



**Developing a Digital Trust Framework between
Government and Private Sector in the Financial Sector**

تطوير إطار الثقة الرقمية بين الجهات الحكومية والخاصة في القطاع المالي

by

SUAAD SALEM YOUSEF AL SHAMSI

**A thesis submitted in partial fulfilment
of the requirements for the degree of
DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE**

at

The British University in Dubai

July 2023



**Developing a Digital Trust Framework between Government and Private
Sector in the Financial Sector**

تطوير إطار الثقة الرقمية بين الجهات الحكومية والخاصة في القطاع المالي

by

SUAAD SALEM YOUSEF AL SHAMSI

A thesis submitted to the Faculty of Engineering and Informatics

in partial fulfilment of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN COMPUTER SCIENCE

at

The British University in Dubai

July 2023

Thesis Supervisor

Professor Sherief Abdallah

Approved for award:

Name

Designation

Name

Designation

Name

Designation

Name

Designation

Date: _____

DECLARATION

I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the contents of this dissertation for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai may make a digital copy available in the institutional repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application.



Signature of the student

COPYRIGHT AND INFORMATION TO USERS

The author whose copyright is declared on the title page of the work has granted to the British University in Dubai the right to lend his/her research work to users of its library and as an open source and to make partial or single copies for educational and research use.

The author has also granted permission to the University to keep or make a digital copy for similar use and for the purpose of preservation of the work digitally.

Multiple copying of this work for scholarly purposes may be granted by either the author, the Registrar or the Dean only.

Copying for financial gain shall only be allowed with the author's express permission. Any use of this work in whole or in part shall respect the moral rights of the author to be acknowledged and to reflect in good faith and without detriment the meaning of the content, and the original authorship.

ABSTRACT

COVID-19 accelerated the transformation to a digital society. It created a necessity for an ecosystem trusted by all parties to avail services, which requires identity to be verified and information to be exchanged. The trusted digital identity of individuals and organizations is a fundamental block in such an ecosystem. Services in critical domains such as finance, health and travel heavily rely on identity verification. This process is known as “Know Your Customer” (KYC). Despite the need for a digital service offering, regulators mandate the physical verification of individuals and their documents. This process is usually lengthy, inefficient, costly and inconvenient to the customer. It mandates the customer to visit each service provider at least once to conduct customer identification and verification prior to availing the service or obtaining digital credentials. Regulators requirements need to be identified and addressed in a digital mean which is accepted and trusted by all involved parties, service providers, customers, and document issuers, in order to transform KYC process to a digital process which is trusted and efficient. The physical identity of individuals must be mapped to a digital identity that can be trusted and verified by all service providers. The physical documents of individuals representing their identity or any claim they make about themselves, or their ownership must be transformed into trusted and verifiable digital credentials. This would enable an end-to-end digital service offering without the need for customers to physically visit service providers for customer identification and verification. This paper develop a Digital Trust Framework between the government and private sector in the United Arab Emirates (UAE) that aims to enable service providers to offer an end to end digital service through the development of a unified trusted digital identity and credentials that eliminate the need for the initial physical identification and verification, and improve the

continuous KYC monitoring of the customer therefore improving the efficiency and the user experience, reducing the cost, and increasing the transparency of the KYC processes. The framework uses decentralized identity and verifiable credentials (VCs) as a layer on top of blockchain technology to address the challenges faced in KYC processes while adopting Privacy-by-Design principles. Hence, this research paper follows a design science research methodology (DSRM) as research method to develop the framework. The focus is on the financial sector in the UAE. The DSRM research method integrates existing theoretical knowledge and insights from industry practitioners obtained through semi-structured expert interviews. The proposed framework to improve the KYC process was successfully implemented as prototype system, and it was evaluated through a case study evaluation with real users to verify its feasibility. The results of the demonstration were used to evaluate the prototype system through different performance metrics. The results of the evaluation showed satisfactory performance across various metrics indicating the system stability and reliability.

الخلاصة

لقد سرعت جائحة كوفيد-19 عجلت التحول إلى مجتمع رقمي، حيث خلقت الحاجة إلى وجود منظومة رقمية تمكن من توفير خدمات رقمية للمجتمع، يثق فيها جميع الأطراف. الحصول على أي خدمة يتطلب التحقق من هوية الشخص وتوفير مستندات ثبوتية مختلفة، وبالأخص الخدمات التي يتم توفيرها من القطاعات الحيوية مثل الخدمات المالية والصحية والسفر، حيث تفرض الجهات التنظيمية على مزودي الخدمات التحقق الفعلي من هوية الأفراد ومستنداتهم قبل توفير أي خدمة للمتعامل وتُعرف هذه العملية أيضاً بـ "تعرف على عميلك" (KYC)، وفي الغالب تستغرق هذه العملية وقت كبير وتكون غير فعالة ومكلفة ومجهدة للمتعامل، حيث تفرض على المتعامل زيارة كل مزود خدمة مرة واحدة على الأقل لإجراء عملية التحقق من هوية المتعامل قبل الاستفادة من الخدمة أو الحصول على مستندات رقمية. لتحويل عملية "تعرف على عميلك" إلى عملية رقمية موثوقة وفعالة، يجب تحديد متطلبات الجهات التنظيمية ومعالجتها بطريقة رقمية مقبولة وموثوقة من قبل جميع الأطراف المعنية والتي تشمل مقدمي الخدمات والمتعاملين ومصدري المستندات، كما ويجب أن تُسقط الهوية الحقيقية للأفراد على هوية رقمية يمكن لجميع مزودي الخدمات الوثوق بها والتحقق منها، بالإضافة إلى ذلك يجب تحويل المستندات الفعلية للأفراد والتي تمثل هوية الفرد أو ما يدعي من صفات أو ممتلكات إلى بيانات رقمية موثوقة يمكن الثقة بها والتحقق منها، حيث سيمكّن هذا من تقديم خدمة رقمية شاملة دون الحاجة إلى أن يزور المتعامل مزود الخدمة لتحقيق من هويته. تدرس هذه الرسالة إمكانية تطوير إطار الثقة الرقمية بين الجهات الحكومية والخاصة في دولة الإمارات العربية المتحدة، ويهدف الإطار إلى تمكين مزودي الخدمات من تقديم خدمة رقمية متكاملة من خلال تطوير هوية رقمية موثوقة وموحدة وبيانات رقمية موثوقة تلغي الحاجة إلى التحقق الفعلي الأولي، وتحسن من إجراءات التحقق المستمر لعملية "تعرف على عميلك" وبالتالي تحسن الكفاءة وتجربة المستخدم، وتقلل التكلفة، وتزيد شفافية عمليات تعرف على عميلك، ويستخدم الإطار الهوية اللامركزية وبيانات رقمية موثوقة (VCS) المبنية على تقنية البلوكتشين لمعالجة التحديات التي تواجهها عمليات "تعرف على عميلك" مع الأخذ بعين الاعتبار مبادئ الخصوصية في التصميم. تتبع الدراسة في هذه الرسالة منهجية بحث علم التصميم (DSRM) لتطوير الإطار، وتركز على القطاع المالي في دولة الإمارات العربية المتحدة، تدمج منهجية بحث DSRM المعرفة النظرية الحالية ووجهات نظر وخبرات المختصين في هذا المجال والتي تم الحصول عليها من خلال المقابلات مع الخبراء، وتم تطوير الإطار المقترح لتحسين عملية "تعرف على عميلك" بنجاح كنظام نموذجي، كما وتم تقييمه من خلال دراسة حالة مع مستخدمين حقيقيين للتحقق من جدواه، واستخدمت نتائج الدراسة

لتقييم النظام النموذجي من خلال مقاييس أداء مختلفة، وأظهرت نتائج التقييم أداءً مرضياً عبر مقاييس مختلفة مما يشير إلى استقرار النظام وموثوقيته.

ACKNOWLEDGEMENTS

First and foremost, I express my deepest gratitude to Allah the Almighty for His abundant blessings and guidance throughout this research journey.

I also extend my sincere appreciation and respect to my esteemed research supervisor, Prof. Sherief Abdallah. His unwavering support, invaluable guidance and comprehensive knowledge have been instrumental in shaping the outcome of this thesis. His visionary insights and unwavering dedication have inspired me and enriched my academic and personal growth.

I am immensely grateful to the participants who generously devoted their time and shared their valuable feedback, enabling the development of a comprehensive understanding of the subject matter. Their contributions have greatly contributed to creating a happier and safer digital environment.

I also express my heartfelt gratitude to my beloved family, especially my mother and sisters, for their unwavering support throughout this journey. Their unconditional love, encouragement and belief in my abilities have been a constant source of strength and motivation. I am truly indebted to them for their unwavering faith and guidance.

I also thank my aunt and colleagues for their continuous support, follow-up and motivation. Their presence and encouragement have played a significant role in keeping me focused and inspired.

In conclusion, I am profoundly grateful to everyone who has contributed to the successful completion of this thesis. Your support, guidance, and encouragement have been invaluable, and I am sincerely thankful for your presence in my life.

TABLE OF CONTENTS

Chapter 1: Introduction.....	1
1.1 Overview	1
1.2 Problem Statement	5
1.3 Research Questions	6
1.4 Research Aim	7
1.5 Research Objectives	7
1.6 Scope of this Thesis.....	8
1.7 Thesis Outlines	9
Chapter 2: Background	11
2.1 Introduction	11
2.2 What is “Know Your Customer”?.....	12
2.3 Digital Identity	16
2.4 Blockchain.....	29
2.5 Privacy.....	36
Chapter 3: Literature Review	38
3.1 Introduction	38
3.2 Using Blockchain to Improve Financial Sector KYC	38
3.3 Using Blockchain in Health Sector	45
3.4 Using Blockchain in Digital Identity Management.....	49
3.5 Summary and Research Gaps.....	57

Chapter 4: Research Design and Methodology	59
4.1 Introduction	59
4.2 Conceptual Design Framework	59
4.3 Selection of Research Approach	61
4.3.1 Design Science Research	63
4.3.2 Design Science Research Methodology	68
4.4 Research Design	78
4.4.1 Conceptual Phase	81
4.4.2 Design Phase	86
4.4.3 Implementation Phase	93
4.4.4 Evaluation Phase	95
4.4.5 Communication Phase	103
4.5 Data Sampling	103
4.6 Data Collection	105
4.7 The Role of the Researcher	112
4.8 Ethical Consideration	112
4.9 Trustworthiness	114
4.10 Limitations and Delimitation	117
4.11 Summary	118
Chapter 5: Design Objectives	119
5.1 Introduction	119
5.2 Design Objectives Definition	119

5.3 Evaluation of the Design Objectives	132
5.3.1 Evaluation Summary	132
5.3.2 Experts' Feedback	133
5.4 Summary	141
Chapter 6: Digital Trust Framework	142
6.1 Introduction	142
6.2 Solution Architecture	146
6.3 Key Processes.....	157
6.3.1 Issuance of Verifiable Credentials	158
6.3.2 Revocation of Verifiable Credentials	163
6.3.3 Sharing Verifiable Credentials	166
6.3.4 Verification of Verifiable Credentials.....	170
6.3.5 KYC Process	172
6.4 Digital Wallet Prototype.....	183
6.5 Evaluation.....	189
6.5.1 Experts' Feedback	189
6.5.2 End User Concept Testing.....	199
6.6 Design Principles.....	207
6.7 Summary and Conclusion	213
Chapter 7: Implementation of Prototype System.....	214
7.1 Introduction	214
7.2 Prototyping	214

7.3 Prototype Functionalities.....	215
7.4 High Level Design	216
7.5 Technology Stack	219
7.6 Main APIs	221
7.6.1 Authentication	221
7.6.2 Create DID Document.....	223
7.6.3 Request Credential	225
7.6.4 Create Proof of Issuance Document.....	226
7.6.5 Receive Presentation Request from Service Provider.....	228
7.6.6 Share Presentation to Service Provider	230
7.6.7 Credential Verification API	231
7.7 Chapter Summary.....	232
Chapter 8: Prototype Demonstration and Evaluation.....	234
8.1 Introduction	234
8.2 Evaluation Settings.....	234
8.2.1 Case Study Selection.....	235
8.2.2 Sampling.....	235
8.2.3 User and Scenario Preparations.....	237
8.2.4 Service Providers on Boarding.....	238
8.3 KYC Process Efficiency.....	241
8.4 Overall System Efficiency	241
8.5 Chapter Summary.....	252

Chapter 9: Conclusions and Recommendations.....	254
9.1 Introduction	254
9.2 Research Aim and Objectives	254
9.2.1 Objective One.....	258
9.2.2 Objective Two	259
9.2.3 Objective Three	261
9.2.4 Objective Four.....	262
9.2.5 Objective Five	263
9.3 Conclusion on Research Problem	264
9.4 Implications and Contributions	266
9.5 Recommendations for Future Work	268
References	270
Appendices	297
Appendix A: Expert’s Consent Forms	297
Appendix B : Open-ended Interview Questions	300
Appendix B.1: Problem Identification	300
Appendix B.2: Solution Evaluation	302
Appendix C : Concept Testing Survey Questions.....	304

LIST OF TABLES

Table 1	Comparsaion between natual, social and design sciences	63
Table 2:	Artifact Types	66
Table 3:	DSR Evaluation Strategy Selection Framework.....	73
Table 4:	DSR Evaluation Method Selection Framework.....	75
Table 5:	Evaluation criteria for DSR artifacts.....	76
Table 6:	DSR evaluation activities and evaluation criteria	77
Table 7:	Participating experts’ details in evaluating the problem and the objectives	85
Table 8:	Participating experts’ details in evaluating the IT artifact	89
Table 9:	Concept testing participants’ demographics	92
Table 10:	Forms of evaluation	96
Table 11:	Evaluation Method.....	99
Table 13:	Data collection method used in this research paper.....	110
Table 13:	Design Objectives mapping to stakeholder needs.....	120
Table 14:	Technology Stack of the proof-of- principle.....	220
Table 15:	The structure of the JWT token issued.....	222
Table 16:	Required Sample Size	236
Table 17:	Case study participants’ demographics.....	237
Table 18:	Performance Metrics Input.....	242
Table 19:	Performance Metrics - Window Input	243
Table 20:	Performance Metrics Expected Results	243

LIST OF FIGURES

Figure 1: KYC process of a customer availing services from three banks	13
Figure 2: Correspondence between entities, identities and characteristics	17
Figure 3: Simple IdM actors' interactions.....	20
Figure 4: The roles and information flows of VCs	27
Figure 5: Conceptual Design framework	60
Figure 6: The ISDSR conceptual framework.....	65
Figure 7: Design Cycle Process	67
Figure 8: DSRM Process.....	70
Figure 9: Adaption of DSRM for research design	78
Figure 10: Research Design	80
Figure 11: Prototype implementation process model.....	93
Figure 13: Digital Trust Framework architecture	148
Figure 14: Decentralized identity of actors	150
Figure 15: Example of Verifiable Credential structure.....	151
Figure 16: Example of Verifiable Presentation.....	152
Figure 17: Transaction and key flow to increase trust	155
Figure 18: Correlating between on-chain and off-chain trust	157
Figure 19: Retrieving documents (VCs) from the Issuer (Sequence diagram – Part 1).....	161
Figure 20: Retrieving documents (VCs) from the Issuer – (Sequence diagram – Part 2).....	162
Figure 21: Business revoking a verifiable credential	164
Figure 22: Data revoking a verifiable credential.....	165
Figure 23: Sharing Verifiable Presentations – (Sequence diagram – Part 1).....	168
Figure 24: Sharing Verifiable Presentations – (Sequence diagram – Part 2).....	169

Figure 25: Various digital signatures on the Verifiable Presentation	170
Figure 26: Verification of the Verifiable Presentation.....	171
Figure 27: Verification of the verifiable credential.....	172
Figure 28: KYC process completely new onboarding – (Sequence diagram – Part 1).....	177
Figure 29: KYC process completely new onboarding – (Sequence diagram – Part 2).....	178
Figure 30: KYC process completely new onboarding – (Sequence diagram – Part 3).....	179
Figure 31: KYC process completely new onboarding – (Sequence diagram – Part 4).....	180
Figure 32: Login screen.....	186
Figure 33: Home screen	186
Figure 34: User consent to share successfully screen	186
Figure 35: Documents list screen	187
Figure 36: Document view screen front side screen	187
Figure 37: Document view screen back side screen	187
Figure 38: Adding document screen	188
Figure 39: Selecting documents from the Issuer screen.....	188
Figure 40: Documents added successfully screen.....	188
Figure 41: Concept testing results – Impression	201
Figure 42: Concept testing results – Uniqueness	201
Figure 43: Concept testing results – Appeal	202
Figure 44: Concept testing results – Likability	202
Figure 45: Concept testing results – Believability	203
Figure 46: Concept testing results – Relevance	203
Figure 47: Concept testing results – Demand	204
Figure 48: Concept testing results – Security.....	206

Figure 48: Logical View of the Digital Trust Framework	217
Figure 49: Digital Trust Framework Functional Decoposition	218
Figure 50: Service Orchestration.....	219
Figure 51: Citizen Authentication Flow	222
Figure 52: Partner Authentication Sequence Diagram.....	223
Figure 53: Create DID Document - Sample Request/Response	224
Figure 54: Request Credential - Sample Request/Response	225
Figure 55: Create Proof of Issuance Document - Sample Request	226
Figure 56: Create Proof of Issuance Document - Sample Response.....	227
Figure 57: Send Raw Transaction – Sample Request/Response.....	228
Figure 58: 7.4.5 Receive Presentation Request – Sample Request/Response	229
Figure 59: 7.4.6 Share Presentation in Service Provider – Sample Request/Response	230
Figure 60: Credential Verification API – Sample Request/Response.....	231
Figure 61: Service Provider Stepwise Verification	232
Figure 62: Case Study Financial Institute A – Initiation.....	238
Figure 63: Case Study Financial Institute A – Completion	239
Figure 64: Case Study Financial Institute B – Initiation.....	240
Figure 65: Case Study Financial Institute B – Completion.....	240
Figure 66: Create DID API Throughput and Response Time	246
Figure 67: Create DID API Resource Utilization	246
Figure 68: Send Transaction API Throughput and Response Time.....	247
Figure 69: Send Transaction API Resource Utilization	247
Figure 70: Create POI API Throughput and Response Time.....	249
Figure 71: Create POI API Resource Utilization	249

Figure 72: Combined Blockchain APIs Resource Utilization 250

LIST OF ABBREVIATIONS

Abbreviation	Meaning
AAA	Authentication, Authorization and Accounting
AML	Anti-Money Laundering
API	Application Programming Interface
BPM	Business Process Modeling
CDD	Customer Due Diligence
CEO	Chief Executive Officer
COVID	Coronavirus disease
DID	Decentralized identifiers
DLT	Distributed Ledger Technology
DSR	Design Science Research
EMR	Electronic Medical Record
FATF	Financial Action Task Force
GCC	Gulf Cooperation Council
GDPR	The General Data Protection Regulation
IAM	Identity Access Management
IDFF	Identity Federation Framework
IPFS	Interplanetary File System
ISDSR	Information System Design Science Research
ITU	International Telecommunication Union

KYC	Know Your Customer
MFA	Multifactor Authentication
MLA	Money Laundering Act
NIST	National Institution of Standards and Technology
OIDC	OpenID Connect
PEP	Politically Exposed Person
PII	Personal Identifiable Information
PKI	Public-Key Infrastructure
SAML	Security Assertion Markup Language
SILO	Standalone identity
SIM	A subscriber identity module is a removable smart card for mobile phones
SOR	System of Record
SSI	Self-Sovereign Identity
TDRA	Telecommunications and Digital Government Regulatory Authority
TEE	Trusted Execution Environment
UAE	United Arab Emirates
URL	Uniform Resource Locator
USD	United States Dollar
UUID	Universal Unique Identifier
VC	Verifiable Credential

VP	Verifiable Presentation
WSF	Web Services Federation
ZKP	Zero-Knowledge Proof

Chapter 1: Introduction

1.1 Overview

In the traditional physical world, when customers avail services from service providers (SPs), they must provide information about their identity, which SPs verify. This process is known as “Know Your Customer” (KYC). The KYC process can be lengthy and complex depending on the services’ criticality. For example, in the financial sector, availing services to customers requires in-depth due diligence verification by financial institutions. Regulators mandate it in the financial sector to ensure market integrity. Several regulatory requirements have been introduced, such as the Financial Action Task Force on Money Laundering (FATF) recommendations, which aim to prevent money laundering and international terrorism financing, and Basel III, in response to the global financial crisis in 2008 (Arner, Barberis and Buckley, 2016). Availing a service to any suspicious user may exploit the system by opening multiple accounts and engaging in a significant volume of transactions, potentially involving money laundering activities (MLAs).

The KYC process is repeated by every SP (i.e. bank). Malhotra, Saini and Singh (2021) stated that the cost of the KYC process conducted by a single bank is estimated to be USD 60 million annually on average. However, this figure does not consider the fines that the bank has to pay due to misconduct of AML or KYC regulations (Parra-Moyano and Ross, 2017). An official in the Hong Kong Securities and Futures Commission stated that the total amount of KYC and fines a bank must pay could be USD 10 billion or more (Parra-Moyano and Ross, 2017). The traditional KYC process delays the ability to grant services to customers and makes it inconvenient for them.

Kolb *et al.* (2020) conducted a survey revealing that 89% of the surveyed customers had a negative experience with the KYC process. Customers expressed dissatisfaction with the time-consuming onboarding procedure, which involved submitting multiple documents. Notably, the KYC process encompasses the initial onboarding of new customers and involves continuous monitoring of transactions to identify suspicious customer behavior (Glaser, 2017), making the process cost-intensive, time-consuming and inconvenient for customers.

COVID-19 accelerated the need to create a digitally trusted society where services can be digitally availed to customers while ensuring that identity verification and data exchange are conducted and trusted. The word “trust” is defined in the Oxford Dictionary as “the firm belief in the truth or ability of someone or something to perform a task in a reliable matter, in a specific context”.¹ A digitally trusted society should be enabled with privacy as its core foundation.

Previous works have proposed the usage of blockchain-based SSI to improve the efficiency of the KYC process, specifically in the financial sector, due to the promising key characteristics that can be leveraged (Soltani, Nguyen and An, 2018, Dong *et al.*, 2020; Schlatt *et al.*, 2022). The decentralized nature of the blockchain enables trust between participating parties. Moreover, the underlined implementation ensures the integrity, reliability and availability of providing information that plays a significant role in identity verification. Moreover, SSI enables individuals to control their digital identity, which plays a significant role in identity provisioning and access while preserving individual privacy. Some of the key

¹ https://www.oxfordlearnersdictionaries.com/definition/english/trust_2

principles of SSI include the independent existence of the digital identity in the real world, which can be a legal person or entity, the consent of users before sharing their identity information with any third party, and the independent verification of digital identity similar to the real world. These key principles are important elements of the KYC process. Chapter 2 provides more information about the KYC process, blockchain and SSI concepts and principles.

While mapping a digital identity to its independent existence in the real world is a crucial SSI principle, previous works have not proposed mechanisms to assure the integrity and accuracy of the mapping (Soltani, Nguyen and An, 2018; Dong *et al.*, 2020; Schlatt *et al.*, 2022). The initial phase of identity and document verification remains a manual process where the customer submits all the documents online, and an employee in the back office verifies them. This approach does not prevent a person from submitting forged documents or exploiting a genuine person's identity during the initial phase (Malhotra, Saini and Singh, 2021). Moreover, Parra-Moyano and Ross (2017) proposed that this step should be manual by visiting the first bank where the user wants to avail service. While this step could ensure that the legal person is mapped to the digital person, it does not ensure the authenticity of the documents submitted. These solutions impact the user experience, so the user must either apply online by filling in forms and uploading all required documents or visit the first bank for the desired association.

Soltani, Nguyen and An (2018), Dong *et al.* (2020) and Schlatt *et al.* (2022) proposed solutions that rely on the verification conducted by the first bank. However, these solutions do not consider that the customer's information and status could change after the initial verification, such as leaving the country or revoking the authority of certain privileges

provided in the form of power of attorney. These changes could impact the first bank's verification to the extent that it could invalidate it. Thus, these critical elements must be considered to enable transacting in a digitally trusted society.

Another challenge with previous works on blockchain-based implementations is data storage. Since data stored on the blockchain cannot be deleted, implementations such as the one proposed by Parra-Moyano and Ross (2017) for storing on the blockchain are not viable. As an alternative, Soltani, Nguyen and An (2018) and Schlatt *et al.* (2022) proposed storing only hashes of the VCs on the blockchain, providing a decentralized distributed immutable ledger while the actual VCs are stored and controlled by the user. This approach provides an element of trust as SPs can independently verify the information exchanged. Moreover, enabling the user to store and manage personal data is a key principle of SSI, analogous to today's physical world, where the user manages physical cards in a physical wallet. However, there is a need to define a simple and easy mechanism for the user to retrieve a digital identity and data in case of loss.

Moreover, previous works have mainly focused on a set of banks where trust has been assumed between them (Parra-Moyano and Ross, 2017; Soltani, Nguyen and An, 2018; Dong *et al.*, 2020; Schlatt *et al.*, 2022). However, trust between financial institutions is not the preferred option as per the expert interviews highlighted by Schlatt *et al.* (2022) and the expert interviews detailed in Chapter 5. Pöhn, Grabatin and Hommel (2021) reviewed SSI and government eID implementations that demonstrated the need to establish trust between participants for the implementation to be successful. Therefore, government and private sectors must collaborate to address the current KYC challenges. Establishing trust between participants drives the need for a governance framework enabling the provisioning of trusted

digital identity, the issuance of credentials by trusted entities and the legal acceptance of digital credentials

This thesis designs and evaluates a Digital Trust Framework leveraging blockchain-based self-sovereign identity (SSI) to address these challenges. The customer's digital identity and information are modeled as verifiable credentials (VCs) that can be issued by issuing authorities and provided to SPs.

1.2 Problem Statement

Blockchain technology and self-sovereign identity (SSI) has shown potential to improve the efficiency of the KYC processes in a digital society. However, converting the initial customer identification and verification to a digital process in which the authenticity and integrity of the identity can be verified, the regulatory acceptance can be obtained and the user experience can be simplified is still a complex issue. Moreover, the ability to continuously monitor the customer eligibility efficiently presents a non-trivial challenge, which further impacts the cost of the KYC process due to the fact that it is required to be conducted periodically. Thus, the research problem that is investigated in this thesis can be summarized as follows:

Despite the recognized potential of blockchain and SSI to improve the efficiency of KYC processes, current approaches in blockchain research:

- a) do not efficiently digitize the initial customer identification and verification as well as continuous monitoring
- b) do not accurately identify the authenticity and integrity of the customer during the initial customer identification and verification

- c) do not incorporate regulatory, servicer provider, document issuer, and customer requirements for the initial customer identification and verification as well as continuous monitoring in a unified accepted framework

As a result, current approaches cannot provide a comprehensive and trusted foundation for the adoption of blockchain in regulated environment that requires a thorough KYC.

The problem described above is a significant barrier towards the adoption of blockchain in a regulated KYC environment in general and in UAE in specific. Therefore, development of a framework that addresses the challenges of initial identification and verification and address the regulatory requirements, can significantly improve the efficiency of the KYC processes for critical domains.

1.3 Research Questions

Based on the research problem, a number of key research questions have been identified below:

- **RQ1:** What are the current requirements of the KYC process and its shortcomings?
How can blockchain in general help to overcome the challenges and provide new capabilities to enable the implementation of efficient and automated KYC process?
- **RQ2:** What are the current status of using blockchain-based SSI implementation in KYC? What are the challenges facing the adoption of blockchain-based SSI implementation in KYC processes?
- **RQ3:** Can a framework be designed and implemented to overcome the current challenges of the adoption of blockchain-based SSI implementation in KYC processes?
 - a) How can the identity of the customer be established?

- b) How can the authenticity and integrity of the identity be verified?
- c) What are the technical features that should be developed to instill trust?
- d) What are the Privacy-by-Design principles that the framework should comply with?
- e) How can the proposed framework be validated and evaluated?
- **RQ4:** How well the proposed framework meets the participants' requirements including individuals, the government as a document issuer, and the private sector as service providers in general and the regulators in specific?

1.4 Research Aim

In recognizing the research problem and addressing the research questions, this thesis aims to design, develop, and evaluate a new framework using SSI and blockchain to improve the KYC process which:

- a) automates the initial verification of the customer through digital identity in which the identity and its credentials can be verified independently,
- b) instill trust and ensure privacy through the utilization of blockchain and SSI capabilities, and
- c) operates in a timely manner.

1.5 Research Objectives

In order to achieve the research aim and address the research questions, the follow objectives are formulated:

1. To understand and analyze the characteristics and capabilities of blockchain, SSI and digital identities

2. To study the underlying concepts, requirements and existing methods and current state of the use of blockchain and SSI in KYC
3. To design a framework for
 - a. Digital identity establishment, management and verification to enable the automation of the initial customer identification and verification and continuous monitoring
 - b. Trust instilment to be accepted by participants in KYC process through blockchain
 - c. Regulatory and legal acceptance
4. To implement a prototype system for blockchain-based SSI and KYC use cases
5. To evaluate the prototype, improve the framework, and identify areas for future development

1.6 Scope of this Thesis

While this thesis focuses on the UAE, specifically the financial sector, to improve KYC use cases, the Digital Trust Framework developed in this thesis can be generalized to any domain and region. The financial domain was selected because it is the most complex regulated domain regarding the KYC use case. Thus, addressing its KYC requirements, implies the ability to address KYC in any other domain. The telecom sector evaluates the framework at a high level to demonstrate the ability to expand the KYC use case implementation to any domain. This thesis focuses on the UAE due to the ability to access information and experts from different domains, which is required to evaluate the alignment and acceptance from all required parties, government entities, private institutions and regulators to realize the value of the Digital Trust Framework.

1.7 Thesis Outlines

This chapter provides background information on the problem statement and thesis objectives, highlighting the research questions mainly focused on digital identity and the initial verification phase of the KYC process. It also describes the key contributions of this study. The remaining chapters of this thesis investigate the research questions and provide further explanation as structured below:

Chapter 2 provides detailed background on the multidisciplinary domains and the intersection between them. These domains include the KYC process, regulation, data privacy in general and the UAE in specific, and technological concepts of digital identity, SSI and blockchain. Next, **Chapter 3** reviews the literature related to implementing decentralized digital identity, SSI, and blockchain in general domains for improving the KYC process efficiency in the financial sector and identity management. It provides a summary of similar implementations and challenges in the health sector. It also presents eID and SSI implementations in governments worldwide, highlighting lessons learnt. The chapter provides the main research gaps in blockchain-based SSI implementations.

Subsequently, **Chapter 4** describes the methodology followed in this thesis to design, develop and evaluate the Digital Trust Framework. It outlines the research approach, data sampling and data collection. It summarizes the researcher's role, ethical considerations, the trustworthiness of the qualitative and quantitative research data, and the limitations of this thesis. Then, **Chapter 5** defines the design objectives of the Digital Trust Framework, including the requirements that need to be addressed by the blockchain-based SSI framework to serve a regulated domain. The chapter provides a summary view of various experts' evaluations of the design objectives.

Moreover, **Chapter 6** describes the design of the Digital Trust Framework, including the architecture, processes and prototype based on the defined design objectives. The chapter highlights the results of the framework design evaluation, including insights from experts and individuals. **Chapter 7** presents the development of the Digital Trust Framework in the form of prototype system based on the design detailed in **Chapter 6**. The chapter describes the functionality of the prototype, the technology stack and the core APIs.

Subsequently, **Chapter 8** details the evaluation of the prototype system through case study demonstrations. The results of the demonstration is used to evaluate the performance of the prototype through performance metrics.

Finally, **Chapter 9** summarizes the achievement of this thesis in addressing the research problem, highlights the limitations of this study, and suggests possible directions for future work.

Chapter 2: Background

2.1 Introduction

In the physical world, individuals are identified through physical credentials such as social security cards and passports. Individuals decide where to store their physical credentials and to whom they disclose their identities. In a digital world, a similar concept is required to be transacted online. Digital credentials must be issued securely, and individuals should hold and manage them to preserve their privacy.

The high velocity of technology advancements and the growth of regulation have created an opportunity in the field of “regtech”. Regtech is a combination of “regulation” and “technology”. This field aims to use technology to improve the implementation of regulations. These opportunities are significant in KYC use cases (Memminger, Baxter and Lin, 2018). For example, Soni and Duggal (2014) proposed using big data analytics to decrease the risk of conducting the KYC process, while Colladon and Remondi (2017) used cluster analysis to identify suspicious financial operations and potentially criminal activities over a network of customers and possible customers. Other research studies have proposed leveraging DLT and blockchain to increase the efficiency and reduce the cost of the KYC process, which is the focus of this thesis (Parra-Moyano and Ross, 2017; Soltani, Nguyen and An, 2018; Dong *et al.*, 2020; Schlatt *et al.*, 2022). Blockchain can provide a trusted audit trail for regulators to verify the process conducted for KYC. Previous works related to blockchain implementation to improve the KYC process are discussed in more detail in Chapter 3. This chapter provides an overview of the underlying concepts related to this research which includes KYC, digital

identity in general, SSI in specific and blockchain, in response to the first objective of this research.

2.2 What is “Know Your Customer”?

KYC is when entities engage with customers to verify their identities. During this process, customers are requested to submit various documentation depending on the industry and the services availed (Soltani, Nguyen and An, 2018; Malhotra, Saini and Singh, 2021). These documents include identity and address proof. The traditional KYC requires customers to visit entities physically to submit papers. However, documents can easily be forged. In some industries, such as the financial sector, KYC is a lengthy process typically involving manual verification, which came into effect as part of the FATF recommendations reviewed in 1996, considering the newest money laundering techniques. These AML recommendations are considered the international standard, adopted by over 130 countries (Butijn, Tamburri and Van Den Heuvel, 2020). Financial institutions are advised not to open accounts with suspicious names or anonymous accounts. Therefore, due diligence is needed to confirm customers' identities using different trusted documents. Depending on regulatory and financial institutions' specific requirements, KYC processes may differ across countries. However, the core KYC verification process that includes the minimal common repeated activities mandated by law to be conducted by all financial institutions are 1) customer identification, where potential customers' data is collected to identify them, including government-issued documents, such as identity cards and passports, documents issued by financial institutions and other personal identification information such as addresses, 2) data verification, 3) name screening, 4) risk assessment verifying customers' risk scores compared to a list of known criminals, terrorists and politically exposed persons (PEPs), 5) enhanced due diligence, 6)

ongoing monitoring to ensure permanent risk monitoring, and 7) record keeping (Schlatt *et al.*, 2022). The financial institution generates an internal document to assure regulators that the KYC process has been conducted and the customer is either accepted or rejected (Parra-Moyano and Ross, 2017). This process of initial verification and ongoing monitoring is repeated for each customer. Hence, every customer goes through the same process for each financial institution where they want to avail services. Sometimes, the process is repeated to avail different services from the same financial institution (Soltani, Nguyen and An, 2018; Schlatt *et al.*, 2022), making the KYC process cost-intensive, time-consuming and inconvenient for customers and financial institutions. The Central Bank of the UAE mandates that financial institutions verify original identity documents as part of the KYC process (Al Tamimi & Company, 2020; Central Bank of the UAE, 2021). Figure 1 demonstrates the KYC process for a customer who wants to avail services from three banks. The KYC process and document submission are repeated three times for the same customer.

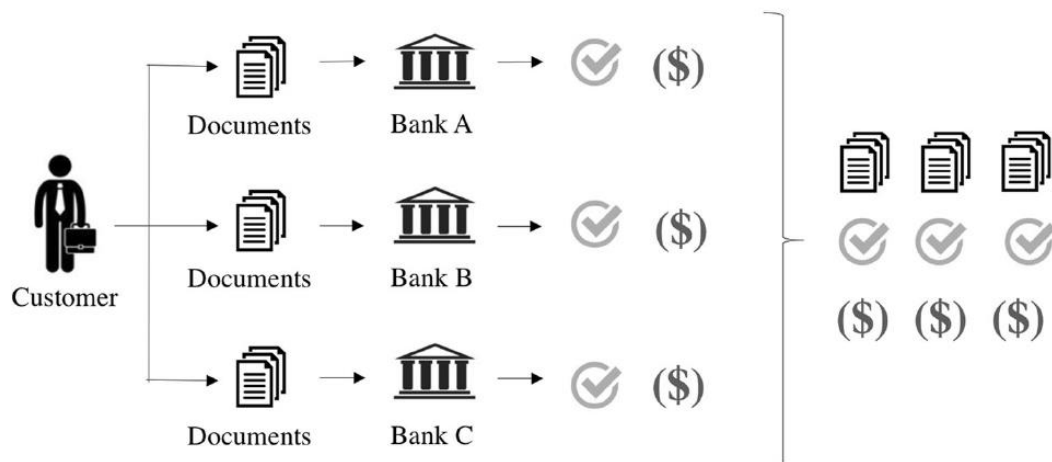


Figure 1: KYC process of a customer availing services from three banks

(Source: Parra-Moyano and Ross, 2017)

In addition to the financial sector, the telecom sector also mandates the KYC process to onboard new customers and for ongoing verification. More than 85% of countries worldwide mandate that telecom providers collect personal information from SIM card holders (Panamax Inc., 2021). Regulators of these sectors enforce penalties on entities if the KYC process is not followed per regulations, increasing the KYC cost (Moyano and Ross, 2017; Soltani, Nguyen and An, 2018). The Telecommunications and Digital Government Regulatory Authority (TDRA), the UAE's federal telecommunications regulatory agency since 2003, issued the "Registration Requirements for Mobile Consumers" regulatory policy. In this policy, telecom providers are mandated to collect information and copy one identification document from consumers after attesting to the original document to provide or renew their SIM cards. Moreover, these providers are mandated to verify the submitted information against the information presented in the submitted documents and verify them against the originals to ensure they are accurate copies (United Arab Emirates Telecommunication Regulatory Authority, 2011).

The challenges of the KYC process from the perspectives of customers, financial institutions and regulators include the following: 1) Due to the lack of an automated KYC process and the ability to verify data with other organizations, a genuine customer can fill in information mistakenly, while a malicious customer may intentionally fill incorrect data or submit fraudulent documents. 2) The KYC process is lengthy, yet customers must conduct a separate KYC for each financial institution, increasing customer overhead while reducing satisfaction. 3) From a financial institution perspective, the KYC process is costly as there is a lead time to onboard a customer and employee costs of verification for a single account or multiple account holders, which is more time-consuming with additional fines to be paid in

case of misconduct in the KYC process. 4) Reputational and regulatory risks may be incurred when onboarding malicious customers due to fraudulent KYC details. 5) A lack of an internationally agreed KYC process exists for cross-border transactions (Malhotra, Saini and Singh, 2021).

