Verifiable Credentials: An implementation for latin-american diplomas proposal

A comprehensive guide to verifiable credentials implementation for latin-american education institutions

Author
Eng. Mateo Gregory Jimenez
mateo.gregory@correounivalle.edu.co

Advisor
MSc. Sebastian Scotti
sebascotti.uru@gmail.com

Co-Advisor
PhD. Maria Trujillo
maria.trujillo@correounivalle.edu.co

Document with a research proposal as requirement for Master Studies

Escuela de ingenieria de Sistemas y Computacion
Universidad del valle
Colombia
September 2023

Contents

1 Introduction

In our increasingly digitalized world, the menace of fraudulent academic certificates has persisted for years[11], affecting not just ordinary individuals but even public figures at the highest echelons of government [3] and doctors wielding forged credentials[11]. Imagine a scenario where many around the globe claim qualifications they don't possess, duping unsuspecting individuals and institutions who often struggle to discern authenticity in this age of sophisticated counterfeits. In today's age, the art of forgery has evolved to such a degree that even experts find themselves second-guessing. For the average individual, differentiating genuine credentials from fake ones becomes a daunting task, often requiring external validation— a process that can be cumbersome or inaccessible [8].

In August 2022, law enforcement in Bogotá, Colombia, dismantled a network of forgers producing fake diplomas and certificates [2]. Additionally, in February 2023, a high-ranking official from Colombia's health ministry was discovered to possess two counterfeit university diplomas, the universities he claimed to have received the certificates from publicly denied any such affiliations [4]. Meanwhile, in Florida, it was revealed that over 7,600 individuals hold fraudulent nursing degrees [10].

As the world grappled with the COVID-19 pandemic, another shadowy crisis emerged: a surge in forged health certificates, including fabricated negative test results and vaccination cards. Think of the immense challenge this posed to authorities, trying their best to uphold public health measures, only to be thwarted by an undercurrent of deception, complicating their efforts to curb the virus's spread.[1][6][7][9].

It's in such challenging times that innovations like verifiable credentials (VCs) shine as beacons of hope, offering a potential lifeline against these rampant fraudulent activities. VCs, which are digital proofs of qualifications, achievements, or statuses, can be securely stored and shared due to cryptographic protection. They are grounded in standards that render them interoperable, verifiable, and nearly impossible to counterfeit [12].

To combat the rampant issue of counterfeit credentials and bolster security measures, KBC has collaborated with Howest, the University of Applied Sciences in West Flanders, to introduce Europe's premier digital student card. Conforming to the latest European identity and data standards, this card will be housed within the KBC Mobile app, offering students easy and secure access to academic services and privileges. Starting from the 2023/2024 academic term, all 9,500 students enrolled at Howest will have the digital means to validate their student status, ensuring heightened pri-

vacy protection. The technological foundation of this digital student card is a decentralized database, or blockchain. This ensures that only pertinent data is revealed to those verifying the card's authenticity [5].

The European Blockchain Services Infrastructure (EBSI) has been spearheading numerous projects involving VC across different domains, such as education and social security. The aim is to create a common standard for easy verification and almost impossible faking of documents. This includes developing EBSI-conformant digital wallets, issuing and verifying credentials, and engaging various stakeholders in these processes, including universities, employers, IT service providers, and national authorities.

In today's rapidly digitalizing era, the challenge of countering sophisticated, AI-fueled forgery of academic and professional credentials in Latin America, particularly in Colombia, has never been more pressing. This paper will delve into the depth of this pervasive problem and introduce verifiable credentials under the Hyperledger Aries technology as a promising and potent solution. By the conclusion, readers will be equipped with a comprehensive guide tailored for Latin American institutions, underscored by a prototype implementation at Univalle, demonstrating the feasibility and imperative of this innovative approach

1.1 Problem Statement

In the digital era, the bedrock of any online interaction or transaction is trust. Yet, cultivating this trust in a vast, impersonal online landscape proves daunting. The prevailing models, which predominantly depend on centralized authorities, are not only susceptible to security breaches and data misuse but also fall short in flexibility, failing to cater to the multifaceted needs of various users.

Enter the Trust Over Internet Protocol (ToIP)—a beacon of hope that promises a decentralized approach to trust, diminishing dependency on centralized entities and granting individuals greater agency over their personal data. Nevertheless, the road to integrating ToIP protocols is riddled with complexities, necessitating a profound comprehension of the intricacies of this technology.

