methods, showcasing their superiority in addressing issues like data breaches and identity theft.

The third chapter presents a practical perspective through real-world case studies. It examines three distinct applications of DIDs across various sectors, including healthcare, government and IoT. Each case study provides empirical evidence of how DIDs are being implemented and the impact they are having on these sectors. This section not only highlights the versatility and adaptability of DIDs but also discusses the challenges and future prospects in their broader application.

In conclusion, this thesis underscores the transformative potential of DIDs in revolutionizing digital identification. By leveraging blockchain technology, DIDs offer a more secure, efficient, and user-centric approach to identity management. The findings from the case studies suggest a growing trend towards the adoption of DIDs, indicating their pivotal role in the future of digital interactions. The thesis concludes by emphasizing the need for ongoing research and development in this field to fully realize the potential of DIDs in fostering a more secure and equitable digital world.



## Keywords

Decentralized Identifiers, DIDs, Verifiable Credentials, W3C, Blockchain Technology, Cryptography, Digital Identity, Security, Privacy, Interoperability, Identity Management

# Contents

**Table Cataloge**



**Figure Cataloge**

**Periodical Index**

ID: Identification/Identity

DID: Decentralized Identity (**Note:** In this thesis the term DID is used to describe the general concept of Decentralized Identities. Compared to the W3C Recommendation titled "Decentralized Identifiers (DIDs) v1.0" where it is defined as "Decentralized Identifier" .)

SSI: Self-Sovereign Identity

RFID: Radio-Frequency Identification

AI: Artificial Intelligence

GDPR: General Data Protection Regulation

DIF: Decentralized Identity Foundation

VC: Verifiable Credential

ABNF: Augmented Backus–Naur form

JSON: JavaScript Object Notation

JSON-LD: JavaScript Object Notation for Linked Data

IANA: Internet Assigned Numbers Authority

XML: Extensible Markup Language

IoT: Internet of Things

ESSIF: European Self-Sovereign Identity Framework

EBSI: European Blockchain Services Infrastructure

MIT: Massachusetts Institute of Technology

# INTRODUCTION

In an era where digital identity is as crucial as our physical presence, the exploration of secure and efficient identification methods becomes imperative. This thesis delves into the innovative domain of Decentralized Identities (DIDs), anchored in the robust framework of blockchain technology. It aims to dissect the development standards of DIDs, offering a fresh perspective on digital identification challenges and solutions. The following sections will introduce the subject matter, outline the objectives and methodology, highlight the innovative aspects, and describe the structure of this study.

## Subject of the Thesis

This thesis embarks on an exploratory journey into the realm of Decentralized Identities, a concept poised to redefine the standards of digital identity verification and management. At the heart of this transformation lies blockchain technology, a revolutionary framework that underpins the development and functionality of DIDs. By decentralizing identity management, DIDs offer a promising solution to the myriad challenges plaguing traditional digital identification systems, such as data breaches, privacy violations, and centralized control. This study aims to meticulously evaluate the development standards of DIDs, delving into their technical underpinnings, operational mechanisms, and potential to foster a more secure, efficient, and user-centric digital world. As we navigate through this thesis, we will uncover the intricate layers of blockchain technology, assess the current landscape of digital identification, and critically analyze real-world applications of DIDs, thereby contributing to the burgeoning discourse on digital identity in the 21st century.

## Objectives

The primary objective of this thesis is to provide a comprehensive evaluation of the development standards for Decentralized Identities and to understand their role and efficacy in the broader context of digital identification. The specific objectives are as follows:

1. To Understand the Role of Blockchain in DIDs: This involves exploring how blockchain technology serves as the foundational framework for DIDs, focusing on its key features that enable secure and decentralized identity management.

2. To Analyze the Current Digital Identification Landscape: This includes examining the existing digital identification methods, identifying their limitations, and understanding the need for a more secure and user-centric approach.

3. To Examine the Technical Framework of DIDs: The aim here is to dissect the technical aspects of DIDs, including their architecture, protocols, and standards, to understand how they function and are developed.

4. To Evaluate the Effectiveness of DIDs in Addressing Digital Identification Challenges: This involves assessing how DIDs can overcome the issues prevalent in traditional identification systems, such as data breaches, privacy concerns, and centralized control.

5. To Explore Real-World Applications and Case Studies: The objective is to analyze various applications of DIDs across different sectors, providing empirical evidence of their functionality and impact.

## Methodology

The methodology of this thesis is designed to offer a comprehensive evaluation of Decentralized Identities (DIDs), blending theoretical insights with empirical analysis. While a foundational literature review is conducted to align the study with existing knowledge in blockchain and digital identification, significant emphasis is placed on the technical analysis of DIDs. This involves an in-depth examination of their architecture, protocols, and standards, dissecting various technical documents and whitepapers to understand the intricacies of DIDs. Complementing this, the study employs a case study approach, analyzing real-world applications of DIDs across different sectors. These case studies are instrumental in providing empirical evidence and practical insights into the functionality, challenges, and impact of DIDs, thereby enriching the theoretical findings with real-world applications and experiences.

## Innovation

This thesis delves into the groundbreaking aspects of Decentralized Identities (DIDs), a pivotal innovation in digital identification. Central to this innovation is the shift from centralized to decentralized identity management, leveraging blockchain technology to enhance security, privacy, and user autonomy. This approach marks a significant departure from traditional systems, introducing the concept of Self-Sovereign Identity (SSI) where individuals have complete control over their digital identities. Another innovative aspect is the focus on interoperability and the development of universal standards, enabling DIDs to function seamlessly across various platforms and systems. Enhanced security and privacy are achieved through advanced cryptographic techniques, addressing critical vulnerabilities of existing systems. The practical applications of DIDs in sectors like finance, healthcare, and governance demonstrate their versatility and real-world utility, showcasing how they are reshaping the use and management of digital identities. Furthermore, DIDs contribute significantly to building digital trust in online interactions, a crucial element in our increasingly digital world.

## Structure

This thesis is structured to provide a coherent and comprehensive exploration of Decentralized Identities (DIDs). It begins with an introductory chapter that sets the stage for the study, outlining the subject, objectives, and methodology. Following this, the thesis is divided into three main chapters. The first chapter delves into the role of blockchain technology in digital identification, laying the foundational understanding necessary for grasping the concept of DIDs. The second chapter focuses on the technical framework, development, and standards of DIDs, offering an in-depth analysis of their structure and functionality. Finally, the third chapter presents real-world applications and case studies, illustrating the practical implementation and impact of DIDs across various sectors.

# 1 CHAPTER 1: Blockchain and Its Role in Digital Identification

This chapter delves into an exploration of blockchain technology, a cornerstone in the realm of digital identification. This chapter aims to demystify the fundamental aspects of blockchain and point out its pivotal role in enabling Decentralized Identities (DIDs). By delving into the mechanics of blockchain, we lay the groundwork for understanding how this technology supports the security, transparency, and efficiency of digital identities. This exploration serves as a critical foundation for comprehending the subsequent discussions on DIDs and their transformative impact in the digital world. Moreover, it explores the current landscape in the Digital Identification space, as it looks through its history and it explains its drawbacks.

## 1.1 Introduction to Blockchain Technology

Blockchain technology represents a paradigm shift in data management and transaction processing, functioning as a distributed ledger that is maintained across a multitude of servers. This decentralized nature ensures transparency and robust security, as altering any single record would necessitate changes across the entire network, a task that is virtually insurmountable due to the required consensus. The term 'blockchain' is derived from its structural design: data is stored in 'blocks', and each new block is linked to the previous one, forming a 'chain'. This sequential linking of blocks ensures chronological order and integrity of the entire chain. Initially popularized by the advent of Bitcoin in 2009, blockchain technology has since transcended its cryptocurrency origins, demonstrating potential applications in various sectors requiring secure and transparent data management. [16]

A distinctive feature of blockchain is its cryptographic foundation. Each block contains a unique cryptographic code, known as a hash, along with the hash of its preceding block. This cryptographic chaining safeguards the ledger against tampering, as any alteration in a block's data would be immediately evident to the network participants.

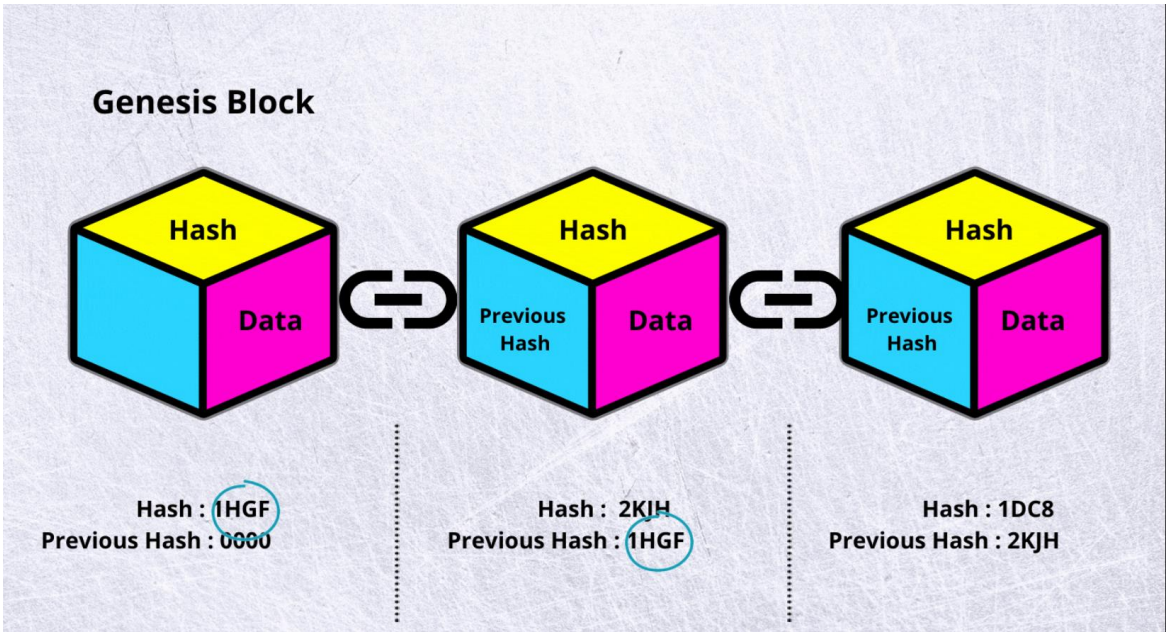


**Figure 1.1 : Blocks that are linked through the hash code of the previous blocks**

Beyond its robust security, blockchain technology democratizes data control. By distributing data across a network rather than centralizing it in a single entity, blockchain empowers individual users, particularly in applications like digital identities. This decentralization is pivotal in the context of digital identities, offering enhanced control and security over personal information.

In essence, blockchain technology offers a secure, transparent, and decentralized framework for data handling and transaction recording. Its implications are particularly significant in the realm of digital identities, where Decentralized Identities (DIDs) leverage blockchain to revolutionize identity management in the digital era.

## 1.2 Key Components of Blockchain Relevant to DIDs

Blockchain Technology is an inseparable part of Decentralized Identities (DIDs) because of its many components, ideal for this implementation. It's inherent features—decentralization, cryptographic security, and transparency—make it an indispensable tool in the realm of digital identification. The decentralized nature of blockchain is a fundamental shift from traditional, centralized identity systems. In a blockchain network, control over identity data is distributed across numerous nodes, enhancing security and reducing the risk of centralized data breaches. This distribution not only bolsters the integrity of the system but also fosters a more transparent and accessible approach to identity management.

Cryptography lies at the heart of blockchain's security mechanism. By employing advanced cryptographic techniques, such as hash functions and digital signatures, blockchain ensures the authenticity and immutability of digital identities. Each identity record on the blockchain is unique and tamper-evident, instilling confidence in the veracity of the data. This cryptographic foundation is crucial for maintaining the trustworthiness of digital identities in various applications. [8] [16]

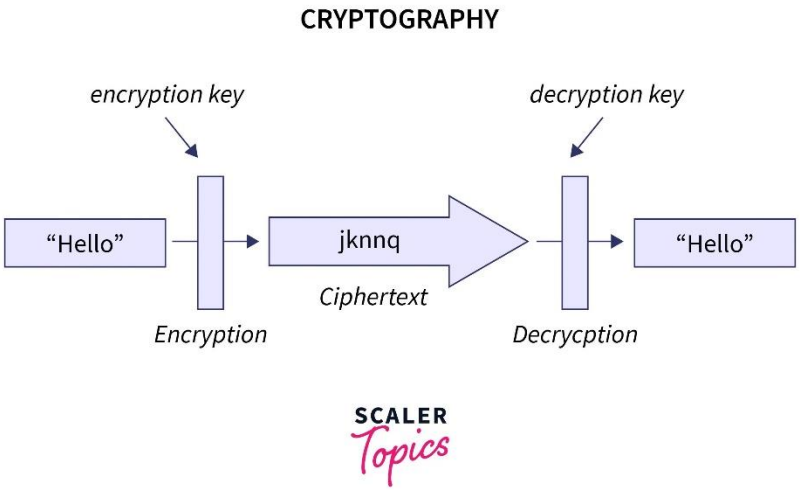



**Figure 1.2 : Basic interpretation of how cryptography works**

The empowerment of users is a key advantage of blockchain in identity management. The concept of Self-Sovereign Identity (SSI) is a testament to this, where individuals have complete control over their identity data. Blockchain facilitates this empowerment by providing a platform where users can manage and share their identity data securely, without depending on centralized authorities. This shift towards user-centric identity management represents a significant advancement in how personal data is handled in the digital age. Trust and verification are paramount in digital interactions, and blockchain excels in these aspects. The technology's transparent yet secure nature allows for a reliable verification process. Entities can verify the authenticity of identity data without needing direct access to the data itself, thereby preserving privacy and security. This streamlined verification process, enabled by blockchain, simplifies various operations, from user onboarding to accessing services. Privacy considerations are integral to blockchain-based digital identities. While blockchain provides a secure environment, balancing transparency with privacy is essential. Techniques like zero-knowledge proofs are employed to validate transactions or identities without exposing underlying personal information, thus maintaining privacy while leveraging blockchain's security benefits. [8] [11] [13]

Interoperability is another critical feature of blockchain in the context of DIDs. The digital world is replete with diverse systems and platforms, and for blockchain-based identities to be effective, they must be universally recognizable and operable. Standardization efforts in blockchain aim to address this challenge, creating a unified framework for digital identities that can be seamlessly integrated across different platforms.