Therefore, many industries have shifted to digitization and automation of the process to improve the customer experience and reduce compliance costs. One solution adopted is the e-KYC (Schlatt *et al.*, 2022). Indeed, a domain-specific e-KYC solution could eliminate the need to execute repeated KYC processes at different financial institutions. These systems leverage biometrics, such as fingerprints, iris scans and facial recognition. Then, the customers' biometric and personally identifiable data, such as names and ages, are stored on smart ID in a central repository. During the KYC process, customers' biometric data are captured and matched against the central repository (Schlatt *et al.*, 2022). India's Aadhaar system is an example of an e-KYC system, as citizens must provide various demographic and biometric data stored in a central repository (Casino, Dasaklis and Patsakis, 2019). The Aadhaar system has reduced the KYC onboarding process and losses from fraud and corruption (Maliki and Seigneur, 2007). However, with digitization, addressing fraud and cybercrimes while maintaining individual privacy has become crucial. Several data breaches in the Aadhaar system have raised concerns about the privacy and security of the system (Casino, Dasaklis and Patsakis, 2019). Moreover, there are potential risks in operating identity systems centrally. For example, when operated centrally by a government authority, they can be used by the government without citizens' knowledge, while if operated by the private sector, they may lead to threats of monopolies and market power that may not incentive financial institutions to participate in such a system (Casino, Dasaklis and Patsakis, 2019).

While e-KYC improves process efficiency and enhances the user experience, the design of these identity systems should incorporate robust privacy and security measures since they manage highly sensitive data (Maler and Reed, 2008). Indeed, attackers are attracted to centralized repositories that store users' personal data.

2.3 Digital Identity

Identity represents an entity (e.g. a person or a legal organization) with a distinct existence that can be measured through various attributes. An attribute is a named property that belongs to an entity in a context. Hence, the value of an attribute can be used to identify an entity. An attribute uniquely identifying an entity within a context is called an identifier. The value is either provided by an entity or a trusted third party. A trusted third party is an entity that other entities trust within a context. An entity exists and operates under a specific environment considered a context or domain. In a digital world, a domain is an application (Ferdous, Chowdhury and Alassafi, 2019).

For example, a bank customer's personal data constitutes the customer's identity in the banking domain. An entity could have no or more than one identity in a domain. For example, an individual could be a customer and an employee of a retail shop. The entity could have different identities in different domains. Moreover, an entity could have different characteristics or attributes. Characteristics have different properties, such as permanent versus temporary and self-selected versus issued by authority. These characteristics are different based on the type of entity. A person can have a date of birth, while organizations can have a national company registration number. Figure 2 demonstrates the relationship between entities, identities and characteristics (Ahn, Ko and Shehab, 2009).

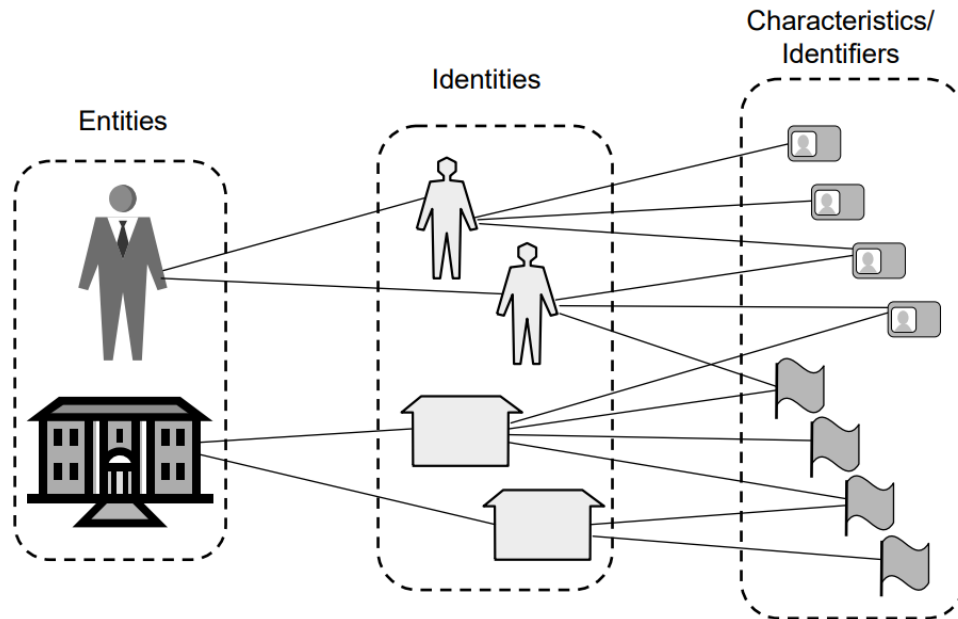


Figure 2: Correspondence between entities, identities and characteristics

(Source: Ahn, Ko and Shehab, 2009)

Digital identity is defined by the National Institution of Standards and Technology (NIST) as

the unique representation of a subject engaged in an online transaction. A digital identity is always unique in the context of a digital service but does not necessarily need to uniquely identify the subject in all contexts. In other words, accessing a digital service may not mean that the subject's real-life identity is known. (Grassi, 2017)

Moreover, the International Telecommunication Union defines digital identity as “a digital representation of the information known about a specific individual, group, or organization” (ITU; Soltani, Nguyen and An, 2021). Cameron (2005) defined digital identity as “a set of claims made by one digital subject about itself or another digital subject”. Partial identity or persona is a subset of identity attributes of an entity within a specific domain or context, while

the total identity of an entity is the sum of all its partial identities in all domains (Ferdous, Chowdhury and Alassafi, 2019; Soltani, Nguyen and An, 2021).

In addition, Cameron (2005) defined the seven laws of identity: 1) users should be in control of the sharing of their identity information, 2) identity information accessed or shared should be only the minimum required information and should be kept by the other party as long as needed, 3) users should be aware of entities managing their identity information, 4) an unauthorized entity should not be allowed to perform data correlation, pattern recognition or entity identification, 5) different systems that manage identity should be interoperable, 6) the interaction between users and machines should be reliable and secure, and 7) the user experience should be consistent among different contexts and technologies. Digital identity plays a significant role in a digital society. Most people have various digital identities associated with their workplaces, education, businesses and financial institutions. Digital identity is owned by an entity and is used for digital identification, authentication and proof of authorization requests (Sedlmeir *et al.*, 2021).

Digital identity is managed through identity management (IdM), also called identity and access management. IdM is a set of policies, processes and technologies to manage digital identities and their associated roles and privileges within an organization or network (Soltani, Nguyen and An, 2021). IdM is used to identify and represent entities with their digital identities to be leveraged to access digital services in different application domains and ensure resources within an organization are accessed by authorized entities only (Ferdous, Chowdhury and Alassafi, 2019; Liu *et al.*, 2020a). Many standards and frameworks are related to IdM, such as the Security Assertion Markup Language (SAML), the Web Services Federation (WSFed), the Identity Federation Framework (IDFF) and the Identity Web

Services Framework (ID-WSF; Wason, n.d.; Cantor *et al.*, 2005; Cahill, 2007; OASIS Open, 2020).

Before exploring different IdM models, defining the building blocks of IdM and its core operations is critical. Liu *et al.* (2020a) identified three main actors in IdM:

- The **user** is the entity owning the digital identity and wants to avail a service or access a resource from a service provider. User identity is stored in an identity provider, so users request their identities from an identity provider that provides it to a service provider to avail a service or access a resource.
- The **identity provider** provides users with identity services, such as registration, authentication and management. It is responsible for storing the user's partial identity within its specific domain and sharing it across different domains.
- The **service provider** provides users with digital services upon identity verification based on the information shared and verification conducted through the identity provider.

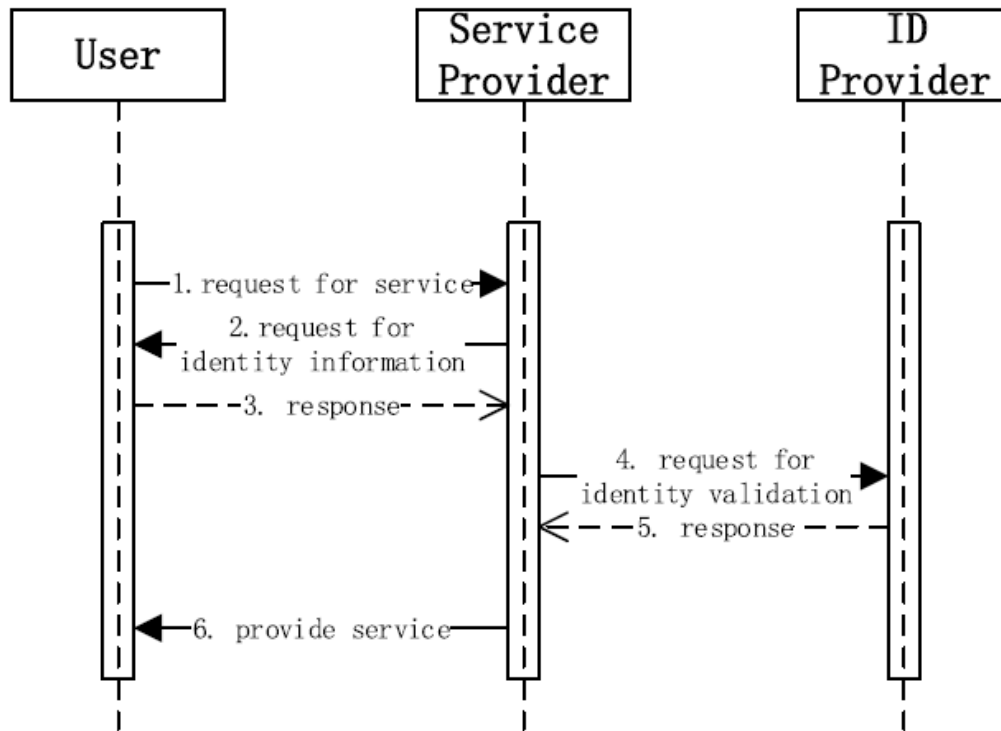


Figure 3: Simple IdM actors' interactions

(Source: Liu et al., 2020a)

There are four main operations of an IdM: 1) identification, where a user or an entity claims an identity that needs to be recognized by a service provider; 2) identity verification or identity proofing, where certain identity attributes are truthfully associated with the user or entity they represent; 3) authentication, where the identity of the user or the entity is verified as a prerequisite for granting access to resources; and 4) authorization, where the user or the entity is granted access rights determining their privileges against the target resource (Soltani, Nguyen and An, 2021). Authentication can be conducted with one or more factors, known as multifactor authentication (MFA). MFA involves three fundamental factors, which are something the user knows (e.g. a password or PIN), something the user has (e.g. a mobile phone or hard token) and something representing the user with biometrics (e.g. a fingerprint). In addition to MFA, the trending concept of continuous authentication is where the user is

continuously authenticated in the background with no or limited knowledge from the user to make it more convenient (Soltani, Nguyen and An, 2021).

The rapid evolution of the internet and digital services expedited the need for convenient, secure and privacy-preserving digital identity and access management (IdM) architectures. Thus, IdM evolved from a simple model to different complex models, with five total IdM models developed. The first is the isolated use identity (SILO) model, also known as independent IAM, in which the service provider (SP) and the identity provider (IdP) are coupled. The SP manages its users' identification, authentication, and authorization (Soltani, Nguyen and An, 2018). Every SP provides an identifier, such as a username and the corresponding credential, such as a password, to users who want to avail SP services. Every SP has a unique identity domain in which identity operations conducted in a specific domain are not considered valid in other domains (Ferdous, Chowdhury and Alassafi, 2019). While this model is the simplest and most common, it forces the user to create a different digital identity for every SP accessed without the ability to reuse it since it is not interoperable (Liu *et al.*, 2020).

The second IdM model is the centralized identity model, where the IdP is separated from the SP in a trusted domain. The IdP stores and manages digital identities for SPs in the same trusted domain (Liu *et al.*, 2020a). Users authenticate through the IdP before accessing the SP (Ahn, Ko and Shehab, 2009). This simple implementation is usually conducted within the same organization without external third-party involvement. However, with the increased adoption of online services, this model has become inconvenient to users who must remember login credentials for services across different domains. In addition, users must repeatedly supplement additional information and verify the required attributes (Maliki and Seigneur,

2007; Sedlmeir *et al.*, 2021), so they tend to reuse passwords across services, resulting in potential security risks. Hence, passwords can be stolen through password theft schemes, such as viruses, keylogging, phishing and malware (Herley, 2009). Moreover, SPs must rely on users' data for quality and validity.

The third IdM model is the federated identity model, where a federation is formed between multiple SPs and one or more IdPs in a single identity domain. The federation establishes trust between SPs and IdPs. The IdP issues identifiers and related credentials to users. The SP relies on the IdP for authenticating the user and sharing user attributes and values. Users are allowed to use the same credential to authenticate and access any of the federated SPs. Once users authenticate themselves, they can access any service from any SPs in the federation without authenticating themselves again. Moreover, identity-related information is exchanged between SPs (Maler and Reed, 2008). The shared identity domain is defined as the federated identity domain. IdPs manage users' digital identities. SPs, also known as relying parties, can leverage these credentials to provide users access to their services. Any system that implements SAML is an example of this model. The federated identity model improves the user experience by not requiring users to remember multiple usernames and passwords (Lim *et al.*, 2018). However, it increases privacy and security issues due to the centralized storage of users' full digital identities and associated attributes (Maler and Reed, 2008).

The fourth IdM model is the user-centric identity model (Chadwick, 2009), which is similar to the federated identity model but does not need to establish the notion of trust. The SP in this model trusts the IdP (Ferdous, Chowdhury and Alassafi, 2019). The focus of this model is on user experience and privacy control. The user can select the preferred identity

provider and the identity attribute to share with SPs while defining the policies through which the identity attributes are shared with selected SPs (Soltani, Nguyen and An, 2018; Soltani, Nguyen and An, 2021). Systems based on OpenID and OAuth protocols, such as Google and Facebook, are examples of this model (*OpenID Authentication 2.0 – Final*, 2007; Hardt, 2012; Ferdous, Chowdhury and Alassafi, 2019).

The fifth IdM model is SSI, still in its initial stages with no agreed definition. However, different initiatives have attempted to define it, identify its principles and describe its architectural components (Abraham, Theuermann and Kirchengast, 2018; Houtan, Hafid and Makrakis, 2020; Toth and Anderson-Priddy, 2019; Tambe and Tambay, 2020). Abraham, Theuermann and Kirchengast (2018) proposed a mathematical formalization of the concept of SSI using mathematical notions and properties. SSI is defined by the Sovrin Foundation,² a nonprofit organization administrating the governance framework governing a decentralized global public network that enables SSI, known as the Sovrin network, as

the individual (or organization) to whom the identity pertains completely owns, controls and manages their identity. In this sense, the individual is the identity provider since there is no external party who can claim to “provide” the identity for them because it is intrinsically theirs. . . . You can reveal some or all of it some of the time or all of the time. You can record your consent to share data with others and easily facilitate that sharing. It is persistent and not reliant on any single third party. Claims made about you in identity transactions can be self-asserted or asserted by a 3rd party

² <https://sovrin.org/>

whose authenticity can be independently verified by a relying party. (Tobin and Reed, 2017)

In the SSI model, users have complete control and ownership over their digital identity. Users can create their identifiers using public-key cryptography. These identifiers are also known as decentralized identifiers (DIDs). After creating DIDs, users can append information or attributes to these identifiers (Schlatt *et al.*, 2022). Users store these DIDs in the Digital Wallet on any device, giving them full ownership and control of their identities (Naik and Jenkins, 2020). Allen (2016) defined ten principles of the SSI model described below. In addition, extended SSI principles have been defined (Naik and Jenkins, 2020; Ferdous, Chowdhury and Alassafi, 2019), also described below, including data storage control, decentralized and verifiable. Ferdous, Chowdhury and Alassafi (2019) divided the principles into foundational, flexibility and sustainability. SSI principles are as follows:

- **Existence:** Users must have an independent existence in the real world and be able to encode their characteristics digitally to exist in a digital domain.
- **Control:** Users must fully control their identities, including information encoding them. Control and ownership should be distinguished. Users may have control over an identity claim issued but not own the claim. For instance, the government issues driving license numbers and can revoke them. Users can control and share them under their conditions (Soltani, Nguyen and An, 2021).
- **Access:** Users must have access to their identity information and be aware of any modifications. This principle does not indicate that users can modify their identity data.
- **Data Storage Control:** Users must control and maintain the storage of their data.

- **Transparency:** Algorithms and systems must be transparent and visible to every entity involved. Users should be aware of their identities and any related interactions and be able to retrieve this information.
- **Persistence:** Identities must remain for the long term, and the data should be persistent until the identity holder decommissions them.
- **Portability:** Identities must be transportable to another medium or platform if the previous one no longer exists.
- **Interoperability:** Identities should be widely used to the extent possible with heterogeneous systems and services, supporting the availability and durability of the identity information.
- **Consent:** Users must agree before sharing identity information with third parties.
- **Minimization:** Claims disclosure must be minimized.
- **Protection:** User rights must be protected with up-to-date cryptographic mechanisms to ensure confidentiality, integrity, authenticity and non-repudiation. Any interaction that includes the identity must be authorized.
- **Decentralized:** Digital identity should be managed by decentralized infrastructure.
- **Verifiable:** Digital identity must be verifiable, similar to the real world.

In this model, the IdPs do not need to store user identity data, reducing the possibility of data breaches and identity thefts. Identity data and the associated cryptographic should be stored in digital wallets to leverage edge devices, such as smartphones or computers, or cloud storage (Schlatt *et al.*, 2022). Smartphones are becoming a vital part of our lives. They are used to store credentials and perform payments. Thus, to increase the adoption of SSI implementation, storing identity data on mobile devices a promising option (Soltani, Nguyen

and An, 2018). However, Samir *et al* (2021) argues that storing identity data in single location represented by digital wallet is a potential point of failure as it can be lost.

SSI significantly depends on the characteristics of digital identity. These characteristics need to be trusted. Therefore, characteristics are modeled as verifiable credentials which comprised of claims and attestations. An attested claim could be name, address, or an age. A claim is any statement or characteristic an entity makes about itself or by trusted third party. It consists of attributes which are name-value pairs. W3C working groups specify standards for decentralized identifiers (DIDs) and VCs data models. A DID uniquely references a digital identity (Gruner, Mühle and Meinel, 2019).

In the physical world, a credential is a claim made about a person. For example, a driving license is a credential enabling a person to assert the capability of driving a vehicle, while a university degree enables a person to assert a specific level of education. These credentials contain information related to 1) the entity, such as a name or identification number; 2) the issuing authority, such as a government authority; 3) the type of credential, such as an insurance health card; 4) specific attributes asserted by issuing authority, such as the category of vehicle to drive; 5) the constraints on the credential, such as the expiry date; and 6) evidence related to how the credential was derived. VCs can represent the same information as physical credentials and be revoked or transferred. Using technology such as digital signature makes VCs more secure, tamperproof and trustworthy than physical credentials (Sporny, Longley and Chadwick, 2022). There are five important roles in the SSI and decentralized identity ecosystem: 1) the holder, which is an entity holding VCs and can share them, such as student or employee; 2) the issuer, which is the entity that creates a VC by asserting claims about subject and transmitting the verifiable credential to the holder such as

government authority; and 3) the subject, which is the entity about which the claim is made, such as individuals. In many cases, the subject and the holders are the same. However, there are cases where they differ, for instance, if a parent is the holder of a VC of a child, who is the subject in this case; 4) the verifier, which is the entity that receives and processes VCs in the form of verifiable presentation,³ such as an employer; and 5) the verifiable data registry, which is the system mediating the creation and verification of relevant data required to use VCs, such as databases and distributed ledgers (Sporny, Longley and Chadwick, 2022).

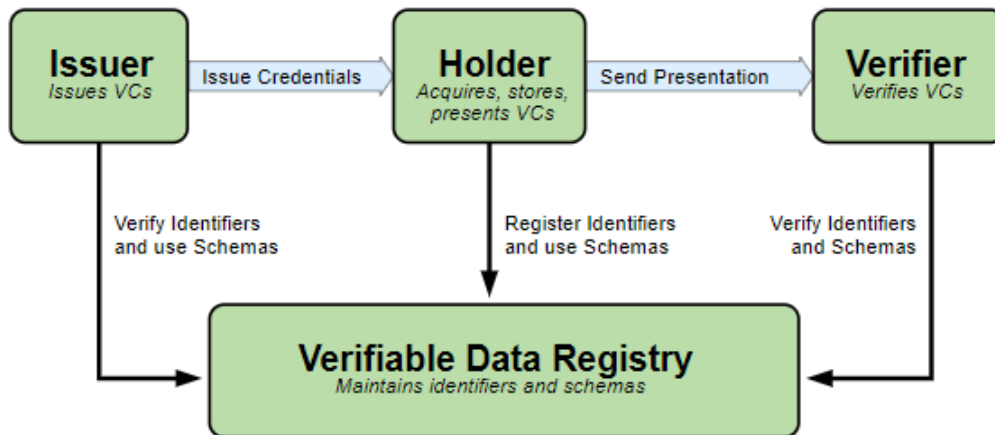


Figure 4: The roles and information flows of VCs

(Source: Sporny, Longley and Chadwick, 2022)

Čučko, Keršič and Turkanović (2023) have reviewed and analyzed existing knowledge which includes literature, technical documentation and SSI implementations and presented thirty-five SSI design patterns that can be used to design SSI systems. The technical documentation and SSI implementations review covered World Wide Web Consortium (W3C)

³ Verifiable Presentation (VP) is defined by W3C Verifiable Credentials Working Group. VP defines the methods by which verifiable credentials are signed and presented by the holder.

documentation and standards, Decentralised Identity Foundation (DIF), European Self-Sovereign Identity Framework (ESSIF) documentation by the European Blockchain Services Infrastructure (EBSI), Sovrin documentation and Veramo (Sporny, Longley and Chadwick, 2021; Sporny, Longley and Chadwick, 2022; Steele, Sporny, 2022; Decentralized Identity Foundation, 2022; EBSI, 2022; Sovrin, 2022; Veramo, 2022). The SSI design patterns were categorized into six groups each with its own subgroups. The main pattern categories are 1) Trusted Registries which enable the formation of trust between entities through a decentralized identity ecosystem, 2) Onboarding of entities to interact with other entities in the ecosystem, 3) Verifiable Credentials and Presentations to support data exchange, 4) Decentralised Identifiers and Cryptographic Keys to manage DID, DID documents and cryptographic keys, 5) Qualified Electronic Certificates (QEC) for legal validity, and (6) Wallet and Off-Chain Storage. The design of the Digital Trust Framework is based on these main design patterns categories and some of their subcategories. The design patterns related to QEC are core in the Digital Trust Framework as its main objective is to instill trust in regulated domains and to provide evidence that the VC was issued by legal entity and it was sent to the holder or that the VP was shared by the holder and verification took place by the service provider to comply with legal and audit requirements (Lemieux *et al.* 2021).

While the SSI model is the latest and most recent evolution of IdM, it has advantages and challenges. Soltani, Nguyen and An (2021) highlighted a few challenges to consider when implementing SSI models: 1) the lack of standardized protocols, practices and policies of data management, data exchange, wallets and user experience; 2) the risk of losing cryptographic keys by the user who manages them; 3) implementing and verifying user consent without causing consent fatigue where the user is loaded with privacy or sharing notifications; 4)

balancing between centralization and decentralization to govern the ecosystem and ensure the trustworthiness of key operations, including identity claim issuance, identity lookup and data storage; and 5) forming trust among entities and data exchanged. Moreover, Privacy-by-Design (PbD) and Security-by-Design principles should be considered in any SSI implementation (Soltani, Nguyen and An, 2021).

The principles of SSI are better realized when implemented through distributed ledger technology (DLT) due to the decentralized nature of the network that ensures integrity, reliability, trustworthiness and the availability of publicly provisioned information. It enables SPs to independently verify VCs. It also ensures the user's privacy (Soltani, Nguyen and An, 2018).

2.4 Blockchain

A blockchain is a decentralized ledger of information that is cryptographically secure. Transactions in blockchain are batched into blocks. Each block in the blockchain holds the previous block's hash value. Thus, blocks form an append-only structure (chain). The first block of the chain is called the genesis block. The main objective of blockchain is to establish a tamper-resistant historical record (Butijn, Tamburri and Van Den Heuvel, 2020).

Blockchain is an implementation relying on DLT, which defines an immutable time-stamped append-only distributed ledger containing a set of cryptographically hashed transactions. DLT is a peer-to-peer network in which data are replicated across multiple peers. In the network, specific nodes operate an associated consensus protocol to ensure that the state modifications are valid (transactions) and synchronize all replicas (Glaser, 2017; Kolb *et al.*, 2020). Public-key cryptography is used to authenticate access on DLT to participate in consensus or authorize transactions. It provides a decentralized consensus-based approach to

process transactions and ensures data integrity (Soltani, Nguyen and An, 2018). Due to the architecture of DLT, it is highly available. Moreover, it is resistant to malicious behavior and the unavailability of a small subset of nodes.

Blockchain uses digital signature and cryptographic hash function, or message digest, between the blocks to establish peer trust. Creating or adding a new block to the chain should follow a process of validating, mining and block-addition steps. Moreover, to generate and add a transaction to the blockchain, it should first be broadcasted to all the nodes in the network to be validated. Once the transaction is validated, it is added to a pre-defined pool of unconfirmed transactions. The miner, a participant who dedicates computational resources to adding blocks in the chain (i.e. mining), conducts the mining to include a set of transactions into a block. Once the transactions are gathered from the pool of unconfirmed transactions for a specific time, and a difficult computational puzzle is solved, the new block is created. The first miner to solve the computational puzzle receives a monetary reward in cryptocurrency known as “gas”. The block is then broadcasted to the network for validation. Every node in the network validates the block, so once all nodes reach consensus, the block is added to the network. Every peer then updates its local copy (Malhotra, Saini and Singh, 2021).

One of the key concepts in blockchain is the smart contract, a computer code which is decentralized, self-executing, self-verifying and tamper-resistant (Malhotra, Saini and Singh, 2021). The smart contract is deployed on the blockchain, requiring a virtual machine to be executed. An event triggers the execution of the contract, and it cannot be modified. The smart contract code contains a set of rules and can digitally validate, facilitate or enforce the negotiation or execution of a contract without a third party (Butijn, Tamburri and Van Den Heuvel, 2020). The contract is required to be signed between two anonymous parties. It can be

used to control the ownership of tangible properties (e.g. jewelry) or intangible properties (e.g. patents). All smart contract actions are recorded and immutable, so they can be used for audit trail. The smart contract is mainly used in Ethereum blockchain (Malhotra, Saini and Singh, 2021).

There are four key characteristics of blockchain per Malhotra, Saini and Singh (2021): 1) security, as it has the potential to solve the double spending challenge so that a user cannot spend the currency more than once; 2) trust between the participating nodes; 3) privacy since any transaction in the block is cryptographically hashed, so no one can read it or update it; and 4) anonymity, as blockchain generates a unique anonymous identity to miners.

The initial use cases of blockchain implementation were in the cryptocurrency field. Nakamoto (2009) published the first research paper on cryptocurrency proposing decentralizing digital money architecture in “Bitcoin: A Peer-to-Peer Electronic Cash System”. Blockchain allows transactions to be conducted without central intermediaries or authorities (Soltani, Nguyen and An, 2018). The most common example of blockchain cryptocurrency is Bitcoin. However, various public and private authorities have realized the potential of blockchain in digitizing cross-organizational processes, which has led to the expansion of blockchain use cases to other domains (Casino, Dasaklis and Patsakis, 2019). Noizat (2015) proposed using blockchain in electronic voting to address issues related to the authenticity of voting, while Mougayar (2016), Beck *et al.* (2017), Parra-Moyano and Ross (2017), Bhaskaran *et al.* (2018) and Lootsma (2019) proposed the use of blockchain to enhance the KYC process in the banking sector.

The properties of blockchain make it appropriate for various application domains. Ferdous, Chowdhury and Alassafi (2019) described these properties as 1) the distributed

consensus on the ledger state enabling the verification of the state of any transaction by any authorized entity without the need to rely on a trusted third party; 2) the immutability and irreversibility of the ledger state enabled through the large number of nodes participating in the consensus; 3) data or transaction persistence since they are stored in a distributed manner; 4) data provenance since data is stored through transactions, so every transaction should be digitally signed using public-key cryptography ensuring the authenticity of the source of data; 5) distributed data control since data stored or retrieved from the ledger can be performed in a distributed manner ensuring no single point of failure; and 6) accountability and transparency since the state of the ledger and every interaction between participating entities can be verified by the authorized entity.

There are two common types of blockchain implementation: public and private. As the name indicates, the network is public and unpermissioned in public blockchain, so anyone can create and validate blocks. Moreover, anyone can modify the ledger state by storing or updating data using transactions. The ledger state and its transactions, including stored data, are accessible to everyone (Ferdous, Chowdhury and Alassafi, 2019). Since it is public, usually, there are many participating entities. Thus, the consensus mechanism requires more time and resources, leading to lower transaction throughput (Soltani, Nguyen and An, 2018). Public blockchain can raise privacy concerns in cases where data privacy is key. In private blockchain, also known as permissioned, access to the network is restricted to a set of entities that are authorized and trusted to participate in activities within the network, such as validating and writing transactions to the ledger (Ferdous, Chowdhury and Alassafi, 2019). Thus, it forms a smaller network leading to higher transaction throughput. While private blockchain provides more privacy, it offers less transparency on the content of the transaction. Moreover,

Rathee and Singh (2022) highlighted consortium blockchain, a semi-private, permissioned and controlled blockchain. The main difference between private and consortium is that blockchain consensus is conducted by a group of approved users, making it more secure than private and partially decentralized. Each category of blockchain implementation can be more appropriate for specific use cases.

Blockchain can play an important role in realizing SSI, providing the required functionality to perform distributed IdM tasks (Soltani, Nguyen and An, 2018). Different SSI and decentralized identity solutions can be leveraged in blockchain, including Sovrin, uPort, ShoCard, Jolocom, Blockstack, Civic, Veres One, Hyperledger Indy, Selfkey, LifeID, and Mattr (Gruner, Mühle and Meinel, 2019; Liu *et al.*, 2020a; Soltani, Nguyen and An, 2021). First, Sovrin is an open-source user-centric SSI built on a public blockchain based on Hyperledger, enabling it to be scalable and accessible. The blockchain is owned by Sovrin and is called Sovrin Ledger. It uses Plenum as a consensus algorithm (Ferdous, Chowdhury and Alassafi, 2019). It implements PbD by identifying private users under pseudonyms and adopting zero-knowledge proof (ZKP) encryption (Liu *et al.*, 2020b). It consists of a mobile application and website that the user can use to create, manage and share identity data. In addition, it has agents that can certify the user's identity data similar to a trusted third party (Ferdous, Chowdhury and Alassafi, 2019).

Next, uPort consists of a mobile application and a set of smart contracts built on Ethereum, so the Ethereum account address is the identity on which users interact, which is permanent. The user uses the mobile application to create, manage and share identity information with others. The mobile application stores the user's private key of uPort identity,

while identity information is stored in a distributed file system, the Interplanetary File System (IPFS; Ferdous, Chowdhury and Alassafi, 2019).

Jolocom is an open-source SSI platform implemented using smart contracts stored on Ethereum. It is similar to uPort, as users use a mobile application to manage their identities. However, it follows different implementations in terms of identity data structure and representation (Ferdous, Chowdhury and Alassafi, 2019; Gruner, Mühle and Meinel, 2019). Moreover, ShoCard is used as IdM and issues SFN coins for payments. ShoCard stores the authentication code of user data on the blockchain to ensure the validity of personal identity and enable third-party verification (Liu *et al.*, 2020b).

In comparison, Blockstack does not depend on any specific blockchain as it is implemented using a meta approach (Gruner, Mühle and Meinel, 2019), while Civic is a decentralized IdM platform based on Ethereum that provides users with a proprietary mobile application to manage their identity (Soltani, Nguyen and An, 2021). Furthermore, Veres One is a decentralized identity that supports public permissionless blockchain and uses DIDs, decentralized key management and VCs (Soltani, Nguyen and An, 2021).

Hyperledger Indy is a decentralized identity implementation using public permissioned DLT addressing SSI use cases, initially developed by Evernym to support DIDs, VCs and ZKPs. It adheres to PbD principles and does not store personally identifiable information without user approval (Soltani, Nguyen and An, 2021). In addition, Selfkey is an SSI network that relies on ZKPs to ensure the users share minimum data, while LifeID is a decentralized identity implementation using a public permissionless blockchain that implements the concepts of DID and ZKP to ensure decentralization and data minimization. Finally, Mattr is an SSI implementation based on DIDs and VC implementation.

Ferdous, Chowdhury and Alassafi (2019) compared uPort, Sovrin and Jolocom considering their fulfillment of the SSI principles. They had a few more principles that were described in their research. However, they were insignificant and could be covered under other principles. The total number of principles used in the comparison was 17. Regarding satisfaction with the SSI principles of these three platforms, Sovrin scored 76%, uPort scored 65%, and Jolo solved 53%.

Although blockchain can solve unique challenges in different domains, it has its own constraints, including scalability, throughput, latency and cost (Malhotra, Saini and Singh, 2021). Since mining requires intensive resources, it consumes significant energy that prevents its scalability in terms of adoption by many miners. The throughput of blockchain transactions that can be processed in seconds is very low compared to normal systems such as the Visa network. The throughput of Bitcoin is 0.28%, which is the throughput of the Visa network (Karame, 2016). Moreover, adding a new block to the blockchain takes significant time, leading to delayed processes, while Bitcoins take approximately ten minutes (Squarepants, 2008). In addition, since mining activities require providing gas to miners, blockchain is not suitable for micro-transactions. Adding more transactions requires a high amount of cryptocurrency, eventually resulting in excess gas requirements (Malhotra, Saini and Singh, 2021).

In blockchain-based IdM solutions, new challenges could prevent SPs from adopting and accepting services in regulated domains such as finance and telecom. These challenges include the feasibility of SPs trusting and accepting attributes of individuals of uncertain reputations (Liu *et al.*, 2020b). Service providers must be able to perform their due diligence and verify the individual identity to ensure the completion of the KYC process before

approving any transaction to avoid fraud that could lead to potential legal and financial implications. Hence, a balance between centralized and decentralized models is required.

2.5 Privacy

Recently, a growing interest has been noticed in developing privacy frameworks focusing on user protection. The GDPR is the strongest privacy and security law in the world as the law is enforced in the EU and for any entity in the world targeting or collecting data related to people in the EU. It aims to harmonize the privacy laws in Europe and protect users' personal data, consisting of 11 chapters, 99 articles and 173 recitals. The key principles defined as part of Article 5 related to personal data are 1) data must be processed in a lawful, fair and transparent way, 2) purpose limitation, 3) data minimization, 4) accuracy, 5) storage limitation, 6) integrity and confidentiality and 7) accountability (Soltani, Nguyen and An, 2018). SSI is aligned with the GDPR principles as it gives users control over their identity information and streamlines sharing of identity information between the identity holder and verifier (Soltani, Nguyen and An, 2021).

Similar to the GDPR, the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection is also enforced concerning any entity collecting or processing data about people in the UAE worldwide (Al Tamimi & Company, 2021b). The key principles of the law are 1) data must be processed in a fair, transparent and lawful manner, 2) data must be collected for a clear and specific purpose, 3) data must be kept accurately, 4) data must be kept securely, and 5) data must be kept for a required period depending on the purpose, and then it should be either deleted or anonymized it.

Electronic Identification and Trust Services (eIDAS) was introduced by the European Union in 2016 to standardize the electronic signature, electronic timestamp, and electronic

identification of natural and legal persons (Regulation (EU) No 910/2014 of the European Parliament and o... - EUR-Lex, 2014). eIDAS aims to create a foundation for the diverse electronic identification systems developed independently by every EU state.

To protect data through technology, PbD defines seven principles: 1) be proactive, not reactive and preventative, not remedial; 2) privacy is the default setting; 3) design to embed privacy; 4) preserving positive-sum, not zero-sum; 5) security from end-to-end and protection of the full lifecycle; 6) visibility and transparency and 7) respecting user privacy (Soltani, Nguyen and An, 2018). Privacy engineering covers the processes, metrics, taxonomies, tools and techniques to implement PbD. It complements SSI implementations by addressing important requirements, such as consent and data minimization.

Chapter 3: Literature Review

3.1 Introduction

This chapter reviews the literature related to implementing decentralized digital identity, SSI, and blockchain for improving the KYC process efficiency in the financial and health sectors. It presents eID and SSI implementations in governments worldwide, highlighting lessons learnt. It provides an overview of the requirements and existing methods and the current state of the use of blockchain and SSI in KYC, in response to the second objective of this research.

3.2 Using Blockchain to Improve Financial Sector KYC

There has been growing research on improving the efficiency of the KYC in general and the banking sector in specific using SSI and DLT. The banking sector is considered the strictest sector for KYC verification due to domain criticality and the rigid regulations from central banks. Malhotra, Saini and Singh (2021) systematically reviewed all research papers between January 2014 and May 2021 related to blockchain and KYC from various academic databases. The final list of publications reviewed after applying different filters was 63 research papers, which demonstrated that there are various domains in which user identification is required to be verified by SPs, including healthcare, banking, accommodation and travel, mutual funds, outsourcing vendors, transportation, lending and card issuing and e-commerce and payments.

These papers' contributions were classified into case studies, frameworks and reviews based on the methodology followed. Most research papers were related to the first two categories, with 45.5% case studies and 43.6% frameworks. The case studies investigated the

usage of blockchain in KYC in different examples, including the banking sector, such as requesting loans, cross-border payments and facilitating communication between entities. The framework category was further classified based on the platform used to implement it into Ethereum and Hyperledger. The Ethereum implementation constituted 66.7% of the total framework category. Most studies proposed leveraging smart contracts.

Concerning data storage, the review highlighted that most papers proposed storing data off-chain with only hashes of the data on-chain, while a few papers proposed storing the data off-chain in an encrypted format. Three papers proposed using the IPFS to store the data off-chain (Malhotra, Saini and Singh, 2021). Using passwords was proposed to protect the hashes stored in the public chain. Encryption was suggested to prevent the data from malicious users, while compression during data storage on-chain was suggested to reduce the gas required. However, compression increased the time required to extract the data. Regarding privacy, scalability and storage concerns, the review highlighted a few studies that used the concept of ZKP where the data is not stored on-chain only but proof of transactions are stored for verification purposes.

Soltani, Nguyen and An (2018) proposed using SSI and DLT to improve the KYC process. The technology of choice was Hyperledger Indy, a public, permissioned distributed ledger purpose-built for decentralized identity. The proposed approach included a manual step as initial verification where the customer provides all the required documents to the first bank. The bank conducts all the required verification and issues the customer a verifiable credential as proof of a successful KYC. The VC is stored in the client's mobile application. When the customer interacts with the second bank, the customer can share the VC that the first bank issued. The second bank can verify the VC and provide the requested service to the customer.

The banks that issue VCs are registered as trusted issuers. Following this approach still requires the customer to go through the lengthy KYC process once. In this initial manual verification process, there is no guarantee that all the submitted documents are genuine. Moreover, if any of the characteristics of the customer change, impacting the status of the KYC (i.e. the issued VC), the changes are not reflected before using it by the second bank for KYC processing.