A conspicuous void exists in the form of accessible, detailed guides that demystify ToIP protocol implementation. This dearth of guidance could stymie ToIP's broader acceptance as potential adopters grapple with its practical application nuances.

This project's essence is to bridge this gap, striving to craft a comprehensive guide tailored to the specificities and roles an organization or

individual might play within the ToIP ecosystem. A guide of this nature holds the promise of simplifying ToIP integration, enabling users to unlock its full potential and fostering a digital world where ToIP gains widespread traction.

1.2 Objectives

1.2.1 General Objective

Develop a comprehensive guide on the implementation of Trust Over Internet protocols, tailored to the specific needs and roles an entity may need to assume within the Trust over IP framework. to facilitate the practical application of already established Trust Over Internet implementations, guiding users on how to effectively utilize these systems.

1.2.2 Specific Objectives

1. Establish distinct agents for the roles of Issuer and Verifier within the trust triangle.
2. Utilize a wallet as the Holder, interfacing with both Issuer and Verifier agents via interoperable constructs.
3. Define and document the modes and extents of interactions among trust triangle components, enhancing comprehension of individual and collective trust dynamics.
4. Chronicle the steps and considerations for implementing each segment of the Trust over Internet protocol corresponding to the trust triangle.
5. Leveraging the documentation, create a detailed guide assisting entities in assuming roles as verifiers, issuers, holders, or multifaceted combinations thereof.
6. Outline the legal considerations and ramifications tied to verifiable credentials within the ambit of Trust Over Internet protocols.

1.2.3 Scope

This guide primarily targets Latin American entities, with a specific focus on Colombia, but its principles can be adapted to broader contexts. The objective is both to provide a hands-on implementation guide and to address the legal and practical nuances associated with Trust Over Internet protocols in the region.

1.3 Work Structure

1.3.1 Introduction

1. Brief about the importance of Trust Over Internet protocols in the digital age.
2. The problem statement that led to this research.

1.3.2 State of the art

1. Comprehensive analysis of the present landscape, highlighting recent advancements.
2. An overview of established best practices within the Trust Over Internet domain.

1.3.3 Methodology

1. Deep dive into existing literature to establish a foundation for the project.
2. Details on creating distinct agents for the roles of Issuer and Verifier within the trust triangle.
3. Steps and rationale behind using a wallet as the Holder.
4. Explanation of how interactions between the trust triangle components are charted.
5. Description of how findings from the above steps will be integrated into a comprehensive guide for Trust Over Internet protocols.
6. A projection of the time required for each phase of the project.

1.3.4 Expected Results

1. A detailed forecast of the project's outcomes, spotlighting the creation of the comprehensive guide.
2. The significance of distinct agents for the Issuer and Verifier in the trust triangle.

1.3.5 Discussion

1. Potential challenges in implementing the guide.

2. Implications of the research and its findings for the wider industry.

1.3.6 Bibliography

1. A meticulously curated list of all references and sources consulted during the research.

2 State of the Art

At the core of the Trust over IP framework lies a dual stack of digital trust technologies. The foundational layer concerns itself with verifiable digital identity, leveraging decentralized identifiers (DIDs) and verifiable credentials (VCs) as the bedrock of trustworthiness. Layered on top of this foundation is the governance layer, providing the necessary rules, regulations, and conventions that dictate how DIDs and VCs should be used, authenticated, and managed. It presents a trust triangle paradigm, comprising of Issuers, Verifiers, and Holders.

For the application of these concepts, it is important to recognize the tools that are at our disposal to use, although at the time of writing this document these concepts are relatively new, there are organizations and people really interested in in giving back to people the control over their digital identities and make fair and transparent the way how we trust each other in the internet. A multitude of Trust over IP implementations have surfaced across various sectors, demonstrating the framework's flexibility and wide-ranging applicability. Industries like healthcare, finance, and education are leveraging ToIP to ensure secure identity verification and data protection. The versatility of the ToIP architecture, combined with the robustness of the verifiable credentials mechanism, makes it a promising solution to address the escalating issues of identity theft, fraud, and data breaches.

As Trust over IP continues to evolve, it is poised to profoundly influence how digital trust is perceived and managed. The promise of increased privacy, security, and control over personal data is potentially transformative. However, the ToIP framework is not without its challenges. Interoperability, scaling, public awareness, and regulatory acceptance are among the obstacles that must be overcome for Trust over IP to realize its full potential. Trust over IP represents an ambitious effort to redefine digital trust at the scale of the internet. As an emerging technology, it is rapidly evolving and presents enormous potential to revolutionize multiple sectors.