In summary, blockchain technology is not just a supporting structure but a cornerstone in the development and implementation of Decentralized Identities. Its ability to provide a secure, transparent, and user-centric platform for identity management positions it as a crucial component in the evolution of digital identities. As blockchain technology continues to evolve, its role in reshaping digital identity management becomes increasingly significant, offering promising prospects for a more secure and efficient digital future.

## 1.3 The Evolution of Digital Identification Systems

The inception of digital identification systems can be traced back to the latter half of the 20th century. Initially, these systems were rudimentary, often merely digital versions of paper-based methods. Early forms of digital IDs included simple photo IDs and magnetic stripe cards, which were revolutionary for their time. These systems marked the first step in a long journey towards more sophisticated forms of digital identification. As technology advanced, so did the methods of digital identification. The introduction of databases and networked systems allowed for more efficient storage and retrieval of identity information. This era saw the birth of the first digital databases, which could store vast amounts of data and were accessible remotely. The late 20th and early 21st centuries witnessed significant advancements, including the development of smart cards, biometric identification methods, and the integration of RFID technology. Each of these technologies represented a leap forward in terms of security and functionality.

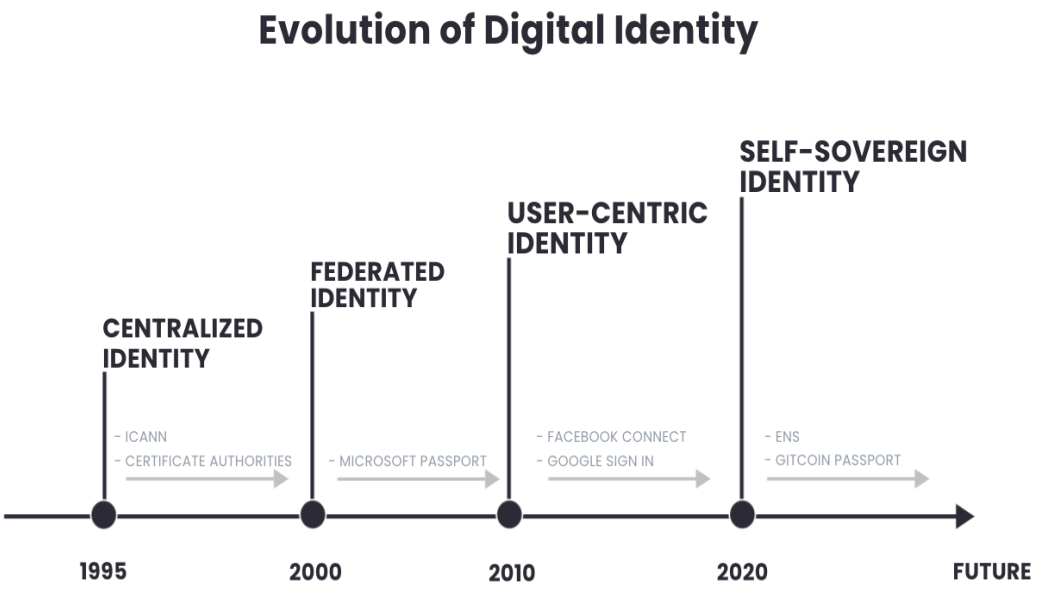



**Figure 1.3 : The evolution of Digital Identity**

The advent of biometric technology marked a significant shift in digital identification. Fingerprint scanning, facial recognition, and iris scanning brought a new level of security, making it much harder to forge or steal an identity. The integration of artificial intelligence and machine learning further enhanced these systems, allowing for more accurate and efficient identity verification processes. These technologies not only improved security but also streamlined the user experience, making identity verification quicker and more user-friendly. With these technological advancements came a change in user expectations. The digital age has ushered in a demand for instant, seamless verification processes. Users now expect a level of convenience and efficiency that was unimaginable a few decades ago. This shift has been a driving force behind many of the innovations in digital identification, pushing the industry towards more integrated, user-centric solutions.

The evolution of digital identification systems is a testament to the ingenuity and adaptability of technology in meeting the changing needs of society. From simple digital replicas of paper IDs to sophisticated biometric and AI-powered systems, digital identification has come a long way. This journey sets the stage for the emergence of decentralized identity solutions, which promise to address many of the challenges faced by traditional systems.

## 1.4 Challenges in Current Digital Identification Systems

Security breaches in digital identification systems have been alarmingly frequent and impactful. The 2017 Equifax data breach is a prime example, where a massive security lapse led to the exposure of sensitive personal information of over 147 million individuals. This breach not only compromised names, Social Security numbers, and birth dates but also shook the public's trust in centralized data systems. Another significant incident was the 2013 Yahoo data breach, where 3 billion accounts were compromised, underscoring the magnitude of risk associated with digital identification systems. These incidents highlight the vulnerabilities of centralized databases and the catastrophic consequences of their failure, emphasizing the need for more secure and decentralized solutions.

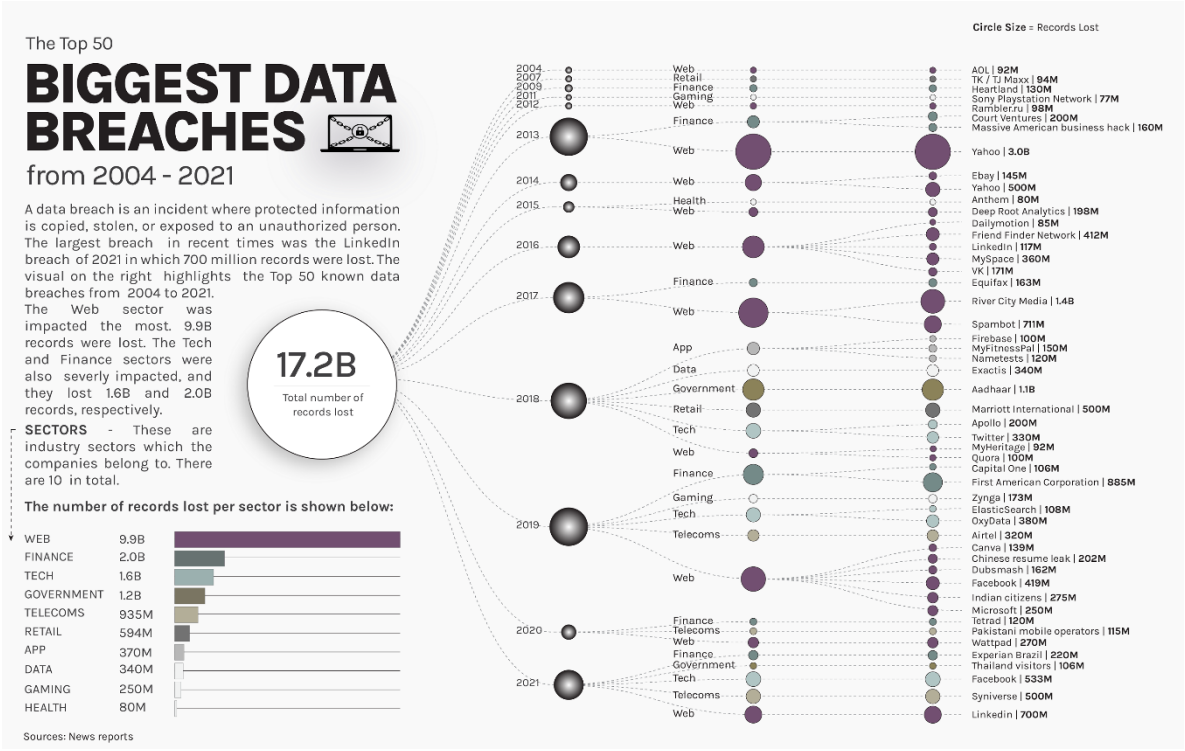



**Figure 1.4 : Biggest Data Breaches from 2004 - 2021**

Privacy in digital identification systems has become a global concern, especially in the wake of incidents like the Cambridge Analytica scandal in 2018. This scandal revealed how personal data from millions of Facebook profiles were harvested without consent and used for political advertising. Such incidents raise critical questions about the control and ownership of personal data. The current digital ID systems often involve extensive data collection, stored in centralized repositories, leading to fears of surveillance and misuse. The lack of transparency and control over personal data exacerbates these concerns, creating a significant trust deficit.


**Figure 1.5 : Percentage of user data being sold to third parties**

The accuracy and reliability of digital identification systems are also under scrutiny. Biometric systems, while advanced, are not infallible and can be prone to errors. Issues such as incorrect data entry, poor-quality biometric scans, and system errors can lead to misidentification, with serious implications for individuals.

Centralized digital identification systems pose challenges in terms of efficiency and control. These systems often result in bottlenecks and are susceptible to administrative biases. The centralized control of data also means individuals have limited oversight or autonomy over their identity information. Also, the lack of interoperability among various digital identification systems is a significant hurdle. Without standardized protocols, it becomes challenging for different systems to communicate and share information, leading to inefficiencies and compatibility issues. Furthermore, navigating the complex legal and regulatory landscape of digital identification is another challenge. Compliance with diverse privacy laws, like GDPR in Europe, adds layers of complexity to the design and implementation of these systems.

Finally, ensuring accessibility and inclusivity in digital identification systems is crucial. The digital divide remains a significant barrier, with not everyone having equal access to the necessary technology. Additionally, these systems must cater to diverse populations, including those with limited technological literacy.

# 2 CHAPTER 2: Decentralized Identities (DIDs)

As we transition into the second chapter of this thesis, its focus shifts to the intricate world of Decentralized Identities (DIDs). This chapter is dedicated to unraveling the concept of DIDs, tracing their evolution, and understanding the standards that govern their development. In the wake of the challenges highlighted in the previous chapter, DIDs emerge as a beacon of innovation, offering a new paradigm in digital identification that promises enhanced security, privacy, and user autonomy.

## 2.1 Defining Decentralized Identities (DIDs)

At its heart, a Decentralized Identity (DID) represents a radical shift from traditional identity systems. Unlike conventional models where identity data is centrally stored and managed, DIDs operate on a decentralized model, primarily using blockchain technology. This means that the control and management of an identity lie not with a central authority but with the individual to whom the identity belongs. DIDs are digital identities that are self-managed and self-verified, providing a new level of autonomy and control to users. The decentralized nature of DIDs is their most defining characteristic, setting them apart from traditional identity systems. This decentralization ensures that individuals have full control and ownership over their identity data, aligning with the principles of Self-Sovereign Identity (SSI). Moreover, DIDs enhance privacy and security, enabling individuals to selectively share their identity information. The cryptographic underpinnings of DIDs ensure that any shared information is authentic and tamper-proof. [13]

Central to the functionality of DIDs are DID documents. These documents contain essential information such as public keys, authentication details, and service endpoints, enabling the verification and management of the identity. Another critical component is verifiable credentials, which are digital attestations linked to a DID, providing trusted and verifiable information about the identity. [1]

The development and use of DIDs are guided by several core principles. Interoperability is a key principle, ensuring that DIDs can function across different systems and platforms. User consent and control are paramount, ensuring that individuals have a say in how their identity data is used. Additionally, the design and implementation of DIDs are driven by considerations of inclusivity and accessibility, ensuring that they are equitable and available to all.

Blockchain technology plays a pivotal role in the functionality of DIDs. It provides a decentralized infrastructure that is secure, transparent, and resistant to censorship. The immutable nature of blockchain ensures that once identity data is recorded, it cannot be altered, enhancing the trustworthiness and reliability of DIDs.

## 2.2 The Evolution and Development of DIDs

The concept of DIDs emerged from the need to address the limitations of traditional digital identity systems, particularly issues related to centralization, security, and user autonomy. The foundational ideas of DIDs were rooted in the principle of shifting control from centralized entities to the individual, thus empowering users and enhancing privacy. The evolution of blockchain technology and advancements in cryptography were crucial in making DIDs a viable solution. Blockchain's decentralized nature provided the perfect infrastructure for DIDs, ensuring security, transparency, and immutability. Cryptographic methods, essential for secure and private verification, further bolstered the trustworthiness of DIDs.