Parra-Moyano and Ross (2017) conducted another study in which a system based on DLT was proposed to reduce the aggregate cost and increase user satisfaction with the KYC process for financial institutions within the same jurisdiction. They proposed a system that requires the customer to conduct a KYC process only once with the first financial institution, sharing the documents outside the DLT. The financial institution stores the documents submitted by the customer in its local database and then verifies them. The financial institution produces a digitally signed document that includes the result of the core verification process and stores it in the DLT along with the hash of each document submitted by the customer. The original documents submitted by the customer used by the financial institution during the KYC verification, along with a digitally signed document of the verification process and results, are stored in the financial institution database and a permissioned database maintained by the regulator and shared with the customer. The customer can then share the KYC certificate with any subsequent financial institution that can verify it from the DLT. They can also access the documents from the permissioned database. One of the challenges in the proposed design is storing customer data in a permissioned database maintained by the regulator, creating a honeypot of customer data stored centrally with the potential for misuse and attack. In addition, the proposed solution suggested an integrity check from a local read

operation on one node, which did not satisfy the objective of using decentralized distributed technology. Furthermore, the proposed solution did not address the first step of verification in terms of efficiency, nor did it consider changes that could occur to the document submitted by the customer (i.e. changes to customer status that could invalidate the KYC status).

Parra-Moyano and Ross (2017) proposed an e-KYC solution to increase the efficiency of the KYC process, reduce its cost, ensure the anonymity of the relationship between banks and customers and increase the trust and throughput using Hyperledger and the smart contract. The blockchain network suggested was a permissioned network controlled by a central regulatory that enrolls Financial Institutions into the network. During enrollment, financial institutions are issued two identity certificates. One is a long-term certificate used to identify financial institutions, while another is a short-term certificate used for every transaction conducted with a customer. The short-term certificate contains the pseudonym of the bank instead of the original identity. The central authority maps the short-term certificates and the bank's original identity. The objective of the short-term certificate is to ensure the anonymity of the bank identity while sharing the KYC evidence of a customer with another bank. The customer interacts with the e-KYC through a portal. The customer is issued an identity certificate upon signing in to the portal. However, the verification process in which the customer's physical identity is verified to issue a digital identity is not discussed. Similar to the previous solutions, the initiation phase of the first bank to perform a KYC process is manual (Parra-Moyano and Ross, 2017; Soltani, Nguyen and An, 2018). The customer has to visit the bank and submit the documents. Upon verification, the documents are stored off-chain in an IPFS while the documents' hash and links to the off-chain storage are stored on-chain. When the customer wants to avail services from another bank, the bank can retrieve the

documents verified by the first bank without revealing the bank's identity that conducted the KYC verification. The bank accesses customer information after customer consent. The customer logs into the portal, reviews the request, verifies the bank through the identity certificate and consents to share requested documents. The customer consent is registered in the blockchain. Parra-Moyano and Ross (2017) proposed that implementation does not use SSI and W3C DID standards. The challenge of relying on the validity of the submitted documents for first-time verification without further verification at a later stage is present in this study.

Dong *et al.* (2020) proposed using an enhanced version of uPort for open banking to facilitate new business, such as loan approvals, through trending data sharing. Banks either provide their services directly to customers or provide their APIs to a third party who offers them services. The main challenge with open banking is customers who do not trust data sharing with third parties (Dong *et al.*, 2020). Dong *et al.* (2020) proposed using blockchain-based SSI to address this challenge where customers fully control their identities and data. Third parties should request customers' permission to access and use their data. Customer-sensitive data is stored off-chain, while insensitive data, such as public keys, are stored on-chain. Dong *et al.* (2020) proposed modifying the smart contract to manage the registry and recovery of customers. The default uPort recovery contract requires two to three witnesses, which Dong *et al.* (2020) viewed as a limitation since the customer may not have added any individuals or organizations to the account before it was lost, while in the case of registry, uPort does not mandate prerequisites, so customers can register themselves with a nickname. Dong *et al.* (2020) mandated providing a physical identity document, such as a passport, to the identity issuer to register the customer. If the physical identity is approved, the identity issuer

provides the customer with an identity credential. The uPort account of the customer is then activated. Dong *et al.* (2020) highlighted that the registration step, which includes verifying the physical identity, can be completed online or offline. However, the authenticity check was not highlighted in terms of proving that the person submitting the document is the document's owner or ensuring the document is genuine. Furthermore, the validity check after account activation was not addressed. Dong *et al.* (2020) highlighted that for the receiver to accept the credential shared, the receiver should trust the credential issuer.

Schlatt *et al.* (2022) proposed a generic framework to guide the design of blockchain-based SSI solutions for all e-KYC processes and initial design principles (DPs) through a DSR approach. The framework and DPs are derived through semi-structured interviews based on the current theoretical knowledge and experts' views. Schlatt *et al.*'s (2022) proposed architecture is an abstract of the one proposed by previous work (Soltani, Nguyen and An, 2018). It extends the framework by adding eIDAS to strengthen the KYC process and validates it through expert interviews. The architecture is built on W3C standards of DIDs and a VC data model.

Schlatt *et al.* (2022) defined six design objectives to be met by the blockchain-based SSI e-KYC framework: 1) the efficiency of the KYC process, including the digital processing of relevant documents end to end, the automation of manual processes and the standardization of e-KYC documents exchange; 2) regulatory compliance to avoid money laundering, which includes compliance to MLA, particularly the identification of customers, the risk associated with them and the storage of their records, the GDPR in term of the processing of data related to natural persons and eIDAS in specific electronic systems in term of means of identification and cross-border interoperability; 3) decentralization of data storage and workflows; 4) trust in

the terms of acceptance of KYC documents attested by banks, the ability to validate the documents and customer authenticity; 5) privacy in terms of data minimization during sharing of information and compliance with the “need-to-know” principle during which only the customer and relevant entities have access to the customer personal data and 6) the user experience, which includes simple experience, availability of different user interfaces, and backup, recovery and support. The framework was evaluated in two rounds by experts in KYC and SSI through interviews. The first round evaluated the design objectives, while the second evaluated the framework.

The proposed architecture did not fully address a few of its design objectives. Regarding efficiency, the proposed flow did not address the digitalization and automation of the first step of onboarding new customers. The suggestion was to submit the documents through traditional means that are manual and prone to errors and misconduct. Moreover, the defined processes did not consider potential changes to the initial documents submitted and their impact on subsequent onboarding. Furthermore, in terms of trust, 67% of the interviewed experts highlighted the challenge of establishing trust between banks and customer trust in terms of the confidentiality of their data. A governance framework is required to define the parties that need to be involved, their role, the issuance of credentials and the legal acceptance of credentials. In addition, 33% of the experts highlighted potential challenges that may result in case users are fully responsible for data storage and its administration. They will need to be educated about the importance of backup and recovery. Furthermore, no prototype was provided to demonstrate the user interface and its simplicity. Schlatt *et al.* (2022) highlighted the need for having a strong binding attribute between the VP and all the VCs it included but did not state the methodology to achieve it. Moreover, their proposed architecture did not

detail wallet provision and management, stating that the bank should provide or recommend it. Thus, the wallet, the user identity and the VCs would need a correlation to bind them.

Malhotra, Saini and Singh (2021) highlighted a few of the main gaps in the existing blockchain implementation specific to KYC: 1) the lack of regulatory-supported international standards to allow cross-country verification, 2) ID verification during the initial document validation phase, 3) the storage of data and scalability impact for on-chain data and the security and privacy impact for off-chain data and 4) the scalability of the network versus the security and privacy of data. According to the current literature, the second challenge related to initial identity verification is the most critical phase which is inefficient and inaccurate phase in KYC process. This could be considered the justification for focusing on the initial identity verification and confirms that the aim of this research, which is highlighted in Section 1.4, is in line with the needs and priorities of the domains which provide critical services such as financial domain.

3.3 Using Blockchain in Health Sector

The health sector is a critical domain for registering patients, updating medical records, accessing and sharing patient information and validating it. Patient information is registered in every hospital or clinic upon the patient visit, establishing an electronic medical record (EMR). However, similar to the banking domain, this information remains in the hospital. When the patient visits another hospital, the patient must register again. The patient and hospital do not have access to the previous EMR of the patient. Accessing a previous EMR is important for diagnosis and treatment plans in the health sector. The EMR is considered to have private information about the patient and the hospital and is mainly stored in the hospital's private local data store. From a government perspective, the EMR needs to be

monitored to find illegal medical procedures, while researchers need access to historical medical data to discover new treatments for existing diseases.

Different studies have proposed using blockchain to record and share patient information, given its characteristics of maintaining traceability and privacy. Shamsi, Khorasani and Shayegan (2020) proposed a KYC blockchain token to share COVID-19 health certificates. The framework models a patient or user who conducts a test, receives and shares the certificate, laboratories where the test is conducted and the certificate is issued and entities that require these certificates. Shamsi, Khorasani and Shayegan (2020) used a private blockchain network using Stellar for two main reasons. The first was the ease of use and efficiency to generate blocks, requiring about five seconds, while the Ethereum network requires 12–14 seconds, and Bitcoin takes ten minutes. The second reason was that it does not use an intensive mining process for its consensus algorithm, increasing efficiency while quickening data exchange. Shamsi, Khorasani and Shayegan (2020) proposed using off-chain data stores to register and store encrypted information about users, laboratories and entities. Subsequently, the on-chain storage is used to produce raw KYC tokens and exchange them with entities requiring medical information from the user. The blockchain is only used when the user wants to share information. The token is issued to the user's wallet with no information. Users who want to share information with an entity select it from a list of registered entities. The data hash is added to the token and registered in the blockchain upon selection. The receiving entity validates the information using the hash and retrieves the patient information from the off-chain storage. However, the proposed solution did not highlight the measures for ensuring the confidentiality and privacy of the off-chain data or its validity and integrity.

Azaria *et al.* (2016) proposed a solution to store and share EMRs focused on the challenge of fragmented, slow access to medical information to improve data quality and quantity for medical research. Azaria *et al.* (2016) proposed the usage of public Ethereum blockchain and smart contracts. The smart contract registers patient-provider relationships that associate a medical record with viewing permission and data retrieval instruction. Only the hash of the data is stored on-chain, while the actual EMR is stored off-chain within the medical provider. The provider can add a new record and associate it with the patient, while the patient can authorize sharing of records between providers. Patients are given a summary of their medical records by different providers. Azaria *et al.* (2016) stated that the smart contract in the proposed solution is used to implement any policy required by regulations or participation.

For example, a policy could state that an EMR can be shared upon approval of the patient and the medical provider. Three smart contracts are suggested in the proposed solution: 1) a registrar contract for registering the identity of participants in the blockchain and mapping them to their physical identity, 2) a patient-provider relationship contract responsible for defining the EMR data points and associated access permission identifying the medical provider holding the records and its associated patient, and 3) a summary contract that provides a summary of all current and previous patient-provider relationship contracts so that the patient can view all medical providers while providers can overview the patients they provide services to and the third party allowed to view patient data. Upon adding or modifying the patient-provider relationship contract, a notification can be provided to patients. While the prototype is promising, no details were provided about privacy and confidentiality of information storage and sharing and its compliance with privacy laws and regulations,

particularly the proposal to leverage public blockchain. This concept includes the identity data registered on-chain and the ability to view who is requesting to view patient information by another medical provider. Regulators and medical providers did not validate the proposed solution.

Fan *et al.* (2018) proposed using blockchain to access and retrieve EMRs of patient medical information across all participating hospitals. The proposed solution uses a hybrid consensus mechanism and submits requests by turns to be more efficient and reduce energy consumption and network congestion. Fan *et al.* (2018) also proposed a customized access control protocol and symmetric cryptography to increase the security and privacy of information. The proposed solution consists of 1) certificate authority (CA) to generate, distribute, and manage digital certificates as well as patients' public and private keys, 2) a user, a patient who visits a hospital and encrypts the medical information generated during the visit using a public key and signs using a private key and the hospital's private key so that the user can always retrieve the summary of past medical information stored on-chain and the detailed EMR with a private key; and 3) a processing layer with hospital servers and databases where each component plays a different role, such as a consensus node and committers that add blocks to the ledger to increase the efficiency of the system.

While the data encrypted and stored on-chain cannot be accessed unless the user has the private key, Fan *et al.* (2018) highlighted that the CA could use the patient's private key to decrypt data on-chain. However, they did not mention how it would be regulated, which could be viewed as not preserving individual privacy. Moreover, storing the summary of EMRs on-chain would grow the chain's size and impact its performance. The overall governance framework regarding onboarding and creating identities for participants, the information

storage, regulatory and privacy considerations and validations and information access by different parties was not addressed. Moreover, the solution did not detail the user's channels to store keys or access the EMR.

Soltani, Nguyen and An (2020) identified different requirements to be addressed for adopting SSI in the healthcare sector. They highlighted a few advantages and presented a use case involving various stakeholders. Hasan *et al.* (2020) conducted a study that focused on the potential of blockchain identity implementation in the healthcare domain and highlighted that a blockchain-based SSI solution is suitable when implemented in a standardized healthcare ecosystem that supports interoperability.

3.4 Using Blockchain in Digital Identity Management

A growing number of studies are exploring the usage of blockchain in IdM as well as decentralized identity and SSI with and without blockchain. For example, Rathee and Singh (2022) conducted a systematic literature mapping IdM using blockchain from 2009 to 2020. Thirty research papers were reviewed after applying various criteria. The study highlighted that 65% of the research was conducted after 2016. The amount of study in these years grew significantly, increasing by 100% for two sequential years. The study highlighted that 60% of the implementation were permissioned, while 40% were permissionless. The government sector prefers permissioned blockchain.

The study highlighted the advantages and challenges of blockchain implementations in IdM. The advantages included 1) improving security by removing the dependency on centralized authority and the need for a trusted third party; 2) improving trust through the immutable, distributed and decentralized nature of blockchain while ensuring that users and transactions are genuine and not modified; 3) improving the privacy through the hashes of the

addresses of the transactions, decentralized personal data management where users own and control their data, a decentralized computation platform with guaranteed privacy and a peer-to-peer cloud storage network; and 4) maintaining anonymity through mixing services, ring signature, non-interactive ZKF, blind signature and smart contracts, multiple input, change of addresses, associations with IP and using centralized addresses. In contrast, the blockchain challenges that should be addressed include scalability, interoperability, gas cost, data protection and authentication and data storage and replication. Privacy remains a challenge despite different research papers proposing on-chain and off-chain solutions.

Cucko and Turkanović (2021) conducted a systematic mapping study to provide a coarse-grained overview of decentralized and SSI studies and classify them based on specific parameters. The study also aimed to determine the nature and scope of the research and acquire insights into trends, demographics, challenges and gaps. The study included blockchain- and non-blockchain-based implementation between January 2013 and January 2021. The sources of these research papers were limited to two databases: IEEE Xplore and Science Direct. Cucko and Turkanović (2021) highlighted the exponential growth in the number of research papers on decentralized identity and SSI with or without blockchain, similar to the growth in the research papers related to blockchain usage in IdM (Rathee and Singh, 2022). The number of papers published from 2017 to 2021 grew by 96.7%. The initial years experienced the most growth. For instance, from 2017 to 2018, the growth was 83.3%, while it was 58.6% from 2018 to 2019. The US's contribution was 19.2%, the highest in the research field, followed by China at 13.3%, and the UK's and Germany's contributions at 11.7% each. Notably, the UAE contributed 3.3% (Cucko and Turkanović, 2021). The main

contributions of these research papers were in systems and solutions at 26.7%, architecture at 18.3% and frameworks at 18.3%.

Cucko and Turkanović (2021) distinguished the study on SSI from those on decentralized identity. There were 66.7% of papers related to SSI and 33.3% of papers related to decentralized identity. They also highlighted that these research papers proposed different levels of decentralization. For example, some studies proposed balancing centralization and decentralization by using a central server to store key pairs and identity attributes while mediating between participants. The use cases of identity implementations varied, with 24.2% in IoT, 8.3% in transport and smart vehicles, 7.5% in healthcare, 6.7% in banking and finance, 5.8% each in the government, retail and commerce, supply chain and industry and 0% in education. In addition, the topics of identity implementations differed with 18.3% in security, 15.8% trust, 13.3% in privacy, 0.8% in user experience and 0% in usability.

Hardman *et al.* (2019) reviewed five studies related to the usage of smart contracts in the field of decentralized identity with seven categories: IdM, record keeping, healthcare, supply chain, IoT, voting and BPM. Soltani, Nguyen and An (2020) and Hasan *et al.* (2020) conducted a survey specific to blockchain-based SSI solutions. Hasan *et al.* (2020) surveyed academics and industry with five categories: 1) data control and protection, 2) digital identity, 3) social insurance, 4) social data governance and 5) healthcare and patient data. They highlighted a few challenges regarding security and privacy, the lack of standard implementation methods, and the lack of proven real implementation, as current solutions were either in testing or beta stages.

Lucking *et al.* (2020) and Zhu and Badr (2018) analyzed existing blockchain-based IdM solutions that claimed to conform to SSI principles. Many of these solutions were

evaluated and compared based on the law of identity (Dunphy and Petitcolas, 2018; Lux *et al.*, 2020; Theodouli *et al.*, 2020) and SSI principles (Abraham, Theuermann and Kirchengast, 2018). The evaluation mainly technically highlighted differences, such as blockchain types, data storage, key management and GDPR compliance. SSI's key concepts and architecture were discussed, and the research gaps and challenges were highlighted. In addition, they compared existing solutions considering their features and compliance with GDPR principles, such as confidentiality, integrity, transparency, lawfulness and data minimization. Lux *et al.* (2020) evaluated and compared Sovrin, uPort and ShoCard based on Cameron's law of identity. Lux *et al.* (2020) also analyzed 50 papers and patents on blockchain-based IdM published between 2017 and 2020 in three main categories: authentication, privacy and trust. The research gaps and opportunities were identified and highlighted, as well as the challenges, such as identity wallet leakage and identity changes.

Dunphy, Garratt and Petitcolas (2018) systematically surveyed existing blockchain-based identity and access management solutions and developed an evaluation framework of 75 criteria to evaluate decentralized and SSI-based management systems. The total number of solutions analyzed and evaluated in detail using these criteria was 43. The criteria included end-user functionality, compliance, standardization and integration and regulation. Liu *et al.* (2020a) conducted another systematic survey of 30 research papers published between 2009 and 2020. The objective was to identify the research trends and challenges, analyze IdM frameworks, identify research projects and initiatives related to blockchain-based IdM and determine common consensus algorithms. The survey highlighted blockchain's potential to overcome traditional IdM systems' limitations.

SSI has been used in different countries. For example, Pöhn, Grabatin and Hommel (2021) studied the eID and SSI implementations within governments worldwide and highlighted the challenges faced and lessons learnt from these implementations. The study covered government eID implementations in 23 countries. The core lessons highlighted included the need for 1) developing solutions considering the ease of use from an end-user perspective and availability of services to accelerate user adoption, 2) designing the solution architecture to be as modular as possible to adapt to different integration models and technological changes, 3) providing information and documentation publicly to gain trust and acceptance and enable other entities to participate, 4) developing solutions considering the security and privacy aspects as the incidents of identity theft and data leaks have increased, 5) educating users about the importance of the eID and its usage and 6) providing simple identification for users to remember with different levels of assurance to avail services balancing between usability and security. Pöhn, Grabatin and Hommel (2021) studied SSI implementations in eight countries with non-profit organizations that implemented SSI with the government as a trust anchor. The focus was on implementations intersecting government-issued eIDs and SSIs. The study included unsuccessful projects, such as ZugID, “Blockchain on the Move” and the Brazil initiative. ZugID was a digital blockchain-based ID developed in Switzerland and implemented using uPort. Only 267 citizens had digital IDs at the end of the project. One of the core reasons for termination was the low adoption of users because only two services were available for the end user. The low availability of services was because developing them requires resources. Another challenge the ZugID faced was that the technology chosen for the implementation, uPort, was not maintained. This lesson is crucial to consider in future implementations. Since SSI is still in its initial stages, the velocity of change

is high. The implementation should be as technology-agnostic as possible. Moreover, the architecture should be modular to adapt to any changes. The “Blockchain on the Move” project was driven by the Flemish government and faced similar challenges in terms of a lack of manpower and financial resources leading to the withdrawal of the project. The government of Brazil collaborated with different alliances from the private sector to establish SSI projects and reduce the efforts, which did not lead to successful implementation. The review of projects in Europe and South Korea highlighted the need for amendments to laws, policies and regulations to increase the adoption of SSI solutions.

Pöhn, Grabatin and Hommel (2021) summarized the lesson learnt from an evaluation conducted under five main categories. The first category was the project and top management, including the need to have sufficient resources to onboard various services to bring more benefits for the end user, eventually leading to an increase in adoption. Moreover, having adequate resources within a project reduces the risk of knowledge loss that could lead to the ending of the project. In addition, having top management support, different business models and marketing could lead to project success.

The second category was technical factors. Technical choices in terms of protocol and technical components are key to increasing adoption by providing different integration options and sustaining the velocity of technology changes. An example of a protocol change is the change from SAML to OIDC. Regarding SSI, due to its evolving technology, choosing the best-fit solution should be considered. Based on the eID and SSI implementations within governments worldwide, the most common technologies are Hyperledger Indy and Aries, in addition to the implementation of the DID and VC standards using Ethereum blockchain (Pöhn, Grabatin and Hommel, 2021). Another three considerations of technical choice include

technical neutrality, modularity and offline support so that people without the internet can participate. Other technical factors to consider are the novelty of the technology, the legacy systems, integration options and the availability of documentation.

The third category is stakeholder management. The usability and benefits should be considered to increase user adoption. In the example of ZugID, users provided positive feedback to the election using the app; however, the benefits to the end user were low with only two services. In addition, providing incentives to join, such as free-of-charge usage, may encourage users and SPs to explore the possibilities. Transparency in terms of providing public information about the project, challenges the project faces and the reasons, and the next steps, including timelines, can help gain more trust from end users and SPs. The exchange of information and helping other countries could increase the level of eIDs and SSI maturity worldwide. Moreover, collaborating and having alliances could lead to successful projects and the possibility to expand to further regions in the future.

The fourth category is nonfunctional factors like security and privacy. From a security perspective, both system security and user education and awareness should be considered. From a privacy perspective, while SSI principles are centered on the user, legacy systems could impact their fulfillment. Indeed, a balance is required between security, privacy and adoption.

The fifth category is project-specific factors, which include identification, harmonization, trust and legislation. The identification needs to consider identity creation in SSI, identity association with VCs and regaining them if lost or destroyed. The process could follow the physical world in issuing new or replacement cards for lost identity cards.

Harmonization enables interoperability and expansion, while trust focuses on the confidence

between participants, which is usually achieved through different elements such as the Level of Assurance (LoA) and contracts. In SSI, trust can be established through centralized trust management, hybrid approaches integrating certificate authorities, the Web of Trust and consortia. Trust in the user can be established using robust vetting mechanisms for registration and authentication, such as biometrics. Schardong and Custódio (2022) conducted a rigorous systematic review and systematic mapping of the literature and theoretical and practical advances in SSI. The characteristics of the reviewed work have been mapped to taxonomies under conceptual and practical facets. These taxonomies cover core elements such as identity derivation, identity assurance, auditability, and backup and recovery. Identity derivation refers to method to derive SSI identity from non-SSI identity. This could ease the identity creation and increases the trust. Abraham *et al.* (2020) proposed using privacy-preserving eID to derive SSI identity. Bathen *et al.* (2019) and Mishra *et al.* (2019) proposed using biometrics to create a SSI identity. Finally, regulations must be up to date to support technological advancement.

Anthony (2022) conducted a study to understand the governance issues of DLT adoption. While these emerging technologies bring opportunities, they also change the way organizations conduct their business. Governance decision challenges need to be addressed in order to increase the adoption of DLT. Anthony (2022) presented governance factors that could lead to the acceleration of DLT adoption. These factors are economic factors related to allocation of incentives and cost incurred, technological factors related to interoperability and scalability, compatibility of smart contracts, and implemented consensus algorithms, and political factors related to GDPRs compliance failure, undistributed control structures, and absence of main control, and social factors related to specifying decision rights and openness issue.

3.5 Summary and Research Gaps

Studies on digital identity, decentralized digital identity and SSI have demonstrated growing interest and the potential to address different challenges in various domains, such as the financial sector and the KYC process. These studies have proposed using blockchain as a fundamental underlying technology due to its decentralization, integrity and reliability advantages. The studies have proposed different blockchain implementations and have tried to address different challenges required to increase the efficiency of the KYC process, such as the need to establish trust among banks, incentivizing and sharing the cost of KYC among banks, data storage, the privacy of the user data and the bank that conducted the KYC verification to be shared with other banks, governance with the need for central regulatory and user account recovery since in SSI the responsibility of key management relies on the user.

However, these studies have not included end-to-end digital processing and the automation of manual processes of the KYC for customer identification, where data about potential customers is collected to identify, verify and monitor them. These steps were either manual or not addressed, impacting the user experience and efficiency of the KYC process. Moreover, the research has not addressed the governance framework considering trust between the banks, trust in the digital credentials issuance ability to validate customer authenticity and the legal acceptance of the ecosystem and its proofs. There have been no prototypes presented to illustrate the simplicity of user experience.

Therefore, this thesis aims to address these gaps in the challenge related to initial identity verification. Hence, the lessons learnt from government implementations of SSI projects, the support from top management, technical factors including the technical choice,

security and privacy, establishing trust between participants and the changes required in regulations are considered.

Chapter 4: Research Design and Methodology

4.1 Introduction

The design is an essential structure of any scientific work as it provides direction to research. Research design is defined as a plan, structure, or blueprint of how the research is intended to be performed in order to address the research questions (Calmeyer *et al.*, 2011). The conceptual structure of investigation, methods of analysis, and procedures are established through the design reducing errors and enhancing the reliability of the results.

This chapter outlines the design of the research and rationalizes the methodology employed to address the research questions and fulfill the objectives and aim previously outlined in Chapter 1. It commences with an overview of the conceptual design framework aimed at tackling the research problem and accomplishing the research aim. The selected research methodology is introduced with a brief discussion of its historical roots and theoretical foundation. Subsequently, the appropriateness of the chosen methodology is justified, accompanied by a detailed exploration of its application within the context of this research. The chapter concludes by presenting the overall structure of the research design.

4.2 Conceptual Design Framework

In order to address the research questions mentioned earlier and achieve the research aim outlined in Sections 1.3 and 1.4, a conceptual design framework has been formulated. This framework seeks to bring forth an innovative method to improve the KYC process through a derived digital identity that can be verified independently in a govern environment. Figure 5 represents the conceptual design framework, illustrating the relationships among the research components which are context, elements, methods, and outcomes.

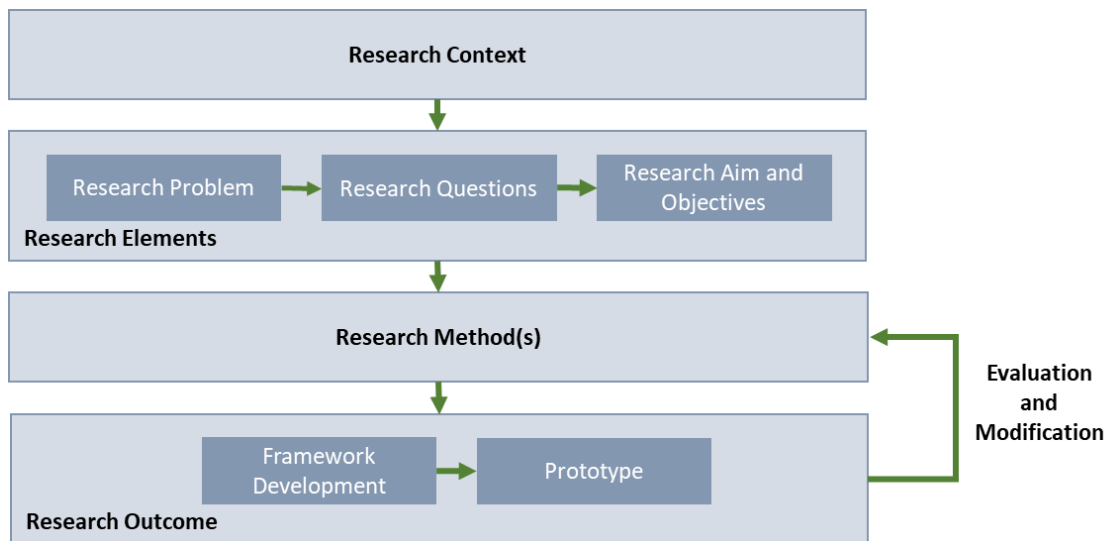


Figure 5: Conceptual Design framework

As depicted in the figure above, comprehending the research context and reviewing previous studies establishes the necessity and rationale for the forthcoming research. The research methodology outlines the approach for conducting this study. Formulating a research methodology to serve as the blueprint for the research process is a fundamental prerequisite for achieving the research outcomes. A methodology is a compilation of problem-solving methods guided by a set of principles and a shared philosophy for addressing specific problems (Checkland, 1999). It precisely explains the steps for accomplishing the research objectives and rationalizes the choice of method in alignment with those objectives (Ogwe, 2013). This research adopts the Design Science Research Methodology (DSRM), a widely utilized approach in engineering and information systems research. DSRM aims to generate new knowledge by designing innovative artifacts (Hevner *et al.*, 2004; Oates, 2006). It focuses on problem-solving (March and Storey, 2008) and aims to solve identified problems in a specific context or environment by creating and evaluating purposeful artifacts with a

practical impact to enable the transformation from the current state to the designed state (March and Smith, 1995; Hevner *et al.*, 2004; March and Storey, 2008).

The subsequent section provides more details about the theoretical foundation and historical evolution of DSRM, followed by a thorough discussion of its characteristics and primary steps.

4.3 Selection of Research Approach

In general, science can be categorized into two main types: empirical science and formal science, forming the basis for science classification. Formal sciences, such as Mathematics, involve deductive analysis of formal systems without direct application to nature or human beings (Löwe, 2002; Wazlawick, 2010). They focus on demonstrating or proving statements based on logical or mathematical principles, often without experimental confirmation. In contrast, empirical sciences investigate real-world phenomena, seeking to establish and understand facts, using observations as the basis for their discoveries (Bunge, 1967; Bunge, 1985; Wazlawick, 2010). Empirical sciences are further divided into natural sciences, which explore nature, and social sciences, which study human relationships and individuals (Dresch, Lacerda and Antunes, 2014).

Natural science aims to comprehend existing laws, known or unknown (Bergeå *et al.*, 2006; Simon, 1996). It encompasses research in physical, biological, and behavioral domains, aiming to understand and generate descriptive and analytical knowledge about observed facts. On the other hand, social sciences systematically study human society, including disciplines such as anthropology, economics, geography, history, political science, social studies, and sociology (Perry and Perry, 2015). The mission of both social and natural sciences is the pursuit of truth, describing, explaining, and predicting knowledge in their respective areas.

The objectives of social and natural sciences may not seamlessly align with dynamic contexts like engineering or architecture, which emphasize creation.

Engineering represents a branch of science with distinct objectives, primarily centered around problem-solving and practical guidance (Akkermans and Gordijn, 2006). Research in engineering aims to discover solutions to defined problems or create artifacts to efficiently accomplish specific tasks. Merely explaining a given situation may not suffice for advancing knowledge in applied fields like engineering. The imperative for research in designing and constructing artifacts emphasizes the requirement for a scientific approach that understands real world problems and offers applicable solutions (Simon, 1996). Consequently, the act of designing or proposing solutions to real-world problems can be regarded as a form of scientific research.

The concept of Design Science has emerged in response to calls from applied fields like engineering, medicine, information systems, and business management (Denyer, Tranfield and Aken, 2008; Simon, 1996; Wieringa, 2014). Design science balances between traditional scientific approaches and context-related problem-solving knowledge generated in real practical situations (Dresch, Lacerda and Antunes, 2014). The primary goal of Design Science Research (DSR) is to create artifacts as tools for solving real problems, distinguishing it from traditional natural sciences. A comparison of between natural, social, and design sciences is provided in Table 1.

Table 1 Comparsaion between natual, social and design sciences

Source: (Dresch, Lacerda and Antunes, 2014)

	Purpose	Research Goal	Applicable Areas
Natural Sciences	Comprehend complex phenomena, uncover their current state, and provide justifications for their existence.	Explore, describe, explain, and predict	Physics, chemistry, and biology.
Social Sciences	Describe, understand, and contemplate human beings and their actions.	Explore, describe, explain, and predict.	Anthropology, economics, politics, sociology, and history.
Design Sciences	Design and create systems, either entirely new or by enhancing existing situations, with a focus on delivering improved outcomes.	Prescribe solutions and address problems.	Engineering, information systems, medicine, and management.

The table above highlights strong alignment between design science and this research in term of scope and goals, making it an effective problem-solving approach to develop the framework needed to tackle the research problem. Consequently, this research adheres to the design science research paradigm. The Peffers *et al.* design science research methodology is employed in this research (Peffers *et al.*, 2007).

4.3.1 Design Science Research

4.3.1.1 Emergence of Design Science Research

The Design Science as a term was initially stated by R. Buckminster Fuller in 1963 (Fuller, Inventory and Architects, 1965). However, its importance grew in the late 1960s when Herbert Simon published "The Sciences of the Artificial" in 1969 (Simon, 1996). Simon, in this work, highlighted distinctions between natural science and design science, formulating the concept of Design Science Research (DSR) as intellectually rigorous, analytical, formalizable,

and teachable (Simon, 1996). Takeda *et al.* (1990) echoed Simon's ideas with a more applied perspective which influenced subsequent studies (March and Smith, 1995; Vaishnavi and Kuechler, 2009). These studies expanded the concept, particularly in the context of information technology and computer science. Nunamaker and Chen (1990) conducted a study focusing on research in design science within the information systems domain. Walls, Widmeyer and Sawy (1992), Gibbons *et al.* (1994), and Romme (2003) played crucial roles in advancing design science research. With the evolution of DSR in information technology, its interest extended to academic and industry researchers in diverse fields such as business and e-commerce, management, and accounting (Au, 2001; Van Aken and Romme, 2009; Geerts, 2011).

The adoption of Design Science Research (DSR) is widespread in various fields due to its enablement to balance research relevance and rigor. Hevner *et al.* (2004), published a paper that characterized the DSR paradigm and offered guidelines for its application in information systems (IS) research, which is considered to be the main contribution in the DSR. Subsequently, a growing number of research papers in the information system (IS) domain have adopted the DSR paradigm, referred to as information system design science research (ISDSR) as a feasible research method. Figure 6 presents a conceptual framework for

understanding, executing and evaluating ISDSR (Hevner *et al.*, 2004). In addition, Peffers *et al.* (2007) introduced a methodological framework that gained academic attention.

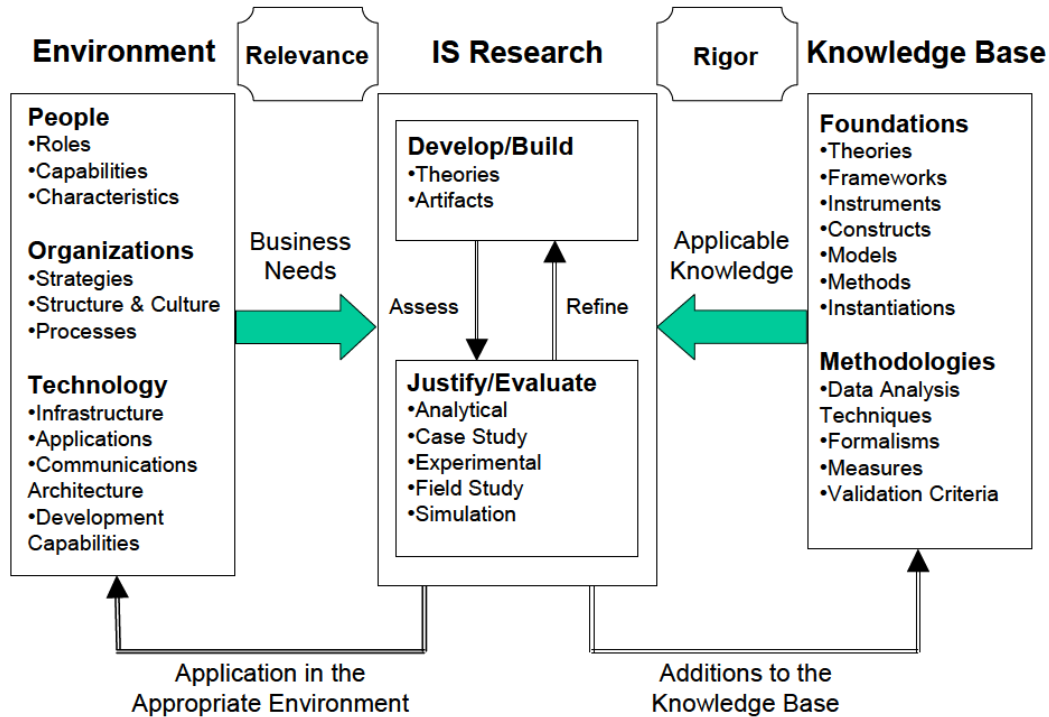


Figure 6: The ISDSR conceptual framework

(Source: Hevner *et al.*, 2004)

4.3.1.2 Design Science Research Paradigm

Design Science Research (DSR) is a form of research within a specific discipline that aims to generate innovative and useful artifact as an outcome of the research (Lukka, 2003; Aken, 2007). The artifact must be applicable in the corresponding environment in which it is trying to solve a business issue and should be built on previous IS research to ensure rigor in the design process (Hevner *et al.*, 2004; Brocke *et al.*, 2020). Peffers *et al.* (2007) describes artefacts as "designed objects with an embedded solution to an understood research problem.". There are four categories of artifacts which are constructs, models, methods, and instantiations (March and Smith, 1995). Algorithms, representing formal logical instructions, fall into the

classification of methods, while tangible hardware or software realizations are designated as instantiations (Peffer *et al.*, 2007). Table 2 illustrates the various types of artefacts in DSR.

Table 2: Artifact Types

Artifact Type	Description
Construct	Set of statements that describes a concept (a problem within a domain and its solution)
Instantiation	Implementation of an artifact within its environment that operationalize constructs, models, and methods in form of system hardware or software
Method	Set of instructions which are actionable not algorithmic
Model	Set of statements that expresses relationships between constructs

This thesis develops artifacts of two different types which are model and instantiation as part of the Digital Trust Framework. These artifacts are considered as specific type of information system (IS) artifacts. The architecture and process artifacts of the Digital Trust Framework are of type model, while the prototype is of type instantiation. All the artifacts that are generated based on IS research should be rigorous and relevant (Hevner *et al.*, 2004). Relevance implies that the artifact must effectively address significant business challenges, while rigorousness implies that the artifact must provide unique and innovate solution to contribute to the knowledge base. This thesis develops artifacts through a rigorous research process in order to satisfy these criteria.

Design disciplines build knowledge base through a continual build and evaluate process of the artifact to validate its performance. Takeda *et al.* (1990) published one of the early publication that aims to analyze and present the steps of general design cycle in order to formalize an approach to conduct a design science research. Figure 7, demonstrates the general design cycle.