Verifiable credentials, are an integral component of the decentralized identity architecture, present a paradigm shift in how identity information is handled, offering unparalleled autonomy, privacy, and security. The Hyperledger Aries, as a decentralized identity framework, serves as an essential vehicle in actualizing these potentials. This infrastructure provides a unified set of tools and libraries for creating, transmitting, storing, and verifying credentials across diverse use-cases. As of today, Aries has been instrumental in establishing standards and interoperability, mitigating fragmentation in the digital identity domain

Verifiable credentials are cryptographically created credentials that have four basic pieces of information inside, who issued the credential, to whom the credential was issued, whether the credential was tampered with, and if the credential was revoked. Also, in the scenes where VCs are useful should be a core set of actors each with a specific role in the model. The W3C presents the following actors. (W3C, 2022)

- 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). For more information about these special cases, see Appendix C. Subject-Holder Relationships.
- 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

These actors interact with each other as shown in figure 1, the issuer issues the credentials to the holder then the holder can send the presentation to the verifier, all of them relying on the verifiable data registry, not in

each other directly but in the verifiable data registry which allows them to trust each other. As the holder can register their credentials in the VDR confirming that the issuer verifies the identifiers, them the verifier can prove that the holder VC was issued by who they say were issued by verifying the identifiers in the VDR and can check to whom it was registered to by the same process, reviewing the identifiers registered by the holder

Another important concept in the scope of this work is the Trust over IP (ToIP) framework which emerges as an innovative approach to digital trust, aiming to establish trust at internet scale. Drawing from the lessons of the past and anticipating the needs of the future, ToIP redefines how trust is conveyed, authenticated, and managed online. This section delves into the state of the art of the Trust over IP, examining its underlying principles, architecture, use-cases, and potential for the future.

An aspect in the implementation of verifiable credentials in the Hyperledger Aries stack relies on AnonCreds which have something called selective disclosure, that allows the holder of the credential to only share a selection of the claims issued in a verifiable credential, and along with zero knowledge proof. AnonCreds in the Aries tech stack allows it to (Hyperledger Foundation, 2022):

- Avoidance of identifiers: No correlatable identifiers are required in presenting data to a verifier. Correlatable identifiers may be applied in a use case specific manner.
- Verifier assurances: Credentials are bound to the holder, so verifiers know that credentials presented together were all issued to the holder providing the presentation.
- Minimal data sharing: Data to be shared by a holder to a verifier is minimized using selective disclosure and ZKP predicates.

AnonCreds is a ledger-agnostic client-agnostic verifiable credential model with a formal open specification which allows it to be adopted by everyone needing a verifiable credential model. As it implements the whole layer 3 verifiable credential in the "Trust Triangle" of the ToIP model, which we are going to discuss later. Figure 2 shows how the Hyperledger technologies connect with each other.

Another element in the stack is the Ursa cryptographic library also part of the Linux Foundation projects but as the date of this document it was set to an "end of life" state this does not mean that it cannot be used, but is not actively maintained anymore, this library is still being used as part

of the cryptographic core of the Aries architecture allowing the generation of asymmetric keys and ZKP validations.

Other piece of technology we are going to talk about in this chapter is Indy another Linux Foundation project, in this case Indy provides tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers, Indy was the original project from the Linux Foundation to achieve digital identities until they started to modularize items from it, for example the Indy agents were replaced by the Aries agents creating the Hyperledger Aries which is blockchain-agnostic and removing the agent implementation from Indy and putting in into this new modular project, Aries. Indy have the following key characteristics (Hyperledger Foundation, 2022):

1. Distributed ledger purpose-built for decentralized identity
2. Correlation-resistant by design
3. DIDs (Decentralized Identifiers) that are globally unique and resolvable (via a ledger) without requiring any centralized resolution authority
4. Pairwise Identifiers create secure, 1:1 relationships between any two entities
5. Verifiable Credentials in an interoperable format for exchange of digital identity attributes and relationships, currently in the standardization pipeline at the W3C.
6. Zero Knowledge Proofs which prove that some or all of the data in a set of Claims is true without revealing any additional information, including the identity of the Prover