A landmark in the development of DIDs was the publication of the W3C recommendation titled "Decentralized Identifiers (DIDs) v1.0". It's First Public Working Draft was released at 7th of November 2019 and it became a W3C Recommendation, with its final version, on the 19th of July 2022. This document, the first formal publication on the subject, laid the groundwork for the standardization of DIDs. It provided a framework for understanding DIDs, outlining their structure, properties, and functionalities. This recommendation was instrumental in defining the core concepts of DIDs and guiding their subsequent development. Following the W3C's recommendation, the development of DIDs gained momentum, marked by significant milestones. These included the establishment of protocols and standards, the creation of various DID methods, and the launch of platforms and ecosystems supporting DIDs. Organizations like the Decentralized Identity Foundation (DIF) played a key role in fostering collaboration and innovation in the DID space. [1] [4]

The path to developing DIDs involved overcoming numerous challenges, including scalability, interoperability, and user adoption. The DID community responded with innovative solutions, continually refining the technology. Breakthroughs in areas like DID resolution and verifiable credentials (VCs) have been critical in addressing these challenges. [2]

A list of notable additions is as follows:

- **Decentralized Identifier Resolution (DID Resolution) :** A technical specification that outlines the process and mechanisms for resolving a Decentralized Identifier (DID) into a DID document. This resolution process is a crucial aspect of the DID infrastructure, as it enables the retrieval of metadata and other relevant information associated with a DID. (Draft Community Group Report, 18 January 2023) [3]

  Key aspects of the "DID Resolution" draft include:

  1. Resolution Process: It defines the standardized method by which a DID can be resolved to its corresponding DID document. This process involves taking a DID and using specific resolution protocols to access the DID document, which contains essential information like public keys, authentication details, and service endpoints.

  2. Interoperability: The draft aims to ensure interoperability across different DID methods and systems. By providing a common framework for DID resolution, it allows various decentralized systems to work together seamlessly.

3. Protocol Specifications: The document details the technical specifications and protocols required for resolving DIDs. This includes the necessary steps, components, and potential error handling mechanisms involved in the resolution process.

4. Use Cases and Applications: While primarily technical, the draft may also touch on various use cases and applications of DID resolution, demonstrating its importance in the broader context of decentralized identity management.

- **DID Specification Registries :** A comprehensive collection of specifications related to Decentralized Identifiers (DIDs). This document is crucial for the standardization and interoperability of DIDs across different platforms and systems. (W3C Group Note, 27 October 2023) [4]

  Key aspects of the "DID Specification Registries" include:

  1. Registry of DID Methods: It provides a detailed registry of various DID methods, each tailored to specific blockchains or distributed ledger technologies. This registry helps in understanding the diverse approaches to implementing DIDs and ensures compatibility across different systems.

  2. Standardization of Properties and Extensions: The note includes specifications for standard DID properties, as well as extensions and parameters. This standardization is vital for ensuring that DIDs function uniformly, regardless of the underlying technology or platform.

  3. Interoperability Guidelines: By offering a centralized reference for DID specifications, the note aids in promoting interoperability among different DID solutions. This is essential for the widespread adoption and practical application of DIDs.

  4. Community-Driven Updates: The document is maintained as a living document, allowing for continuous updates and contributions from the community. This ensures that the registries stay current with the latest developments and innovations in the field of DIDs.

- **Use Cases and Requirements for Decentralized Identifiers :** A document that outlines various practical scenarios and the corresponding requirements for the effective use of Decentralized Identifiers (DIDs). This draft is instrumental in guiding the development and implementation of DIDs by providing real-world contexts and the needs that DIDs should fulfill. (W3C Editor's Draft, 16 June 2021) [5]

  Key aspects of this draft include:

  1. Diverse Use Cases: The document presents a range of use cases across different industries and contexts, demonstrating the versatility and applicability of DIDs. These scenarios may include personal identity verification, secure online transactions, access control in IoT devices, and more.

2. Requirements for DIDs: Based on the outlined use cases, the draft specifies the requirements that DIDs must meet to be effective. This includes aspects like security, privacy, interoperability, scalability, and user control.

3. Guidance for Developers and Implementers: By linking specific use cases with requirements, the draft serves as a valuable guide for developers and implementers of DIDs. It helps in understanding the practical considerations and challenges in deploying DIDs in real-world applications.

4. Framework for Standardization: The document contributes to the standardization efforts of DIDs by identifying common needs and expectations across different use cases. This aids in creating a more unified and consistent approach to DID development.

- **Verifiable Credentials Data Model v1.1 :** Data model for expressing cryptographically secure digital credentials on the web. Verifiable Presentations are generated from VCs and presented by users for verification. (W3C Recommendation, 3 March 2022) [2]

  Key aspects of this recommendation include:

  1. Data Model for Verifiable Credentials: The document defines a detailed data model for verifiable credentials, which are digital statements made by an issuer about a subject. This model ensures that credentials are structured in a consistent and interoperable manner, facilitating their use across different platforms and applications.

  2. Verification Mechanism: A core component of the recommendation is the mechanism for verifying the authenticity and integrity of credentials. This includes the use of cryptographic techniques to ensure that credentials are tamper-evident and can be trusted.

  3. Issuer, Holder, and Verifier Roles: The recommendation delineates the roles of different entities in the verifiable credentials ecosystem, namely the issuer (entity that issues the credentials), the holder (entity that possesses the credentials), and the verifier (entity that verifies the credentials).

  4. Privacy Considerations: The document emphasizes privacy and user control, outlining approaches to protect personal data and ensure that credential holders can control how their information is shared.

  5. Use Cases and Applications: While primarily technical, the recommendation also touches on various use cases for verifiable credentials, such as in education, employment, and access control, demonstrating their broad applicability.

- **Verifiable Credentials Use Cases :** Outline of several interactions involving verifiable credentials to demonstrate value and utility of VC-based systems. (W3C Editor's Draft, 10 November 2023) [6]

  Key aspects of this draft include:

  1. Diverse Application Scenarios: The document outlines a range of scenarios across different sectors where verifiable credentials can be utilized. These scenarios may include education, employment, finance, healthcare, and government services, among others.

  2. Real-World Relevance: Each use case demonstrates how verifiable credentials can solve real-world problems, such as streamlining processes, enhancing security, improving privacy, and increasing efficiency.

  3. Illustration of Benefits: The draft highlights the benefits of using verifiable credentials in each scenario, such as reducing fraud, enabling portable and self-sovereign identities, and facilitating trust in digital interactions.

  4. Guidance for Implementation: By presenting specific use cases, the draft serves as a guide for developers, policymakers, and organizations interested in implementing verifiable credentials. It helps in understanding the practical considerations and potential impacts of these credentials.

Today, DIDs are at a crucial juncture, with increasing implementation across various sectors. The technology is evolving, driven by ongoing developments in standards, new DID methods, and broader industry adoption. The potential of DIDs to revolutionize digital identity management is increasingly being recognized.

## 2.3 Technical Framework and Standards for DIDs

In this chapter, we delve into the technical components and standards of Decentralized Identities (DIDs) as outlined in the World Wide Web Consortium (W3C) specifications for "Decentralized Identifiers (DIDs) v1.0" and "Verifiable Credentials. This exploration is essential to understand the building blocks that make up DIDs and how they function within a standardized framework. [1] [2]

The building blocks of these frameworks are the following:

- DIDs (Decentralized Identifiers)
- DID Subject
- DID Controller
- DID Methods
- DID Document
- DID Resolution
- Verifiable Credentials

### 2.3.1 DIDs

A Decentralized Identifier, or DID, is a URI composed of three parts: the scheme did:, a method identifier, and a unique, method-specific identifier specified by the DID method. DIDs are resolvable to DID documents. A DID URL extends the syntax of a basic DID to incorporate other standard URI components such as path, query, and fragment in order to locate a particular resource—for example, a cryptographic public key inside a DID document, or a resource external to the DID document. [1]

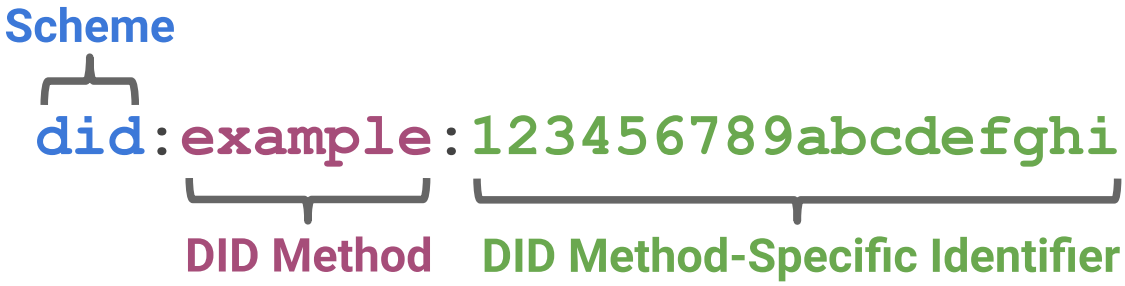



**Figure 2.1 : A simple example of a decentralized identifier (DID)**

**The DID Syntax ABNF Rules**

```
did                = "did:" method-name ":" method-specific-id
method-name        = 1*method-char
method-char        = %x61-7A / DIGIT
method-specific-id = *( *idchar ":" ) 1*idchar
idchar             = ALPHA / DIGIT / "." / "-" / "_" / pct-encoded
pct-encoded        = "%" HEXDIG HEXDIG
```

**Figure 2.2 : The Syntax ABNF Rules for DIDs**

### 2.3.2 DID Subject

The subject of a DID is, by definition, the entity identified by the DID. The DID subject might also be the DID controller. Anything can be the subject of a DID: person, group, organization, thing, or concept. The DID for a particular DID subject is expressed using the "id" property in the DID document. [1]

```
{
  "id": "did:example:123456789abcdefghijk"
}
```

**Figure 2.3 : A simple example of how a DID subject is presented in a DID Document**

### 2.3.3 DID Controller

The controller of a DID is the entity (person, organization, or autonomous software) that has the capability—as defined by a DID method—to make changes to a DID document. This capability is typically asserted by the control of a set of cryptographic keys used by software acting on behalf of the controller, though it might also be asserted via other mechanisms. Note that a DID might have more than one controller, and the DID subject can be the DID controller, or one of them. The controller of the DID, if present in the DID document, is defined with the property "controller". [1]

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  "id": "did:example:123456789abcdefghi",
  "controller": "did:example:bcehfew7h32f32h7af3",
}
```

**Figure 2.4 : Example of a DID document with the "controller" property**

### 2.3.4 DID Methods

A DID method defines how implementers can realize the features described by this specification. DID methods are often associated with a particular verifiable data registry. New DID methods are defined in their own specifications to enable interoperability between different implementations of the same DID method. Each DID method corresponds to a specific protocol or set of rules, defined in the W3C specifications, that govern how DIDs are created, resolved, updated, and deactivated on a particular verifiable data registry. These methods ensure that DIDs can operate across various platforms and technologies, maintaining a consistent approach to identity management. [1]

Methods must follow a specific syntax. The requirements for all DID method specifications when defining the method-specific DID Syntax are as follows:

1. A DID method specification MUST define exactly one method-specific DID scheme that is identified by exactly one method name.
2. The DID method specification MUST specify how to generate the method-specific-id component of a DID.
3. The DID method specification MUST define sensitivity and normalization of the value of the method-specific-id.
4. The method-specific-id value MUST be unique within a DID method. The method-specific-id value itself might be globally unique.
5. Any DID generated by a DID method MUST be globally unique.
6. To reduce the chances of method-name conflicts, a DID method specification SHOULD be registered in the DID Specification Registries [DID-SPEC-REGISTRIES].
7. A DID method MAY define multiple method-specific-id formats.
8. The method-specific-id format MAY include colons. The use of colons MUST comply syntactically with the method-specific-id ABNF rule.
9. A DID method specification MAY specify ABNF rules for DID paths that are more restrictive than the generic rules in Path.
10. A DID method specification MAY specify ABNF rules for DID queries that are more restrictive than the generic rules in this section.
11. A DID method specification MAY specify ABNF rules for DID fragments that are more restrictive than the generic rules in this section.

| Property | Required? | Value Constraints |
|---|---|---|
| **Id** | Yes | A string that conforms to the DID URL Syntax rules. |
| **controller** | Yes | A string that conforms to the DID Syntax rules. |
| **Type** | Yes | A string. |
| **publicKeyJwk** | No | A map representing a JSON Web Key. |
| **publicKeyMultibase** | No | A string that conforms to a MULTIBASE encoded public key. |

**Table 1 : Verification Method Properties**

One very important DID Method, that has been defined in the original Decentralized Identifiers W3C Recommendation, is the Verification Method; a set of parameters that can be used together with a process to independently verify a proof. For example, a cryptographic public key can be used as a verification method with respect to a digital signature; in such usage, it verifies that the signer possessed the associated cryptographic private key.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/jws-2020/v1"
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  ....
  "verificationMethod": [{
    "id": ...,
    "type": ...,
    "controller": ...,
    "publicKeyJwk": ...
  }, {
    "id": ...,
    "type": ...,
    "controller": ...,
    "publicKeyMultibase": ...
  }]
   }
```

**Figure 2.5 : Example of Verification Method Structure**

The "type" parameter is used to determine the type of Verification Material used in a Verification Method. Verification material is any information that is used by a process that applies a verification method. Examples of verification material properties are publicKeyJwk or publicKeyMultibase.