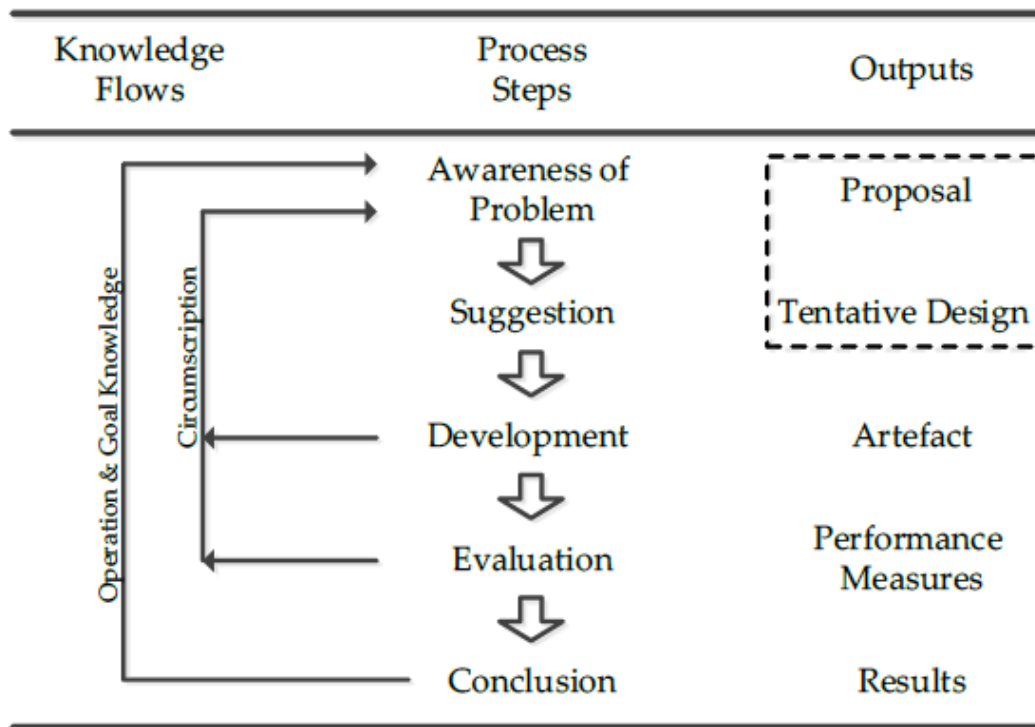


Figure 7: Design Cycle Process

(Source: Takeda et al. 1990)

In the model of the design cycle, the process initiates with an Awareness of a problem, involving the identification of an issue through a comparison of the considered object with specifications. The first phase output is a problem description and proposal of a research plan. The subsequent phase, Suggestions for a problem solution, introduces concepts to assist researchers in addressing the identified problem. Initial suggestions are derived from existing knowledge through abduction (Vaishnavi and Kuechler, 2009). The output of this stage is one or more Tentative Designs aimed at resolving the previously defined problem. In the Development phase, one or more artifacts are constructed using different techniques based on the nature of the artifacts being created (Manson, 2006).

In the Evaluation phase, successfully developed artifacts are tested and performance measures for the artifacts are identified and calculated. These performance measures gauge the effectiveness of the artifact in solving the identified problems (Manson, 2006). Evaluation constitutes a critical aspect of design science research (Hevner *et al.*, 2004). In the Conclusion step, research results are analyzed, consolidated, and documented. Furthermore, the insights gained from all phases of the research are synthesized, and the research's contribution to the identified problems is justified (Takeda *et al.*, 1990).

The Development, Evaluation, and further Suggestions are iterative processes in design science research as illustrated in figure 7. This iterative nature is symbolized by Circumscription, signifying an understanding achieved through the specific act of construction (Vaishnavi and Kuechler, 2009). The arrows labeled "Circumscription" and "Operation and Goal Knowledge" represent pathways of generating new knowledge (Takeda *et al.*, 1990).

Hevner *et al.* (2004) introduced guidelines for design science researchers; however, the model did not include a process flow and sequence of activities that is sufficiently detailed to be followed. Peffers *et al.* (2007) addressed this gap by proposing a method for conducting research under the design science paradigm by synthesizing selected literature. The next section outlines an overview of this method, known as Design Science Research Methodology (DSRM).

4.3.2 Design Science Research Methodology

Peffers *et al.* (2007) propose the Design Science Research Methodology (DSRM) as a sequential process model for conducting design science research. The process consists of six activities, which are (1) problem identification and motivation, (2) definition of solution

objectives, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication as illustrated in figure 8. While this process is sequential, researchers are not required to strictly follow the sequence from Activity 1 to Activity 6 (Peppers *et al.*, 2007). The process can follow an iterative research procedure by design, which assists in refining the problem identification or solution design based on the feedback from the environment or knowledge base. The activities can be conducted by the researcher alone or in collaboration with experts or practitioners, which assists in reducing the gap between research and the business environment. The process combines different qualitative and quantitative research methods in IS studies. The DSRM aims to achieve three objectives: (1) aligning with prior literature, (2) presenting a standard process for conducting design science research, and (3) providing a conceptual model for presenting and evaluating design science research, especially in the information systems domain. DSRM aims to maintain consistency with the foundational principles of design science research proposed by previous researches, with a focus on enhancing the production, presentation, and evaluation of design science research (Nunamaker and Chen, 1990; Walls, Widmeyer and Sawy, 1992; Hevner *et al.*, 2004; Cole *et al.*, 2005).

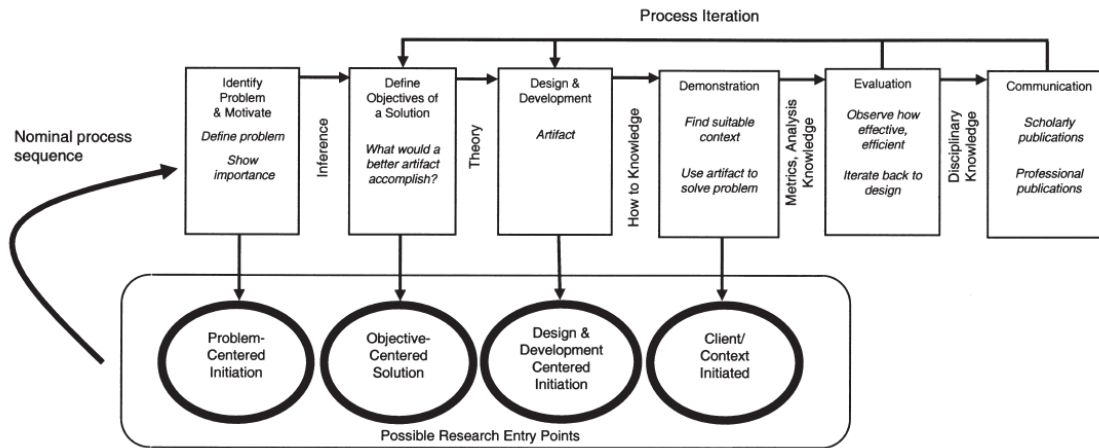


Figure 8: DSRM Process

(Source: Peffers et al, 2007)

As illustrated in figure 8, the first activity of the DSRM “problem identification and motivation”, which identifies a problem with practical relevance (Benbasat and Zmud, 1999; Rosemann and Vessey, 2008) and maps to the research questions related to a business problem, a need to increase business process efficiency or an opportunity offered by new technology. Moreover, the problem defined in this activity should be related to IS research and of interest to more than one entity (Benbasat and Zmud, 2003). Justifying a solution serves two purposes. The first motivates the researcher and the audience to pursue the solution and accept the outcomes. The second is helping to comprehend the reasoning behind the researcher’s understanding of the problem. This activity requires knowledge of the current state of the problem and an understanding of the significance of finding a solution. During the “problem identification and motivation” activity, the state of the art of the specific topic or problem is analyzed through a literature review covering possible obstacles and difficulties surrounding its solution. In addition, researchers using the DSR approach are encouraged to build on previous DSR concepts in the respective domains (Brocke et al., 2020).

The second activity of the DSRM is “establishing solution objectives”, where the objectives of the solution are inferred based on the problem definition and knowledge of what is feasible to create meaningful artifacts. Dresch, Lacerda and Antunes (2014) term this stage as the "definition of expected results." This activity aims to address the question of "How should the problem be solved?" and articulates the criteria that the proposed solution must fulfill in resolving the identified problem (Peppers *et al.*, 2007). The objectives can be quantitative or qualitative, reflecting desired improvements or addressing previously unaddressed problems logically derived from the problem specification. The knowledge of the current state of problems, existing solutions (if any) and their effectiveness is required to define the objectives. The defined problem and objectives must be generalized to be applicable in a more generic setting to be relevant to more entities (Jones and Gregor, 2007).

The third activity of the DSRM is “design and development”, where an IT artifact is created as the solution by incorporating a research contribution within its design. This activity involves defining the artifact’s desired functionality and architecture and creating the actual artifact, requiring reviewing the relevant literature related to the solution. The literature review in this activity focuses mainly on scientific publications. The research rigor must be ensured by leveraging the existing knowledge, including the state of the art. Hevner and Gregor (2022) stated that the IT artifact design should profoundly disturb how the business traditionally operates.

The fourth activity of the DSRM is “demonstration” in which the uses of the artifact to solve one or more instances of the problem demonstrated, involving experimentation, simulation, case studies and proofs, among other appropriate activities. Effective knowledge of how to utilize the artifact for problem-solving is required for the demonstration.

The fifth activity of the DSRM is “evaluation” in which the degree of the effectiveness of the artifact in solving the problem is observed and measured. Once the solution design is sufficiently developed, the evaluation phase can be initiated. The evaluation phase is important in testing if the IT artifact achieves its development objective using rigorous methods (Venable, Pries-Heje and Baskerville, 2012). This activity compares the solution objectives with the actual results of using the artifact in the demonstration and requires knowledge of relevant metrics and analysis techniques. Evaluation can take different forms depending on the problem venue and the artifact, including comparisons, quantitative performance measures, user feedback and simulations. At the end of the “evaluation” activity, researchers can decide whether to iterate back to Activity 3 for further improvement or proceed to communication, depending on the feasibility and necessity of iteration in their research context (Peffer *et al.*, 2007).

The last activity of the DSRM is “communication”, where the artifact, its utility, novelty, design rigor and effectiveness to researchers and relevant audiences are communicated effectively. Communication can take the form of scholarly research publications or other suitable means of dissemination.

Evaluation is a critical aspect in Information Systems Design Science Research (DSR) and it is not limited to the Evaluation activity. It can be embedded within each activity of the DSRM. However, there is lack of comprehensive guidance on selecting and designing an appropriate evaluation strategy. Pries-Heje, Baskerville and Venable (2008) introduced a 2-by-2 framework for DSR evaluation strategies, offering insights on considerations for choosing among them. The framework encompasses two dimensions: the contrast between artificial and naturalistic evaluation, and ex ante versus ex post evaluation. Artificial evaluation involves

methods like laboratory experiments, field experiments, simulations, criteria-based analysis, theoretical arguments, and mathematical proofs. On the other hand, naturalistic evaluation explores the performance of a solution technology in its real organizational environment, embracing the complexities of human practice. Naturalistic evaluation is empirical and may adopt interpretive, positivist, and/or critical approaches. Methods of naturalistic evaluation include case studies, field studies, surveys, ethnography, phenomenology, hermeneutic methods, and action research. The dominance of the naturalistic paradigm brings stronger internal validity to naturalistic DSR evaluation. Ex ante evaluation is performed on an uninstantiated artifact, such as a design or model while, Ex post evaluation is performed on an instantiated artifact (i.e. an instantiation).

Venable, Pries-Heje and Baskerville (2012) enhanced the existing DSR Evaluation Strategy Framework proposed by Pries-Heje, Baskerville and Venable with three additions (Pries-Heje, Baskerville and Venable, 2008). The first part of the extended framework maps contextual aspects of DSR evaluations, such as resources, purpose, goals, and priorities, to the dimensions and quadrants of the Pries-Heje, Baskerville and Venable DSR Evaluation Strategy Framework as illustrated in table 3.

Table 3: DSR Evaluation Strategy Selection Framework

(Source: Venable, Pries-Heje and Baskerville 2012)

DSR Evaluation Strategy Selection Framework	Ex Ante	Ex Post
	Formative Lower Build Cost Faster Evaluate design, partial prototype or full prototype Less risk to participant	Summative Higher build cost Slower Evaluate instantiation Higher risk to participant

		Higher risk of false positive	Lower risk of false positive
Naturalistic	Diverse Stakeholders Substantial conflict Socio-technical artifacts Higher cost Longer time Access to organization is required Artifact effectiveness evaluation Desired Rigor “Proof of Pudding” Higher risk to participant Lower risk of false positive	Real users, real problems and somewhat unreal system Low to medium cost Medium speed Low risk to participants Higher risk of false positive	Real users, real problems and real system High cost Highest risk to participants Best evaluation of effectiveness Identification of side effect Lowest risk of false positive
Artificial	Few homologous stakeholder Little or no conflict Technical Artifact Low cost Less time Desired Rigor “Control of Variable” Artifact efficiency evaluation Less risk during evaluation Higher risk of false positive	Unreal users, problems and system Lowest cost Fastest Low risk to participants Highest risk of false positive	Real systems, unreal problems and possible unreal users Medium to high cost Medium speed Low medium risk to participants

The second part maps the selected DSR evaluation strategy or strategies to relevant research methods for conducting evaluations as illustrated in table 4. The third part outlines a four-step method for designing evaluation components in a DSR project. This new framework and method aim to assist DSR researchers, especially those new to the field, in enhancing the efficiency and effectiveness of their DSR evaluation activities. It aids in identifying an appropriate DSR evaluation strategy or combination of strategies and supports decision-making on the most suitable evaluation method(s) to achieve those strategies.

Table 4: DSR Evaluation Method Selection Framework*(Source: Venable, Pries-Heje and Baskerville 2012)*

DSR Evaluation Method Selection Framework	Ex Ante	Ex Post
Naturalistic	• Action Research • Focus Group	• Action Research • Case Study • Focus Group • Participant Observation • Ethnography • Phenomenology • Survey (Qualitative or Quantitative)
Artificial	• Mathematical or logical proof • Criteria based evaluation • Lab experiment • Computer Simulation	• Mathematical or logical proof • Lab experiment • Role Playing Simulation • Computer Simulation • Field Experiment

March and Smith (1995) introduced criteria for DSR evaluation based on the artifact type, applicable in both ex ante and/or ex post evaluations, as depicted in Table 5. Sonnenberg and Brocke (2012) puts principles for evaluating DSR artifacts that not only assess the artifact's utility but also evaluate the design decisions made during its construction. To formulate evaluation patterns, a comprehensive understanding of the purpose and scope of individual evaluation activities in DSR is essential. The nature of these activities, along with potential evaluation criteria and methods, is summarized in Table 6 (Sonnenberg and Brocke, 2012). The following section provides details on the process of adopting DSRM in this thesis as well as the research design details.

Table 5: Evaluation criteria for DSR artifacts*(Source: March and Smith, 1995)*

	Construct	Model	Method	Instantiation
Completeness	X	X		
Ease of use	X		X	
Effectiveness				X
Efficiency			X	X
Elegance	X			
Fidelity with real world phenomena		X		
Generality			X	
Impact on the environment and on the artifact's users				X
Internal consistency		X		
Level of detail		X		
Operationality			X	
Robustness		X		
Simplicity	X			
Understandability	X			

Table 6: DSR evaluation activities and evaluation criteria*(Source: Sonnenberg and Brocke 2012)*

Activity	Input	Output (mandatory)	Evaluation Criteria (exemplary)	Evaluation Methods (exemplary)
Evaluation (1)	Problem statement/ Observation of a problem Research need Design objectives Design theory Existing solution to a practical problem	Justified problem statement Justified research gap Justified design objectives	Applicability, suitability, importance, novelty, (economic) feasibility	Literature review, review of practitioner initiatives, expert interview, focus groups, survey
Evaluation (2)	Design specification Design objectives Stakeholders of the design specification Design tool/ design methodology	Validated design specification Justified design tool/ methodology	Feasibility, accessibility, understandability, clarity, simplicity, elegance, completeness, level of detail, internal consistency, applicability, operationality,	Mathematical proof, logical reasoning, demonstration, simulation, benchmarking, survey, expert interview, focus group
Evaluation (3)	Instance of an artifact (prototype)	Validated artifact instance in an <i>artificial setting</i> (proof of applicability)	Feasibility, ease of use, effectiveness, efficiency, fidelity with real world phenomenon, operationality, robustness, suitability	Demonstration with prototype, experiment with prototype, experiment with system, benchmarking, survey, expert interview, focus group
Evaluation (4)	Instance of an artifact	Validated artifact instance in a naturalistic setting (proof of usefulness)	Applicability, effectiveness, efficiency, fidelity with real world phenomenon, generality, impact on artifact environment and user, internal consistency, external consistency	Case study, field experiment, survey, expert interview, focus group

4.4 Research Design

This section explains how the research incorporates DSRM components to fit its framework and shape the research design. It also shows how the research design phases, objectives, and thesis chapters are related. Figure 9 illustrates how the DSRM is adapted to structure the research design.

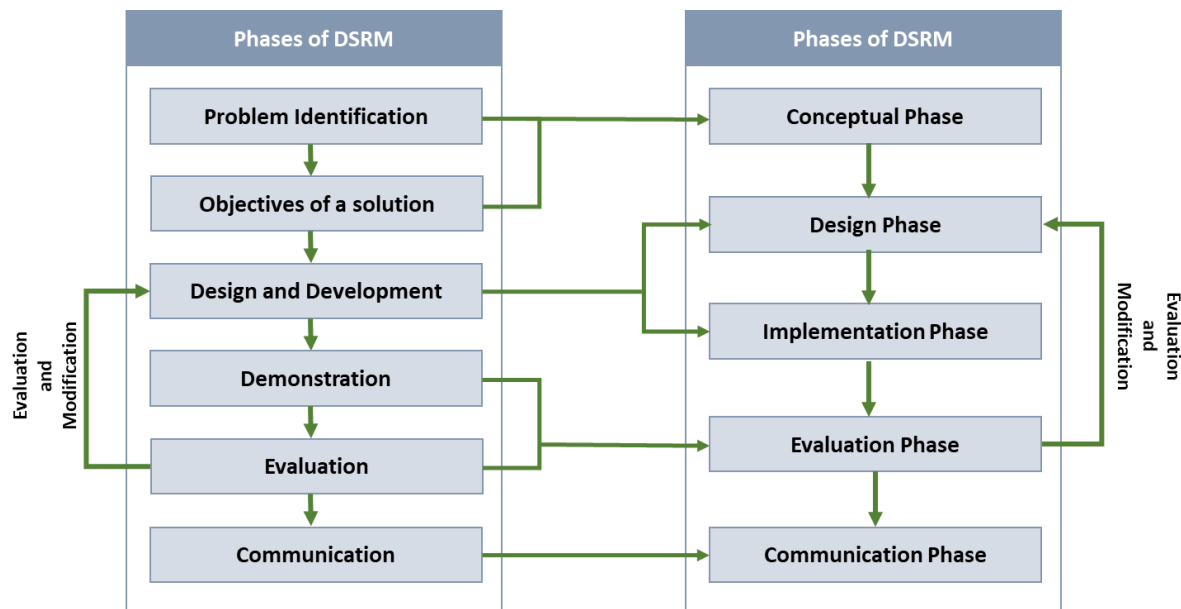


Figure 9: Adaption of DSRM for research design

As seen in Figure 9, the research design's phases are based on components from the Design Science Research Methodology (DSRM). Compared to Peffers *et al.*'s DSRM model, the research design combines "problem identification" and "objectives of a solution" to "conceptual phase", while the "design and development" phase in DSRM is split into two phases in the research design: the "design phase" and the "implementation phase." (Peffers *et al.*, 2007). After the "implementation phase," the research design combines the DSRM's "demonstration" and "evaluation" phases to form the "evaluation phase." Lastly, the DSRM's

"communication" phase is directly integrated into the research design as its final step. Figure 10 depicts the relationship between research phases, objectives, and thesis chapters, followed by a detailed discussion on each phase's methods in the research design.

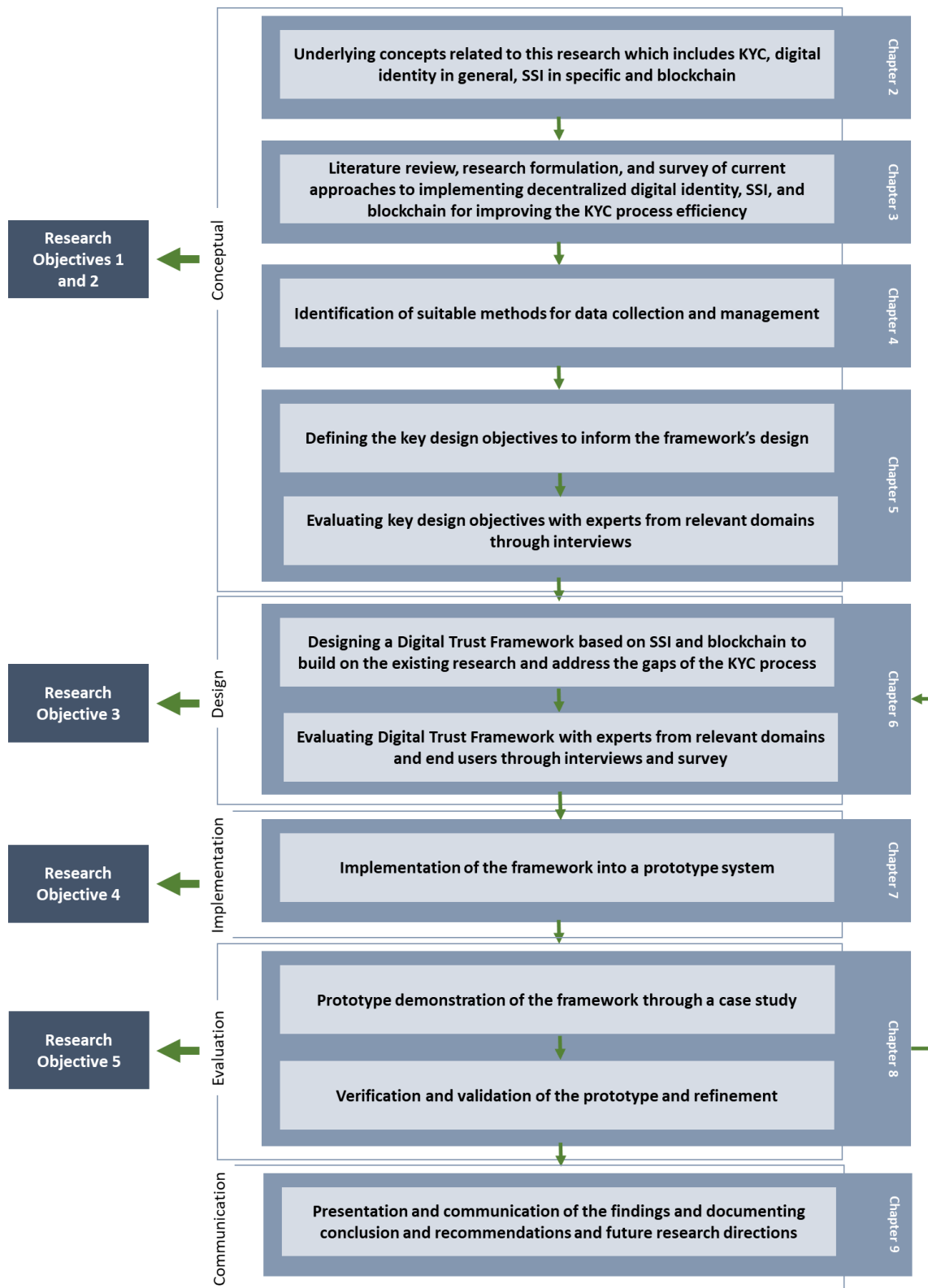


Figure 10: Research Design

4.4.1 Conceptual Phase

4.4.1.1 Understanding underlying Concepts

In order to be able to build artifacts that solve business challenges, it is important to understand fundamental concepts related to business as well as the state of art of technologies. This thesis conducted a detailed review on the multidisciplinary domains and the intersection between them. These domains include the KYC process, regulation, data privacy in general and the UAE in specific, and technological concepts of digital identity, SSI and blockchain. The KYC process is defined and the implications of it in two key domains, which are financial and telecom, are highlighted. The challenges of the KYC process from the perspectives of customers, financial institutions and regulators are also described. The digital identity been one of the cores technical elements of this thesis is also been defined and its characteristics and principles are highlighted with emphasis on SSI. The design patterns of SSI are described serving as baseline of artifacts implementation in this thesis. Since blockchain can play an important role in realizing SSI, this thesis describes its key characteristics, properties, types of implementations, use cases and challenges. Moreover, privacy principles are highlighted to ensure the artifacts design and implementation adheres to them.

4.4.1.2 Literature review, research formulation, and survey of current approaches

A literature review is a comprehensive and critical synthesis of a subject area, aiming to facilitate the identification of specific research questions (Bolderston, 2008; Rowley and Slack, 2004). It serves as a valuable foundation for exploring new research topics (Seuring and Müller, 2008). In addition, researchers using the DSR approach are encouraged to build on previous DSR concepts in the respective domains (Brocke et al., 2020). In line with these definitions, a thorough literature review has been conducted to pinpoint existing problems

within KYC process which includes inefficiency during the initial verification phase, the lack of ongoing verification after the initial KYC, regulatory compliance, privacy and user experience. Once these issues were identified, the literature review examines the potential role of decentralized digital identity, SSI, and blockchain in addressing the challenges. Studies on digital identity, decentralized digital identity and SSI have demonstrated growing interest and the potential to address different challenges in various domains, such as the financial sector and the KYC process. These studies have proposed using blockchain as a fundamental underlying technology due to its decentralization, integrity and reliability advantages. The literature review also examined current approaches to utilizing SSI based blockchain in the context of KYC process optimization as well as eID and SSI implementations in governments worldwide, highlighting lessons learnt. In addition, different principles and laws such as DPs, SSI principles, the law of identity, PbD principles and privacy laws in the UAE and internationally were reviewed. Various sources, such as books, journal articles, conference proceedings, technical reports, government publications, and web content, were utilized for the literature review phase. The outcomes of this review were presented in the preceding chapter, and the research questions were formulated based on the summary of the literature review.

4.4.1.3 Define the key design objectives

The solution objectives are defined by examining the relevant literature and regulatory guidelines pertaining to the KYC process, digital identity and blockchain. They aid in specifying the requirements of the framework. These objectives are further refined into eight key areas to be addressed by the Digital Trust Framework, each with specific requirements. The objectives and requirements are described in detail in Chapter 5.

4.4.1.4 Evaluate the key design objectives

In order to ensure that the design objectives are justified they need to be evaluated. As per the DSR evaluation activities and criteria that were illustrated in table 6, the design objective can be evaluated through expert interviews and focus groups. The evaluation criteria could be applicability, suitability, importance, novelty, (economic) feasibility (Sonnenberg and Brocke, 2012). Moreover, the defined problem and objectives must be generalized to be applicable in a more generic setting to be relevant to more entities (Jones and Gregor, 2007) by evaluating these objectives with experts from different organizations and experts in the form of interviews and focus groups. Qualitative interviews are frequently used IS research method to generate rich data (Myers and Newman, 2007). A qualitative research method is considered suitable for exploratory studies as it assists in defining the challenges that need to be addressed or considered in-depth and accurately (Maramba, Chatterjee and Newman, 2019).

This thesis conducted six individual one-on-one interviews to identify the problem's relevance and evaluate its hypotheses with experts from different backgrounds, locally and internationally. The aim was to generalize the problem to make it relevant to more entities to serve as a Digital Trust Framework on a national level serving different domains and on an international level in the future. The interviews were semi-structured to ask appropriate follow-up questions when required (Kallio *et al.*, 2016). The hypothesis was defined as utility theory (Chatterjee, 2006): "Using blockchain-based SSI implementation in the KYC process increases its efficiency, saves costs and improves the customer experience". Table 7 summarizes the methods used to validate the problem identification and the objectives' relevance and completeness.

The interviewed experts represented real environments covering different expertise and organizations. The main focus was on experts with KYC and SSI knowledge representing banking and financial institutions, government authorities and technology firms. Involving experts from different entities assisted in generalizing the problem while helping avoid bias (Myers and Newman, 2007). The main objective of the interviews was to validate the hypotheses and the defined objectives and understand any pre-assumption required to support the objective from a practical applicability perspective in the existing environment, with technical maturity and feasibility. The selection of the experts was based on defined criteria, including in-depth knowledge of the domain, thorough experience in their job and the ability to provide detailed information in their domain of expertise (Morse, 1991). The total minutes spent on this activity with experts was 280. The interviews were recorded, transcribed and later analyzed. The interview results appear in Chapter 5.

Table 7: Participating experts' details in evaluating the problem and the objectives

ID	Collaboration Methods	Expertise	Role	Entity	Background	Duration
A	One-on-one	Blockchain and SSI expert (International)	Executive	System Integrator A	Complex IT systems, including blockchain in the financial sector in the UAE and internationally	50 minutes
B	One-on-one	IT solutions in the financial sector in compliance with the KYC process	Executive	Bank A	Complex IT systems in the financial sector worked in leading local banks in the UAE	38 minutes
C	One-on-one	Digital government strategy and implementation	Director	Government A	Overseeing digital government transformation initiatives, which includes systems and policies in the UAE with in-depth knowledge of digital identity and digital signature	60 minutes
D	One-on-one	Blockchain and SSI expert	Chief Technical Architect	System Integrator B	Managing technical implementations of mission-critical government systems in the UAE	45 minutes
E	One-on-one	Financial KYC compliance	Manager	Bank B	Compliance, financial crime risk, sanctions and AML in leading UAE local banks and international banks in different countries	34 minutes
F	One-on-one	Blockchain and SSI expert (International)	Executive	System Integrator C	Digital and IT strategy, transformation and innovation programs in international consulting firms with in-depth knowledge of blockchain	53 minutes

4.4.2 Design Phase

The design phase involves formulating the overall structure of the artefacts, where a framework is crafted by integrating the challenges and findings identified during the conceptual phase. This phase directly addresses research objective 3 and sets the groundwork for addressing research objectives 4 and 5 in the subsequent implementation and evaluation phases. It aids in outlining the artifacts of the Digital Trust Framework, which consists of architecture, processes and a user experience prototype of a Digital Wallet application. The framework is defined in detail yet designed with flexibility, allowing for the incorporation of various mechanisms and solutions during the implementation phase. In this thesis, design phase was conducted iteratively to better understand the problem and improve the solution (Hevner *et al.*, 2004). The models that have been designed as part of the Digital Trust Framework, which are the architecture and processes, have been evaluated by Experts through interviews and focus groups. The models are considered as Ex Ante and evaluating them through a naturalistic setting is the most suitable strategy as highlighted in table 3. Sonnenberg and Brocke (2012) and Venable, Pries-Heje and Baskerville (2012) have highlighted that expert interview and focus groups are appropriate evaluation methods for models during the design phase. While Digital Wallet application user experience prototype could be considered as instance of an artifact (prototype) and it can be evaluated in the form of a digital survey by citizens.

4.4.2.1 Designing the Digital Trust Framework

The Digital Trust Framework streamlines the KYC process using blockchain's decentralized features. It meets regulatory needs, providing an audit trail and independent verification. This ensures legal certainty in digital identification, aligning with privacy laws

and empowering users to manage their identities. The solution architecture leverage Blockchain and digital signatures using public-key cryptography to establish trust in the Digital Trust Framework. The design of the solution architecture is based on the SSI design patterns defined by Čučko, Keršič and Turkanović (Čučko, Keršič and Turkanović, 2023). The processes of the Digital Trust Platform were defined as general processes that can be applied to any KYC process. Financial KYC is detailed as an example of a single use case. In addition, a user experience prototype of a mobile digital wallet was designed to address the requirements of design objective 6 related to the user experience. The term 'user experience' encompasses various meanings, spanning from conventional usability to aesthetic, pleasurable, emotional, or experiential aspects of technology use (Hassenzahl and Tractinsky, 2006). A user experience prototype centers on the dynamic interaction between humans and the overall interface of a system or product, primarily employed to facilitate user-focused research. No former research papers had an end-user prototype designed and presented.

4.4.2.2 Evaluate the Digital Trust Framework

The IT artifacts which are the architecture and processes of the Digital Trust Framework were evaluated for functionality, completeness, accuracy, reliability, usability and fit within the organization (Hevner *et al.*, 2004) using a criteria-based assessment to determine whether the solution objectives were fulfilled. Establishing evaluation criteria specific to the environment was essential to assess the IT artifact (March and Smith, 1995). Sonnenberg and Brocke (2012) highlighted that design specification should be evaluated in term of being understandable and meaningful to all relevant stakeholders.

The initial model design was evaluated with two major banks, a financial regulatory and a digital government, through focus group sessions in real context settings. The

architecture and prototypes were demonstrated to the interviewees. The insights from these sessions were used to refine the design of the solution. The sessions focused on regulatory compliance and user experience. Once the model reached a concrete state, it was also evaluated by an additional financial institution and telecom regulator to ensure its applicability to more entities, domains and general settings. The total number of minutes spent in this activity with experts, in one-on-one interviews and focus groups, was 1,253. Table 8 summarizes the expert interviews and focus group sessions to evaluate the IT artifacts. The interviews were recorded, transcribed and later analysed. The results are described in Chapter 6.

Table 8: Participating experts' details in evaluating the IT artifact

ID	Collaboration Methods	Expertise	Role	Entity	Background	Duration	Audience
G	One-on-one	Financial KYC compliance	Executive	Bank B	Financial crime risks at onboarding clients, screening and monitoring of portfolio and transactions working in a leading local bank in the UAE	30 minutes	1
H	One on one	Blockchain and SSI expert	Lead Technical Architect	System Integrator B	Delivering technical implementations of mission-critical government systems in the UAE	98 minutes	1
I	One on one	Digital government policies	Director	Government A	Government laws, policies and regulations related to digital transformation in the UAE with experience in PKI, digital identity, digital signature and data protection	45 minutes	1
1	Focus group	Financial KYC, business, compliance and IT	Executives Managers	Bank B	Developing and validating the KYC process in a leading bank in the UAE and international banks	120 minutes	6
2	Focus group	Financial KYC experts	Executives Managers	Bank C	User research, business and technical experts in the development of financial systems working in a leading bank in the UAE with previous experience in international banking systems	420 Minutes	6
3	Focus group	Financial KYC experts	Executive Managers	Bank D	Compliance, business and technical experts in the development of financial systems working in a leading bank in the UAE with previous experience in international banking systems	120 minutes	7

4	Focus group	Financial regulation	Directors Specialist	Government A Government B	Government financial KYC regulation and government digital identity and digital signature program in the UAE	180 minutes	3
5	Focus group	Telecomm regulation	Directors	Government A Government C	Government telecommunication KYC compliance and government digital identity and digital signature program in the UAE	120 minutes	2
6	Focus group	Digital identity and security	CEO Executive Director Directors	Government A Government D Government E	Implementation of government digital transformation initiatives such as digital identity and information security compliance	120 minutes	4

In addition, the user experience prototype was evaluated by the end users of financial services through concept testing, assessing the viability, attractiveness, and potential success of a new product before its actual development (Wind, Mahajan and Cardozo, 1981; Schwartz, 1987). It employs research techniques such as A/B testing, surveys and customer interviews to place the potential user at the forefront of the ideation process. Concept testing aims to gather users' insights and feedback to determine the product concept's feasibility and desirability (Wind, Mahajan and Cardozo, 1981; Schwartz, 1987). Based on research by Harvard Business School, approximately 95% of new products fail (Nobel, 2011). Concept testing assists in understanding user feedback early on.

The end user is the main beneficiary and key stakeholder in the KYC process. The concept testing ran as unmoderated testing in the form of a survey. A brief about the concept was provided to users to give them sufficient context about the product. Users were also provided with an interactive prototype to explore core functionalities. After that, users were asked to answer a mix of open-ended and closed questions, including demographics for customer segmentation, concept validation questions and security- and privacy-related questions to measure the trust and willingness to use the application. The factors considered part of concept validation were uniqueness, appeal, likeability, believability, relevance and assessing needs.

Uniqueness determines if the concept stands out from existing solutions. Appeal measures attractiveness compared to similar products. Likeability measures positive or negative reactions. Believability determines if respondents trust the outcomes. Relevance validates the concept's alignment with consumer needs. Assessing needs helps determine demand.

The survey included open-ended questions to uncover strengths and weaknesses in the concept. It was sent to an approachable network of individuals to participate. Nielsen (2006) suggested that a sample size of 20 users should be sufficient for quantitative concept testing, providing a 90% confidence level. In this thesis, the confidence level was increased to 95% with a margin of error of 15%, which increased the sample size to 43. The total number of end users who participated in the survey was 57, bringing the margin of error down to 13%. Individuals who participated represented different population demographics in terms of age, gender and nationality, as illustrated in Table 9. Consent was obtained from experts and end users prior to participating in the research. Chapter 6 details the results of the experts' interviews and end-user evaluations.

Table 9: Concept testing participants' demographics

CATEGORY	SUB-CATEGORY	FREQUENCY (N)	PERCENT (%)
AGE	Below 20	3	5.3%
	20 to 29	7	12.3%
	30 to 39	20	35%
	40 to 49	22	38.6%
	50 to 59	4	7%
	60 and above	1	1.75%
GENDER	Male	38	66.7%
	Female	19	33.3%
NATIONALITY	UAE National	27	47.4%
	GCC	1	1.75%
	Ex-pat	29	50.9%

4.4.3 Implementation Phase

After completing the design phase, a prototype system is created to validate the concepts proposed in the design phase. The development of the prototype directly corresponds to achieving the fourth objective of this research.

Prototyping is a vital aspect of the design process, serving as a means to refine and communicate design ideas (Tr  tteberg, 2007). Additionally, a prototype is an initial version of a system used to showcase and validate design concepts and to identify potential issues and solutions (Sommerville, 2011). In the context of design science research, prototyping aids in the development and implementation of the artifact, supporting the demonstration and evaluation phases. System prototypes enable design researchers to assess how well the system aligns with the objectives and identify strengths and weaknesses in the framework design.

Figure 11 depicts prototype implementation process model.

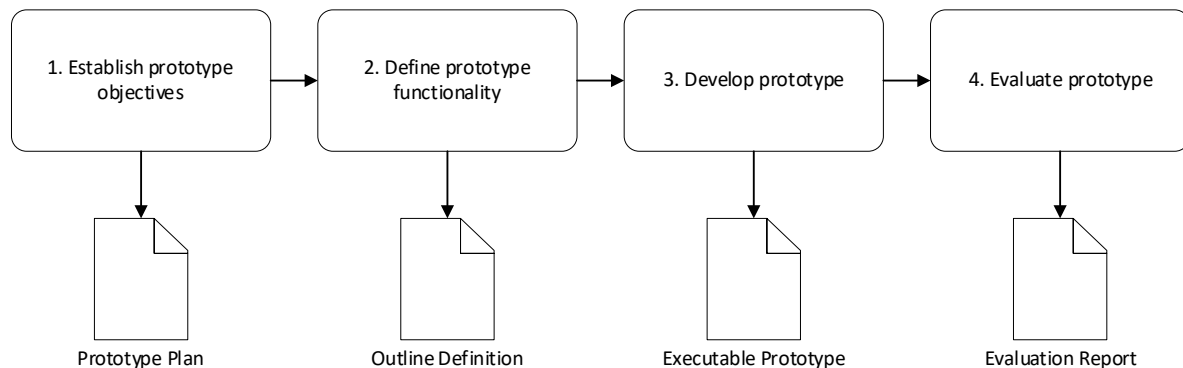


Figure 11: Prototype implementation process model

(Source: Sommerville, 2011)

The initial step in the prototyping process as illustrated in Figure 11, is outlining the objectives of the prototype implementation. These objectives may vary, encompassing aspects like showcasing the user interface, demonstrating system feasibility, and validating the

architecture and functions of a framework. Since there is no universal prototyping solution to address all these aspects, a clearly defined objective for the prototype is crucial in determining its functionality. In the context of this research, prototypes can be categorized into 1) proof-of-principle prototype, 2) user experience prototype, 3) visual prototype, and 4) functional prototype (Merkel, Hopf, and Müller, 2012; Shukla and Saxena, 2013).