The last project of the Linux Foundation in this tech stack is Aries, it "is infrastructure for blockchain-rooted, peer-to-peer interactions. It includes a shared cryptographic storage for blockchain clients as well as a communications protocol for allowing off-ledger interactions between those clients" (Hyperledger Foundation, 2022)

Aries is the one who holds the rest of the elements together, it is like the structure where the other blocks are attached to it. "Aries provides a shared, reusable, interoperable tool kit designed for initiatives and solutions focused on creating, transmitting, and storing verifiable digital credentials. It is infrastructure for blockchain-rooted, peer-to-peer interactions. This

project consumes the cryptographic support provided by Hyperledger Ursa, to provide secure secret management and decentralized key management functionality." (Hyperledger Foundation, 2022). Some key characteristics of Aries are:

1. A blockchain interface layer (known as a resolver) for creating, signing, and reading blockchain transactions.

2. A cryptographic storage element that can be used for secure storage of cryptographic secrets, verifiable credentials, and other information used to build clients for exchanging (issuing, proving) verifiable credentials.

3. An encrypted, peer-to-peer messaging system (called DIDComm) based on Decentralized Identifiers (DIDs) supporting off-ledger interaction between those clients using multiple transport protocols.

4. Support for exchanging (issuing and proving) verifiable credentials in multiple formats, including an implementation of ZKP-capable verifiable credentials using the ZKP primitives found in Ursa.

5. A series of higher-level protocols and a subset of those protocols versioned "Aries Interop Profiles" to enable the independent implementation and deployment of interoperable Aries agents.

6. A set of production-ready (and several proof of concept) Aries framework implementations enabling different use cases and deployments. The frameworks are dependency in use case specific implementations of Aries agents, such as a mobile wallet, an enterprise verifiable credential issuer/verifier, etc.

7. An agent test harness to enable continuous interoperability testing of agents and agent frameworks.

3 Theoretical Framework

The rapid advancement of internet technologies has created an imperative for robust, secure, and user-centric systems to establish trust over internet protocols. This study aims to develop a comprehensive guide for implementing Trust Over Internet Protocols, specifically tailored to the various roles an entity may need to assume within this framework. Our objective is to demystify and facilitate the application of existing Trust Over Internet systems, providing actionable guidance for users to effectively employ these technologies.

Situated at the intersection between blockchain and self-sovereign identity—both of which address the topic of verifiable credentials—this research contributes to two major fields of study. Given the misconceptions surrounding blockchain, primarily due to its association with cryptocurrencies, there is a pressing need to decouple blockchain from this narrow application and explore its broader capabilities. This theoretical framework serves to provide the intellectual scaffolding for such an endeavor, integrating key concepts like Trust Over Internet, Trust Over IP, Self-Sovereign Identity, blockchain, digital wallets, and digital identity.

Understanding the theoretical principles behind these technologies is crucial, not only for academic rigor but also for the practical application of the guide. By grounding this study in a comprehensive theoretical framework, we aim to offer a nuanced understanding that goes beyond the surface-level associations commonly made about blockchain technology. This will enable users, researchers, and stakeholders to approach the practical applications of Trust Over Internet Protocols with a well-rounded perspective, informed by established theories and models.

To fully grasp the intricacies of this research, it is essential to define key terms and concepts that form the basis of our inquiry. This section elucidates terminology such as 'Trust Over the Internet,' 'Trust Over IP,' 'Self-Sovereign Identity,' and 'Blockchain,' among others. These definitions will not only provide clarity but will also establish a shared language for discussing the complex issues surrounding digital trust and identity. By grounding these terms in a well-defined context, we aim to facilitate a more nuanced understanding of the theoretical underpinnings driving this study.

3.1 Trust Over Internet

Trust Over the Internet is a board concept that refers to the intricate web of trust relationships established among various entities over the internet.

This term encompasses a wide range of technologies, protocols, and methods used to secure and authenticate digital interactions. It also covers the user's subjective perception of trust, which is shaped by factors like reliability, security, and privacy features of online platforms and services. The concept serves as an umbrella term under which various models and approaches, including Trust Over IP, are developed to address specific challenges in online trust.

3.2 Trust Over IP

Trust Over IP (ToIP) is an independent project hosted by the Linux Foundation that aims to provide a robust, common standard and complete architecture for internet-scale digital trust. It combines both cryptographic trust and at the machine layer and and human trust at the business, legal and social layers. the ToIP-enabled internet is a digital trust ecosystem of digital trust ecosystems, where the interconnections between each digital trust ecosystem are facilitate through the ToIP stack.