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://w3id.org/security/suites/jws-2020/v1",
    "https://w3id.org/security/suites/ed25519-2020/v1"
  ]
  "id": "did:example:123456789abcdefghi",
  ...
  "verificationMethod": [{
    "id": "did:example:123#_Qq0UL2Fq651Q0Fjd6TvnYE-faHiOpRlPVQcY_-tA4A",
    "type": "JsonWebKey2020", // external (property value)
    "controller": "did:example:123",
    "publicKeyJwk": {
      "crv": "Ed25519", // external (property name)
      "x": "VCpo2LMLhn6iWku8MKvSLg2ZAoC-nlOyPVQaO3FxVeQ", // external (property
name)

     "kty": "OKP", // external (property name)
      "kid": "_Qq0UL2Fq651Q0Fjd6TvnYE-faHiOpRlPVQcY_-tA4A" // external
(property name)
    }
  }, {
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2020", // external (property value)
    "controller": "did:example:pqrstuvwxyz0987654321",
    "publicKeyMultibase": "zH3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }],
  ...
}
```

**Figure 2.6 : Example of Verification methods using publicKeyJwk and publicKeyMultibase**

### 2.3.5 DID Document

At the heart of a DID is the DID document. This crucial component contains the necessary information to authenticate and interact with the DID, including public keys, authentication protocols, and service endpoints. The DID document is what enables the DID to be used for secure transactions and communications. The structure and content of DID documents are standardized to ensure interoperability and reliability. [1]

```
{
    "@context": [
      "https://www.w3.org/ns/did/v1",
      "https://w3id.org/security/suites/ed25519-2020/v1"
    ],
    "id": "did:example:123",
    "authentication": [
      {
        "id":
"did:example:123#z6MkecaLyHuYWkayBDLw5ihndj3T1m6zKTGqau3A51G7RBf3",
        "type": "Ed25519VerificationKey2020", // external (property value)
        "controller": "did:example:123",
        "publicKeyMultibase": "zAKJP3f7BD6W4iWEQ9jwndVTCBq8ua2Utt8EEjJ6Vxsf"
      }
    ],
    "capabilityInvocation": [
      {
        "id":
"did:example:123#z6MkhdmzFu659ZJ4XKj31vtEDmjvsi5yDZG5L7Caz63oP39k",
        "type": "Ed25519VerificationKey2020", // external (property value)
        "controller": "did:example:123",
        "publicKeyMultibase": "z4BWwfeqdp1obQptLLMvPNgBw48p7og1ie6Hf9p5nTpNN"
      }
    ],
    "capabilityDelegation": [
      {
        "id":
"did:example:123#z6Mkw94ByR26zMSkNdCUi6FNRsWnc2DFEeDXyBGJ5KTzSWyi",
        "type": "Ed25519VerificationKey2020", // external (property value)
        "controller": "did:example:123",
        "publicKeyMultibase": "zHgo9PAmfeoxHG8Mn2XHXamxnnSwPpkyBHAMNF3VyXJCL"
      }
    ],
    "assertionMethod": [
      {
        "id":
"did:example:123#z6MkiukuAuQAE8ozxvmahnQGzApvtW7KT5XXKfojjwbdEomY",
        "type": "Ed25519VerificationKey2020", // external (property value)
        "controller": "did:example:123",
        "publicKeyMultibase": "z5TVraf9itbKXrRvt2DSS95Gw4vqU3CHAdetoufdcKazA"
      }
    ]
}
```

**Figure 2.7 : Example of a DID Document with multiple DID Methods**

| Property | Required? | Value Constraints |
|---|---|---|
| **Id** | Yes | A string that conforms to the DID Syntax rules. |
| **alsoKnownAs** | No | A set of strings that conform to the rules of URIs. |
| **controller** | No | A string or a set of strings that conform to the DID Syntax rules. |
| **verificationMethod** | No | A set of Verification Method maps that conform to the rules in Verification Method properties. |
| **authentication** | No | A set of either Verification Method maps that conform to the rules in Verification Method properties or strings that conform to the rules of the DID URL Syntax. |
| **assertionMethod** | No | |
| **keyAgreement** | No | |
| **capabilityInvocation** | No | |
| **capabilityDeligation** | No | |
| **service** | No | A set of Service Endpoint maps that conform to the rules of Service properties. |

**Table 2 : DID Document Properties**

A DID document consists of a map of entries, where each entry consists of a key/value pair. The DID document data model contains at least two different classes of entries. The first class of entries is called properties and the second class is made up of representation-specific entries.

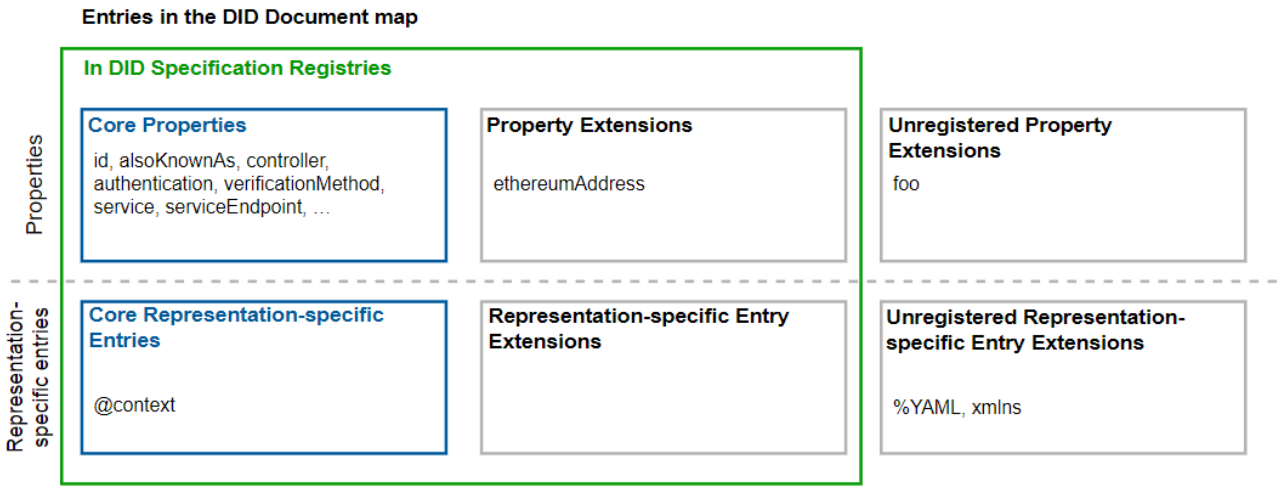



**Figure 2.8 : The entries in a DID Document**

### 2.3.6 DID Resolution

DID resolution is the process by which a DID is translated into a DID document. This process is facilitated by DID resolvers, which take a DID and use the appropriate DID method to retrieve the corresponding DID document. The resolution process is critical for the practical use of DIDs, as it allows for the verification and utilization of the identity information contained within DID documents. A representation is created by serializing the data model through a process called production. A representation is transformed into the data model through a process called consumption. The production and consumption processes enable the conversion of information from one representation to another. This specification defines representations for JSON and JSON-LD. [1] [3]

The requirements for all representations are as follows:

1. A representation MUST define deterministic production and consumption rules for all data types.
2. A representation MUST be uniquely associated with an IANA-registered Media Type.
3. A representation MUST define fragment processing rules for its Media Type.
4. A representation SHOULD use the lexical representation of data model data types. For example, JSON and JSON-LD use the XML Schema dateTime lexical serialization to represent datetimes. A representation MAY choose to serialize the data model data types using a different lexical serializations as long as the consumption process back into the data model is lossless.
5. A representation MAY define representation-specific entries that are stored in a representation-specific entries map for use during the production and consumption process. These entries are used when consuming or producing to aid in ensuring lossless conversion.
6. In order to maximize interoperability, representation specification authors SHOULD register their representation in the DID Specification Registries.

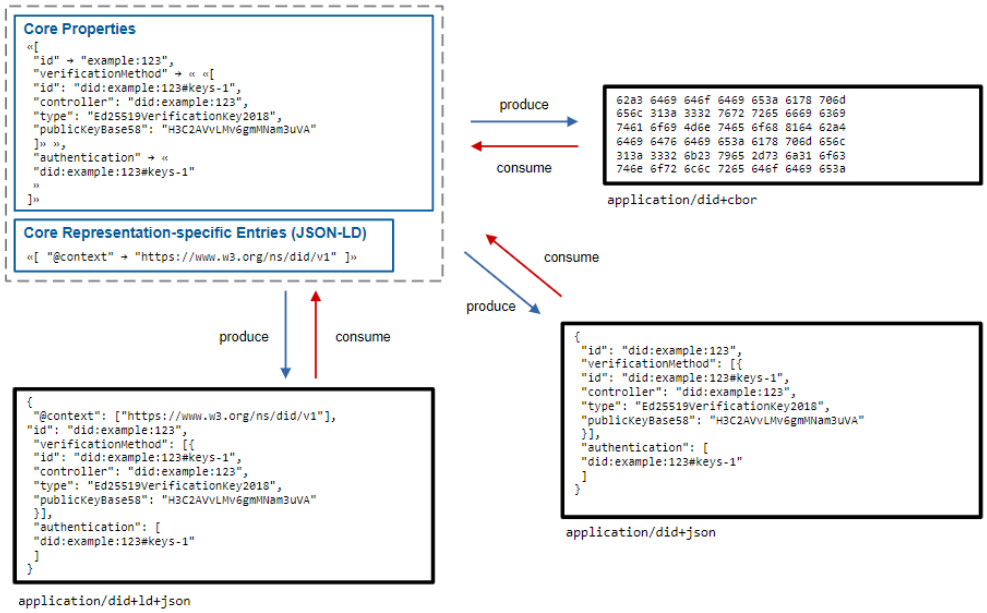



**Figure 2.9 : Production and Consumption of Representations**

### JSON Representation

The DID document, DID document data structures, and representation-specific entries map MUST be serialized to the JSON representation according to the following production rules:

| Data Type | JSON Representation Type |
|---|---|
| **Map** | A JSON Object, where each entry is serialized as a member of the JSON Object with the entry key as a JSON String member name and the entry value according to its type, as defined in this table. |
| **List** | A JSON Array, where each element of the list is serialized, in order, as a value of the array according to its type, as defined in this table. |
| **Set** | A JSON Array, where each element of the set is added, in order, as a value of the array according to its type, as defined in this table. |
| **datetime** | A JSON String serialized as an XML Datetime normalized to UTC 00:00:00 and without sub-second decimal precision. For example: 2023-12-20T19:17:47Z. |
| **String** | A JSON String. |
| **integer** | A JSON Number without a decimal or fractional component. |
| **double** | A JSON Number with a decimal and fractional component. |
| **boolean** | A JSON Boolean. |
| **Null** | A JSON null literal. |

**Table 3 : JSON Production Rules**

```
{
  "id": "did:example:123456789abcdefghi",
  "authentication": [{
    "id": "did:example:123456789abcdefghi#keys-1",
    "type": "Ed25519VerificationKey2018",
    "controller": "did:example:123456789abcdefghi",
    "publicKeyBase58": "H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV"
  }]
}
```

**Figure 2.10 : Example of DID Document in JSON representation**

**JSON-LD Representation**

The DID document, DID document data structures, and representation-specific entries map MUST be serialized to the JSON-LD representation according to the JSON representation production rules. In addition to using the JSON representation production rules, JSON-LD production MUST include the representation-specific @context entry. The serialized value of @context MUST be the JSON String https://www.w3.org/ns/did/v1, or a JSON Array where the first item is the JSON String https://www.w3.org/ns/did/v1 and the subsequent items are serialized according to the JSON representation production rules. [17]

```
{
  "@context": "https://www.w3.org/ns/did/v1",
  ...
}
```

**Figure 2.11 : An example of a valid serialization of a simple @context entry.**