1) Proof-of-Principle Prototype

The aim of Proof-of-principle, also known as proof-of-concept prototypes is to test specific aspects of the intended design and assess feasibility without precisely replicating visual appearance. These prototypes verify that the proposed architecture and functions in a design approach can be experimentally tested (Kendig, 2015).

2) User Experience Prototype

The term 'user experience' encompasses various meanings, including traditional usability and the aesthetic, emotional, or experiential aspects of technology use (Hassenzahl and Tractinsky, 2006). The focus of a user experience prototype is on active human interaction with the overall interface, primarily supporting user-focused research.

3) Visual Prototype

Visual prototypes are employed in market research or executive reviews to represent intended design aesthetics, including layout, appearance, color themes, and function positioning. Unlike other types, visual prototypes do not assess the functionality of the designed system (Merkel, Hopf, and Müller, 2012).

4) Functional Prototype

A functional prototype closely resembles the actual system both visually and functionally. It simulates the final design, aesthetics, and functionality but in a more compact form (Sokolowski and Banks, 2010).

In this thesis, emphasis is placed on developing a proof-of-principle prototype during the implementation phase. The third step in the prototyping process model as demostarted in figure 11, involves converting the designed architecture into an executable system using appropriate technologies and resources. To simplify the prototyping complexity and expedite the development, unnecessary requirements and functionalities may be omitted (Sommerville, 2011). The details of prototype implementation is provide in Chapter 7. The developed prototype should be evaluated as final stage of the prototype process model. Although prototype evaluation is a vital part of the development process, this thesis performs the evaluation in the demonstration and evaluation phase, which is explained in Chapter 8.

4.4.4 Evaluation Phase

In this phase, the Digital Trust Framework's feasibility and performance are demonstrated and assessed for design science research evaluation purposes. Initially, the feasibility of the developed prototype is confirmed through a case study demonstration. Subsequently, the prototype's overall performance, considering KYC efficiency and overall system efficiency, is evaluated and validated. Design science research considers evaluation as a validation or proof process, assessing how well an artefact performs or fulfills its intended purpose (Gregor, 2006; Hevner *et al.*, 2004; March and Smith, 1995; Vaishnavi and Kuechler, 2009). Hevner *et al.* (2004) emphasize that evaluation in DSR is vital, requiring researchers to rigorously demonstrate the utility, quality, and efficacy of a design artefact using well-

executed methods. DSR evaluation focuses on assessing "how well" an artefact performs its specified functions, rather than examining the "why" or "how" of its operation (Jain, Sinha and Vitharana, 2011).

In order to conduct the evaluation, it is important to select an appropriate evaluation method, providing evidence that the designed framework functions as intended. A thorough evaluation aids in verifying the framework without the need for additional justifications. Different criteria and evaluation methods are proposed by various studies for DSR. Hevner *et al.* (2004) identify five fundamental evaluation methods in the information systems domain which are: 1) observational, 2) analytical, 3) experimental, 4) testing, and 5) descriptive. Specific techniques for each evaluation form are detailed in Table 10.

Table 10: Forms of evaluation

(Source: Hevner *et al.*, 2004)

Form of evaluation	Methods and techniques
Observational	Case Study: In-depth examination of the artefact in a real-world setting.
	Field Study: Monitoring the artefact's usage across various projects.
Analytical	Static Analysis: Examining the artefact's structure for static qualities like complexity.
	Architecture Analysis: Assessing how well the artefact fits into technical architecture.
	Optimization: Demonstrating the inherent optimal properties of the artefact or establishing optimality bounds on its behavior.
	Dynamic Analysis: Studying dynamic qualities such as performance.
Experimental	Controlled Experiment: Investigating the artefact in a controlled environment, focusing on qualities like usability.
	Simulation: Executing the artefact with artificial data.
Testing	Functional Testing: Executing artefact interfaces to discover failures and identify defects.

	Structural Testing: Conducting coverage testing of specific metrics (e.g., execution paths) in the artefact implementation.
Descriptive	Informed Argument: Making a convincing argument for the artefact's utility using information from the knowledge base.
	Scenarios: Developing detailed scenarios around the artefact to demonstrate its utility.

Hevner *et al.* (2004) present twelve descriptive techniques and methods for each of the five types of evaluation. Despite the fact that these methods include informed arguments as well as scenarios, they lack detailed guidance on the selection of the appropriate method and the design of the evaluation. Vaishnavi and Kuechler (2009) consider both quantitative and qualitative methods for evaluating design science, incorporating non-empirical analysis but they also lack specific guidance on method selection or designing an appropriate evaluation process within design science research. Peffers *et al.* (2007) propose a design science research methodology that divides the commonly referenced "evaluation" into two activities, which are demonstration, and evaluation.

Peffers *et al.* (2007) define demonstration as utilizing the artefact to address identified problems through experimentation, simulation, case studies, proofs, or other relevant activities. These activities align with some forms of DSR evaluation suggested by Hevner *et al.*, as outlined in Table 10 (e.g., observational and experimental) (Hevner *et al.*, 2004). Consequently, demonstration can be viewed as a partial or complete evaluation process in design science research. Peffers *et al.*, (2007) stress the importance of evaluating the artefact by comparing the observed results from using the artefact in the demonstration to the objectives of a solution, measuring quantitative performance indicators like budgets, gathering findings from satisfaction surveys, feedback from clients, or simulations or measurable aspects

of system performance, such as response time or availability. The following section provides a detailed description of the demonstration and evaluation of the Digital Trust Framework.

4.4.4.1 Demonstration

Demonstration serves as a lightweight evaluation, confirming that the artefact effectively addresses one or more instances of the problem and achieves its intended purpose in one context at minimum (Pries-Heje et al., 2008). In this thesis, the demonstration phase employs a case study approach to validate the feasibility of the Digital Trust Framework real-world settings and gain a deep understanding of its performance with a high degree of realism. This is aligned to Table 3 as it's considered an Ex-Post naturalistic evaluation. Moreover, case study is an appropriate method of evaluation as per table 4 and 6.

A case study involves an objective and thorough exploration of a contemporary phenomenon within its real-life context, particularly when the investigator has limited control over events, offering valuable insights and detailed descriptions (Aberdeen, 2013; Baxter and Jack, 2015; Dresch, Lacerda and Antunes, 2014). It is suitable for investigating complex problems, ensuring in-depth exploration and understanding of identified problems (Dubé and Paré, 2003b). It is particularly fitting for design-centric research, such as information systems and software engineering, where the objects of study are contemporary phenomena and artefacts that are challenging to examine in isolation (Runeson and Höst, 2008).

4.4.4.2 Evaluation

Design Science Research (DSR), specifically in the information systems field, involves two main activities which are build and evaluate (March and Smith, 1995). Literature strongly promotes the evaluation of design science artifacts (Hevner *et al.*, 2004; Peffers *et al.*, 2007).

However, the majority of the design science-related work emphasizes the building aspect. Few of the design-science research address the evaluation of design science research more specifically (Cleven, Gubler and Hüner, 2009; Venable, Pries-Heje and Baskerville, 2012; Sonnenberg and Brocke, 2012). However, they lack a systematic consideration of evaluation criteria and their relevance to the evaluation methods. Thus, it is important for design science researchers to consider the research objectives and the functionalities of the artifact and select a suitable performance evaluation methods and criteria based on them.

The evaluation process goes beyond merely confirming whether an artifact functions or not. It refers to the establishment of criteria and the rigorous assessment of the artifact's performance against these criteria (Hevner *et al.*, 2004; March and Smith, 1995). Performance, in this context, is defined as the extent to which a system and its components fulfill the objectives for which they were designed and implemented (Smith and Williams, 2001). Lilja (2005) suggests three methods for evaluating performance, which are simulation, analytical modeling, and empirical evaluation. Table 7 provides a high-level description about these methods.

Table 11: Evaluation Method

(Source: Pahl, Bošković and Hasselbring, 2008)

Evaluation Method	Description
Simulation	Imitates program execution with concentrations on specific areas. It is flexible and less expensive in comparison to building a real system for empirical evaluation, although it may lack accuracy.
Analytical Modeling	Involves mathematically describing a system. Results of an analytical model may be less accurate than real-system measurements.
Empirical Evaluation	Evaluation on real input data, performed through calculating measurements and metrics. It provides the most accurate results.

The empirical evaluation emerges as a more promising method for justifying artifact performance in terms of intended objectives. In empirical performance evaluation, performance of a prototype is measured by conducting tests on datasets, and examining the outputs, typically using quantitative measures (Liu and Haralick, 2002). Performing empirical evaluation could be challenging due to costs and time requirements to implement and deployment of a prototype (Pahl, Bošković and Hasselbring, 2008). Given that this research has reliable access to existing datasets and face no difficulty in implementing a prototype, empirical evaluation is chosen as evaluation method to evaluate the performance of the Digital Trust Platform based on the results of the case-study demonstration. The primary justifications for opting for this approach are:

- Access to both the prototype and empirical data is readily available.
- This method offers the most precise results in comparison to alternative approaches.
- It allows for the assessment of the correlation between the Digital Trust Framework performance in real-world scenarios and the defined objectives.
- Facilitates straightforward comparisons of results with other studies using quantitative measures.

In empirical evaluation, various techniques can be employed to analyze the outputs. Three primary techniques within the empirical evaluation domain have been identified based on a summary of several studies which are user comparisons, performance metrics, and graphical representations.

User comparison is an interactive method that relies on users' judgments to assess the success of a query immediately after the system processes it. This approach requires a baseline system for comparison; however, it could be challenging and time-consuming to obtain a large number of user comparisons for a thorough evaluation (Müller *et al.*, 2001).

Performance metrics function as analytical tools in the performance evaluation process, utilizing measurements to display results and guide subsequent actions without requiring extensive prototype testing development efforts. These metrics form the basis of experimental computer science and engineering, evaluating new ideas, frameworks, and engineering progress. Müller *et al.* (2001) describe performance metrics as single-valued measures (Rose, 1995; Williamson, Stark and Booker, 2014; Eyerman and Eeckhout, 2008; Voiskunskii, 1997).

Graphical representations, also known as graphical plots, are typically two-dimensional plots with axes representing different performance metrics, error rates, and processing times. These representations unveil the relationship between performance metrics and other variables. They also indicate whether observed conditions can fulfill multiple performance metrics simultaneously in the same process. An example of a graphical evaluation plot is the Receiver Operating Characteristic (ROC) curve (Müller *et al.*, 2001; Ja, 1989).

In accordance with the definitions of the aforementioned techniques and considering their appropriateness for the objectives of this thesis, various performance metrics and graphical plots were employed to assess the Digital Trust Framework. This choice stems from the capability of the techniques to offer a measurable and tangible means for evaluating the overall design performance in alignment with the specified objectives. Furthermore, graphical

plots afford a visual representation of immediate consequences related to the performance and reliability of the framework. Another rationale for opting for performance metrics and graphical plots, among the mentioned techniques, is the constrained availability of resources and time, hindering the execution of user-based evaluations. The subsequent section provides an overview of the evaluation process for the KYC process efficiency overall system efficiency.

- ***KYC Process Efficiency***

The Proof of Principle prototype has been integrated with two major national banks in UAE and Identity government authority in order to evaluate the Digital Trust Framework against the defined objectives. From a business efficiency perspective, the framework has been evaluated using three main performance matrices which are processing time, accuracy of verification, and cost per KYC. Processing time is the time taken to complete the KYC process for an individual. The accuracy of verification is the percentage of accurate verifications compared to total verifications. The cost per KYC is the cost incurred per individual or for the KYC process.

The individual data has been used from real systems with the consent from the users to simulate real data and users. Each bank conducted a KYC for 200 users. The total number of KYC performed was 400 with mix of new customers and existing customers to the bank.

- ***Overall System Efficiency***

Digital Trust Framework is built using emerging technology. Thus, verifying the efficiency of the overall system is crucial to ensure the scalability and robustness of the system. Three different performance matrices are used to measure the overall system efficiency which are throughput, response times (average and 90th percentile), and error

rates. Throughput measures the rate of successful transaction processed per second. It evaluates the system scalability through the ability of the system to handle a growing number of users and transactions. The response time measures the overall average response time and the 90th Percentile which shows the response time that 90% of requests fell under. This helps identify outlier cases. Error Rate provides the percentage of failed requests which helps in measuring the resilience of the system. Moreover, the performance of the blockchain has been measured using various standards performance metrics which are transaction throughput, response times (average and 90th percentile), error rates, CPU utilization, and memory utilization. The CPU and memory utilization is measured through the efficient use of computing resources.

The data used to evaluate the performance metrics have been generated user tools to simulate real load on the Digital Trust Framework.

4.4.5 Communication Phase

The communication phase critically assesses and consolidates the outcomes of this study, offering insights to diverse audiences with varying perspectives. Within this phase, the research's limitations and implications are thoroughly examined, and recommendations for future research are outlined.

4.5 Data Sampling

Since reaching out to a whole population is impossible, sampling is used to obtain information about the targeted audience. The population is expected to be a large group of people. Sampling selects a subset of the population (Kothari, 2004). Any population subset is called the sample (Shaughnessy, Zechmeister and Zechmeister, 2016). This research paper

primarily focuses on the KYC of the financial sector, so the population consists of the key roles and entities involved in the ecosystem described in Section 4.4. From an entity perspective, it covers the financial institutions, financial regulators and digital governments representing the digital identity and anchor of trust. From the experts and role perspectives, it covers experts from all domains and roles required, which spans technology (SSI and blockchain), regulation, compliance, KYC experts and user experience. In addition, since the intended framework serves the end user of financial services, the population is all digitally literate individuals living in the UAE eligible to apply for financial services (e.g., above 18).

There are two approaches to selecting a sample: random and convenient (Shaughnessy, Zechmeister and Zechmeister, 2016). In random sampling, every individual in the population has an equal chance of being selected (Shaughnessy, Zechmeister and Zechmeister, 2016). This approach is also called probability sampling (Kothari, 2004). In convenience sampling, the targeted sample is a group of approachable individuals willing to participate (Shaughnessy, Zechmeister and Zechmeister, 2016). In this thesis, the approach chosen to select the sample of the KYC representative was purposeful convenience sampling, where defined criteria were used to select the participants (Creswell, 2014).

The participants selected represented four leading banks in the UAE, two government regulators, two digital governments, a government information security, a local system integrator and two international system integrators. Some participants previously had international experience working in different countries, while two were international participants with expertise in blockchain and SSI. The details of the participants appear in Section 4.4. The participants selected to evaluate the prototype, the end users of financial services, were selected using convenience sampling. A survey was developed and sent to an

approachable network of individuals to participate. Individuals who participated represented different population demographics in terms of age, gender and nationality, as illustrated in Table 9.

4.6 Data Collection

This thesis collected data mainly through experts' collaboration in different focus groups and one-on-one interviews to collect the requirements, design the framework and validate it. In addition, a questionnaire was used to collect end users' feedback on the prototype. UAE regulations related to the financial sectors and telecom's KYC were reviewed with the literature review. During the evaluation phase of the framework, data was collected through data entry.

The first data collection method used was qualitative exploratory semi-structured interviews with experts from different domains to refine and validate the design objectives of the Digital Trust Framework. Experts from blockchain and SSI domains were interviewed to examine the opportunity the technology brings for solving KYC inefficiency while validating preassumptions for its success, while experts with IT solution experience in the financial sector were interviewed to validate the relevance and completeness of the framework to solve the KYC inefficiency and validate its fitness to the real environment. An expert from financial KYC compliance was interviewed to validate the design objectives from a business and compliance perspective, while an expert from the digital government was interviewed to validate design objectives related to the government's role, digital identity and signature laws and implementation and the intent of government support to ensure the sustainability of the proposed solution. In addition, international experts were interviewed to ensure the generalization of the design objectives. The interviews included experts from different

domains to acquire a holistic view of the problem and the requirements to be addressed while confirming the viability of addressing the problem. It also helped in terms of generalization and the acceptance of a solution from a different set of entities. The experts were asked questions related to various design objectives based on their experiences to collect different perspectives and avoid potential bias.

A series of focus group sessions followed the interviews to evaluate the Digital Trust Framework artifact's functionality, completeness, accuracy, reliability, usability and fit within real environmental settings from business, compliance, regulators and digital government perspectives. Focus group sessions allowed the researcher to identify and explore relevant factors, validate assumptions and understand knowledge processes (Ørngreen, 2017). In addition, semi-structured interviews were conducted to achieve more in-depth validation for each domain. One focus group session targeted the telecom sector's KYC to evaluate the framework's generalization and applicability to different domains. Moreover, some experts who participated in the evaluation had previous working experience in different countries, which assisted in generalizing the proposed solution.

All interviews were conducted remotely through virtual conference meetings, while all focus group sessions were in person. The physical focus group sessions were conducted in different places, including participating bank and government offices where the experts worked. Interviews and sessions brought insights and knowledge that differed from document analysis. Document analysis provided information about the process and procedures followed and other knowledge necessary, while the sessions provided space for collaborative negotiation of meaning and facilitated the organization of gathered data through previous methods (Ørngreen, 2017). Each interview and session lasted from 60 to 120 minutes.

Although the interviews consumed more time than the questionnaires, they allowed the researcher to acquire more in-depth information. The interviews also assisted in avoiding misinterpreting the questions since the researcher could adjust to the interviewee's language and provide clarification (Kothari, 2004). All interviews were recorded after verbally obtaining the participants' informed consent and transcribed using Happy Scribe,⁴ coded using QDA Miner Lite⁵ and analyzed using Microsoft Word. The researcher noted information during focus group sessions which was then compared, analyzed and triangulated with the results from interviews and document analysis.

The second data collection method was document analysis, which included a review of the KYC process, existing KYC regulations and a literature review. The review aimed to understand the business challenge in more depth from a business and regulation perspective regarding processes and requirements, the needs and the impact of the regulations in terms of costs, time and user experience. Moreover, the review aimed to ensure the rigor of the challenge and the solution. Similar to the analysis of interview transcripts, document analysis is considered a form of qualitative research that includes coding document content into themes (Bowen, 2009). Document analysis supports verifying findings and evidence gathered from different sources.

In this thesis, document analysis was used in combination with interviews and focus group sessions as a means of triangulation to validate the findings and reduce the impact of potential biases (Bowen, 2009). All documents used were digital and either publicly available

⁴ <https://www.happyscribe.com/>

⁵ <https://provalisresearch.com/products/qualitative-data-analysis-software/freeware/>

or accessed through the British University in Dubai's digital library through the student account provided. Digital documents were annotated using Acrobat Reader. Copies of the digital documents were kept on the researcher's laptop. They will be removed after five years following the final approval of the research committee.

The third data collection method was through the Digital Wallet mobile application. The data were used to evaluate Digital Trust Framework in terms of new KYC process efficiency and accuracy. Minimal data logs were directly saved to a hosting server, and it was registered into the Blockchain. This data could be accessed only through login credentials available only for the researcher. Data collected through the Digital Wallet mobile application was analysed using Microsoft Excel.

The data collection instruments from the interviews, focus group sessions and document analysis aimed to validate the identified problem, understand the business and regulation requirements, identify the required participants and validate the design of the proposed solution. Some of the key findings of these workshops included ensuring regulatory acceptance and confirming the need for the government to play the role of a trust anchor. The focus group sessions with the two banks aimed at informing and validating the design of the proposed solution regarding IT artifacts and the KYC process within their environments from a business process, user experience and technology fitment. The focus group sessions facilitated investigated the user's first impression. The design went through a few iterations. One key outcome was reducing the number of steps and applications the user interacts with. Initially, the digital identity and the user wallet were two different applications, but the discussion evolved to merge them into a unified application.

The fourth means of data collection was a digital questionnaire, a common method of collecting data as it is low in cost, can be filled in by many respondents, is free of researcher bias and allows sufficient time for respondents to provide well-thought answers. Hence, the results are more dependable and reliable (Kothari, 2004). A digital questionnaire was used in this thesis to validate the user experience and willingness to use the application and was developed and analyzed using Qualtrics XM.⁶ It was used to analyze quantitative data and the correlation between them, while for qualitative data, Qualtrics XM was used for correlation. However, data were manually coded, given the small sample, and analyzed using Microsoft Excel.

⁶ <https://www.qualtrics.com>

Table 13 summarizes the data collection methods used in this thesis and the research questions they intended to address.

More details about each collection method can be found in the mentioned sections.

Table 12: Data collection method used in this research paper

Research Question	Data Method Collection	Aim	Section
RQ1: What are the current requirements of the KYC process and its shortcomings? How can blockchain in general help to overcome the challenges and provide new capabilities to enable the implementation of efficient and automated KYC process?	Literature review	Review KYC process, regulations and laws on national and international levels and current challenges	2.2
	One-on-one interviews	Validate the design objectives from business and technical perspectives	5.2
RQ2: What are the current status of using blockchain-based SSI implementation in KYC? What are the challenges facing the adoption of blockchain-based SSI implementation in KYC processes?	Literature review	Review previous studies of using blockchain to improve the KYC efficiency in financial sector and identity management	3.2, 3.4
RQ3: Can a framework be designed and implemented to overcome the current challenges of the adoption of blockchain-based SSI implementation in KYC processes? a) How can the identity of the customer be established? b) How can the authenticity and integrity of the identity be verified? c) What are the technical features that should be developed to instill trust?	Literature review	Review different research approaches	4.3
	One-on-one interviews	Validate solution and key design coverage and viability and generalize the solution on an international level	6.5
	Focus group sessions	Validate solution and key design coverage and viability and generalize the solution to different domains	6.5
	Questionnaires	Validate solution viability and user satisfaction	6.6

d) What are the Privacy-by-Design principles that the framework should comply with? e) How can the proposed framework be validated and evaluated?			
RQ4: How well the proposed framework meets the participants' requirements including individuals, the government as a document issuer, and the private sector as service providers in general and the regulators in specific?	One-on-one interviews	Validate solution and key design coverage and viability and generalize the solution on an international level	6.5
	Focus group sessions	Validate solution and key design coverage and viability and generalize the solution to different domains	6.5
	Questionnaires	Validate solution viability and user satisfaction	6.6
	Data Entry	Case Study to validate the Digital Trust Framework in real world setting	8.3

4.7 The Role of the Researcher

The researcher holds a Bachelor of Science in Computer Systems and a Master of Science in Information Technology (Knowledge and Data Management). The researcher has worked in the software development field for 18 years. The researcher is a senior manager of digital development at a government organization. None of the participants had a direct relationship with the researcher to signify a conflict of interest or impart bias on the research. Moreover, the participants had no reporting or employment relationship with the researcher.

The researcher's role as a senior manager of digital development was fitting as the research paper requires in-depth knowledge of technology and the ability to reach out to different stakeholders in various organizations. In addition, the researcher was trained on the methodology for conducting qualitative research through qualitative research courses at the British University in Dubai in the Computer Science discipline.

4.8 Ethical Consideration

Soanes and Stevenson (2004) defined ethics as “the moral principles governing or influencing conduct” of a “branch of knowledge concerned with moral principles”. Myers and Venable (2014) highlighted four reasons regarding the importance of considering ethical principles by design science researchers: 1) the dual potential of information technology used to improve or destroy human dignity stated by Mason (1986); 2) the increased focus in teaching ethics in business schools; 3) the growing focus of institutional review boards on the ethical principles that must be followed in research projects and 4) the different ethical priorities that design science researchers have compared to behavioral researchers in IS (Mason, 1986).

Ethical principles were considered as priority elements throughout the research. In alignment with the reasons Mason (1986) highlighted, the researcher followed the university's ethical guidelines. These guidelines included a Research Ethics Form filled out by the researcher and submitted to the academic program office. In addition, the guidelines mandated that the research should be conducted after receiving signed approval from the Research Ethics Committee.

The ethical guidelines also included the need to obtain informed consent from any participant involved in the research. Informed consent forms were obtained from the experts using the Expert's Consent Form (Appendix A). Informed consent is an important requirement before any research involving human participants (Creswell, 2014; Mason, 1986). The structure of the informed consent forms followed the guidelines outlined by Shaughnessy, Zechmeister and Zechmeister (2016). The structure suggested that the form should include the purpose of the study, processes to be followed, the potential risks and benefits of participation, the degree of confidentiality and identification of personal data and demographics, the potential consequences of declining or withdrawing and contact information in case of queries about the research.

The university's ethical guidelines align with some of the principles proposed by Mason (1986), who proposed six ethical principles for ISDSR: 1) explicitly identifying all stakeholders who may be affected once the resulting artifact is in use and the kind of benefit or damage that may result; 2) obtaining informed consent from any individual involved in the research; 3) protecting the privacy of the individuals directly involved and those who may use or be affected by the developed software, the IS or the IS development method in the future; 4) ensuring honesty and accuracy in ideas and reporting findings; 5) agreeing on the IP

ownership and information ownership and rights in term of publication and 6) ensuring the quality of the artifact.

All stakeholders were identified during the study. A sample of key stakeholders was consulted, including experts from KYC and SSI domains. These experts also represented a sample of stakeholders impacted once the artifact is used. The information collected from these stakeholders was mainly related to their experience in the domain and their core business in terms of KYC, including their feedback about the artifact. The information collected did not include any personal information. Moreover, the core business discussed was either related to regulation, which is publicly known information, or an application that end users use to avail services publicly available now or later. Any material or information shared not publically available was kept safely on a hard drive on the researcher's laptop, including notes taken during the interviews and focus groups and interview recordings. All materials will be kept for five years after the final approval of the research committee and deleted afterwards. Any information that could potentially identify the identity of participants was removed from the documents and transcripts before analyzing them. Data collected from the questionnaire is stored in the cloud and protected by a password known to the researcher. The consent form highlighted how the data would be used. There were no associated risks for the participating experts.

4.9 Trustworthiness

Different methods are used to form trustworthiness in quantitative and qualitative research. In quantitative research, the trustworthiness of the data is established through validity, reliability and objectivity, while in qualitative research, trustworthiness is established through credibility, transferability, dependability and confirmability (Kaminski and Pitney,

2004). These methods ensure data accuracy, the applicability of the results to other settings and the consistency of results for replication and neutrality.

Because different methodologies were used to collect data, various methods established trustworthiness during each data collection and analysis phase. Credibility was established through four methods in this research. First, participants were selected through purposeful sampling to ensure sufficient experience and knowledge in the domain related to this research (Lincoln and Guba, 1986). Second, the researcher's prolonged engagement with participants due to the proximity and work dynamic with the experts from the same organization and the various interactions with internal and external experts over the study helped create trust between the researcher and participants. Third, the data collected through document analysis and expert collaboration during focus group sessions and interviews were ensured to be adequate to provide credibility by demonstrating saturation (Charmaz, 2006). Fourth, different sources and data collection methods were used for each research question, as described in Table 13, to produce triangulation. Of the four types of triangulations, this research paper used data and methodological triangulation. Data triangulation means the usage of different sources of data from existing research, while methodological triangulation means using more than one method (Morse, 2000). Triangulation is a strategy to obtain consistent and dependable data (Merriam and Tisdell, 2015).

Credibility was ensured through referential adequacy, where the raw research data was stored for examination and comparison with future studies at a later stage. However, since data related to this thesis will be unavailable after five years of the final approval of the research committee, there is a potential limitation to the credibility of this thesis in the future.

Transparently and transferability were established by providing descriptive information about the context, participant, artifact and outcome to assist in understanding the strengths and limitations of the research while increasing the dependability of the results. Moreover, the information can be assessed regarding applicability to other domains or situations and whether it can be generalized (Kaminski and Pitney, 2004). In addition, to ensure generalization, this thesis validates the artifact's relevance in another KYC domain: telecom. While the data collected in this thesis covers a fair amount of sample individuals in one-on-one interviews and focus group sessions, as found in Tables 7 and 8, the data were collected mainly from financial domains. Other domains should be examined to ensure transferability and generalization.

Moreover, the research findings should be ensured to be objective and neutral to provide confirmability, not based on biases and beliefs of the researcher as a senior manager (Kaminski and Pitney, 2004). Qualitative methods generally have the downside of biased and subjective interpretation. For example, due to the document's creator and the reader, in this case, the researcher can be biased, possibly leading to an issue when the document is analysed (Bowen, 2009; O'Leary, 2017). Moreover, the level of guidance the researcher provides to individuals participating in the data collection phases, including interviews and focus groups, can be influential (Kothari, 2004; Ørngreen, 2017). The presence of the researcher and sometimes the need to record can likely impact the participants.

Nevertheless, the value of data collected through qualitative research methods cannot be negated (Creswell, 2014). To establish confirmability, the researcher ensured creating a positive atmosphere, providing minimal prompting and cautious communicating verbally with no extra nonverbal communication. Moreover, the solution relevance was evaluated with

different focus groups representing different organizations and expertise, as illustrated in Table 8, to reduce the bias risk. In addition, the solution was evaluated as case study in a real world settings with two leading banks.

The trustworthiness of the quantitative methods was established through internal and external validity. The internal validity was established by controlling the variables impacting the dependent variable. In this research paper, a survey was used for internal validity, which was sent to end users to measure their acceptance and satisfaction. Participants in the survey had no previous knowledge about the artifacts generated in this thesis. External validity is the ability to generalize the study by selecting a subset representing the whole population (Trochim, 2007; United Nations, 2008). The interview and focus group sessions were conducted with leading banks, government regulators, digital governments and international experts. In addition, a session was conducted with the telecom sector.

4.10 Limitations and Delimitation

Some limitations should be highlighted. The research focused on data and views from experts, mainly in the financial sector. The telecommunication sector engagement was limited. No other sector was studied as part of the research. The artifact was assumed to be generalized and applied in different domains. The data collection focused on the KYC regulation related to the UAE. Limited consideration was given to international KYC regulations. The two banks where more in-depth sessions were conducted were two of the largest national banks in the UAE. Thus, their requirements and validations were mainly related to UAE regulations, so there is a need to conduct focus group sessions with leading international banks to ensure no gaps are identified in the case of international requirements. Moreover, the evaluation of the design of the prototype was limited to end-user surveys and experts from business and user

experience. Hence, there is a need to conduct interviews with end users to acquire an in-depth understanding of the feedback provided through the survey.

4.11 Summary

The objective of this chapter was to outline the research methodology used to address the research questions. It described the research approach, process and activities in detail. Peffers *et al.*'s (2007) DSR process was used to develop and evaluate the IT artifacts using rigorous methods by combining qualitative and quantitative research methods. The chapter summarized the data sampling and data collection used. Purposeful convenience sampling was used for expert selection, while convenience sampling was used to survey end users. Data was collected mainly through experts in various focus groups and one-on-one interviews. The questionnaire was used to collect end users' feedback.

Finally, the chapter summarized the role of the researcher, the ethical considerations and the trustworthiness of qualitative and quantitative research through different methods, including credibility, transferability, confirmability and validity. The limitations were also highlighted.

Subsequently, Chapters 5 and 6 present details on the design objectives, the IT artifact development and the evaluation of these objectives and IT artifacts. These two following chapters demonstrate in detail how the methodology described in this chapter was followed while highlighting the study's results.

Chapter 5: Design Objectives

5.1 Introduction

This thesis aims to address the gaps associated with digitising and automating the first two steps of the KYC process related to the initial phase of identity verification. The first step in the KYC process is customer identification, in which potential customers' data is collected to identify them. The data includes documents issued by the government, such as identity cards and passports, documents issued by other financial institutions and other personal identification information, such as addresses. The second step is where the financial institution verifies the submitted data. In addition to the research gap related to the initial phase of identity verification, this thesis addresses two more research gaps related to the efficiency and automation of the ongoing KYC monitoring to ensure permanent risk monitoring and the acceptance of the framework by the various parties involved in the actual setting environment of the framework, which is financial institutions, regulators, the government and individuals to enable its deployment in the real world.

This thesis contributes to developing the IT artifacts that construct the Digital Trust Framework, leveraging SSI and blockchain to improve the KYC process efficiency. This chapter aims to define the key design objectives to inform the framework's design and evaluate them with experts from relevant domains: compliance, government, financial institutions and technology.

5.2 Design Objectives Definition

The first stage of the DSR process involved identifying the problem and the requirements mapped to design objectives that the Digital Trust Framework should address:

blockchain-based SSI. The design objectives ensured that the framework comprehensively addressed the challenges of the KYC process, as identified in Chapter 3. The design objectives were derived from the literature review of the KYC process and regulations, privacy, identity and technology. Eight main design objectives were identified with their associated requirements: efficiency, regulatory compliance, decentralization, trust establishment, privacy protection, user experience, sustainability and technology advancement. These design objectives are derived from the needs of the stakeholders. Sonnenberg and Brocke (2012) highlighted that design specification should be evaluated in terms of being understandable and meaningful to all relevant stakeholders. Moreover, given that the stakeholders of the Digital Trust Framework are diverse with substantial conflict, it is important to evaluate the specification during EX Ante through naturalistic setting such as focus group (Venable, Pries-Heje and Baskerville, 2012). Table 13 maps the design objectives with different stakeholders' needs.

Table 13: Design Objectives mapping to stakeholder needs

Sr .	Design Objective	Technical	Government	Regulator/Compliance	KYC Experts	End Users
1	Efficiency	X		X	X	X
2	Regulation Compliance	X	X	X	X	
3	Decentralization	X	X		X	
4	Trust Establishment	X	X	X		X
5	Privacy Protection	X	X	X		X
6	User Experience		X			X
7	Sustainability	X	X	X		
8	Technological Advancements	X				

The design objectives are described in more detail in the following sections.

Design Objective 1: Efficiency

Financial institutions face significant challenges due to the high cost of conducting the KYC process caused by the leading time to onboard a customer, employee costs of verifying single and multiple account holders, which is time-consuming and fines that must be paid due to misconduct in the KYC process. In addition, there is a lack of automated KYC processes and abilities to verify data with other organizations (Malhotra, Saini and Singh, 2021).

To address these challenges and gain a competitive advantage, financial institutions must provide fast and convenient means of collecting and verifying identity documents (Jessel, Lowmaster and Neill, 2018). The more efficient the KYC process is, the higher customer satisfaction. Thus, a few key requirements should be satisfied to develop an efficient KYC process. The first requirement (R1.1) is seamless digital submission and processing of relevant documents end-to-end (Arner *et al.*, 2018). Customers must have digital identities with high assurance levels mapped to their physical identities to satisfy this requirement (Ferdous, Chowdhury and Alassafi, 2019; Malhotra, Saini and Singh, 2021). Moreover, customers should have digital documents that are trusted and verifiable (Schlatt *et al.*, 2022), enabling them to apply digitally without the need for the initial verification to be physical.

The second requirement (R1.2) is automating all the manual processes related to verifying customer-submitted documents for KYC purposes by financial institutions, which includes many steps such as verifying the validity of the documents submitted and the authenticity of the documents in terms of their ownership by the customer submitting them

(Zetzsche, Buckley and Arner, 2018). The ongoing KYC monitoring step also needs to be automated as part of the end-to-end KYC process. None of the research papers reviewed in Chapter 3 considered this step. In the framework proposed by Schlatt *et al.* (2022), the ongoing KYC monitoring process is described in brief without sufficient details to conduct it. Automating the initial phase of verification is insufficient. Customer status may change, impacting on the current services obtained by the customer and subsequent services. The financial institution needs to be updated as soon as there is a change in the customer status rather than manually asking for updates per the frequency defined by the regulator. This need defines the third requirement (1.3): having up-to-date customer statuses.

The fourth requirement (R1.4) is to define a standardized means to integrate and exchange documents in trusted IT infrastructure. The data and documents exchanged should be of high quality and accuracy to reduce errors and risks in the data exchanged, which could lead to legal and regulatory implications. Human errors in filling out KYC forms were one of the issues highlighted by Malhotra, Saini and Singh (2021). Achieving these requirements can increase the KYC process efficiency and reduce friction.

Design Objective 2: Regulatory Compliance

Ensuring compliance with regulations is a fundamental requirement of the KYC process and the core reason for its existence (Ostern and Riedel, 2020). The KYC process aims to prevent money laundering. In a digital KYC process, the key requirement is to satisfy the compliance requirements of relevant national and international regulations (Arner *et al.*, 2018). One of these regulations is the Money Laundering Act (MLA; R2.1), which specifies requirements for customer identification and record keeping, as well as determining and documenting the risk associated with customers.

The second regulation is the GDPR (R.2.2), which applies to personal data processing and includes privacy requirements, PbD, transparency, portability, purpose limitation, data minimization, storage limitation, the right to erasure, accuracy, information integrity and confidentiality. While this regulation applies within the EU, similar requirements exist in other jurisdictions worldwide. In the UAE, a law was issued similar to the GDPR: the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection. It aims to bring UAE's federal law in line with international data protection standards. It uses the term "controls" for personal data processing, which includes processing personal data in a transparent, legal manner, gathering personal data only for a clear and specific purpose, processing personal data only as necessary for a specific or similar purpose, maintaining accurate personal data and amending or erasing inaccurate data, keeping personal data secure, and keeping personal data only for as long as necessary based on the specific purpose while then erasing or anonymizing it. These principles align with the key data protection laws worldwide, such as the GDPR.

Additionally, in the digital KYC process, it is necessary to verify the authenticity of the customer's identification and related documents. The 5th EU AML Directive recognizes electronic identification systems that meet eIDAS standards as a valid form of identification for KYC processes. eIDAS imposes specific requirements on these electronic identification methods, including adherence to certain security levels (known as the LoA) and the ability for systems to work together across borders (known as "interoperability"). Thus, compliance with eIDAS is one of the requirements in this thesis (R.2.3).

While eIDAS applies within the EU, a similar law was issued in the UAE, the UAE Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services, to

ensure legal certainty in electronic interactions similar to eIDAS (Al Tamimi & Company, 2021a). The Telecommunications and Digital Government Regulatory Authority (TDRA) regulates the law. The law provides regulations for electronic identification systems and trust services. Electronic identification helps individuals and businesses verify their identities. The TDRA is responsible for creating rules and standards for electronic identification systems and digital IDs in coordination with relevant bodies. Trust Services are electronic services designed to increase confidence in the security and certainty of electronic transactions. The law provides a regulatory framework for four core trust services categories: electronic signatures, seals, time stamps and registered delivery services.

Since this thesis focuses on the UAE context in specific and worldwide in general, requirements (R 2.2) and (R 2.3) consider both the laws relevant to the UAE which are the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection and the UAE Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services, in addition to international laws, which are GDPR and eIDAS. Although eIDAS is applicable in the EU, it is required in this thesis for two reasons: 1) because of the recognition of the 5th EU AML Directive of the electronic identification systems that meet eIDAS standards as a valid form of identification for KYC processes and 2) because it provides the framework with the potential to be accepted cross border. The thesis also considers the acceptance of the framework by regulatory authorities in the UAE and the possibility of amendment of regulations if required as one of the requirements (R 2.4; Malhotra, Saini and Singh, 2021; Pöhn, Grabatin and Hommel, 2021).