3.3 Self-Sovereign Identity (SSI)

Self-Sovereign Identity is a user-centric approach to identity management that allows individuals to own, control and manage their digital identities without relying on centralized authorities. It is a decentralized identity model that enables users to securely store their identity data on their personal devices, such as smartphones, and selectively disclose it to third parties. SSI is based on the concept of verifiable credentials, which are cryptographically signed credentials that can be verified without relying on a centralized authority.

3.4 Blockchain

Blockchain is a decentralized ledger technology that fundamentally transforms how data is stored, authenticated, and exchanged. Unlike traditional centralized databases, which are managed by a single entity, a blockchain is maintained by a distributed network of nodes. Each block in the chain contains a list of transactions, secured using cryptographic algorithms, and is immutable once added. This creates a transparent, secure, and tamper-proof record accessible to all parties. In the context of this research blockchain serves as a critical technological foundation for implementing both Trust Over IP and Self-Sovereign Identity. It offers a robust architecture for creating and maintaining trust over Internet, contributing to the study's overar-

ching aim of facilitating secure, interoperable, and user-centric digital trust systems.

3.5 Verifiable Credentials

Verifiable Credentials are digital statements made by an issuer about a subject, which can be independently verified by a third party. In essence, they are the digital counterparts of physical credentials, such as passports, driver's licenses, or academic degrees. These credentials are cryptographically secured, often utilizing blockchain technology or other decentralized systems to ensure their authenticity and integrity. Within this research framework, Verifiable Credentials play a significant role in establishing digital trust, particularly in conjunction with Self-Sovereign Identity and Trust Over IP models. They serve as the building blocks for secure, transparent, and user-controlled identity verification processes, thereby contributing to the overarching goal of achieving robust and interoperable digital trust systems.

3.6 Digital Wallets

Digital Wallets refer to software applications or hardware devices designed to securely store and manage an individual's digital assets, including but not limited to digital identity, verifiable credentials and even cryptocurrencies. These wallets enable users to control their own data, offering a user-centric approach to digital assets management. They often employ robust encryption methods to ensure the security and privacy of the stored information. Within the context of this study, Digital Wallets are instrumental in facilitating Self-Sovereign Identity and Trust Over IP frameworks. They act as the interface through which users interact with digital trust systems, storing and providing access to verifiable credentials and other essential digital assets.

3.7 Digital Identity

Digital Identity refers to the digital representation of an entity, be it an individual, organization or device, in an online environment. It consists of a set of attributes and credentials that authenticate and differentiate one entity from another. These attributes can range from basic information like usernames and passwords to more complex forms of data like biometric scans and verifiable credentials. In the scope of this research, Digital Identity serves as a foundational element linking together the concepts of Trust OVer

Internet, Trust Over IP, and Self-Sovereign Identity. It is the core asset that these frameworks aim to protect, manage and verify, thereby playing a pivotal role in establishing and maintaining digital trust.

4 Methodology

The methodology for this project is designed to provide a systematic and comprehensive approach to achieving the main and specific objectives. It involves a combination of research, software development, interaction mapping, and guide creation. Each step of the methodology is designed to build upon the previous one, ensuring a cohesive and thorough exploration and implementation of Trust Over Internet protocols.

4.1 Literature review and research

This step involves a thorough review of existing literature and research on Trust Over Internet protocols. It could includes academic papers, technical documentation, open source code, development guides, implementation guides and other relevant resources. The goal is to gain a deep understanding of the current state of the field, identify gaps in knowledge, and determine best practices for implementing Trust Over Internet protocols. To fulfil this step, we must:

- Identify relevant sources of information.
- Review and summarize key findings from each source.
- Identify gaps in the current body of knowledge
- Determine best practices for implementing Trust Over Internet protocols.

4.2 Development of agents

This step involves the design and implementation of software agents that can perform the roles of Issuer and Verifier in a Trust Over IP system. This will require a strong understanding of software development and the specific requirements of Trust Over Internet protocols. To fulfil this step, we must:

- Define the functional requirements for the Issuer and Verifier agents.
- Design the software architecture for each agent.
- Implement the agents using appropriate programming languages and technologies.
- Test the agents to ensure they function as expected.