```
{
  "@context": [
    "https://www.w3.org/ns/did/v1",
    "https://did-method-extension.example/v1"
  ],
  ...
}
```

**Figure 2.12 : An example of a valid serialization of a layered @context entry.**

### 2.3.7 Verifiable Credentials

Verifiable Credentials are an integral part of the DID ecosystem. These digital statements, which can be issued, held, and verified, provide a way to establish trust in the digital realm. Verifiable Credentials can be linked to a DID, allowing for a secure and verifiable way to present identity information. Currently it is difficult to express education qualifications, healthcare data, financial account details, and other sorts of third-party verified machine-readable personal information on the Web. The difficulty of expressing digital credentials on the Web makes it challenging to receive the same benefits through the Web that physical credentials provide us in the physical world.

A verifiable credential can represent all of the same information that a physical credential represents. The addition of technologies, such as digital signatures, makes verifiable credentials more tamper-evident and more trustworthy than their physical counterparts. Holders of verifiable credentials can generate verifiable presentations and then share these verifiable presentations with verifiers to prove they possess verifiable credentials with certain characteristics. Both verifiable credentials and verifiable presentations can be transmitted rapidly, making them more convenient than their physical counterparts when trying to establish trust at a distance. [2]

This ecosystem, to function, requires the following roles:

- Holder : A role an entity might perform by possessing one or more verifiable credentials and generating verifiable presentations from them. Example holders include students, employees, and customers.
- Issuer : A role an entity performs by asserting claims about one or more subjects, creating a verifiable credential from these claims, and transmitting the verifiable credential to a holder. Example issuers include corporations, non-profit organizations, trade associations, governments, and individuals.
- Subject : An entity about which claims are made. Example subjects include human beings, animals, and things. In many cases the holder of a verifiable credential is the subject, but in certain cases it is not. For example, a parent (the holder) might hold the verifiable credentials of a child (the subject), or a pet owner (the holder) might hold the verifiable credentials of their pet (the subject).
- Verifier : A role an entity performs by receiving one or more verifiable credentials, optionally inside a verifiable presentation, for processing. Example verifiers include employers, security personnel, and websites.
- Verifiable Data Registry : A role a system might perform by mediating the creation and verification of identifiers, keys, and other relevant data, such as verifiable credential schemas, revocation registries, issuer public keys, and so on, which might be required to use verifiable credentials. Some configurations might require correlatable identifiers for subjects. Example verifiable data registries include trusted databases, decentralized databases, government ID databases, and distributed ledgers. Often there is more than one type of verifiable data registry utilized in an ecosystem.

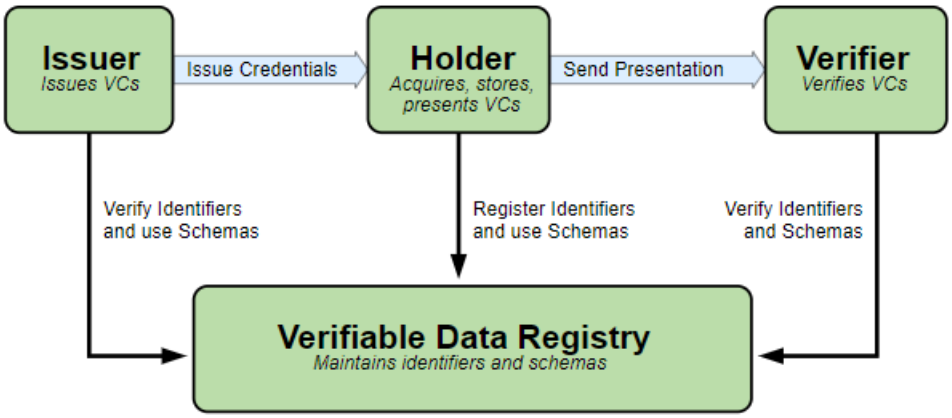



**Figure 2.13 : A presentation of the VC's workings**

- **Here is how it works:**

First are the claims. A claim is a statement about a subject. A subject is a thing about which claims can be made. Claims are expressed using **subject- property-value** relationships.

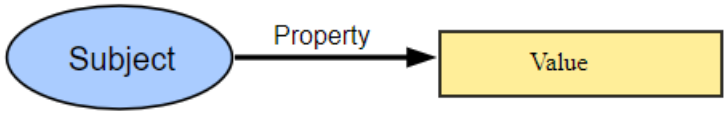



**Figure 2.14 : The basic structure of a claim.**

The data model for claims, illustrated above, is powerful and can be used to express a large variety of statements. For example, whether someone graduated from a particular university can be expressed as shown below.

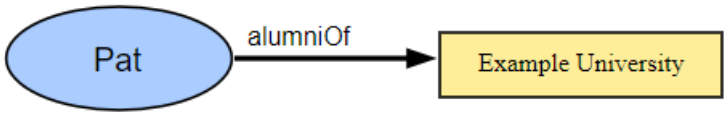



**Figure 2.15 : A basic claim expressing that Pat is an alumni of "Example University".**

Individual claims can be merged together to express a graph of information about a subject. The example shown below extends the previous claim by adding the claims that Pat knows Sam and that Sam is employed as a professor.

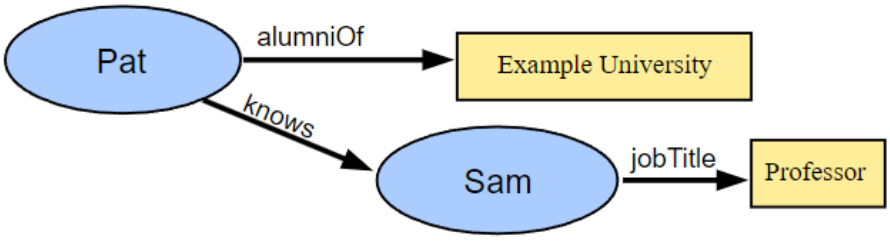



**Figure 2.16 : Multiple claims can be combined to express a graph of information.**

A credential is a set of one or more claims made by the same entity. Credentials might also include an identifier and metadata to describe properties of the credential, such as the issuer, the expiry date and time, a representative image, a public key to use for verification purposes, the revocation mechanism, and so on. The metadata might be signed by the issuer. A verifiable credential is a set of tamper-evident claims and metadata that cryptographically prove who issued it.

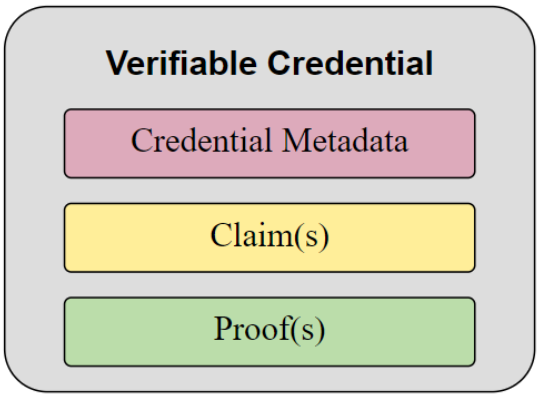



**Figure 2.17 : Basic concepts of a Verifiable Credential.**

The figure below shows a more complete depiction of a verifiable credential, which is normally composed of at least two information graphs. The first graph expresses the verifiable credential itself, which contains credential metadata and claims. The second graph expresses the digital proof, which is usually a digital signature.

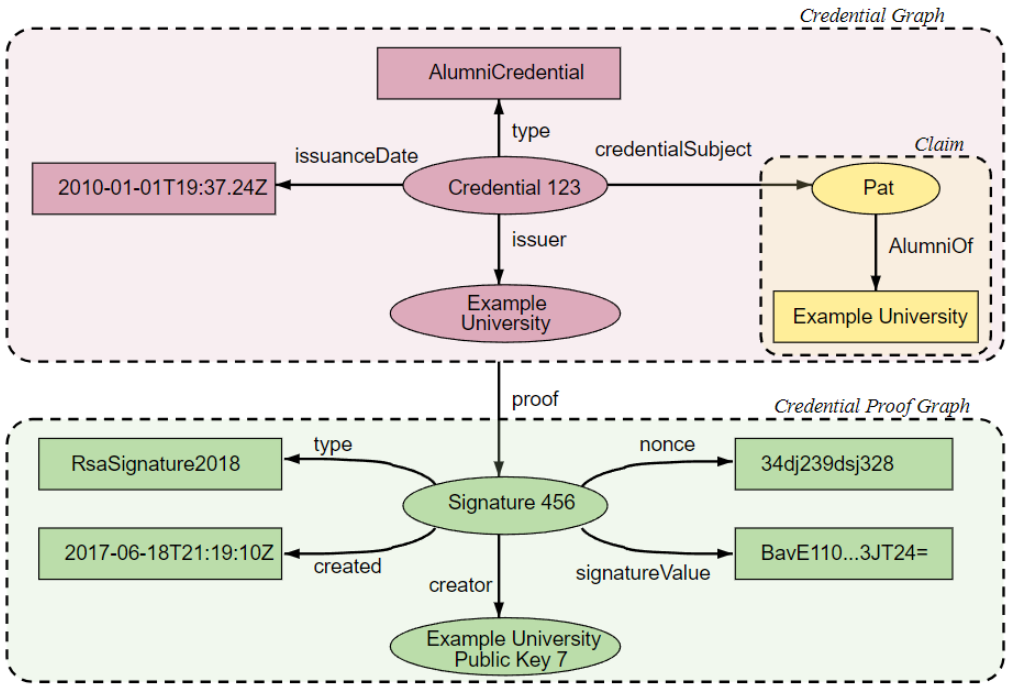



**Figure 2.18 : Information graphs associated with a basic verifiable credential.**

Enhancing privacy is a key design feature of this specification. Therefore, it is important for entities using this technology to be able to express only the portions of their persona that are appropriate for a given situation. The expression of a subset of one's persona is called a verifiable presentation. Examples of different personas include a person's professional persona, their online gaming persona, their family persona, or an incognito persona.

A verifiable presentation expresses data from one or more verifiable credentials, and is packaged in such a way that the authorship of the data is verifiable. If verifiable credentials are presented directly, they become verifiable presentations. Data formats derived from verifiable credentials that are cryptographically verifiable, but do not of themselves contain verifiable credentials, might also be verifiable presentations. The data in a presentation is often about the same subject, but might have been issued by multiple issuers. The aggregation of this information typically expresses an aspect of a person, organization, or entity.

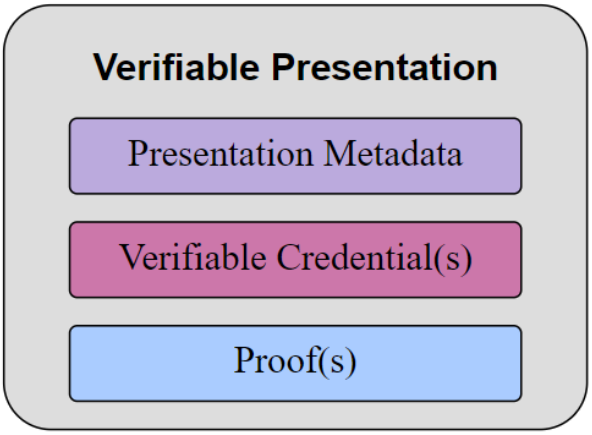



**Figure 2.19 : Basic components of a verifiable presentation.**

The figure below shows a more complete depiction of a verifiable presentation, which is normally composed of at least four information graphs. The first of these information graphs, the Presentation Graph, expresses the verifiable presentation itself, which contains presentation metadata. The verifiableCredential property in the Presentation Graph refers to one or more verifiable credentials, each being one of the second information graphs, i.e., a self-contained Credential Graph, which in turn contains credential metadata and claims. The third information graph, the Credential Proof Graph, expresses the credential graph proof, which is usually a digital signature. The fourth information graph, the Presentation Proof Graph, expresses the presentation graph proof, which is usually a digital signature.

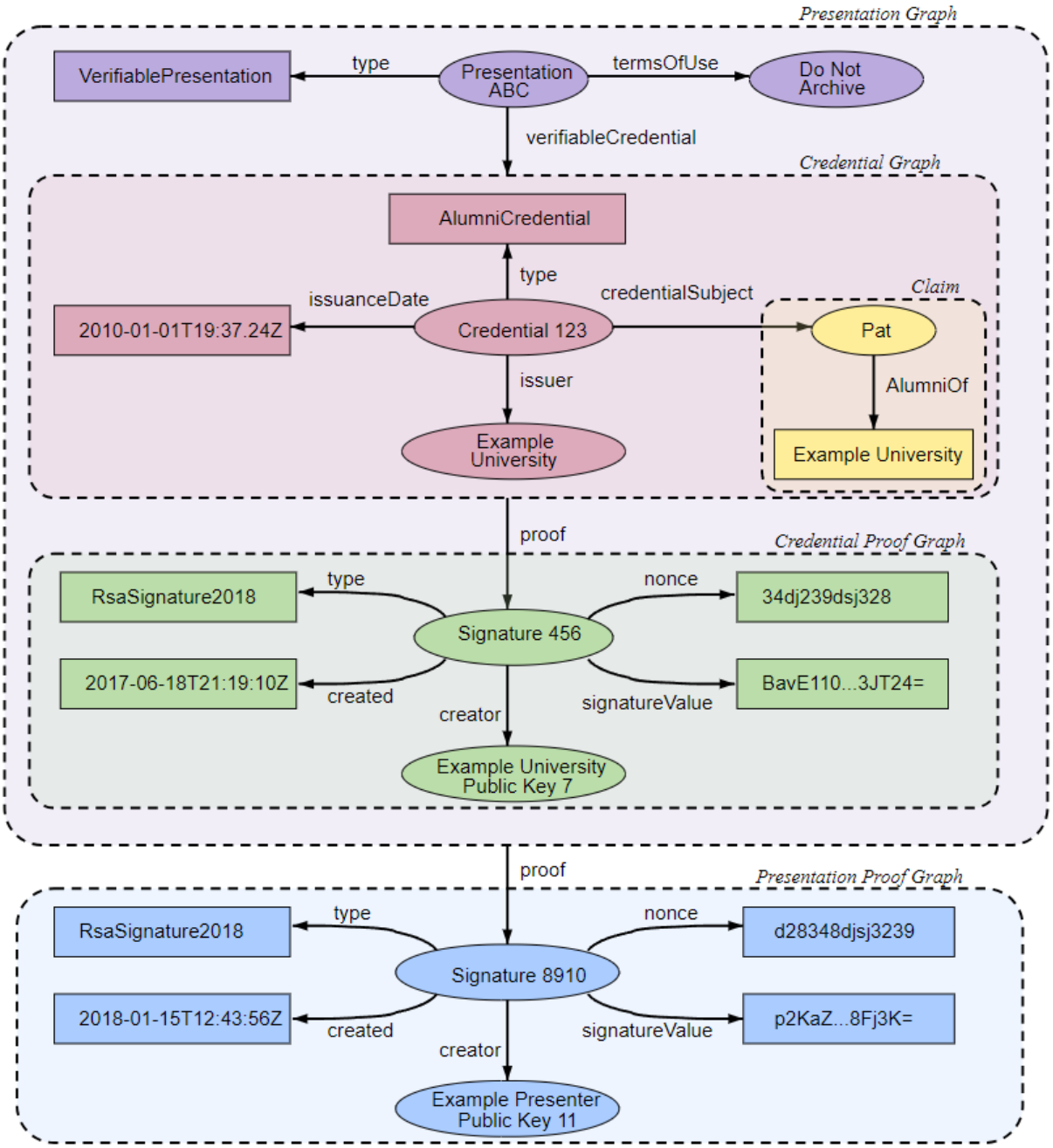



**Figure 2.20 : Information graphs associated with a basic verifiable presentation.**