Design Objective 3: Decentralization

As highlighted in Section 2.2, hackers find it attractive to target customer data silos. Recent data breaches have exposed sensitive customer data in central data silos, significantly reducing confidence in such architectures and data storage (Rajput and Gopinath, 2017). In addition, securing valuable information is not the primary focus of financial institutions, and it can be expensive. Any mistake can result in serious consequences such as reputational damage and fines. Thus, a viable solution for an improved digital KYC process must avoid central storage of customer data to avoid similar data breaches. Data must be distributed across various data storage to prevent a single point of failure (R 3.1), making it more difficult for hackers since there is no central data repository to target.

Moreover, the financial sector is a critical and competitive domain. Financial institutions do not want to risk becoming dependent on a centralized KYC SP. Therefore, the system must be designed to prevent lock-in effects (R 3.2) that could result in the accumulation of market power. Financial institutions must be able to verify customer data independently at any point in time (Schlatt *et al.*, 2022). Decentralization of data storage and workflows is a primary objective of the Digital Trust Framework. There is a need to balance centralization and decentralization to govern the ecosystem and ensure the trustworthiness of key operations, including the issuance of identity claims, the lookup of identity and data storage (R 3.3; Soltani, Nguyen and An, 2021).

Design Objective 4: Trust Establishment

One of the key objectives of this thesis is to create a digital framework trusted between the government and private sector in UAE to address the challenges faced in the KYC process.

All parties involved in the ecosystem, including the government, regulators, the private sector and individuals, must trust each other (Pöhn, Grabatin and Hommel, 2021; Soltani, Nguyen and An, 2021). At the core, regulators must trust the KYC process and its compliance with KYC regulations (R 4.1). Hence, regulators must be able to validate every step in the process, in particular the digital identity of the customer and the intent to transact, the validity and integrity of the digital documents submitted and the verification by the financial institution to grant services to the customer in case of financial KYC, for example. Therefore, the accountability of every party must be defined and measured with sufficient transparency among all parties in terms of visibility into the transactions and the associated data without any privacy breach of the customer data (R 4.2).

Financial institutions must trust the customer's digital identity and the digital documents' integrity to verify them and ensure compliance with regulations to avoid fines. The digital documents submitted by the customer must be tamperproof and include security measures that make them court-proof to be used as evidence in a dispute. Thus, these digital documents should comply with the UAE Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services and eIDAS. They must implement security controls such as using digital signatures. Both regulators and SPs, the financial institutions in this case, must be able to conduct validity checks of the KYC process and the digital documents submitted (R 4.3). The financial institution should also validate that the digital documents submitted are genuine and authentic, issued by an official entity – either the government or a private entity (R 4.4). Hence, the digital identity of the official entity that issued the digital document should be verifiable, so the representation of the digital identity of the entity should be compliant with

the UAE Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services and eIDAS.

In addition, since digital KYC is conducted remotely without employee interaction, financial institutions require high levels of assurance on the authenticity of the customer's digital identity and its association with the digital documents submitted, without the need for a physical presence or manual intervention, such as a video conference (R 4.5; Malhotra, Saini and Singh, 2021; Pöhn, Grabatin and Hommel, 2021). Thus, financial institutions need to validate that the customer's digital identity maps to the customer's physical identity in the real world (Ferdous, Chowdhury and Alassafi, 2019). Trust in customer identity can be solved using biometrics as one approach (Pöhn, Grabatin and Hommel, 2021). The financial institution would also need to be assured by verifying that digital identities were not stolen, so the customers are who they claim to be when applying for a service (Malhotra, Saini and Singh, 2021).

Design Objective 5: Privacy Protection

In the Digital Trust Framework, privacy requirements protect customers' personal data from unauthorized access, misuse and abuse. Customers are becoming more aware of privacy rights due to increasing data breaches. Thus, to ensure the acceptance of the digital KYC process, the framework should be designed with privacy-preserving at the core (Maler and Reed, 2008). One key privacy requirement to be considered when designing and implementing the Digital Trust Framework is compliance with privacy laws and regulations, as highlighted in Objective 2. The Digital Trust Framework must comply with all applicable privacy laws and regulations, including the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection and the GDPR, to ensure that personal data is processed

lawfully, fairly and transparently. Another requirement is the “need-to-know” principle (R 5.1), where only the customers and entities involved in the KYC process can access customers’ personal data. Any unnecessary access or sharing of personal data should be avoided. This principle is also defined as one of Cameron’s seven laws of identity (2005). In addition, it is recommended for information systems from a security perspective (Moor, 1997; Hughes, 1988).

In addition, the seven laws of identity by Cameron (2005) include other requirements related to identity privacy, dictating the importance of restricting the data exchanged to only what is necessary since digital data are more extensive and easier to collect and exploit than their physical counterparts (Arner *et al.*, 2018). This requirement is referred to as data minimization (R 5.2) and is critical for confirming customer privacy and preventing data breaches. Hence, the data collected and processed should only be limited to the intended purpose, a key principle in the GDPR. Moreover, the seven laws of identity state the need for customers to be in control of sharing their identity information. Therefore, customer consent should be obtained before collecting or processing personal data (R 5.3). Indeed, customers should always be informed about the purpose and scope of data collection. As stated by the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection, the purpose of collecting data should be clear to customers, who should be in control of their digital identity in terms of creating it and associating their information with it aligned with SSI principles.

The seven laws of identity also state that there should not be a way in which an unauthorized entity is allowed to perform data correlation, pattern recognition or entity identification. Thus, personal data should be anonymized so that data cannot be linked to any

identifiable individual (R 5.4). In addition, the seven laws of identity and the UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection state that personal data should only be retained for as long as necessary and should be deleted when not required anymore (R 5.5).

Design Objective 6: User Experience

From a customer perspective, the most important requirement in any digital platform is the user experience. Customers will be motivated to use the Digital Trust Framework if it is simple and easy to understand. Therefore, the Digital Trust Framework should be designed to provide a seamless and convenient user experience to the customer (R 6.1; Kokolakis, 2017; Pöhn, Grabatin and Hommel, 2021). The digital KYC process should be fast and straightforward, providing high security without compromising the user experience (Dhamija and Dusseault, 2008). There should always be the right balance between ease of use and security. The Digital Trust Framework should be transparent about the data collected during the KYC process. Customers must be informed about the type of data collected, its purpose and who has access to it (R 6.2). Moreover, sufficient services should be available to increase user adoption (Pöhn, Grabatin and Hommel, 2021).

The digital KYC process defined by the framework should be available on various devices, including mobile phones and laptops (R 6.3). The framework must be designed to accommodate different user interfaces, enabling customers to perform the KYC process from the devices with which they are most comfortable. The Digital Trust Framework should provide a consistent user experience across all devices and user interfaces (Cameron, 2005) to ensure that customers have a consistent experience throughout the KYC process, regardless of

their device, enhancing the user experience while making the KYC process more accessible and convenient.

The Digital Trust Framework should have a built-in backup and recovery mechanism in case of lost or stolen devices (Soltani, Nguyen and An, 2021). Alternatively, customers should be able to request prompt support in case of issues. However, this offering can be challenging if no central third party is responsible for the entire process. Therefore, backup, recovery and support features must be included in the requirements to ensure customer satisfaction (R 6.4).

Design Objective 7: Sustainability

Sustainability is a fundamental aspect to be considered in the design of the Digital Trust Framework. The framework should be generalized, not limited to financial KYC only. It should support other domains, such as telecom and healthcare. Hence, the framework should be adaptable and scalable, supporting many use cases (R 7.1), so the business logic and processes should be maintained within entities. Having different use cases and domains supported by the framework increases the services it offers, increasing the end user adoption (Pöhn, Grabatin and Hommel, 2021). The framework should be designed with a long-term view, considering the continuous changes in regulations and technological advancements.

Another key requirement for the sustainability of the Digital Trust Framework is top management support highlighted by Pöhn, Grabatin and Hommel (2021). The senior management of various parties in this ecosystem must be involved in the project from the beginning to ensure sufficient resources and commitment (R 7.2). Having adequate resources within a project reduces the risk of knowledge loss, potentially leading to ending the project.

Thus, the need for having sufficient resources to build the framework and onboard various services from different financial institutions and other domains to bring more benefits for the end user can eventually lead to an increase in adoption.

Design Objective 8: Technology Advancement

Blockchain is still in its early stages, so the degree of change is high (Pöhn, Grabatin and Hommel, 2021). It evolves with time, so the technology choice is critical in developing a successful blockchain-based SSI. Considering the framework's requirements is essential, including the available technologies on the market and the capabilities and limitations of each. Technical choice in terms of protocol and technical components is key to increasing adoption by providing different integration options and sustaining the velocity of technology changes (R 8.1; Pöhn, Grabatin and Hommel, 2021). The support and stability of technology is also essential. The technology choice should support the nonfunctional requirements of the framework, such as scalability, interoperability, security and privacy. Moreover, the novelty of the technology, the existence of legacy systems to be integrated, integration methods, and the availability of documentation should also be considered while designing and selecting the technical components and protocols of the framework (Pöhn, Grabatin and Hommel, 2021). In the case of blockchain-based SSI, considering the features and capabilities of the underlying blockchain technology is crucial, such as consensus mechanisms, smart contract support and privacy features. Similarly, the choice of SSI technology should be based on its ability to support VCs, selective disclosure and privacy preservation.

Moreover, the Digital Trust Framework should be designed to be as technology-agnostic as possible (Pöhn, Grabatin and Hommel, 2021). The architecture should be modular to adapt to change (Pöhn, Grabatin and Hommel, 2021) and help improve its flexibility,

scalability and maintainability (R 8.2). Modularity refers to the ability to break down the system into smaller, more manageable components, each with its own functionalities and interfaces, enabling efficient development, testing and maintenance with easier integration into other systems and applications. In the context of blockchain-based SSI, modularity can be achieved by breaking down the framework into smaller components, such as identity verification, document verification, data storage and access control. Each of these components can be developed and maintained separately and integrated with other components through well-defined interfaces. This approach also enables the framework to adapt more easily to changing requirements, as new components can be added, or existing ones can be modified without affecting the rest of the framework.

5.3 Evaluation of the Design Objectives

5.3.1 Evaluation Summary

The identified design objectives were evaluated through expert interviews to assess their relevance and completeness. Six experts were interviewed. The challenges of the KYC process were discussed along with the design objectives. The experts represented the private and government sectors. Four experts were working in the UAE, while two were working internationally. The experts had different expertise in KYC, SSI, blockchain and government regulations based on their work for different government and private entities. The diversity of the experts helped in assessing the objectives from different perspectives. Additional information about the experts appears in Chapter 4.

The experts focused on various design objectives of the Digital Trust Framework to provide feedback to enhance efficiency, ensure regulatory compliance, establish trust, protect

privacy, optimize user experience, ensure sustainability and leverage technology advancements. The experts confirmed all the design objectives in terms of relevance and completeness so that an expert confirmed each design objective at least once.

The experts emphasized the need to streamline and automate the KYC process to reduce costs and improve customer satisfaction in adherence to regulations. They stressed the need for a simple and convenient user experience and highlighted the importance of leveraging trusted digital identity as a starting point of any digital service. The experts highlighted the need for various services to accelerate customer adoption. They also acknowledged the readiness of regulatory frameworks in certain regions, including the UAE and the flexibility to adopt technological advancement. The experts stressed the need to balance centralization and decentralization to ensure governance and trustworthiness of operations. Moreover, they emphasized the need for government involvement to gain trust and ensure credibility. They highlighted the importance of data privacy and the need to share only necessary information, obtain customer consent before sharing and explore secure storage options. The experts highlighted the need to select the right technology that supports scalability, interoperability, security and privacy. They emphasized the importance of modular architectures and adherence to established standards. The section below provides more details and insights into the experts' feedback for each design objective.

5.3.2 Experts' Feedback

Design Objective 1: Efficiency

The experts generally agreed with streamlining and automating the KYC process to reduce costs, reduce manual interventions and improve customer satisfaction. They agreed on

the potential of leveraging technology to improve efficiency and accuracy. They acknowledged the importance of addressing challenges in the KYC process, such as document submission, initial verification, name screening and ongoing monitoring.

Expert B highlighted pain points in the KYC process, such as initial verification, name screening and ongoing monitoring. Expert C added more details to the challenges faced during the KYC process, emphasizing its burdensome nature involving extensive documentation and physical document submission. Expert G also agreed with Expert C and highlighted that the current KYC process involves customers showing their original documents to agents or bank staff, who then verify and cite the copy of the original document. This process is cumbersome, requiring additional agents, storage and archiving procedures, particularly if there is a high volume of customers. Moreover, Experts C and G highlighted that the reliance on agents creates a potential risk of misconduct if the agent collaborates with the customer, bypassing regulation requirements using messaging services.

Expert C agreed on the need for a simpler and more digital approach to document submission, enabling secure sharing of identity documents through digital channels. Expert C also stressed the importance of considering the entire process lifecycle, accommodating ongoing monitoring requirements and providing a seamless experience for users. Expert D emphasized automation, accuracy, privacy and security as crucial elements and mentioned their contribution to smoother and friendlier user experience, positively influencing customer happiness. Expert D added a suggestion of tailoring services to the user's profile. Experts A, B and D highlighted the importance of trusted digital identity as a starting point of any digital service.

Expert E agreed on the potential improvement of the KYC process using blockchain for identity, while Expert B suggested extending the blockchain-based SSI for automating and consolidating screening systems and integrating it with various data sources. Experts A, D and F highlighted the importance of following recognized standards to develop the framework, while Expert E emphasized the need for a seamless API to integrate with different entities.

Design Objective 2: Regulatory Compliance

The experts emphasized the importance of compliance with regulations related to data protection. They acknowledged the need for clear policies, stakeholder collaboration and technology to enhance regulatory compliance.

For instance, Expert G stated the importance of consistently assessing whether new initiatives align with the requirements set by the regulators. This evaluation ensures that data sources and information-gathering practices meet the necessary standards and guidelines. Expert C emphasized the importance of compliance with data protection and AML regulations and highlighted the role of clear policies and regulations in establishing credibility, protecting user interests and driving adoption.

Expert A highlighted the readiness of regions, such as the UAE, Asia Pacific, Europe and the UK, regarding regulatory frameworks related to digital transformation. Expert A added that this readiness had been noticed in adopting cryptocurrency. Expert A believed that these regions would effectively lead the digital transformation journey from a technology adoption and regulation perspective. Expert B also highlighted the UAE's readiness regarding regulatory frameworks to support digitization. Expert B discussed the potential advancement of relying purely on digital data without needing documents. All experts highlighted the

benefits of initiatives like the UAE Digital Identity and emphasized the importance of collaboration between stakeholders and regulators.

Experts B, C and E mentioned international guidelines and regulations on customer due diligence (CDD) that the Digital Trust Framework should comply with. They discussed trust between correspondent banks and the importance of maintaining a regulated status and close relationships. Expert F highlighted the interest and efforts in trusted identities and KYC verification across borders, particularly within the EU. Expert F mentioned initiatives like ID Union and the focus on digital product passports and central bank digital currencies requiring identities and KYC processes. Expert F also mentioned standardization efforts by various organizations and acknowledged the complexity involved.

Design Objective 3: Decentralization

Experts A and D emphasized the importance of security and privacy in data storage and sharing. They agreed on the need for better data protection through secure storage and minimizing data exposure.

Expert A focused on data ownership and risk involved in storing and maintaining data, suggesting that the record system of original data should remain with authorized entities, while individuals should control what data they share. Expert A added that large entities can better protect data, highlighting that data should be stored by entities that offer better data security. Expert D highlighted customer preferences and concerns regarding data storage. Customers prefer physical documents in their custody for control and security, so in the digital world, they want their data stored securely by a trusted entity, as highlighted by Expert A.

Expert D highlighted that customers prioritize security, privacy, control and authorized access to their data. Expert A proposed a model where only the endorsement of data is revealed to reduce the risk of data exposure. Expert A emphasized the need to balance decentralization and regulation in establishing a sovereign identity.

Expert D mentioned the importance of establishing a digital identity ecosystem where different actors collaborate to provide a better customer experience. Decentralized identity, such as SSI, allows users to control and share their identity with chosen entities. Expert D mentioned that technologies like blockchain enhance trust and reliability in this ecosystem. Expert E stated that if the government owns the blockchain-based SSI, then the ownership and distribution of nodes are not a significant concern for trust.

Design Objective 4: Trust Establishment

The experts highlighted the importance of government involvement in such initiatives as anchors of trust and regulators. They emphasized the importance of different aspects, such as the balance between decentralization and regulation, the secure sharing of documents and the need for authenticity validation.

All experts confirmed the role of the government as a trust anchor. They highlighted that the framework should be either government-owned or government-endorsed. Experts B and E highlighted the importance of government involvement and endorsement to gain trust from the private sector. They agreed that government support and regulators' approval increase trust and adoption. Expert F mentioned the role of influential public figures and government involvement in establishing trust. Executive orders and adoption by influential institutions drive trust and adoption. Expert E highlighted that financial institutions would not

trust KYC verification by another financial institution as not every institution follows the rules precisely. Moreover, Expert E highlighted that if a financial institution conducts KYC, other financial institutions should not benefit from the KYC free of cost.

Expert C emphasized the need for up-to-date and secure document sharing, clear regulations, reliable services and effective communication from the government to foster trust. Expert A also highlighted the importance of reliability. Expert A stated that trust is established when a platform protects business interests and minimizes risk exposure. At the same time, Expert D confirmed that security, authenticity, limited access and collaboration are key elements for trust.

Design Objective 5: Privacy Protection

The experts highlighted the significance of data security and privacy in the Digital Trust Framework. They emphasized the need for robust security measures, access controls and clear data management and sharing policies.

Expert A emphasized the importance of having data privacy as a fundamental principle in the digital world, proposing to disclose only necessary information rather than the entire data. Expert A highlighted the importance of regulatory acceptance for implementing such practices. Expert D emphasized the importance of safeguarding customer privacy and ensuring that shared data is used only by the intended party. Expert D mentioned that SSI enables users to have control over their personal data, which supported the point highlighted by Expert E in terms of the possibility of privacy regulations requiring users to opt-in to share certain information. Expert B discussed the role of consent and mentioned that customer consent may

not always be necessary if there are specific laws or policies in place, as it might cause user fatigue.

Expert E acknowledged that retrieving data from trusted sources may eliminate the need for document verification, but current policies and regulations may still require it in some cases. Expert F highlighted the complexity of data ownership and storage in the context of SSI, highlighting that maintaining pseudonymity and addressing privacy concerns are important considerations.

Design Objective 6: User Experience

User experience was considered crucial for the success of the Digital Trust Framework. Experts emphasized the need for a simple, convenient and transparent user experience. They discussed customer pain points, such as difficulties in account opening, continuous KYC updates and the importance of convenience and speed.

Expert B highlighted customer pain points related to KYC, such as difficulties opening bank accounts and payment blocks due to the compliance regime. Customers also face challenges in continuously updating their KYC information. Experts B and C confirmed that convenience, simplicity and ease of use are key factors from a customer perspective. Expert C emphasized the need for a simple digital approach to document submission to provide convenience and flexibility. The focus should be on ensuring authenticity, integrity and a user-friendly experience through an app or online portal.

Design Objective 7: Sustainability

The experts discussed various models for sustaining the Digital Trust Framework, including subscription-based fees, accreditation fees, revenue sharing and attracting SPs. They

emphasized the need for a significant user base, the availability of relevant documents and a shared commitment from all stakeholders.

Expert C suggested several possible models for sustaining the framework from a funding perspective, including subscription-based fees, accreditation fees and revenue sharing. The goal is to find a model that leverages the cost savings of SPs and does not burden end users with payment. Expert E stated that banks would be willing to pay for the information provided by the framework and proposed sharing the funding between the government and private entities. Expert E also mentioned the need for commercial benefits or incentives for issuing authorities to continue supporting the framework. Expert D highlighted the need for contributions from all participating parties to build a shared ecosystem, with initial investment being crucial.

From an adoption perspective, Expert B suggested initially focusing on improving KYC efficiency for retail customers before addressing the needs of businesses. Expert B also highlighted the financial sector's complexity and regulatory requirements, emphasizing KYC's applicability to various sectors and use cases. Expert D emphasized the importance of inclusivity and efficiency in the KYC process, while Expert C emphasized that the framework's success in attracting SPs depends on factors such as the number of active users, the availability of relevant documents and the platform's reliability and security measures.

Design Objective 8: Technology Advancement

The experts emphasized the importance of choosing the right technology for the Digital Trust Framework. They discussed the importance of modular blockchain architectures, interoperability, scalability, SSI and the need to stay updated with evolving standards and

technological choices. Interoperability was discussed as a crucial objective for the Digital Trust Framework. The experts emphasized the importance of seamless data exchange between different systems, platforms, and stakeholders, enabling efficient collaboration and integration.

Expert A emphasized the importance of modular blockchain architectures and application-specific blockchains. Expert A encouraged considering advancements in blockchain and technologies aligning with the latest innovations and interoperability capabilities. Expert D emphasized the significance of considering established standards and collaborating with other organizations. Expert D also highlighted the importance of interoperability and portability in implementing SSI. Expert D emphasized the need for widely usable digital identities across different systems and platforms within the ecosystem.

5.4 Summary

This chapter discussed the design objectives and expert evaluations of the Digital Trust Framework, focusing on streamlining the KYC process. The design objectives included efficiency, regulatory compliance, decentralization, trust establishment, privacy protection, user experience, sustainability and technological advancement. Experts agreed with these eight design objectives having each design objective agreed upon at least once by one expert. The evaluation's key insights capitalized on trusted digital identity and having government as a trust anchor. Chapter 6 details the development of the Digital Trust Framework based on these defined design objectives.

Chapter 6: Digital Trust Framework

6.1 Introduction

Based on the literature review described in Chapter 3, which focused on studies related to leveraging blockchain to improve the efficiency of KYC in the financial sector, and the design objectives defined and evaluated by experts in this thesis as illustrated in Chapter 5, this chapter describes the design of a decentralized architecture of Digital Trust Framework based on SSI and blockchain to build on the existing research and address the gaps of the KYC process. The design of the framework addresses the third objective of this research and serves as the basis for the development of the proof-of-concept prototype.

The design of a decentralized architecture to increase KYC efficiency and reduce costs was motivated by Parra-Moyano and Ross (2017). The solution proposed having a permissioned network controlled by central regulatory to enroll financial institutions. Having a central regulatory represented by the government to govern the decentralized distrusted architecture as a trust anchor could address the challenges highlighted by the experts regarding trust between the financial institutions and having non-proprietary IT infrastructure (Schlatt *et al.*, 2022). This need was also highlighted by the different experts interviewed while evaluating the design objectives defined in this thesis, as highlighted in Chapter 5. Parra-Moyano and Ross (2017) proposed that the central regulatory role is issuing identity certificates for financial institutions and customers upon registration. The KYC must be conducted for customers only once by the first financial institution they interact with. When interacting with the second financial institution, the verified documents can be retrieved from the first financial institution based on the customer's consent and without revealing the first

financial institution's identity. However, the solution described by Parra-Moyano and Ross (2017) did not highlight the customer's physical identity verification process before issuing a digital identity.

Parra-Moyano and Ross (2017) also proposed a decentralized architecture for KYC, in which the first bank that conducts the KYC stores the digitally signed document, which includes the result of the core verification process in the DLT along with the hash of each document submitted by the customer. The customer can share the KYC certificate with subsequent financial institutions. The financial institutions can verify the KYC certificate from the DLT. The challenge in the solution proposed by Parra-Moyano and Ross (2017) is that it proposes storing customer data in a centralized, permissioned database maintained by the regulator. Moreover, the proposed solution allows integrity to be checked from a local read operation on one node, which does not satisfy the objective of having a decentralized solution. Soltani, Nguyen and An (2018) proposed a similar concept to Parra-Moyano and Ross (2017) but addressed some of its limitations. Soltani, Nguyen and An's (2018) suggested solution is based on SSI and uses W3C standards regarding DID and VCs. The financial institution is registered as a trusted issuer and issues a VC after conducting the KYC verification. The VC is stored in the customer's mobile application.

The solutions proposed by some previous works did not address the KYC process requirements in terms of ongoing monitoring (Parra-Moyano and Ross, 2017; Soltani, Nguyen and An, 2018). The ongoing monitoring process requires a periodical verification of the status of the documents submitted during the initial verification to ensure that there are no changes to these documents that could impact the user's status and subsequent transactions.

The framework proposed by Schlatt *et al.* (2022) was more detailed, covering all the steps in the KYC process in three main flows: (1) identification of the customer, verification of data submitted and authenticity of identity; (2) name screening, risk assessment and enhanced due diligence; and (3) ongoing monitoring and records keeping. Moreover, it provided different scenarios for the first flow in terms of new customers, existing customers and customers with a wallet but without previously conducted KYC verification. The proposed solution is generalized to SSI but not specific to any technology. Customer data in terms of issued VCs are stored in the customer wallet, which leverages either an edge device or cloud for storage without the mandate of having a centralized repository to protect customer data and its privacy. The solution highlights the usage of eIDAS at a high level but does not discuss the details regarding the financial institutions' certificate-issuing authority and certificate-issuing process. The solution has been evaluated by experts following the DSR approach.

One of the main gaps in the solution proposed by Schlatt *et al.* (2022) is the authenticity of the initial onboarding. The solution does not highlight the mechanism used to ensure that the customer applying is genuine and maps to a physical person in the real world. Moreover, it does not describe the mechanism used to ensure that the customer is applying for himself and not impersonating somebody else. The proposed solution highlights that the customer has two options during the initial verification. The first is that the customer can visit the branch, which does not make the process fully digital or automated. The second option is that the customer can apply online but does not highlight any measure in terms of identity authenticity or the authenticity of the documents submitted, while these form the foundation of issuing the KYC certificate. It states that documents can be submitted as scanned copies,

preventing full automation as it requires an employee to verify them, reducing efficiency. The solutions proposed by previous works also did not address these challenges (Parra-Moyano and Ross, 2017; Soltani, Nguyen and An, 2018).

In addition, the solution proposed by Schlatt *et al.* (2022) did not provide any governance framework in terms of defining the responsible party to onboard the financial institutions to the blockchain, issuing certificates to these financial institutions and customers and operating the blockchain. The type of blockchain was not highlighted, including whether it is a permissioned network. The validation with regulators was not covered as part of the expert evaluation. The ongoing monitoring flow was highlighted from the verification process conducted by the financial institution, but the details of onboarding an issuer and the document issuance lifecycle were not detailed. The transactions registered in the blockchain do not provide a full audit trail in case the customer disputes sharing a document for a specific purpose. No details were provided about the user interface, demonstrating the simplicity and ease of use of the customer experience. The research paper was specific to the financial domain and was not generic to other domains such as telecom and insurance.

The Digital Trust Framework developed in this thesis builds on the solution proposed by Schlatt *et al.* (2022) and addresses the identified gaps. These gaps were added to the design objectives defined in Chapter 5. The Digital Trust Framework aims to provide a seamless digital journey covering the KYC process end to end. It incorporates requirements from stakeholders involved in real environment settings, including financial institutions, regulators, government and end users. It leverages the blockchain characteristics of being a decentralized, distributed and immutable ledger to satisfy the regulatory requirements of having an audit trail for any dispute and provide independent verification for financial institutions. Moreover, it can

ensure legal certainty in the digital identification of individuals and financial institutions and their interactions through digital identities and signatures while providing the ability to verify them. This ability can increase confidence in the security and certainty of identifying and verifying the KYC process and adherence to regulatory requirements. Moreover, since the Digital Trust Framework is a blockchain-based SSI framework, SSI principles enable users to create and manage their identities, aligning with privacy laws and principles.

The Digital Trust Framework is described in more detail in the following sections regarding architecture, processes, prototype development and evaluation by experts and end users. Moreover, DPs are derived from the blockchain-based SSI framework.

6.2 Solution Architecture

Blockchain and digital signatures using public-key cryptography are used to establish trust in the Digital Trust Framework. The Digital Trust Framework uses a private permissioned network with globally visible transactions to ensure transparency so that any node in the network can view the transactions. The permissioned network enables the blockchain to be governed through a defined onboarding process and access for all parties that join the network. This thesis proposes that the national digital government should govern the network. Digital government can form a consortium comprising different government and private entities to govern it. Moreover, a permissioned network can limit the transaction volume, increasing the throughput and scalability of the network. Ethereum is selected as the underlying blockchain technology, given its wide adoption. However, the framework can be implemented using any blockchain technology (Malhotra, Saini and Singh, 2021). All accounts in the blockchain are created as externally owned accounts. Following the general blockchain-based SSI described by Schlatt *et al.* (2022) and the definition of the VCs by

Sporny, Longley and Chadwick (2022), the Digital Trust Framework has three main actors: the Issuer, Holder and Verifier, as illustrated in Figure 13.

The transactions that the Citizen records will be conducted in the blockchain nodes hosted by the digital government, while the Issuer and Verifier can host other nodes. No coupling of any actor accounts to any specific node exists. Issuers and Verifiers can perform necessary operations, whether reading or writing on the network, without relying on a centralized authority.

The Issuer is an issuing authority, such as a government or private organization, responsible for issuing a VC about a Subject and sending the VC to a Holder. A VC is a digital tamper-evident credential with authorship that can be cryptographically verified. In the physical world, a credential is information, such as an ID, driver's license or education qualification related to the Subject of the credential, such as the Citizen of a country or an employee of an organization issued by an issuing authority to provide certain evidence about the Subject. It is difficult to identify forgery in paper-based credentials without verifying them with the issuing authority. Most of the time, the verification process is manual and takes a fair amount of time. A VC is designed to solve these challenges. The Subject is an entity with an issued VC and can be a person or institution. The Holder is the entity that owns or holds one or more VCs and creates verifiable presentations (VP) from these VCs that are shared with a Verifier. The VP is a digital tamper-evident presentation containing data derived from one or more VCs that one or more issuing authorities' issue. The VP can be cryptographically verified. In many cases, the Holder of a VC is the same as the Subject, but in some instances, it is not. For example, a VC may be issued to a child as the Subject but maintained by the partner as the Holder. For simplicity, the Subject and the Holder are the same in the context of

the Digital Trust Framework. A Verifier is an entity that verifies the VCs shared by the Holder in the form of a VP.

For the KYC use case, the Digital Trust Framework demonstrates the Issuer as the government entity responsible for issuing identity cards to Citizens, as this is the primary document for any KYC process. The Holder is the Citizen to whom the ID card is issued. The Holder owns and manages the Digital Wallet, requests VCs and shares them with the Verifier. The Verifier is the entity that performs the KYC process, here the financial institution.

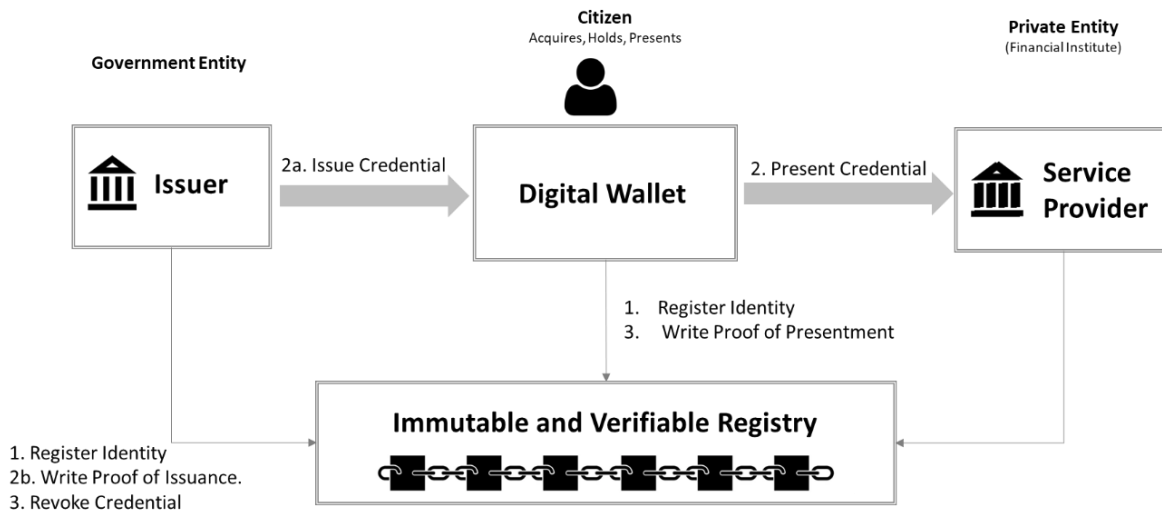


Figure 12: Digital Trust Framework architecture

As illustrated in Figure 13, the first step to add any actors to the Digital Trust Framework is to register their identity. Thus, there is a need to have unique digital identifiers to identify all actors in the ecosystem. A DID, a portable URL-based identifier, is used as the identity for each actor (Sporny *et al.*, 2022) under the actor's control and independent from any centralized registry, identity provider or CA. In the Digital Trust Framework, every actor, including the Issuer, Holder and Verifier, has a unique DID to identify their DID information.

The usage of DID follows similar design considerations as suggested in previous research (Soltani, Nguyen and An, 2018). A DID Document is the metadata associated with a DID, which is public and can be resolved against the DID globally within the namespace. The metadata related to the DID Document contains all the public keys of each actor and is registered in the blockchain to be available publicly.

The Issuer and Verifier are registered into the framework through the provision of the digital government that governs the framework, while Citizens are registered when logging into a Digital Wallet application provided to them. Citizens are identified through the National Digital Identity. As of August 2020, approximately 165 digital or partially digital identity schemes have been implemented by governments worldwide (Domeyer *et al.*, 2020). The Digital Trust Framework leverages the national identity of the UAE to register Citizens. The national identity registration vetting process is based on the highest LoA in which users are verified using their biometrics to provide their digital identities.

In the Digital Trust Framework, the authenticity and integrity of actor identities and data exchange is ascertained by a digital signature that uses public-key cryptography. Each actor is vetted while onboarding Issuers and Verifiers in the Digital Trust Framework, while Citizen registration is seamless through the national identity. Actors receive two digital certificates: one to sign off-chain data and the other to sign data using a blockchain-compatible signature. Digital certificates are issued by a CA, which is government-recognized per the UAE Federal Decree by Law No. 46 of 2021 on Electronic Transactions and Trust Services, to ensure that the digital identities of all actors are legitimate, including transactions conducted and signed by them. The public key of an actor is the only information required to verify its footprints. The digital signature keys issued for all the actors in the ecosystem are issued using

a cryptography device responsible for governing the entire lifecycle of keys. The device generates private and public-key pairs, securely stores private keys and signs and verifies transactions.

Any data created in the form of VCs or shared in the form of VPs contains the actor's DID and digital signature. The digital signature can be independently verified using the signer's public key, which is available in the DID Document. Any actor who wants to verify the signature on the data received as a VC or VP can retrieve the corresponding DID Document from the blockchain using the DID Resolver, which uses the DID as an input to retrieve the DID Document. The DID Document contains the signature of the Subject to prove its integrity. Since the DID Document is controlled and managed by the Subject, it assures the Verifier that the public-key information available in the DID Document is valid and can be trusted.

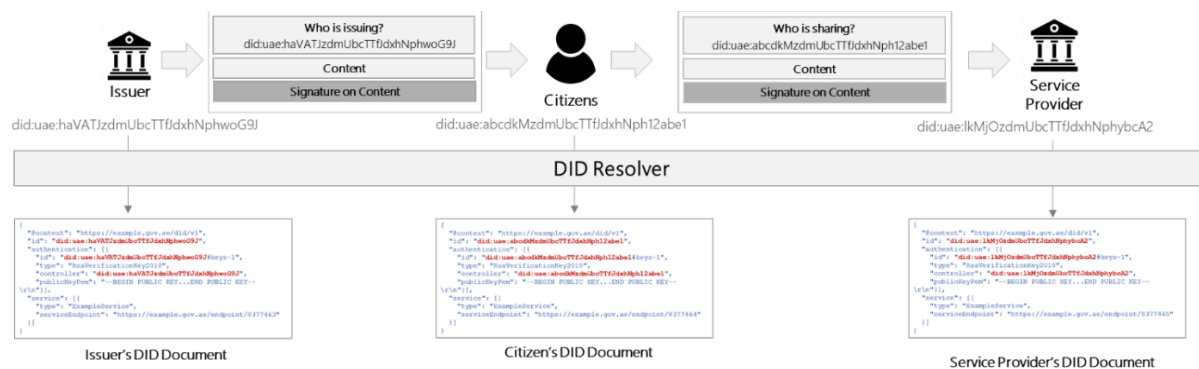


Figure 13: Decentralized identity of actors

VCS consist of three main data elements: the credential metadata header, credential metadata and claim and proof. The credential metadata header contains information about the structure of the VC, credential ID and credential blockchain reference ID. The credential

metadata and claim contain data about the Subject, such as the DID of the Emirates ID Holder (i.e. Subject), type, such as Emirates ID, issuer DID, issuance date and data of the credential (e.g. business ID) and attributes such as name and date of birth. The proof contains the Issuer's cryptographic signature to attest or authenticate the credential of the Subject. The proof assures that the VC is tamper-evident and trustworthy. It also enables systematic and independent verification, which means a Verifier should be able to verify the signature without any interaction with the Issuer. Figure 15 provides an example of the VC structure.



Figure 14: Example of Verifiable Credential structure

The VP consists of presentation metadata, VCs and proof. The presentation metadata contains data about the structure of the VP, VP ID, ID Holder sharing the presentation, the Verifier ID requesting the presentation and the verification request date. The VCs contain information about one or more VCs. The proof is a cryptographic signature added by the Holder, authorizing the Verifier to verify the VCs. Figure 16 illustrates an example of the VP structure.