4.3 Implementing the wallet as a holder

This step involves implementing a wallet to act as a Holder that interacts with the Issuer and Verifier agents using interoperable objects. This will involve more software development and integration work. To fulfil this step, we must:

- Define the functional requirements for the Holder wallet.
- Design the software architecture for the wallet.
- Implement the wallet using appropriate programming languages and technologies.
- Integrate the wallet with the Issuer and Verifier agents.
- Test the wallet and its interactions with the agents.

4.4 Interaction mapping

This step involves mapping out the extent and method of interaction between each component of the trust triangle. This will involve creating diagrams and documentation that clearly illustrate how the Issuer, Verifier, and Holder interact within the system. To fulfil this step, we must:

- Identify interactions between the Issuer, Verifier, and Holder.
- Create diagrams that visually represent these interactions.
- Document the purpose and outcome of each interaction.

4.5 Guide creation

This step involves creating a comprehensive guide based on the research and development work. The guide should explain how to implement Trust Over Internet protocols and be tailored to the specific needs and roles an entity may need to assume within the Trust over IP framework. To fulfil this step, we must:

- Outline the structure and content of the guide.
- Write the guide, incorporating findings from the research and development of the work.
- Review and revise the guide to ensure it is clear and comprehensive.

4.6 Schedule

Activity	Start Date	End Date
Identify relevant sources of information	25-09-2023	15-10-2023
Review and summarize findings	10-10-2023	25-10-2023
Identify gaps in the knowledge	16-10-2023	31-10-2023
Determine the practices to implement Trust Over Internet protocols	20-10-2023	10-11-2023
Define the functional requirements for the agents	01-11-2023	20-11-2023
Design the software architecture for each agent	05-11-2023	25-11-2023
Design the agents	15-11-2023	10-12-2023
Implement the agents	20-11-2023	15-12-2023
Test the agents	01-12-2023	20-12-2023
Integrate a wallet with the agents	16-12-2023	31-12-2023
Identify interactions between the agents	10-11-2023	31-12-2023
Create interaction diagrams	05-12-2023	25-12-2023
Outline the structure and content of the guide	01-01-2024	15-01-2024
Create the guide	10-01-2024	25-01-2024
Test the components	16-01-2024	31-01-2024
Make revisions based on testing results	20-01-2024	05-02-2024

Table 1: Adjusted Project Schedule with Overlapping Tasks, Lasting Approximately 4 Months from September 25, 2023

4.7 Budget

The budget is taking into account the cost of the hardware, services and human resources required to complete the project. The hardware includes a laptop, a home server and a smartphone. The services includes the internet services, cloud services, and other services required to complete the project. The human resources include the student, the advisor and the co-advisor.

Item	Cost	Amount
Laptop	$10,500,000	1
Home Server	$25,000,000	1
Smartphone	$6,500,000	1
Total		$42,000,000

Table 2: Hardware Budget, this table contains the cost of the hardware required to complete the project. The hardware includes a laptop, a home server and a smartphone.

Person	Hourly rate	Hours	Total
Student	$6,500	640	4,160,000
Co-Advisor	$35,000	48	1,680,000
Advisor	$35,500	12	420,000
Total			6,260,000

Table 3: Human Resources Budget, this table contains the cost of the human resources required to complete the project. The human resources include the student, the advisor and the co-advisor.

Service	Monthly rate	Months	Total
Internet	$190,000	4	760,000
Cloud Services	$0	0	0
Other Services	$0	0	0
Total			760,000

Table 4: Services Budget, this table contains the cost of the services required to complete the project. The services include internet, cloud services and other services.

5 Expected Results

Upon completion of this research, we anticipate the following outcomes:

5.1 Comprehensive Guide

A detailed, user-friendly guide aimed at simplifying the process of implementing Trust Over Internet Protocols (ToIP). Tailored to various roles within the ToIP framework, this guide is expected to be instrumental in accelerating the integration and adoption of ToIP. By demystifying complex processes, it empowers users to harness the full potential of these systems.

5.2 Development of Agents

The creation of distinct agents for both the Issuer and the Verifier within the trust triangle. This development aims to provide a lucid understanding of their specific roles, offering users enhanced control and flexibility in tailoring ToIP protocols to their unique requirements.

5.3 Wallet Integration

The use of a wallet as a holder will streamline interactions with the Issuer and Verifier agents through interoperable objects. This is anticipated to simplify the overall creation process, thus enhancing the accessibility and intuitiveness of ToIP implementations.