```
{
  // set the context, which establishes the special terms we will be using
  // such as 'issuer' and 'alumniOf'.
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  // specify the identifier for the credential
  "id": "http://example.edu/credentials/1872",
  // the credential types, which declare what data to expect in the credential
  "type": ["VerifiableCredential", "AlumniCredential"],
  // the entity that issued the credential
  "issuer": "https://example.edu/issuers/565049",
  // when the credential was issued
  "issuanceDate": "2010-01-01T19:23:24Z",
  // claims about the subjects of the credential
  "credentialSubject": {
    // identifier for the only subject of the credential
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    // assertion about the only subject of the credential
    "alumniOf": {
      "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
      "name": [{
        "value": "Example University",
        "lang": "en"
      }, {
        "value": "Exemple d'Université",
        "lang": "fr"
      }]
    }
  },
  // digital proof that makes the credential tamper-evident
  "proof": {
    // the cryptographic signature suite that was used to generate the signature
    "type": "RsaSignature2018",
    // the date the signature was created
    "created": "2017-06-18T21:19:10Z",
    // purpose of this proof
    "proofPurpose": "assertionMethod",
    // the identifier of the public key that can verify the signature
    "verificationMethod": "https://example.edu/issuers/565049#key-1",
    // the digital signature value
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
      sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
      X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
      PAYuNzVBAh4vGHSrQyHUdBBPM"
  }
}
```

**Figure 2.21 : A simple example of a verifiable credential.**