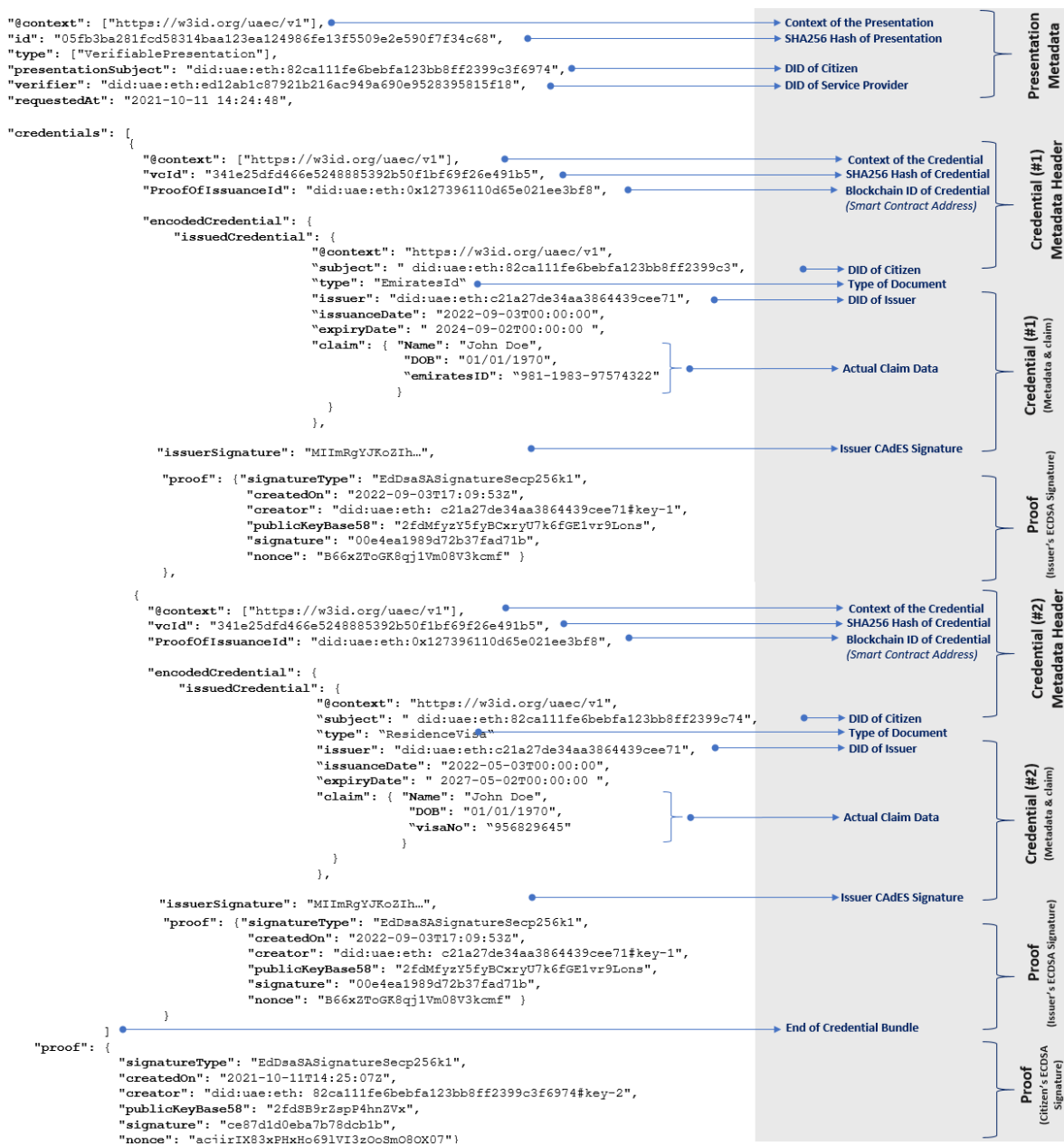


Figure 15: Example of Verifiable Presentation

The Digital Trust Framework registers transactions on the blockchain to be used for KYC audit purposes by regulators and to verify the validity of the VCs by SPs. The transactions registered in the blockchain do not include personally identifiable information (PII). Transactions are stored on the blockchain using smart contracts and serialized signed

transactions. A smart contract allows the data to be updated and enables business logic to be applied, while the serialized signed transaction, the simplest form of blockchain transaction, stores data on the blockchain. Once data is stored, no update or state change is possible.

Two smart contracts are defined in the Digital Trust Framework: the DID Document smart contract and the Proof-of-Issuance smart contract. The DID Document smart contract implements the DID specifications and can be referenced globally on the blockchain against the DID (Sporny *et al.*, 2022). The DID Document contains the public keys of the DID owner and is used to validate the signature of any data issued or presented, claiming the DID owner is conducting it. All actors in the framework will have a DID and DID Document created for them. The Proof-of-Issuance smart contract stores the credential ID and status of the issued VC. The VC is identified against the credential ID, a SHA256 hash of the credentials metadata and a claim corresponding to the credential issued to the Subject by an Issuer.

In comparison, the serialized signed transaction is used as Proof-of-Process, defined in this thesis as proof of the occurrence of an important event within the ecosystem that the originator can potentially deny. These transactions are recorded on the blockchain as permanent footprints to guard against non-repudiation. The main two events registered as part of the Proof-of-Process are the Proof-of-Presentation Request, which occurs upon receiving a request from the Verifier for a VP to be shared by the Subject and the Proof-of-Presentation, which occurs when the Subject chooses to voluntarily respond to the presentation request. In these two events, a transaction is recorded on the blockchain. These transactions and the Proof-of-Issuance enable the regulator to perform a validity check on the process and documents in case of a dispute. They also ensure accountability of every actor's action and provide transparency without revealing PII.

Once the Issuer is registered in the Digital Trust Framework, the Issuer can issue credential-upon-credential requests, creating a new Proof-of-Issuance smart contract on the blockchain. The Issuer can also revoke the credential, which updates the status of the Proof-of-Issuance smart contract. Once the Verifier is registered into the Digital Trust Framework, the Verifier can request for presentation, creating a new blockchain entry for the Proof-of-Presentation Request. Once the Citizen is registered in the framework, the Citizen can request credentials to be issued. The Citizen can also share credentials, internally creating a presentation and sending a transaction to create a blockchain entry for Proof-of-Presentation.

Figure 17 demonstrates the actors, the interaction between them, the interaction between the actors and the blockchain and the type of signature used. The Digital Trust Framework uses two types of digital signatures. The first is a CAdES signature used to sign off-chain data, specifically the VC claim by the Issuer or the VP by the Holder using their respective keys. The signature can be independently verified off-chain to ensure the integrity of the data and verify the identity of the actor who signed them. The digital signature is used as proof in the VC and the VP for on-chain transactions. All interactions need to be signed by an externally owned account. These accounts are backed by key pairs where a public key creates the account identifier and a private key to sign the transactions. In addition to the public keys being the blockchain account of the owner, they are also part of the actor's DID and act as the unique identifier for that actor within the Digital Trust Framework. This provision is critical in cases where actors (i.e. Issuers and Verifiers) host their own nodes. The identifier should be such that it is unique across actors and can be referenced directly from the blockchain.

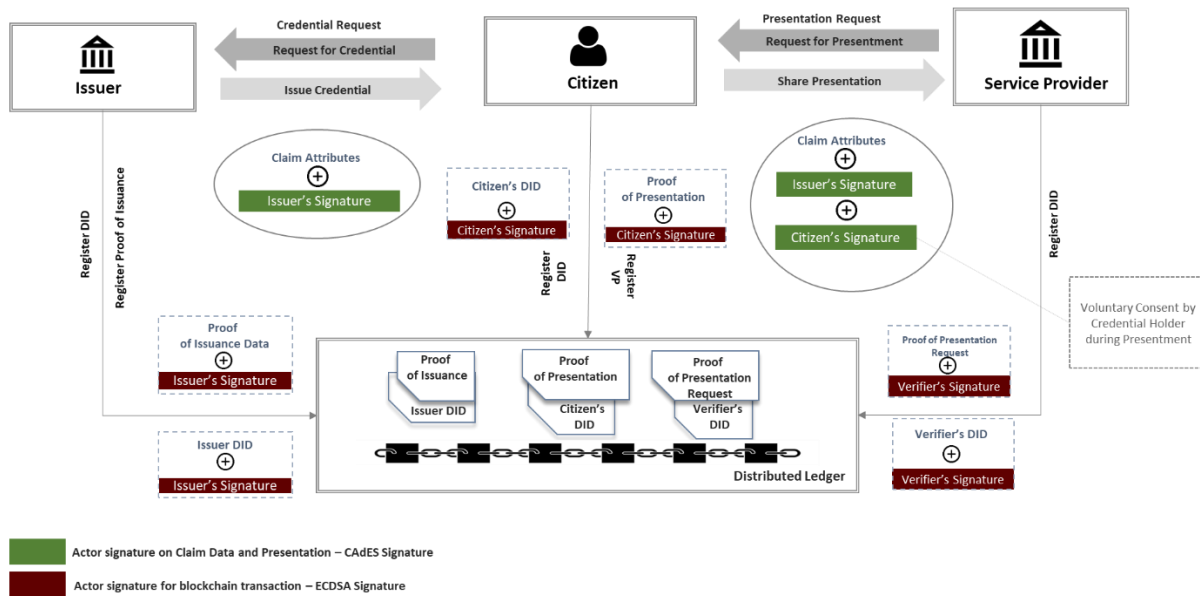


Figure 16: Transaction and key flow to increase trust

Leveraging digital signatures in off-chain data and registering Proof-of-Issuance and Proof-of-Process trust anchors on the blockchain ensures that the framework meets five essential goals: 1) data integrity, so the message received by the recipient is exactly the same message sent by the sender; 2) authenticity, so the message received is from the intended sender; 3) non-repudiation, so the sender cannot disown sending the message; 4) traceability, so every phase of the credential's lifecycle can be traced from the blockchain starting from issuance of a credential; 5) data validity, so up-to-date credential status is always maintained on-chain by the Issuer and 6) decentralization with a distributed blockchain node, so not to create a centralized personal data honeypot.

Figure 18 provides more details about the interaction between the actors and illustrates the correlation between the off-chain and on-chain data. The VCs and the VPs are off-chain data. The VC contains the DIDs of the Issuer and Holders, representing who issued it and to

whom it was issued. It also contains the Proof-of-Issuance ID, credential ID and status. The credentials are signed by the first certificate issued for the Issuer by CA for off-chain data signing, while the VC contains the Issuer signature used to register the VC in the blockchain. The Proof-of-Issuance is stored on the blockchain and correlated by the Proof-of-Issuance ID. It contains the hash of the issued credential and the latest status of the VC, enabling the validation of the validity of a VC as close as possible to the point in time of making a decision or taking action without the need for centralized authority. The status can be active or revoked.

The VP contains the DIDs of the Holder and Verifier, representing who presented it and to whom it was presented. It also contains one or more VCs. The VP also contains the Citizen's signature added to the blockchain as proof. The Proof-of-Presentation Request containing the Verifier DID, the reason for requesting the documents and the list of the document requested is stored on the blockchain and contains the hash of the presentation request. In addition, the Proof-of-Presentation is registered on the blockchain with the hash of the presentation.

The transactions are recorded with time sequences, enabling end-to-end traceability from issuance to sharing. Every actor in the ecosystem can view these transactions. However, no PII is stored in the blockchain since the DID does not directly associate with any recognized data that can reveal the identity of the actors. This omission eliminates privacy challenges. Citizens are provided with an option to securely store the VCs on their edge devices in the trusted execution environment (TEE) or cloud-backed secure storage.

Per the expert interviews, few viewed storing data in a trusted cloud provider that implements the highest security and privacy measures as the preferred option to relieve Citizens from data storage responsibility and risks of data leakage. Leveraging secure cloud

storage enables smoother backup and recovery. However, most experts in the focus group sessions, which included government officials from security and regulatory, requested that data should not be stored in any new location but should continue to be maintained by the issuing authority to avoid any duplication and centralization of data storage. Moreover, Issuer entities have robust security measures to store the data, so, to some extent, the data will be distributed in different issuer systems. This design aligns with the seven laws of identity, as no data stored on-chain can enable performing data correlation, pattern recognition or entity identification (Cameron, 2005).

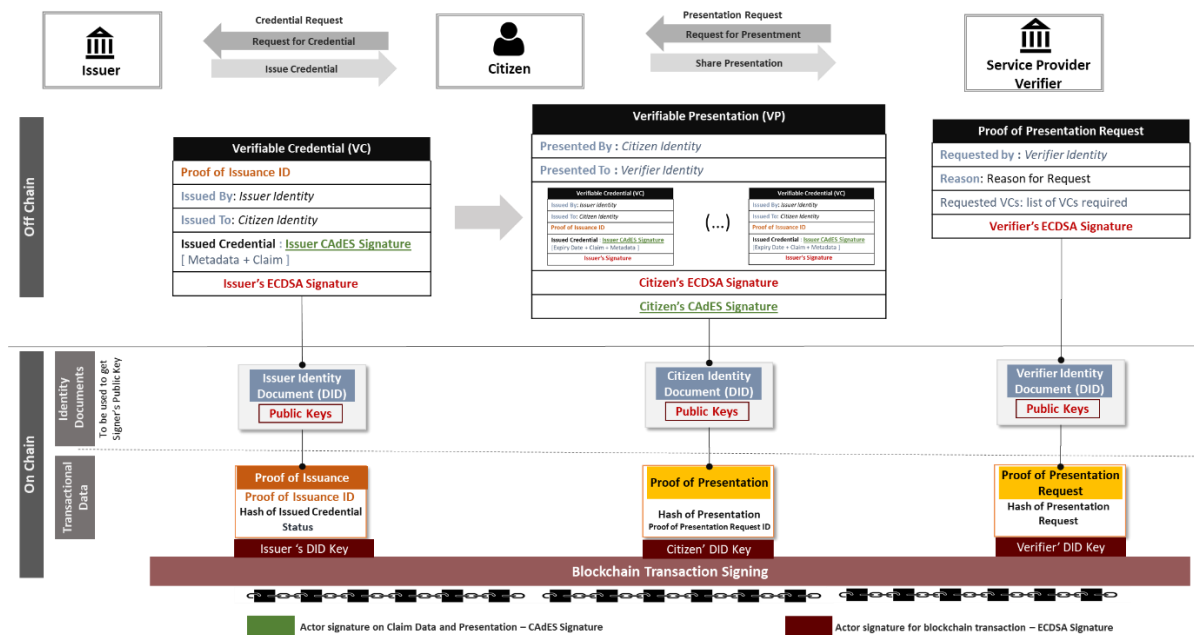


Figure 17: Correlating between on-chain and off-chain trust

6.3 Key Processes

This section details the key processes in the Digital Trust Framework related to VC issuance and revocation by the Issuer, VP sharing by the Citizen and verification by Verifier. These general processes can be applied to any KYC process. Financial KYC is detailed in the following sections as an example of a use case.

6.3.1 Issuance of Verifiable Credentials

To receive official digital trust documents from issuing authorities, Citizens must send a request to a specific Issuer using the Digital Wallet. The issuer will check the availability of the document in the system, and if the document is available, the Issuer will send a digitally trusted document to the Citizen in the form of a VC. The issuer has the option to share only raw data or include a digital copy of documents for the Citizen. The Citizen can view, download and share the digitally trusted document (i.e. a VC using the Digital Wallet application).

At a high level, the process of issuing VCs by the Issuer and sending them to Citizens using the Digital Wallet application as part of the Digital Trust Framework involves the following steps: 1) Citizens request an issuing authority to issue a digital copy of the specific official document in the form of a VC. 2) Issuers retrieve the required official document from their system of records per their current back-office process. 3) Issuers digitally sign the document and data using private keys issued by the trusted CA through the national digital signature eSeal service. 4) Issuers register the VCs on the blockchain. 5) Issuers share this document (i.e. VCs to Citizens through Digital Wallet backend services). 6) Citizens can view, download and share the document in the form of a VP using the Digital Wallet application with SPs to prove eligibility to avail certain services. 6) Issuers can revoke any digital document (i.e. VCs registered on the blockchain) at any time by sending a notice to the Citizen through the Digital Wallet.

When Citizens access the Digital Wallet application, their unique national ID numbers are retrieved from the National Identity System in real time. The numbers are used to retrieve their VCs from the Issuers. Below are the steps to retrieving a VC:

- 1) Citizen's log into the Digital Wallet application and navigate to "Documents" to add a document by selecting a specific Issuer.
- 2) The request goes to the Digital Wallet backend, which sends a request to the Issuer.
- 3) The issuer receives the request from the Digital Wallet backend, retrieves all document metadata from their system of records (SOR) using the Citizen's national ID and sends the response back.
- 4) The Digital Wallet application displays the list of all documents available and their type to the Citizen.
- 5) The Citizen selects the document to be added and clicks on "Add Document".
- 6) The request goes to the Digital Wallet backend, which sends a request to the Issuer with the Citizen's national ID, DID, document(s) ID and type.
- 7) The issuer receives the request from the Digital Wallet backend and retrieves the document details from their SOR using the Citizen's national ID, document types and references.
- 8) The issuer creates a VC and adds the Issuer ID, Citizen ID and document claim data.
- 9) The issuer generates a SHA256 hash of the encoded claim data and sends the hash to the national digital signature eSeal CAdES signing API.
- 10) Once the Issuer receives the signed hash, it adds it to the VC.
- 11) The issuer mines the Proof-of-Issuance transaction on the blockchain using its private keys and receives the Proof-of-Issuance ID.

- 12) The Issuer stores the Proof-of-Issuance ID in the SOR and maps it to the specific credential.
- 13) The issuer adds the Proof-of-Issuance ID to the VC and shares the VC with the Digital Vault backend to conduct cryptographic verification of the Issuer's identity, data integrity and credential status on the blockchain.
- 14) The Digital Wallet shows a successful screen to the Citizen.

Figures 19 and 20 describe the sequence flow between the different actors and systems to issue the VC by the Issuer. As illustrated in the diagram, the Issuer (SOR) stores the Proof-of-Issuance ID of the document in case a Citizen loses an account or the VCs. Then, the Digital Wallet can retrieve all the VCs associated with the Citizen from the Issuers using the Proof-of-Issuance ID associated without storing PII. The issuer SOR can always validate the availability of the credentials on the blockchain using the Proof-of-Issuance ID and the credential hash. Moreover, the Issuer can use the Proof-of-Issuance ID to revoke the VC.

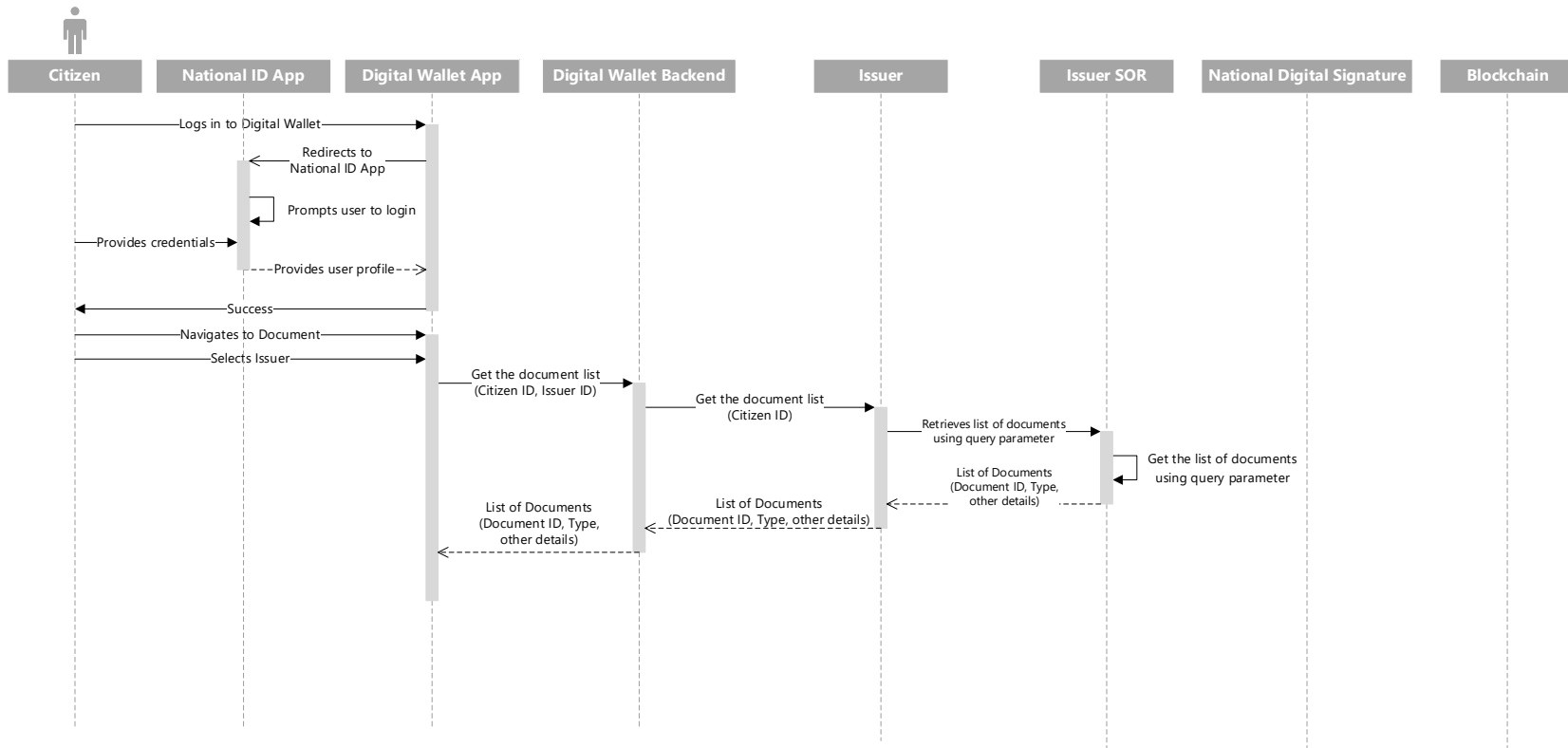


Figure 18: Retrieving documents (VCs) from the Issuer (Sequence diagram – Part 1)

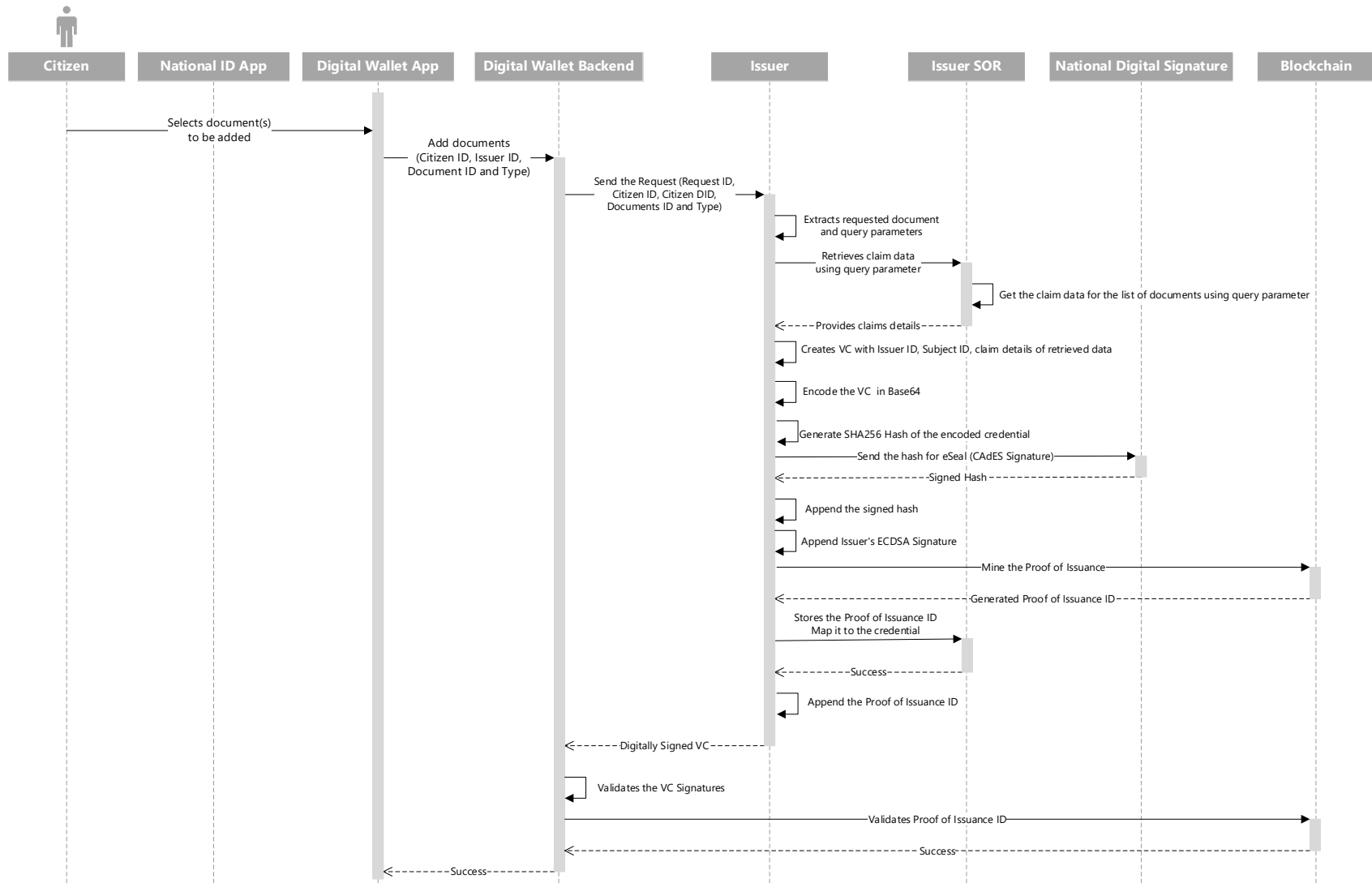


Figure 19: Retrieving documents (VCs) from the Issuer – (Sequence diagram – Part 2)

6.3.2 Revocation of Verifiable Credentials

Revocation is the last phase of a credential's lifecycle. Revocation of a credential occurs when a new document is issued to replace the old one in the real world or the existing document is cancelled. The Issuer must ensure that the revocation is generated for actual business reasons or amendments in the data (e.g. updating the surname in the credential). Depending on the reason for revocation, if a new document is generated, the Citizen should be able to retrieve it. Every document has a set of business attributes, among which a few are key attributes for SPs to guide them in making business decisions related to their processes. For example, a person's name can be a key attribute for an SP, while a document ID may not be a key business attribute. The Issuer should revoke an existing document only if there are changes in key business attributes. Therefore, before revoking a document due to data changes, the Issuer must ensure that at least one key business attribute has changed. The following two sequence flows illustrate the flow of a business-driven revocation and a data change revocation.

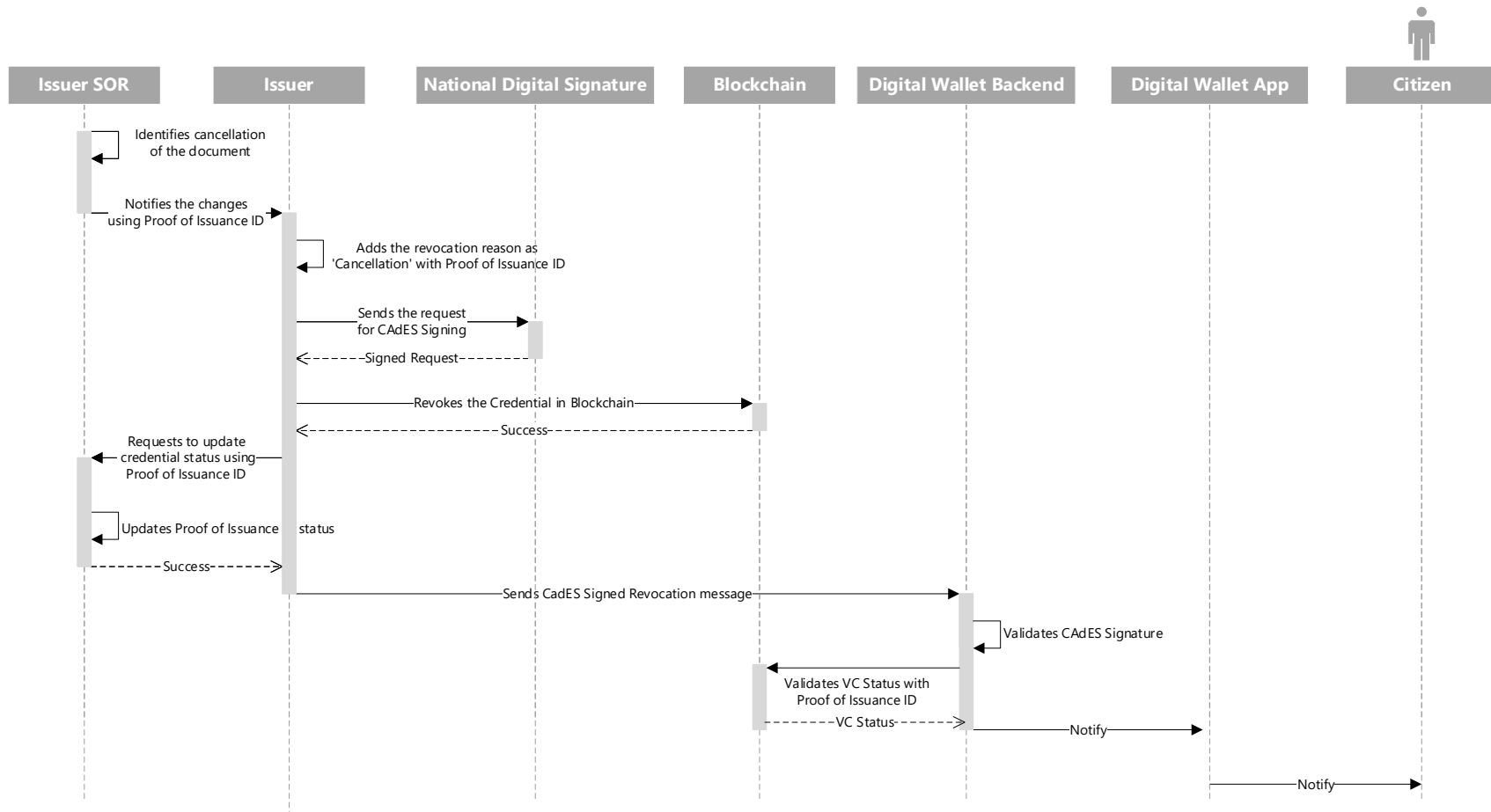


Figure 20: Business revoking a verifiable credential

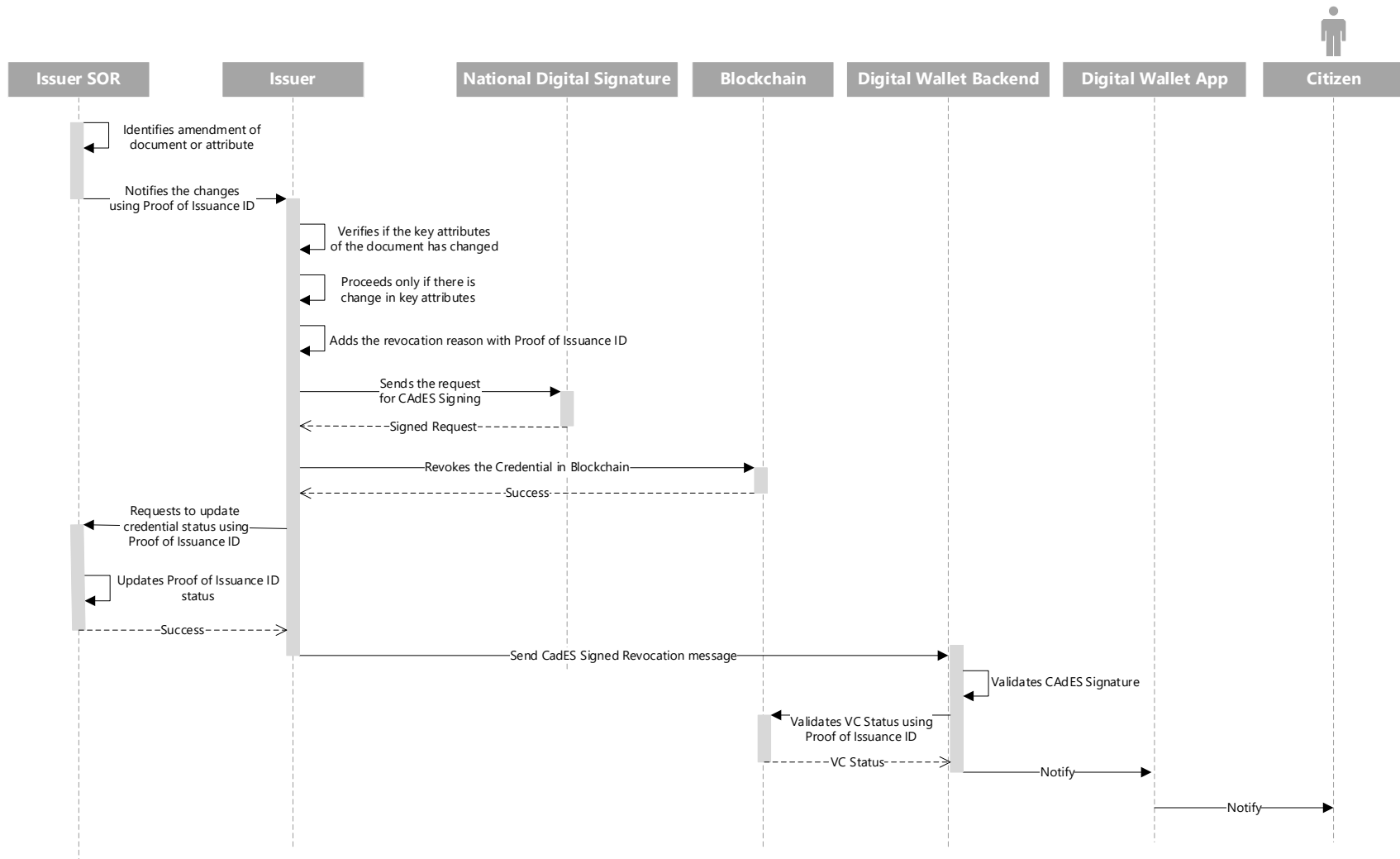


Figure 21: Data revoking a verifiable credential

6.3.3 Sharing Verifiable Credentials

To avail digital services, Citizens apply for them through the supported channels of the SP, which could be a website or mobile application. SPs request Citizens to submit required data and documents through the Digital Wallet application. At a high level, the process of SPs attaining access to data in the Digital Wallet involves five steps: 1) The SP systematically requests data needed to grant a service or product to a Citizen. 2) The Citizen receives a notification in the Digital Wallet application. 3) The Citizen can choose to share the requested data with voluntary consent. 4) The requested information is shared systematically by the Digital Wallet to the SP. 5) Upon receipt of the data, the SP's application can perform several steps to validate the data and provide the service to the Citizen.

The process of availing a service from an SP differs slightly depending on the SP channel the Citizen accesses (i.e. website or mobile), the Digital Wallet channel the Citizen uses and whether the Citizen accesses both channels from the same or different devices. For simplicity, the process is described assuming the Citizen accesses the SP channel through the website from a desktop or laptop while using the Digital Wallet application installed on a mobile phone. The detailed steps involved in sharing data with the SP are as follows:

- 1) The Citizen selects a specific service from the SP's website.
- 2) The SP's website collects basic data about the Citizen and service to determine the VCs to be requested from the Citizen through the Digital Wallet application.
- 3) The SP's website creates a VP request (i.e. data-sharing request), which includes the SP DID, the purpose of request of sharing, request ID, QR ID, QR expiry date, sharing

request expiry date based on the business rules of the SP and requested documents (i.e. VCs) to be shared by the Citizen.

- 4) The SP encodes the VP request in Base64 and generates an HMACSHA256 hash.
- 5) The SP mines the Proof-of-Presentation Request on the blockchain using its private keys to receive the Proof-of-Presentation Request ID, a hash of the request.
- 6) The SP generates a QR code containing the details of the VP Request and the Proof-of-Presentation Request ID.
- 7) The Citizen uses the Digital Wallet application to scan the QR, which sends the details to the backend to verify the request, persist the request ID and automatically open the notification detail screen for the Citizen.
- 8) The Citizen can view the notification details on a mobile device.
- 9) When confirming the sharing, the Citizen is prompted to provide a password to digitally sign the sharing using the National Digital Signature Platform as a means of consent for sharing documents.
- 10) The Digital Wallet backend registers the Proof-of-Presentation on the blockchain, including the hash of the Presentation and the Proof-of-Presentation Request ID, while sharing the details with the SP.
- 11) The SP can verify by cryptographically verifying the CAdES signature of the Citizen and the Issuers of the VCs. Moreover, the SP can verify the status of the VCs using the blockchain. The following section provides more details about the verification process.