5.4 Interaction Mapping

A thorough mapping of the extent and methodology of interactions between the trust triangle components. This deep dive is predicted to enrich our comprehension of the individual and collective roles in trust formation, paving the way for the development of more robust and effective ToIP protocols.

5.5 Documentation

A systematic documentation of the ToIP protocol implementation across the trust triangle. This roadmap aims to clarify the implementation process for users. By providing a clear, step-by-step guide, we expect to foster an environment where ToIP can be widely and confidently adopted, irrespective of a user's technical acumen.

References

[1] Tara Seals. "Telegram Fraudsters Ramp Up Forged COVID-19 Vaccine Card Sales". In: *Threatpost* (2021). URL: https://threatpost.com/telegram-forged-covid-19-vaccine-cards/166093/.

[2] El Tiempo. "Capturan red que falsificaba diplomas y certificaciones desde Bogotá". In: *El Tiempo* (2022). URL: https://www.eltiempo.com/bogota/cae-red-que-falsificaba-diplomas-y-certificaciones-en-bogota-692098.

[3] Actionsa. "Mabuyanes Fraudulent Degree Highlights the Extent of Qualification Scams Among Senior Politicians". In: *Actionsa* (2023). URL: https://www.actionsa.org.za/mabuyanes-fraudulent-degree-highlights-the-extent-of-qualification-scams-among-senior-politicians/.

[4] Camilo Andres and Jaimes Osorio. "Alto funcionario del MinSalud tendría dos títulos falsos: universidades lo dejan en evidencia". In: *RCN Radio* (2023). URL: https://www.rcnradio.com/colombia/alto-funcionario-del-minsalud-tendria-dos-titulos-falsos-universidades-lo-dejan-en.

[5] KBC Group. "Howest and KBC will be launching Europe's first digital student card in the coming academic year". In: *KBC Group* (2023). URL: https://newsroom.kbc.com/howest-and-kbc-will-be-launching-europes-first-digital-student-card-in-the-coming-academic-year.

[6] Felicia Martinez. "COVID-19 Fraudsters Charged in Utah for Allegedly Manufacturing, Selling and Distributing at least 120,000 Counterfeit COVID-19 Vaccination Cards". In: *United States Attorney's Office* (2023). URL: https://www.justice.gov/usao-ut/pr/covid-19-fraudsters-charged-utah-allegedly-manufacturing-selling-and-distributing-least.

[7] Terrence McCoy and Marina Dias. "Bolsonaro's vaccine status falsified before he entered U.S., police say". In: *The Washington Post* (2023). URL: https://www.washingtonpost.com/world/2023/05/03/bolsonaro-vaccination-covid-police-raid/.

[8] Leigh Lane Peine. "The fraud problem: how Educational Credential Evaluators is helping to stop forged documents". In: *University Affairs* (2023). URL: https://www.universityaffairs.ca/magazine/

sponsored-content/the-fraud-problem-how-educational-credential-evaluators-is-helping-to-stop-forged-documents/.

[9] Melanie Porter. "Utah man charged for making and selling thousands of fake COVID-19 vaccine cards". In: *Fox13now* (2023). URL: https://www.fox13now.com/news/crime/utah-man-charged-for-making-and-selling-thousands-of-fake-covid-19-vaccine-cards.

[10] Telemundo. "Hay más de 7,600 personas con títulos falsos de enfermería": desarticulan en Florida una red criminal que vendía credenciales". In: *Telemundo* (2023). URL: https://www.telemundo.com/noticias/noticias-telemundo/salud/hay-mas-de-7600-personas-con-titulos-falsos-de-enfermeria-desarticulan-rcna67555.

[11] Emma Whitford and Janet Novack. "There is an old, but now fast growing degree mill industry doing an estimated 7 billion a year worldwide in fraudulent diplomas and transcripts." In: *Forbes* (2023). URL: https://www.forbes.com/sites/emmawhitford/2023/02/21/how-thousands-of-nurses-got-licensed-with-fake-degrees/?sh=3adcdc8e5c6d.

[12] Ceylan Yeginsu. "What Are the Roadblocks to a 'Vaccine Passport'?" In: *The New York Times* (2023). URL: https://www.fox13now.com/news/crime/utah-man-charged-for-making-and-selling-thousands-of-fake-covid-19-vaccine-cards.