```
{
  "@context": [
    "https://www.w3.org/2018/credentials/v1",
    "https://www.w3.org/2018/credentials/examples/v1"
  ],
  "type": "VerifiablePresentation",
  // the verifiable credential issued in the previous example
  "verifiableCredential": [{
    "@context": [
      "https://www.w3.org/2018/credentials/v1",
      "https://www.w3.org/2018/credentials/examples/v1"
    ],
    "id": "http://example.edu/credentials/1872",
    "type": ["VerifiableCredential", "AlumniCredential"],
    "issuer": "https://example.edu/issuers/565049",
    "issuanceDate": "2010-01-01T19:23:24Z",
    "credentialSubject": {
      "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
      "alumniOf": {
        "id": "did:example:c276e12ec21ebfeb1f712ebc6f1",
        "name": [{
          "value": "Example University",
          "lang": "en"
        }, {
          "value": "Exemple d'Université",
          "lang": "fr"
        }]
      }
    },
    "proof": {
      "type": "RsaSignature2018",
      "created": "2017-06-18T21:19:10Z",
      "proofPurpose": "assertionMethod",
      "verificationMethod": "https://example.edu/issuers/565049#key-1",
      "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..TCYt5X
        sITJX1CxPCT8yAV-TVkIEq_PbChOMqsLfRoPsnsgw5WEuts01mq-pQy7UJiN5mgRxD-WUc
        X16dUEMGlv50aqzpqh4Qktb3rk-BuQy72IFLOqV0G_zS245-kronKb78cPN25DGlcTwLtj
        PAYuNzVBAh4vGHSrQyHUdBBPM"
    }
  }],
  // digital signature by Pat on the presentation
  // protects against replay attacks
  "proof": {
    "type": "RsaSignature2018",
    "created": "2018-09-14T21:19:10Z",
    "proofPurpose": "authentication",
    "verificationMethod": "did:example:ebfeb1f712ebc6f1c276e12ec21#keys-1",
    // 'challenge' and 'domain' protect against replay attacks
    "challenge": "1f44d55f-f161-4938-a659-f8026467f126",
    "domain": "4jt78h47fh47",
    "jws": "eyJhbGciOiJSUzI1NiIsImI2NCI6ZmFsc2UsImNyaXQiOlsiYjY0Il19..kTCYt5
      XsITJX1CxPCT8yAV-TVIw5WEuts01mq-pQy7UJiN5mgREEMGlv50aqzpqh4Qq_PbChOMqs
      LfRoPsnsgxD-WUcX16dUOqV0G_zS245-kronKb78cPktb3rk-BuQy72IFLN25DYuNzVBAh
      4vGHSrQyHUGlcTwLtjPAnKb78"
  }
}
```

**Figure 2.22 : A simple example of a verifiable presentation.**

All the above building blocks come together to create the secure, privacy oriented and decentralized ecosystem of DIDs. To better understand this, the following figures shows how all the parts work together to accomplice this task.

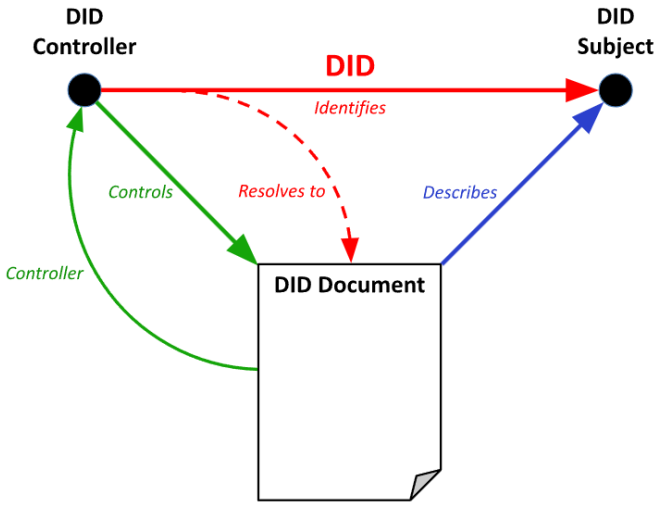



**Figure 2.23 : The DID controller-document-subject relationship.**

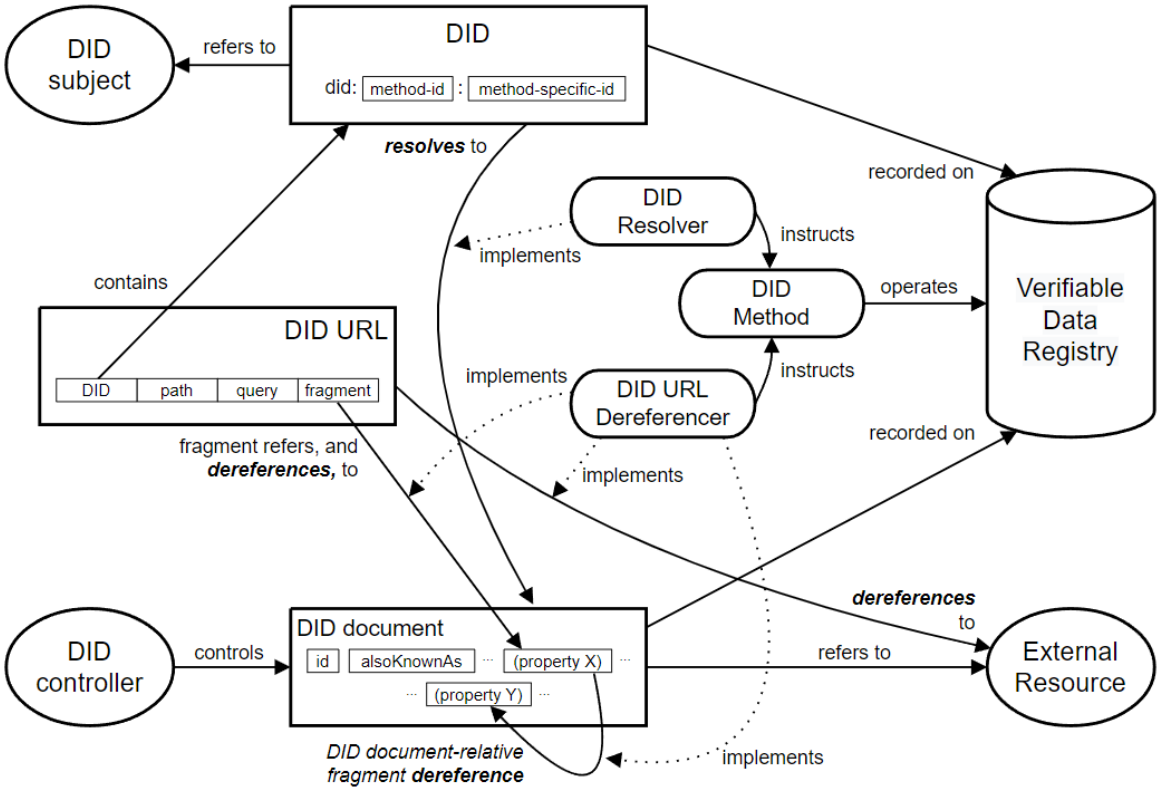



**Figure 2.24 : Detailed overview of DID architecture and the relationship of the basic components.**

## 2.4 DIDs vs Traditional Identification Methods: A Comparative Analysis

This chapter presents a comparative analysis between Decentralized Identifiers (DIDs) and traditional digital identification methods. By examining various facets such as security, privacy, interoperability, and more, we aim to highlight the distinctions and potential advantages of adopting DIDs over conventional systems.

Traditional digital identification systems are predominantly centralized, relying on specific authorities or organizations to manage and control identity data. These systems often use usernames, passwords, and centralized databases to store and manage user information. While they have been the standard for many years, their centralized nature presents several challenges and vulnerabilities. Security is a paramount concern in digital identification. Traditional systems, with their centralized databases, create single points of failure, making them attractive targets for cyber-attacks and data breaches. In contrast, DIDs leverage decentralized structures and cryptographic techniques, offering enhanced security. The decentralized nature of DIDs means there's no central point to attack, and the use of cryptography ensures that only the rightful owner can control their identity.

DIDs represent a significant shift towards privacy and user control through the concept of Self-Sovereign Identity (SSI). Users have full control over their identity and personal data, deciding what to share and with whom. Traditional systems often store user data in centralized repositories, making it difficult for users to control their personal information and leading to potential privacy breaches. Also, DIDs are designed with interoperability in mind, allowing identities to be recognized and used across various platforms and systems. This is facilitated by standardized protocols and formats. Traditional identification systems often operate in silos with proprietary formats, leading to interoperability challenges and inefficiencies. Furthermore, managing and using DIDs could potentially lead to cost savings and efficiency gains due to their decentralized nature, which eliminates the need for centralized infrastructure and intermediaries. In contrast, traditional systems can be costly to maintain and may be less efficient due to their centralized architecture and the need for intermediaries in identity verification processes. [11]

However, there are still challenges that need to be solved before a wider adaption is passible. Firstly, the regulatory and legal landscape for DIDs is still evolving. Integrating DIDs within existing legal frameworks presents challenges but also opportunities for more flexible and user-centric regulations. Traditional systems are well-integrated into current legal frameworks, but they may lack the flexibility to adapt to the changing needs and expectations regarding privacy and data control. In addition, while DIDs promise enhanced security and control, they also face challenges in user experience and global accessibility. The technology is still emerging, and widespread understanding and adoption are in the early stages. Traditional systems, being more established, are generally more accessible and understood by the average user. However, they often lack the flexibility and user-centric design that DIDs aim to provide.

# 3 CHAPTER 3: Real-World Applications and Case Studies of DIDs

In Chapter 3 we transition from the theoretical and technical aspects of Decentralized Identifiers to explore their practical applications and real-world impact. This chapter aims to show the versatility and potential of DIDs through various case studies and scenarios where they are being implemented. We will examine different sectors and domains, from education and governance to securing IoT Networks, to understand how DIDs are solving real-world problems, enhancing security, and empowering individuals with greater control over their digital identities. By analyzing these applications, we can gain insights into the future prospects of DIDs in practice.

## 3.1 Government Services and Humanitarian Efforts

In this chapter, we explore the application of Decentralized Identifiers (DIDs) in the realms of government services and humanitarian efforts, focusing on digital citizenship and providing identity solutions for the undocumented.

The concept of digital citizenship has been revolutionized by the advent of DIDs. Governments around the world are beginning to recognize the potential of DIDs in enhancing the interaction between citizens and public services. A notable example is Estonia's e-Residency Program.


**Figure 3.1 : The e-Residency kit received by the e-resident from the Estonian Government.**

Estonia has been at the forefront of digital governance with its e-Residency program, launched in 2014. This program allows non-Estonians access to Estonian services such as company formation, banking, payment processing, and taxation. The e-Residency digital ID provides a secure and verified digital identity, not tied to any physical document, which users can utilize to sign documents and access services online. While the e-Residency program is based on a centralized model, it showcases many principles relevant to DIDs, such as digital empowerment, enhanced access to services, and improved efficiency in government-citizen interactions. The success of Estonia's program demonstrates the potential benefits of digital identity systems and offers valuable insights for the implementation of DIDs, especially in terms of user adoption, integration with existing services, and the creation of a digital ecosystem. [25]

Another example is the European Self-Sovereign Identity Framework (ESSIF), which is a significant initiative by the European Union aimed at creating a standardized, interoperable framework for digital identity across member states. ESSIF is designed to enable citizens, businesses, and public institutions to control and manage their own identity data, aligning with the principles of self-sovereign identity (SSI) that are central to DIDs. It provides a decentralized approach to identity management, allowing users to share only the necessary information for a particular transaction or interaction, thereby enhancing privacy and security. This framework is part of the broader European Blockchain Services Infrastructure (EBSI), which aims to leverage blockchain technology for public services. [21]

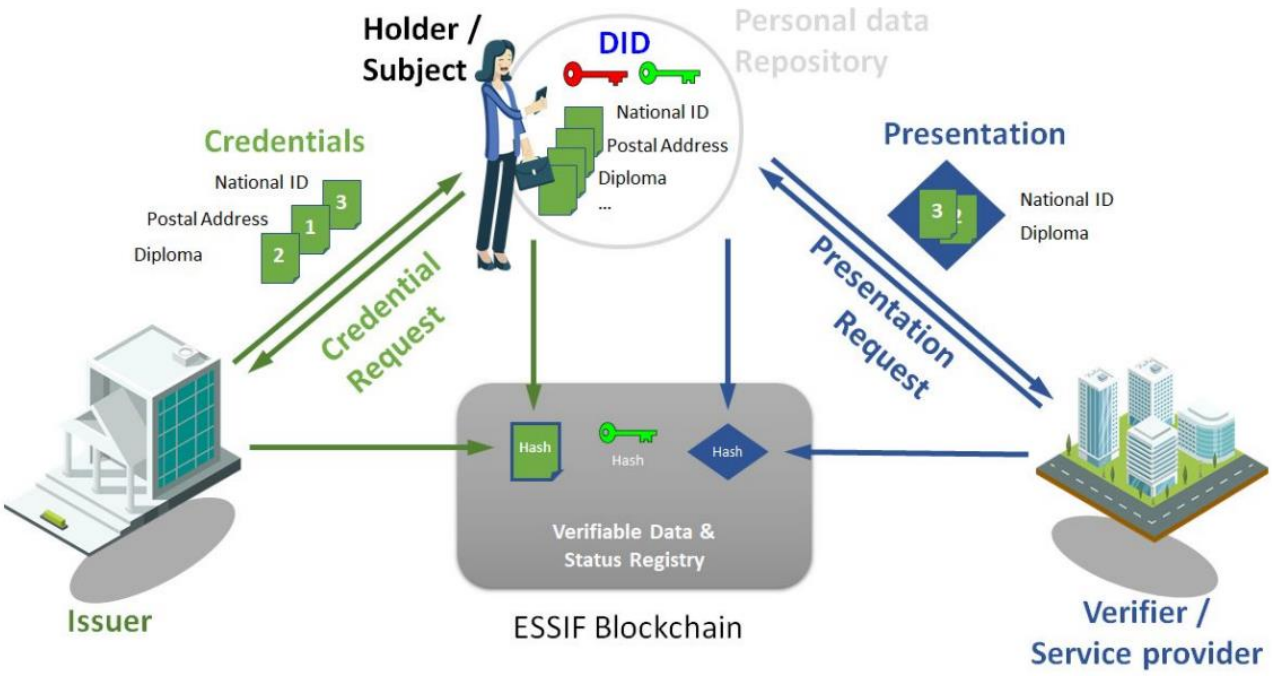



**Figure 3.2 : Example of the ESSIF Solution**

While this implementation is still in early development, it showcases the importance and widespread consideration of a DID solution to the problems that Governments face today.

Perhaps one of the most impactful applications of DIDs is in providing identity solutions for refugees and undocumented individuals. In regions facing humanitarian crises, traditional methods of identity verification are often impractical or inaccessible. DIDs offer a viable alternative. They can be utilized to provide digital identities to refugees, enabling them to access essential services such as healthcare and banking, which were previously unreachable. This approach not only aids in immediate relief efforts but also assists in long-term integration processes.

The United Nations World Food Programme's Building Blocks initiative is an excellent example of using blockchain technology for humanitarian aid. Launched in Pakistan and later expanded to Bangladesh, Jordan, Lebanon and Ukraine, this project uses blockchain to manage and record food assistance transactions. Beneficiaries are verified through biometric data, and transactions are recorded on a blockchain, ensuring security and transparency. [22]

**Figure 3.3 : Using biometrics to do transactions**

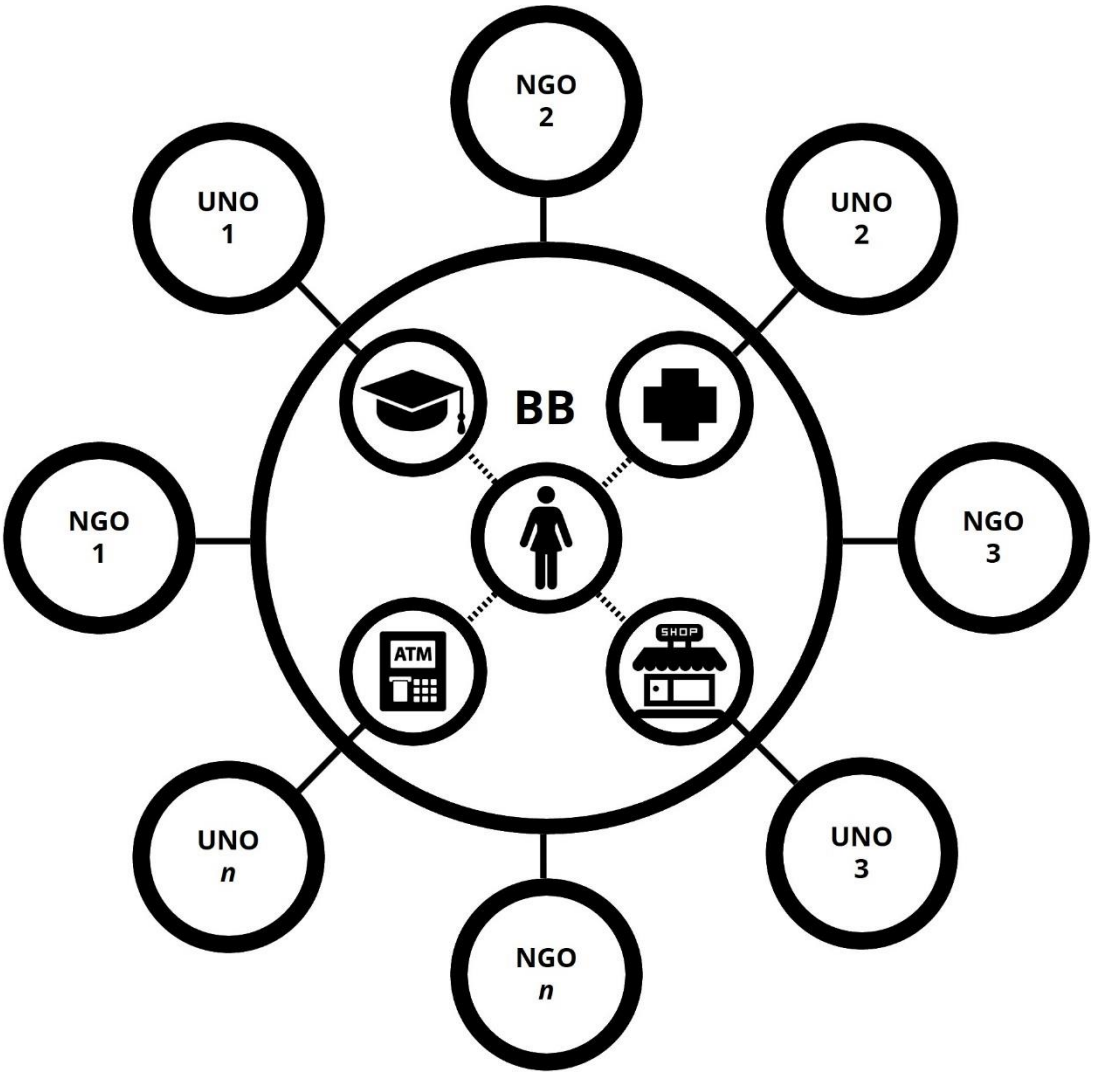



**Figure 3.4 : Building Blocks Network**

While not a DID system in the strict sense, the Building Blocks project aligns with the principles of DIDs in terms of providing secure, verifiable, and decentralized solutions for identity verification and transaction management in challenging environments. This project illustrates the potential of blockchain and related technologies to provide identity and financial solutions in humanitarian settings, offering insights into the scalability, security, and operational challenges and successes.

## 3.2 Education – Credential Verification

In this chapter, we explore the application of Decentralized Identifiers (DIDs) in the education sector, focusing on the verification of academic credentials. This use case demonstrates how DIDs can streamline processes, enhance the integrity of academic qualifications, and provide a more efficient and secure method for credential verification.

The traditional system of credential verification in education is often cumbersome, time-consuming, and prone to fraud. Verifying academic qualifications typically involves manual processes, which can be inefficient and vulnerable to errors. The rise of counterfeit degrees and the complexity of verifying international qualifications further exacerbate these challenges. DIDs offer a transformative solution to these challenges. By utilizing DIDs, educational institutions can issue digital, verifiable credentials to students. These credentials are cryptographically secure, tamper-evident, and can be easily shared with employers or other institutions. This system not only speeds up the verification process but also significantly reduces the potential for fraud.

A pioneering example of using blockchain technology in education is the Massachusetts Institute of Technology's implementation of a digital diploma system. MIT introduced blockchain-based digital diplomas to its graduates as part of a pilot program. These diplomas are issued using a blockchain-driven app called Blockcerts. In this system, graduates receive a digital version of their diploma linked to a unique identifier on the blockchain. This approach allows graduates to securely share a verifiable, tamper-proof version of their credentials with potential employers or other educational institutions. Employers, in turn, can easily and instantly verify the authenticity of these digital diplomas without needing to contact the university. [23]

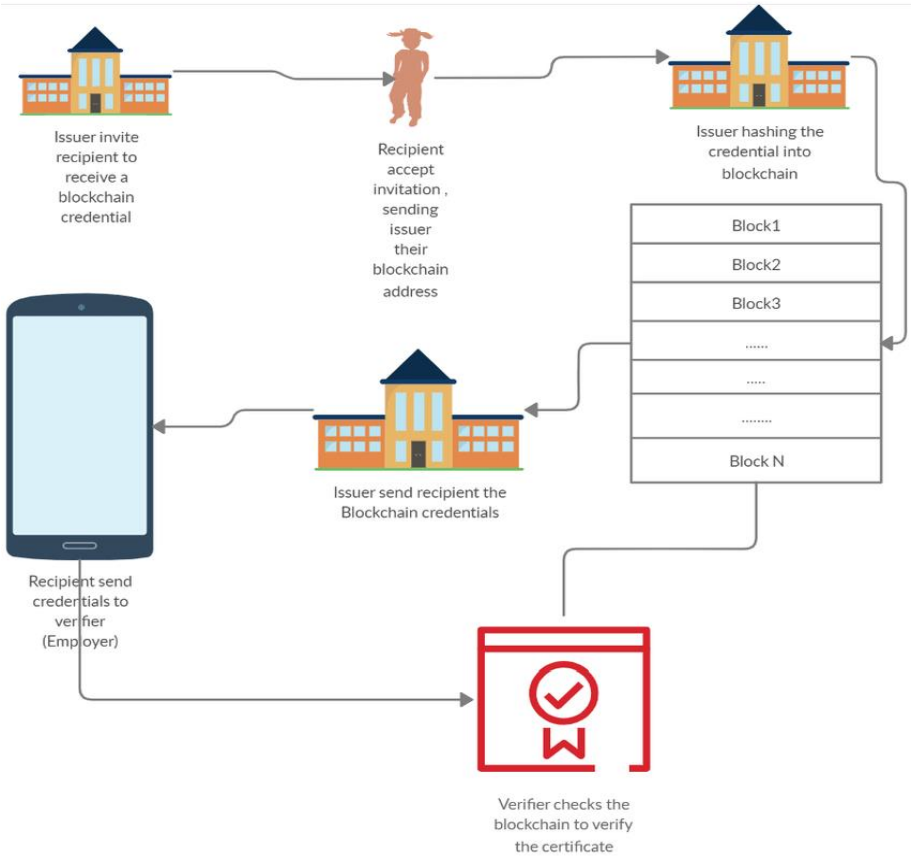



**Figure 3.5 : Representation of Blockcerts**

MIT's initiative serves as a practical demonstration of how DIDs and blockchain technology can be applied in the education sector to modernize and secure the process of credential verification. It showcases the potential for broader adoption of such systems in academic institutions worldwide.

The implementation of DIDs in credential verification has significant implications for the education sector. It not only streamlines administrative processes but also empowers students with control over their academic records. Looking forward, this technology has the potential to create a global, interoperable framework for academic credentials, making it easier for qualifications to be recognized across borders.

## 3.3 IoT – Device Identity and Management

In this chapter, we delve into the application of Decentralized Identifiers (DIDs) within the Internet of Things (IoT) sector, focusing on device identity and management. This use case highlights how DIDs can enhance the security and efficiency of IoT networks.

The IoT ecosystem, characterized by a vast network of interconnected devices, faces significant challenges in identity management and security. Traditional centralized systems struggle with scalability, vulnerability to attacks, and ensuring trust among devices. The lack of a robust and scalable identity management system can lead to security breaches and inefficient operations. DIDs offer a promising solution to these challenges. By assigning a unique, decentralized identifier to each IoT device, DIDs facilitate secure and autonomous device interactions. This decentralized approach ensures that each device can be authenticated and its transactions verified without relying on a central authority, thereby enhancing security and reducing the risk of single points of failure. [14] [15]

Bosch, a global leader in technology and services, has been exploring the use of blockchain and DIDs in their IoT Suite. The Bosch IoT Suite provides a comprehensive set of tools for building and managing IoT applications, and the integration of DIDs offers a new layer of security and efficiency. In this system, each IoT device is assigned a unique DID, enabling secure and autonomous interactions. This approach enhances security, reduces the risk of tampering, and improves scalability. The Bosch IoT Suite serves as a practical example of how DIDs can be applied in large-scale IoT ecosystems, demonstrating the benefits of decentralized technologies in device management. [20]

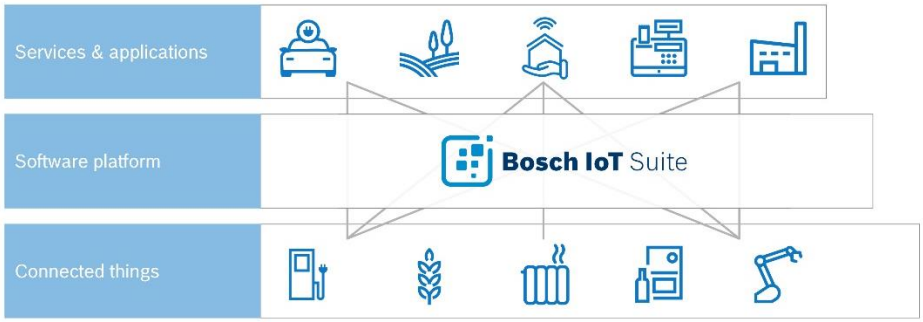



**Figure 3.6 : Showcase of Bosch IoT Suite**

IOTA, with its unique Tangle architecture, presents a novel approach to integrating DIDs in IoT. Unlike traditional blockchain, IOTA's Tangle is designed for high scalability and zero transaction fees, making it well-suited for the IoT environment. In a smart city project utilizing IOTA, IoT devices such as sensors and actuators are assigned DIDs, facilitating secure, autonomous interactions and data exchanges. This setup ensures data integrity, enhances security, and enables functionalities like automated micropayments for services. The integration of DIDs with IOTA's framework showcases the potential for innovative solutions in IoT, addressing challenges like data security and real-time transactions. [19]

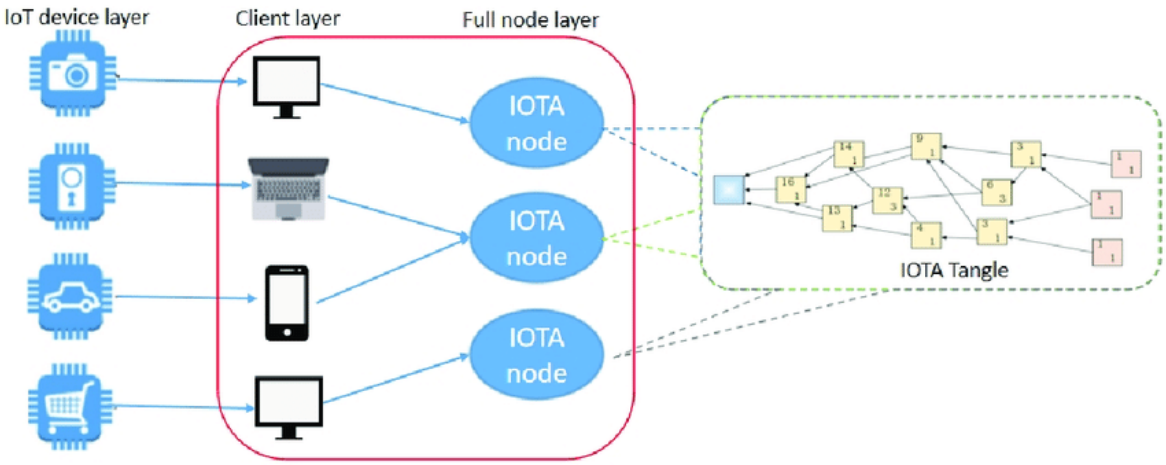



**Figure 3.7 : IoT architecture based on IOTA Tangle**

## 3.4 Discussion: Insights and Implications from the Case Studies

The case studies presented in government services, education, and IoT sectors illustrate the versatility and potential of DIDs in addressing specific challenges. Common themes across these sectors include enhanced security, improved efficiency, and greater user empowerment in managing digital identities. However, each application also revealed unique challenges and adaptations, reflecting the diverse requirements of different sectors. These case studies underscore the transformative potential of DIDs in redefining digital identity management. By offering a decentralized approach, DIDs present a solution to many of the vulnerabilities and inefficiencies of traditional, centralized systems. The scalability of DIDs, demonstrated in these varied applications, suggests their broad applicability across industries.

Despite their potential, the implementation of DIDs faces several challenges. Technical complexities, varying degrees of user adoption, regulatory compliance, and scalability issues are prominent hurdles. The case studies provide valuable insights into addressing these challenges, emphasizing the need for user-friendly designs, clear regulatory frameworks, and scalable infrastructure.

The exploration of DIDs in real-world scenarios reveals a technology with significant potential to revolutionize how digital identities are managed and utilized. While challenges remain, the continued evolution of DIDs, driven by innovation and collaboration, holds promise for a future where digital identities are more secure, private, and user-centric. As we advance, the role of DIDs in shaping the landscape of digital interactions and identity verification will likely be substantial and far-reaching.

# 4 Conclusion

In this concluding chapter, we encapsulate the key findings of our exploration into Decentralized Identifiers (DIDs) and their role in reshaping digital identity management. This thesis has traversed the technical underpinnings of DIDs, their comparison with traditional identification methods, and their practical applications across various sectors.

We began with an introduction to Blockchain technology, a stepping stone for DIDs, and talked about Digital Identification's current state and the problems it faces. Then, an in-depth analysis of the technical framework of DIDs, highlighted their decentralized nature, enhanced security, and user-centric approach. The comparative analysis with traditional digital identification methods revealed DIDs' potential in offering greater security, privacy, and control to users. Finally, the case studies across government services, education, and IoT provided practical insights into the real-world applications of DIDs, demonstrating their versatility and potential to address current challenges in digital identity management.

This thesis has showcased that DIDs emerge as a promising solution to many of the vulnerabilities and inefficiencies of traditional systems, offering a more secure, transparent, and user-controlled approach. The societal, ethical, and technological implications of DIDs suggest a paradigm shift towards a more secure and privacy-preserving digital world. It acknowledges certain limitations, including the rapidly evolving nature of blockchain and DID technologies, which may lead to changes in the technical aspects and applications of DIDs post this study. The scope of the case studies was also limited to specific sectors, and further research could expand to other industries. Future research could focus on exploring the long-term impact of DIDs on various sectors, particularly in terms of user adoption, regulatory challenges, and technological advancements. Studies could also investigate the integration of DIDs with emerging technologies like AI and quantum computing, and their implications for privacy and security.

As we conclude, it is evident that DIDs hold the potential to revolutionize the way we manage and interact with digital identities. This research contributes to the broader understanding of decentralized identity solutions and underscores the importance of continued innovation in this field. The future of DIDs, while promising, will depend on collaborative efforts among technologists, policymakers, and users to realize their full potential and navigate the challenges ahead.

# 5 Bibliography – Citations – Internet Sources

[1] Sporny M., Longley D., Sabadello M., Reed D., Steele O., Allen C., 2022. Decentralized Identifiers (DIDs) v1.0. [online] W3C. Available at: https://www.w3.org/TR/2022/REC-did-core-20220719/ [Accessed 18 January 2024].

[2] Sporny M., Longley D., Chadwick D., 2022. Verifiable Credentials Data Model v1.1. [online] W3C. Available at: https://www.w3.org/TR/2022/REC-vc-data-model-20220303/ [Accessed 18 January 2024].

[3] Sabadello M., Zagidulin D., 2023. Decentralized Identifier Resolution (DID Resolution) v0.3. [online] W3C. Available at: https://w3c-ccg.github.io/did-resolution/ [Accessed 18 January 2024].

[4] Steele O., Sporny M., 2023. DID Specification Registries. [online] W3C. Available at: https://w3c.github.io/did-spec-registries/ [Accessed 18 January 2024].

[5] Hamilton-Duffy K., Grant R., Gropper A., 2021. Use Cases and Requirements for Decentralized Identifiers. [online] W3C. Available at: https://www.w3.org/TR/did-use-cases/ [Accessed 18 January 2024].

[6] Otto N., Lee S., Sletten B., Burnett D., Sporny M., Ebert K., 2023. Verifiable Credentials Use Cases. [online] W3C. Available at: https://w3c.github.io/vc-use-cases/ [Accessed 18 January 2024].

[7] Herman I., 2020. Decentralized Identifiers. Presentation at W3C Chinese Web IG Fintech event, 19 December. Available at: https://iherman.github.io/did-talks/talks/2020-Fintech/#/ [Accessed 18 January 2024].

[8] Wu W., Liu E., Gong X., Wang R., "Blockchain Based Zero-Knowledge Proof of Loca-tion in IoT," ICC 2020 - 2020 IEEE International Conference on Communications (ICC), 2020, doi: 10.1109/ICC40277.2020.9149366

[9] Bodo B., Giannopoulou A., "The logics of technology decentralization - the case of distributed ledger technologies", Blockchain and Web 3.0: Social, Economic, and Technological Challenges, New York: Routledge, 2020.

[10] Granjal J., Monteiro E., Sa Silva J., "Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues", IEEE Communications Surveys & Tutorials, vol. 17, no. 3, pp. 1294-1312, 2015. Available: 10.1109/comst.2015.2388550

[11] Naik N., Jenkins P., "Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology," 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and

Engineering (MobileCloud), 2020, pp. 90-96, doi: 10.1109/MobileCloud48802.2020.00021.

[12] El Ioini N., Pahl C., "A Review of Distributed Ledger Technologies", Lecture Notes in Computer Science, pp. 278-288, 2018. Available: 10.1007/978-3-030-02671-4_16.

[13] Toth K. C., Anderson-Priddy A., "Self-Sovereign Digital Identity: A Paradigm Shift for Identity", IEEE Security & Privacy, vol. 17, no. 3, pp. 17-27, May-June 2019. Doi: 10.1109/MSEC.2018.2888782.

[14] Novo O., "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT", IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1182-1198, 2018. Available: 10.1109/jiot.2018.2812239.

[15] Polychronaki M., Kogias D., Patrikakis C., "Identity Management in Internet of Things with Blockchain", Blockchain based Internet of Things, pp. 209-236, 2022. Available: 10.1007/978-981-16-9260-4_9.

[16] Patrikakis C., Leligkou H., Kogias D., 2023. Blockchain [Postgraduate textbook]. Kallipos, Open Academic Editions. https://dx.doi.org/10.57713/kallipos-171

[17] JSON-RPC (2013). JSON-RPC 2.0 Specification. JSON-RPC Working Group. Online source: https://www.jsonrpc.org/specification [Accessed 18 January 2024].

[18] Xevgenis M., Kogias D., Leligou H., Chatzigeorgiou C., Feidakis M., Patrikakis C. (2020). A survey on the available blockchain platforms and protocols for Supply Chain Management. IOT4SAFE 2020 the 1st International Workshop on IoT infrastructures for safety in pervasive environments, June 2, 2020 (Virtual).

[19] IOTA Foundation, 2024. Home. [online] IOTA. Available at: https://www.iota.org/ [Accessed 18 January 2024].

[20] Bosch Global Software Technologies GmbH, 2024. Bosch IoT Suite - A toolbox in the cloud for IoT developers. [online] Bosch IoT Suite. Available at: https://bosch-iot-suite.com/ [Accessed 18 January 2024].

[21] European Blockchain Forum, 2024. Reports. [online] EU Blockchain Forum. Available at: https://www.eublockchainforum.eu/reports [Accessed 18 January 2024].

[22] World Food Programme, 2024. Building Blocks: Leveraging Blockchain for the World Food Programme. [online] Available at: https://www.wfp.org/building-blocks [Accessed 18 January 2024].

[23] Massachusetts Institute of Technology, 2024. Blockcerts: The Open Standard for Blockchain Credentials. [online] Available at: https://www.blockcerts.org/ [Accessed 18 January 2024].

[24] Srinivasan B., 2022. The Network State. [online] Available at: https://thenetworkstate.com/ [Accessed 18 January 2024].

[25] Estonian Government, 2024. e-Residency. [online] Available at: https://www.e-resident.gov.ee/ [Accessed 18 January 2024].