The sequence diagram below illustrates the steps described:

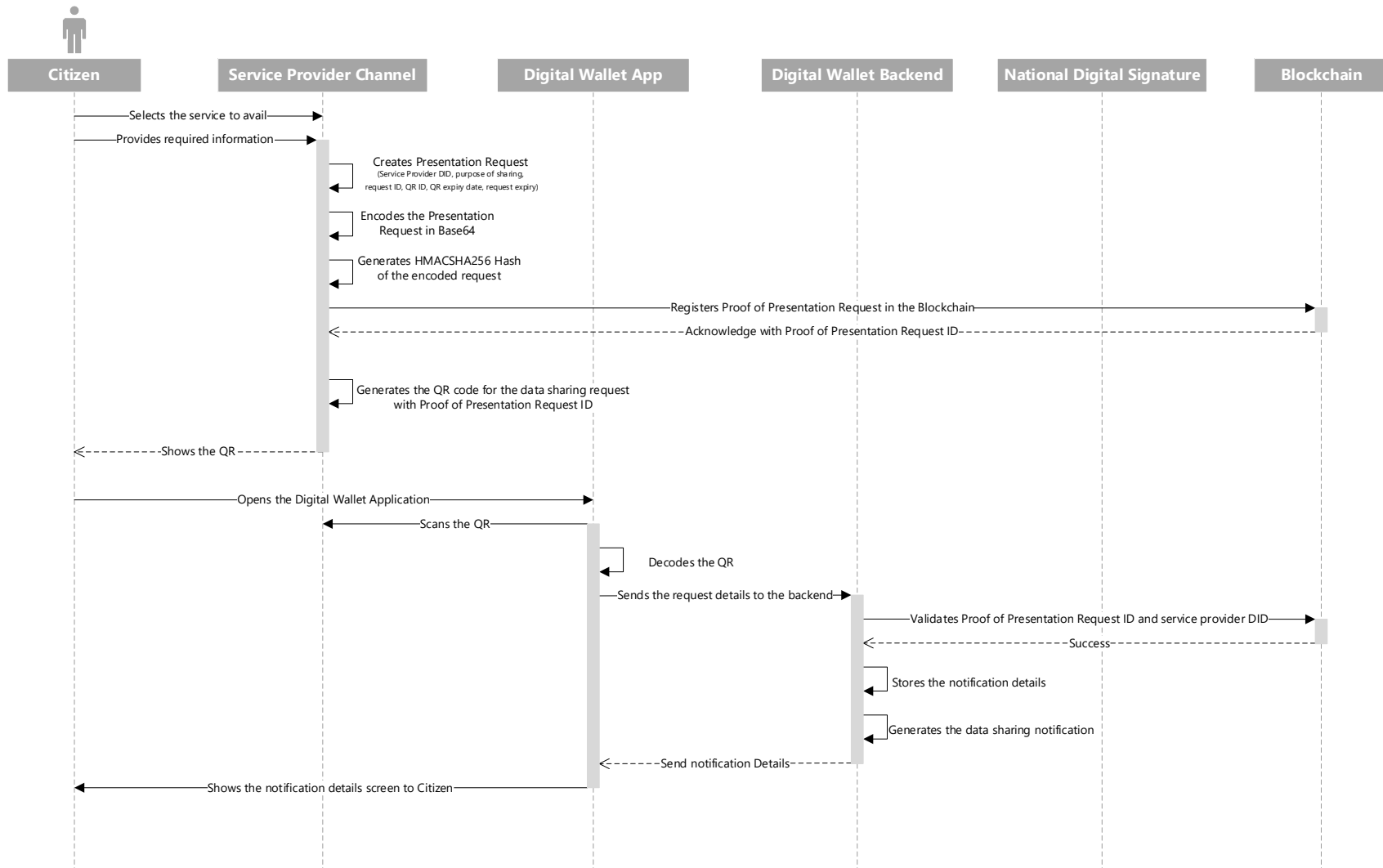


Figure 22: Sharing Verifiable Presentations – (Sequence diagram – Part 1)

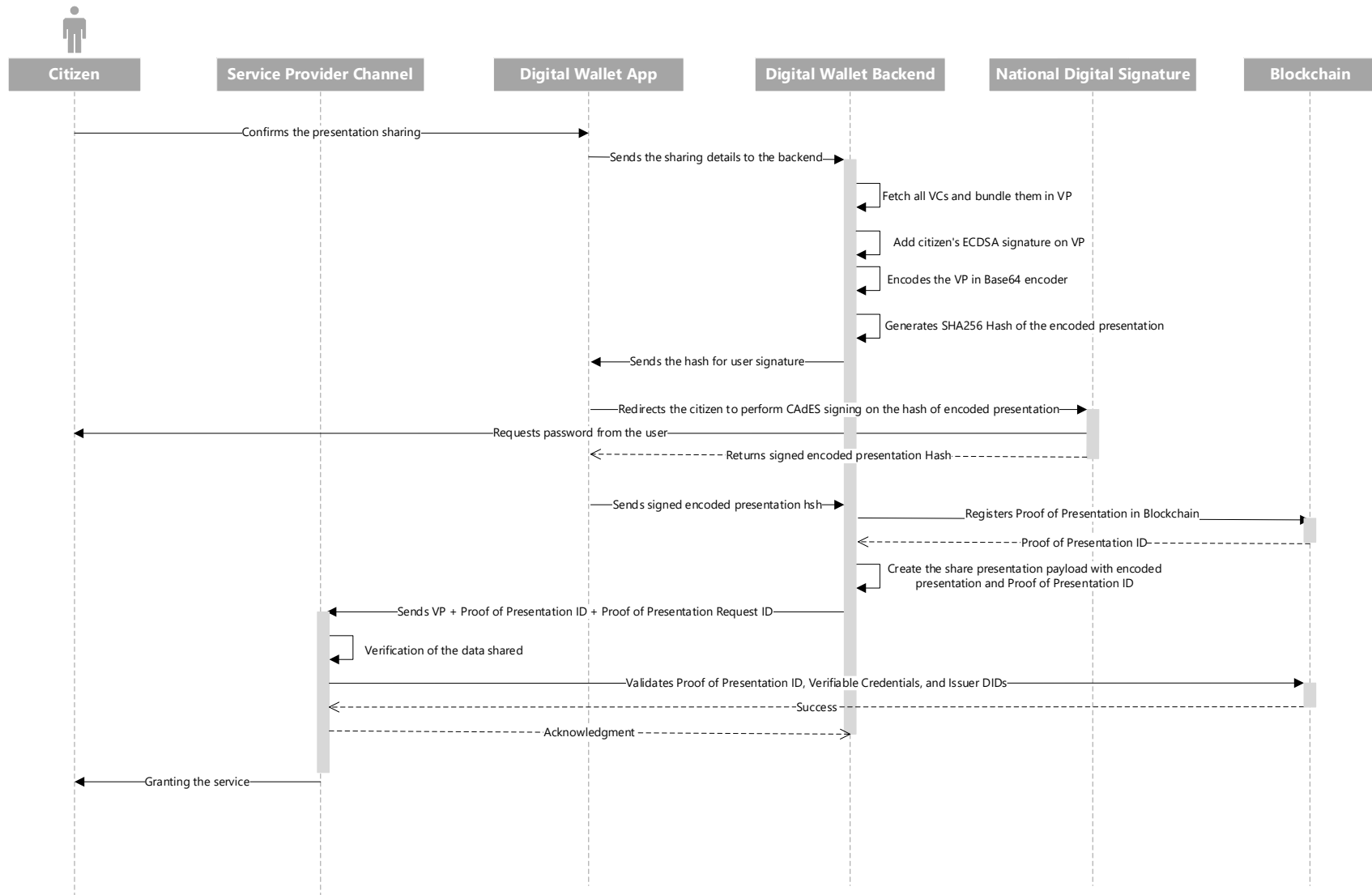


Figure 23: Sharing Verifiable Presentations – (Sequence diagram – Part 2)

6.3.4 Verification of Verifiable Credentials

The SP can verify the integrity and authenticity of the data through various security and identity measures added to the VP described in Section 6.2 with more details on the verification process. Figure 25 demonstrates different digital signatures in the VP that the SP can use to validate the integrity and authenticity of the data received.

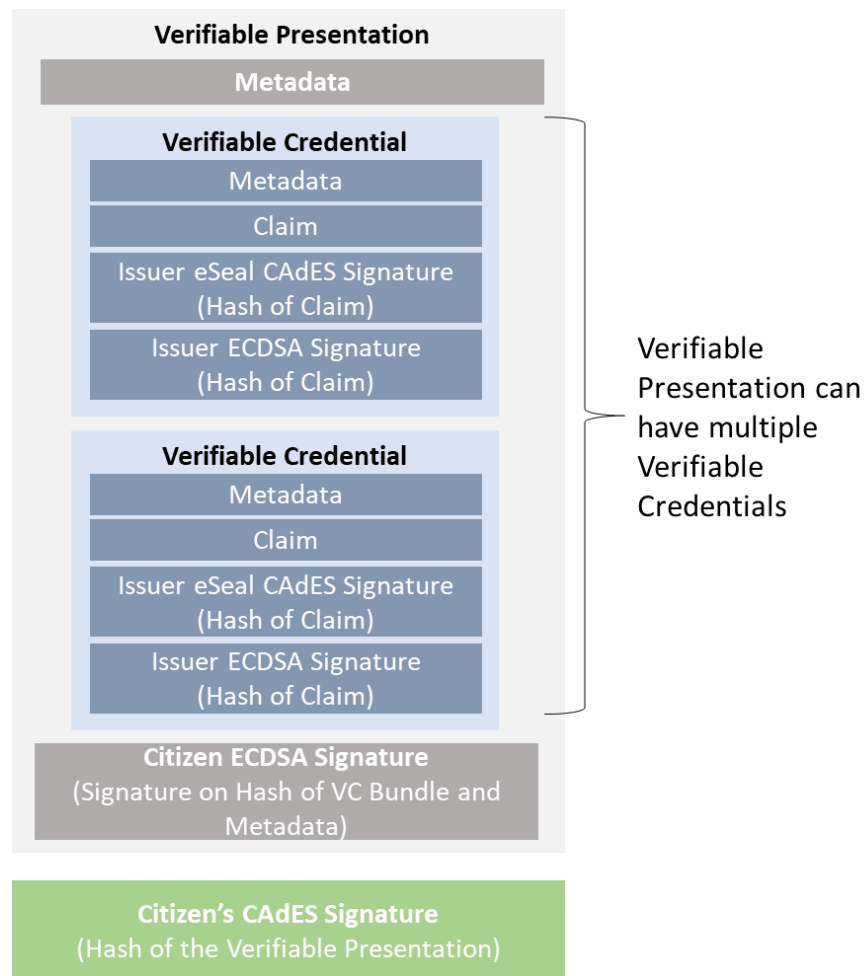


Figure 24: Various digital signatures on the Verifiable Presentation

Based on Figure 25, a service provider's verification process can be divided into two categories: verifying the VP and verifying the VCs. The diagrams below illustrate these two verification processes.

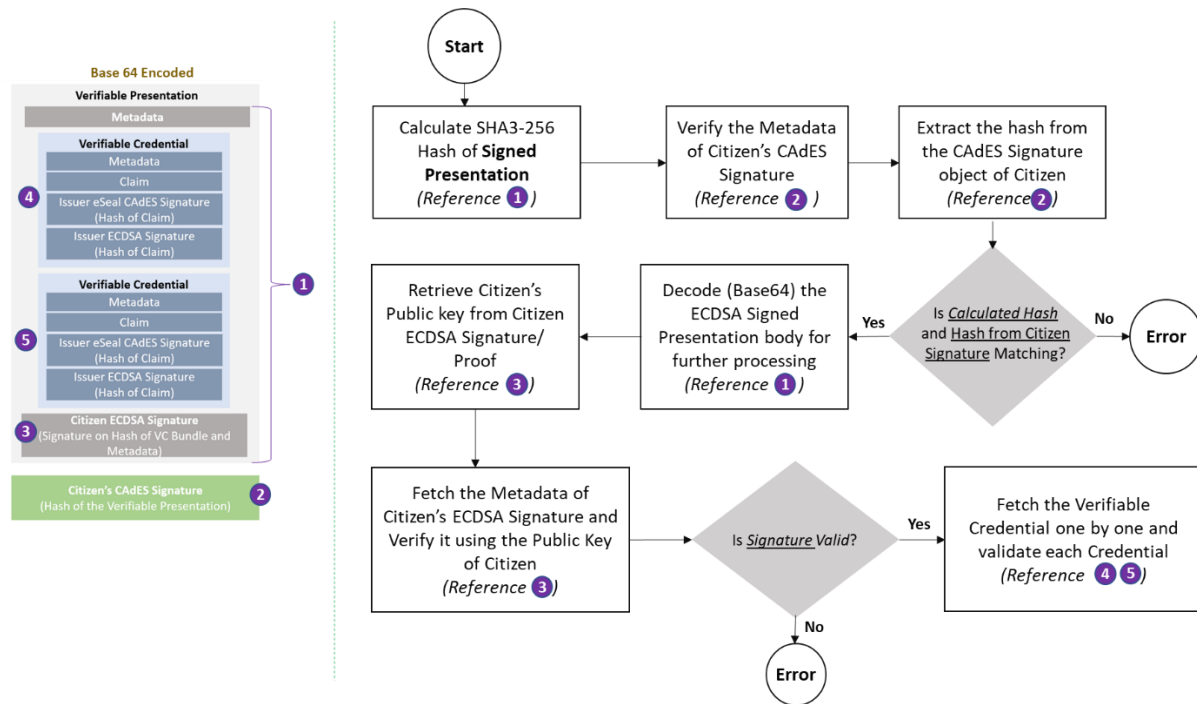


Figure 25: Verification of the Verifiable Presentation

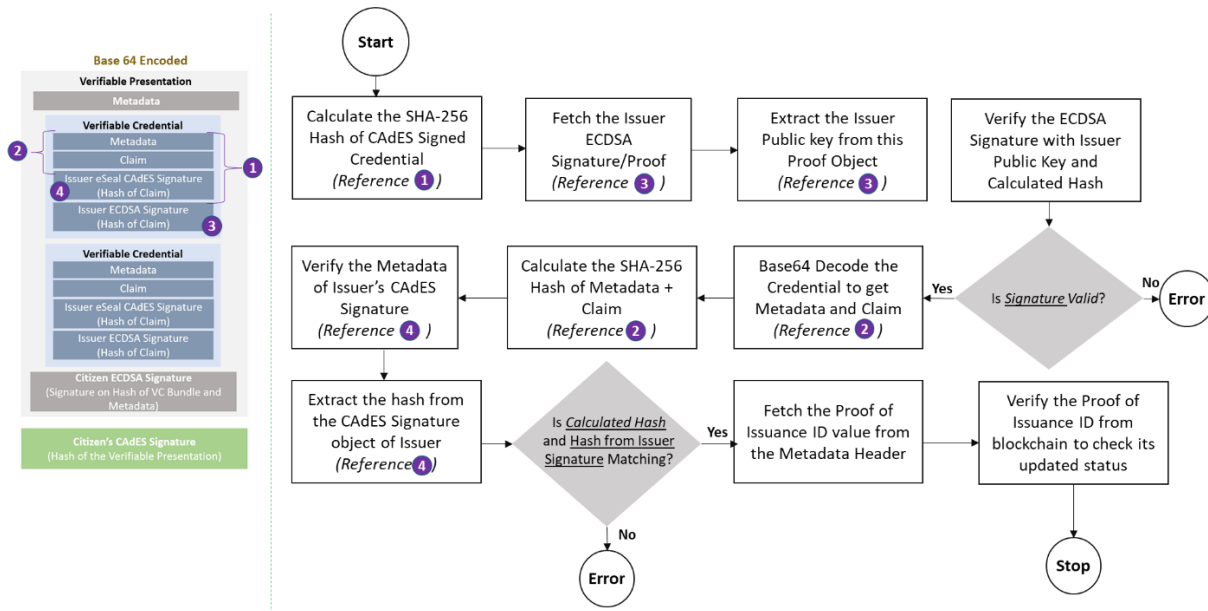


Figure 26: Verification of the verifiable credential

The verification steps enable the Verifier to conduct validity and authenticity checks to determine that the digital documents submitted are genuine and authentic and have been issued by the official entity (R 4.4). They can also validate that the customer's digital identity maps to a physical identity in the real world to ensure that the documents submitted are associated.

6.3.5 KYC Process

This section details the KYC process based on the Digital Trust Framework, a modified process of Schlatt *et al.* (2022), who described a financial KYC process as three main sub-processes: (1) customer identification, data verification and identity authentication; (2) name screening, risk assessment and enhanced due diligence; and (3) ongoing monitoring and records keeping. Schlatt *et al.* (2022) highlighted three scenarios for the first sub-process: 1) completely new onboarding where the customer does not have a wallet, 2) new to KYC where

the customer has a wallet and the required VCs to conduct a KYC process, and 3) fast onboarding where the customer has a wallet and VCs that attest a previously completed KYC process. In this thesis, the third scenario, fast onboarding, is not considered because the Digital Trust Framework asserts trust based on the identity registered by every actor in the echo system. Thus, the VC's identity must be publicly available for verification purposes. Moreover, the framework is designed to be generalized and support different KYC use cases in different domains. Finally, trust between financial institutions is not the preferred option per the expert interviews highlighted by Schlatt *et al.* (2022) and the expert interviews in Chapter 5.

Since new to KYC is a subset of the completely new onboarding, the focus is on demonstrating the completely new onboarding as described below:

- 1) The Citizen downloads and installs the Digital Wallet application.
- 2) The Citizen registers in the Digital Wallet using the National Digital Identity with the highest LoA (e.g. biometrically verified profiles).
- 3) The Digital Wallet backend registers the DID of the Citizen in the blockchain. No PII is stored in the blockchain. The DID is a derived ID from the Universally Unique Identifier (UUID) of the National Digital Identity. The mapping between the UUID and the DID is stored off-chain. The business national ID number retrieved from the National Digital Identity is stored in the Citizen session in the Digital Wallet upon login with the National Digital Identity and the UUID.
- 4) The Citizen can request documents from registered Issuers using the Digital Wallet.

- 5) The Issuer with a DID registered in the Digital Trust Framework issues VCs to the Citizen. The Issuer registers the Proof-of-Issuance on the blockchain using its private keys, consisting of the hash of the issued credential and the credential status.
- 6) The Issuer sends the VC to the Citizen through the Digital Wallet application, which can cryptographically verify the VC and the legal identity of the Issuer.
- 7) The Citizen can view and share the VC with the SP.
- 8) The Citizen accesses a financial institution's digital channel to avail a service (e.g. opening a bank account). The financial institution must be registered in the Digital Trust Framework.
- 9) The registered financial institution with a DID in the Digital Trust Framework request's identity documents from the Citizen in the form of a QR and registers the sharing request in the blockchain as a Proof-of-Presentation Request with the hash of the request using its private keys.
- 10) The Citizen scans the QR code using the Digital Wallet application, which validates the QR code and cryptographically verifies the identity of the financial institution and the sharing request. Upon validation and verification, the Digital Wallet application displays the notification to the Citizen.
- 11) The Citizen verifies the sharing request details containing the financial institution's identity reason for requesting the documents and the list of documents to be shared.
- 12) If Citizens do not add any of the requested documents, they can do so following steps 4 to 6.

- 13) The Citizen consents to the acceptance of sharing the identity documents with the financial institutions by digitally signing the acceptance using a qualified signature from the National Digital Signature Platform.
- 14) The Digital Wallet backend registers the Proof-of-Presentation on the blockchain and shares the VP with the financial institution along with the Proof-of-Presentation ID and Proof-of-Presentation Request ID.
- 15) The financial institution conducts the verification process, which includes verifying the Citizen's identity, the data's integrity, the data's authenticity from a legal issuing authority and the validity of these documents. The verification is conducted through the cryptographic signatures of the Citizen and Issuer to ensure legitimacy. Moreover, document validity is verified through its status on the blockchain.
- 16) The financial institution can conduct name screening. As Schlatt *et al.* (2022) described, the name screening service can be a backend process where the financial institution checks the data against publicly known blacklists associated with terrorism, illegal money laundering activities, PEPs and negative press.
- 17) The financial institution conducts the risk assessment. The outcome of name screening and other information is sent to the risk engine to classify the customer into a risk class, which can be low, standard or high based on the calculated risk score of the risk engine.
- 18) Based on the risk assessment, the financial institution may conduct additional checks requesting the Citizen to share additional documents using the same process.

19) Upon successful verification, the financial institution grants the Citizen the service (e.g. opening a bank account).

The above process is generic and can be applied to any KYC use case from any domain. This process enables end-to-end digitization of the KYC process without the need for manual intervention. The whole process can be completed in a few minutes. The customer does not need to visit the branch for any verification. Moreover, the documents submitted to financial institutions can be trusted legally.

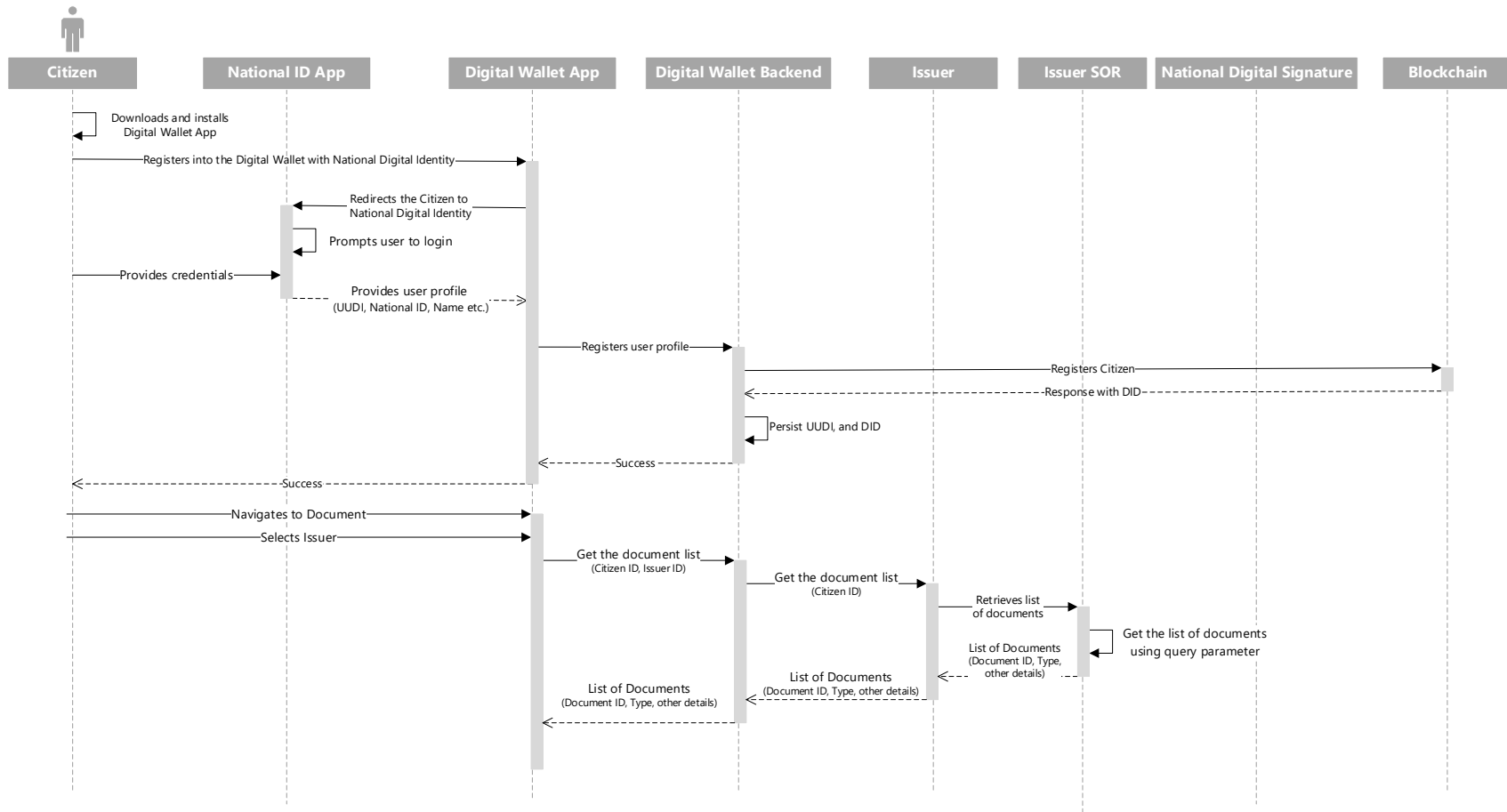


Figure 27: KYC process completely new onboarding – (Sequence diagram – Part 1)

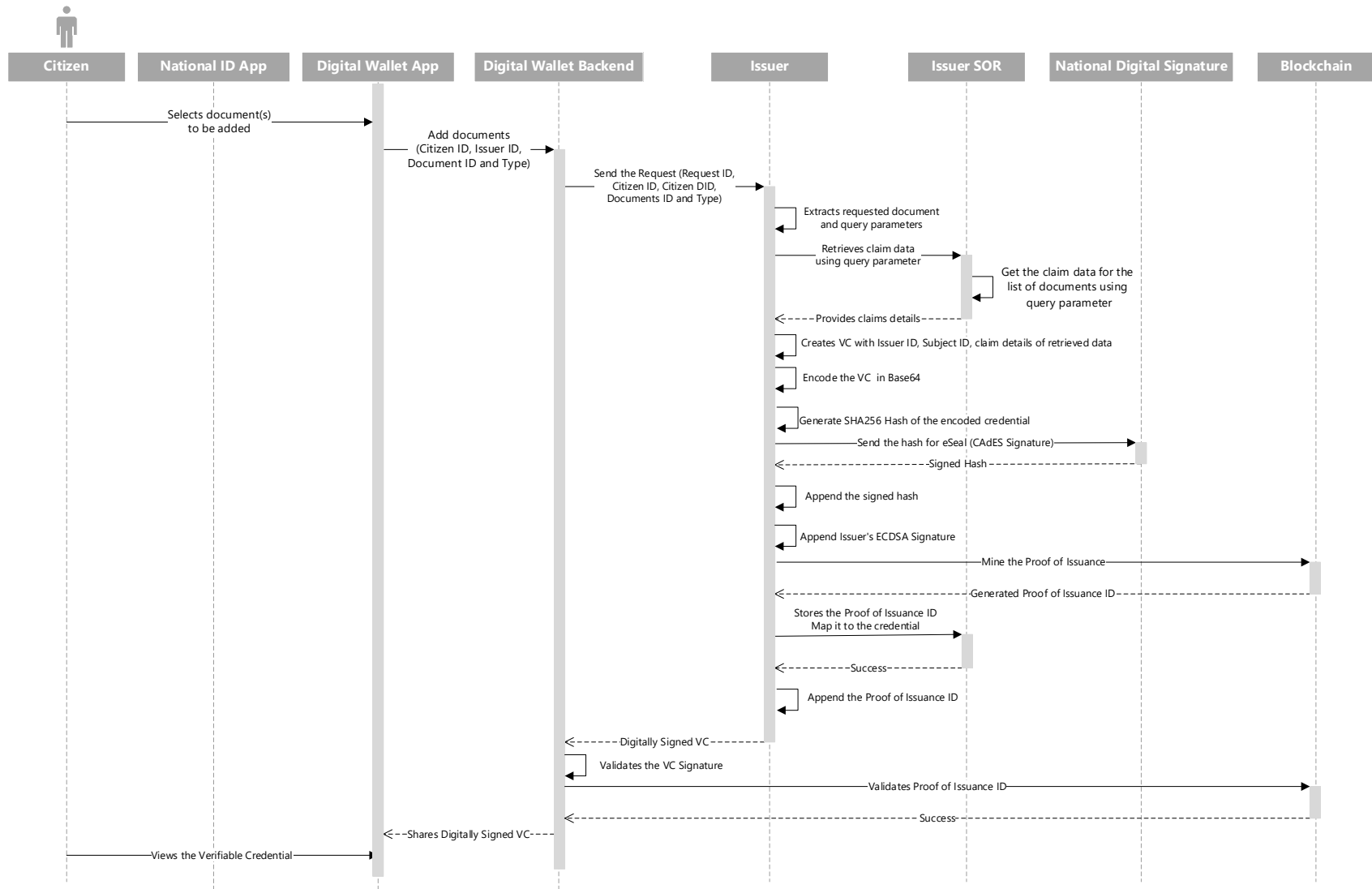


Figure 28: KYC process completely new onboarding – (Sequence diagram – Part 2)

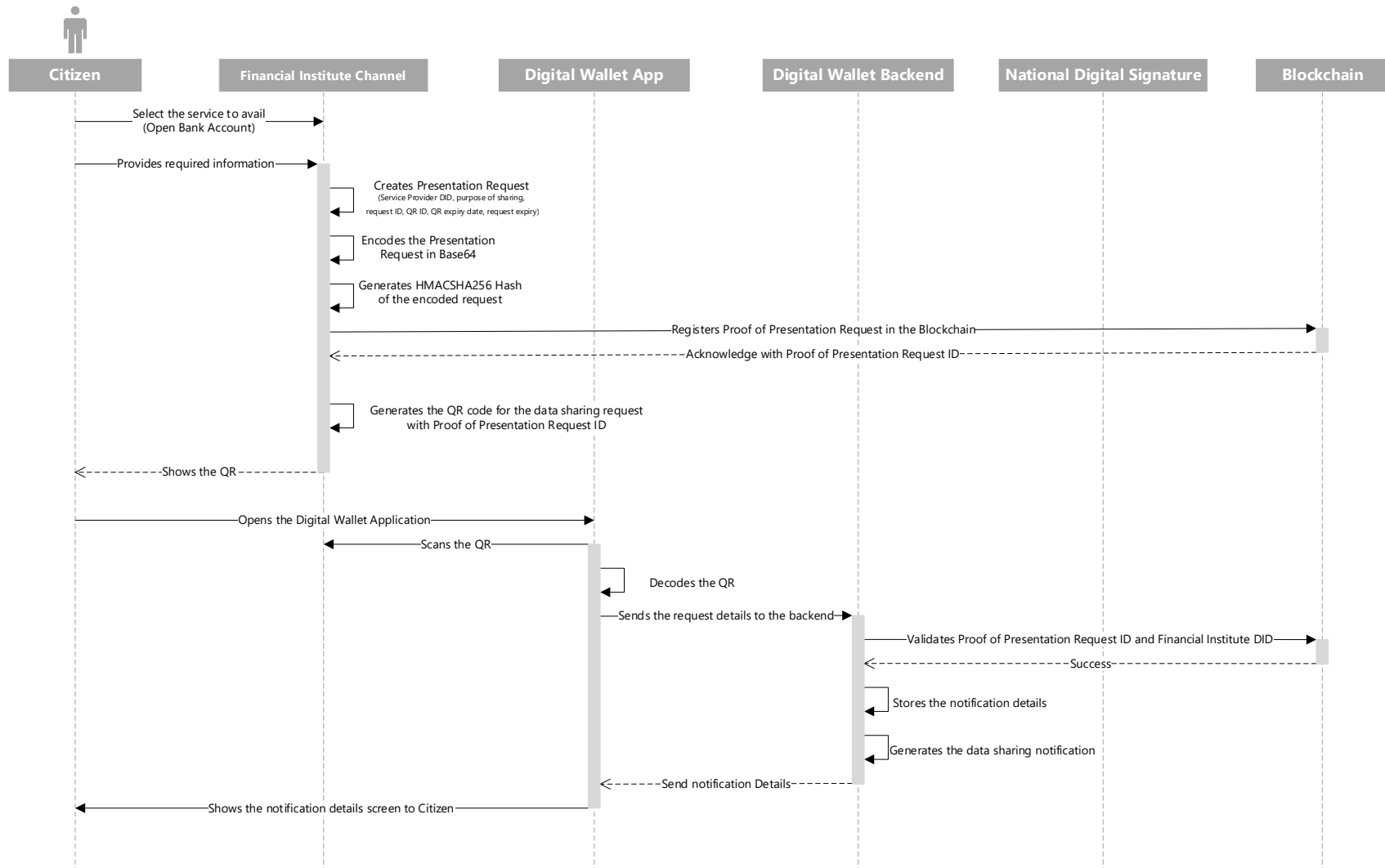


Figure 29: KYC process completely new onboarding – (Sequence diagram – Part 3)

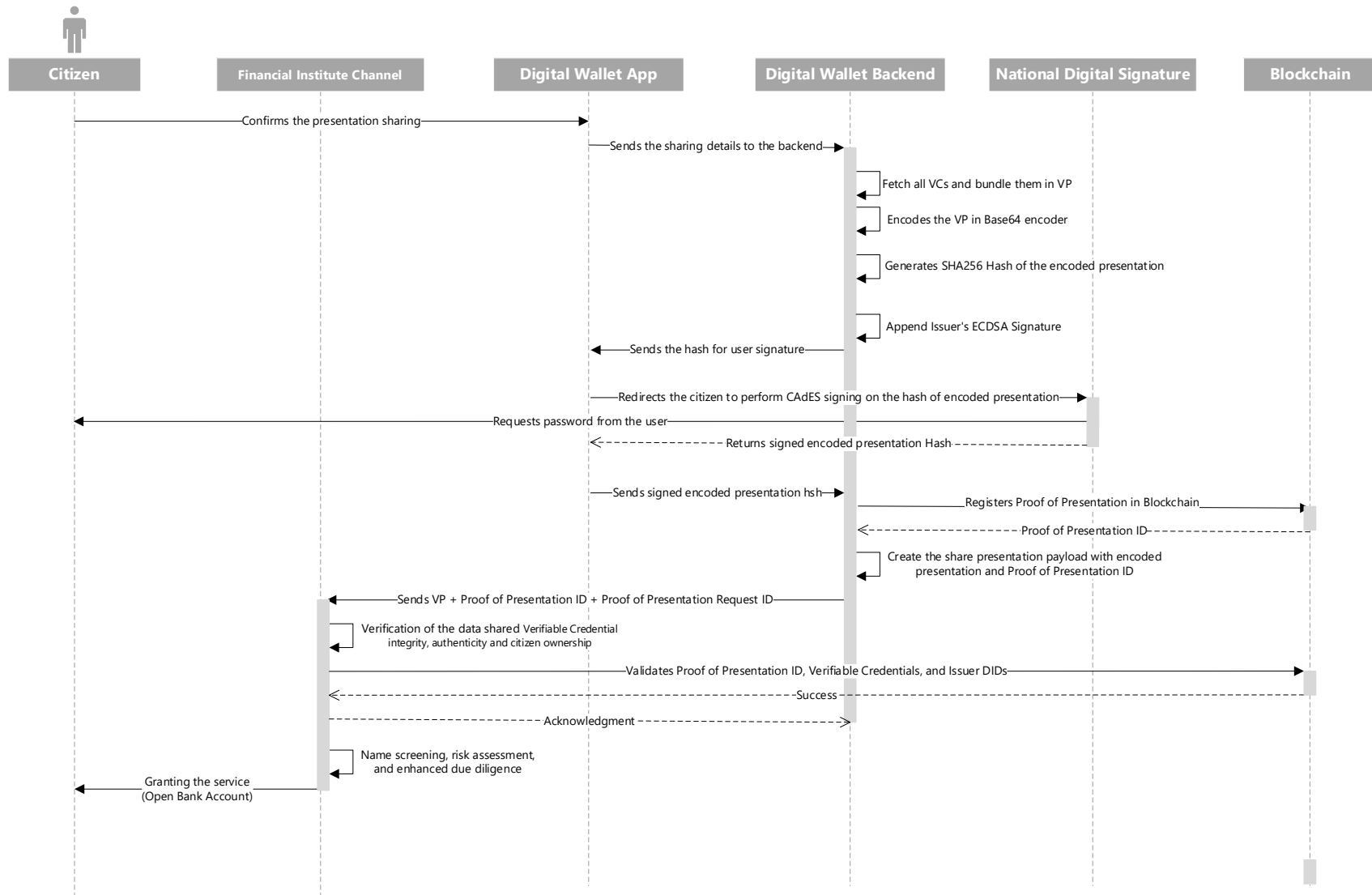


Figure 30: KYC process completely new onboarding – (Sequence diagram – Part 4)

Upon successful account opening for the Citizen, the financial institution must conduct ongoing monitoring as part of the KYC process. Schlatt *et al.* (2022) described the process as continuous checks during the business relationship conducted by the risk engine to compare the customer's ongoing transactions with the expected transaction volume. Moreover, the risk engine checks the transactions to identify suspicious transaction patterns. Beyond Schlatt *et al.* (2022), the Digital Trust Framework enables the financial institution and its risk engine to check whether VCs in the VP have expired based on expiration dates. The risk engine of the financial institution can regularly and independently check the validity of the VCs based on the blockchain status. The VCs may become invalid prior to their expiration dates. If the risk engine identifies during its periodical checks an abnormal transaction behavior or expired or invalid VCs (i.e. revoked), the risk engine can re-evaluate the risk and recommend measures to mitigate these risks if required. The financial institution can also have a blockchain node and use an event listener that can immediately identify the invalidity of any of its customers' VCs.

Upon VC expiry or invalidity, the financial institution can request that the Citizen share new VCs. If the Citizen receives the new VC from the Issuer, the Citizen can consent to share it with one click, ensuring a fully digitized, automated ongoing monitoring process without manual intervention by the financial institution while keeping Citizen records up to date.

The Digital Trust Framework enables Issuers to define key attributes and revoke VCs based on changes in them. This important design considers eliminating VCs' revocation and request when the changes do not impact business.

The concept of SSI theoretically does not require any party to store a Citizen's personal data, so the data is only required to be stored by the Citizen in the Digital Wallet to be acquired on demand. However, financial regulations mandate financial institutions to store customers' personal information for a specific duration in their local storage so that in case of suspicious or illegal conduct, the customer's identity can be identified unambiguously. Thus, financial institutions should store the VP to trace any transaction in case of suspicious or illegal conduct or dispute, ensuring no manipulation of the data or transactions. The sequence of transactions can be traced through blockchain events registered with timestamps and can be cryptographically verified to ensure it is tamperproof and of non-repudiation.

The KYC process described in this thesis provides an end-to-end, seamless and automated experience. The Citizen and the financial institution do not need to conduct manual interactions for the Citizen's identification, data collection and verification. The digital identity and documents in the form of VCs digitally signed with a registered footprint on the blockchain enable authenticity checking while confirming integrity. Moreover, adherence to the UAE Law No. 46 of 2021 on Electronic Transactions and Trust Services, derived from eIDAS, implies that the 5th EU AML Directive recognizes the KYC process as a valid form of identification.

Thus, Citizens can create their own DIDs while registering in the Digital Trust Framework, adding their information. Information is not stored centrally as the Digital Trust Framework is built on a decentralized distributed architecture, so users' DIDs are stored in a decentralized form. The information added by a Citizen is also stored in a distributed manner in the SOR of the issuing authorities. Moreover, leveraging a digital identity that registers a Citizen with the highest LoA conforms to the user existence principle of the SSI, where users

must have an independent existence in the real world while encoding their characteristics digitally to exist in a digital domain. The Digital Trust Framework complies with other SSI principles, such as consent and minimization, as well as different aspects of the GDPR and UAE Federal Decree-Law No. 45 of 2021 Regarding the Protection of Data Protection in terms of collecting data for a specific and clear purpose, conforming to the seven laws of identity defined by Cameron (2005). Moreover, since consent is user-driven and conducted for limited purposes, it addresses the challenge of consent fatigue where users are loaded with sharing notifications, as highlighted by Soltani, Nguyen and An (2021).

6.4 Digital Wallet Prototype

A prototype of a mobile digital wallet was developed to address the requirements of design objective 6 related to the user experience. The prototype was developed using proto.io,⁷ a web-based prototyping platform for building interactive prototypes for any device and screen size, including mobile, tablet and web. It also can share and test the prototype. No former research papers had an end-user prototype designed and presented. The prototype is designed for a mobile application. However, the same design can be extended to a web application, meeting requirement 6.3.

The user can register and log in to the Digital Wallet application using the National Digital Identity, as demonstrated in Figure 32. Once the user logs in to the Digital Wallet, the minimal information retrieved from the National Digital Identity is displayed for a personalized experience, including a photo, name and national ID number. The home screen

⁷ <https://proto.io/>

also provides the end user quick access to sharing requests from the SPs. Figure 33 demonstrates that the user accessed the “Bank of the Emirate” digital channel to open a bank account, so the bank requested an Emirates ID, National ID in the UAE and a passport. The sharing request includes the SP name and logo, the purpose of sharing and the required documents, satisfying requirement 6.2. Moreover, the user is informed about the time remaining for the sharing request in red when approaching the expiry time. The user can easily act on the notification by accepting (i.e. consenting to the sharing or rejecting it), allowing for discarding invalid requests by the user or the SP. The user can swap left to see the active sharing requests. The user can access the notifications by clicking on the “Notification” icon on the bottom navigation bar. The home screen provides the user with information about new SPs and Issuers who have joined the ecosystem, which helps increase the user’s awareness and, therefore, the adoption of the documents the user can retrieve and the services to avail using the Digital Wallet application.

The user can also easily view the documents (i.e. VCs) added to the wallet. Upon clicking on the “Document” icon on the navigation menu, the user is navigated to the document listing screen, as in Figure 35. The user can view all documents requested with the document names and issuance dates. The user can view the document data and visualization as in Figures 36 and 37. The user can also add new documents by clicking on the “+” icon in Figure 35, which navigates to the “Add Document” screen, as in Figure 38, where a list of document types to be added is displayed. The name of the document type, the issuing authority’s name and the issuing authority’s logo are displayed per document type, making it easier for the user to choose the document to be added. In addition, the user can search by document type or issuing authority using the search capability. The user can click on any

document desired to add. Upon clicking on the document, the user is navigated to the document details screen seen in Figure 39. On this screen, the user sees more details about the documents to be added. These documents are retrieved using the user's national ID.

For example, in this case, the user had more than one university certificate available with the Issuer. The document details are displayed to facilitate user selection. The user can either add all or some of the documents. Once the user selects the documents, the user can click on "Add Document". The success screen is then displayed. The initial design considered showing the national ID while receiving the user's confirmation to retrieve the list of documents to ensure the user's privacy in authorizing access. However, per the focus group sessions with the banks, the step was eliminated to balance user privacy and ease of use since the request for the document list is on the user's behalf only for displaying the information to the user. No other action is taken, so no one else can see the information.

The design of the application satisfied requirement 6.1 in providing a seamless and convenient user experience. The user can add documents with four easy clicks without input while sharing data with the SP requires one click. The design of sharing capability considered minimal efforts from the user, who is expected to avail services more frequently than adding documents. The user may, for example, add an Emirates ID once every five years. Moreover, the QR scanner icon in the bottom navigation bar gives the user quick access to the scanner for the QR generated on the SP channel to receive the sharing notification.



Figure 31: Login screen

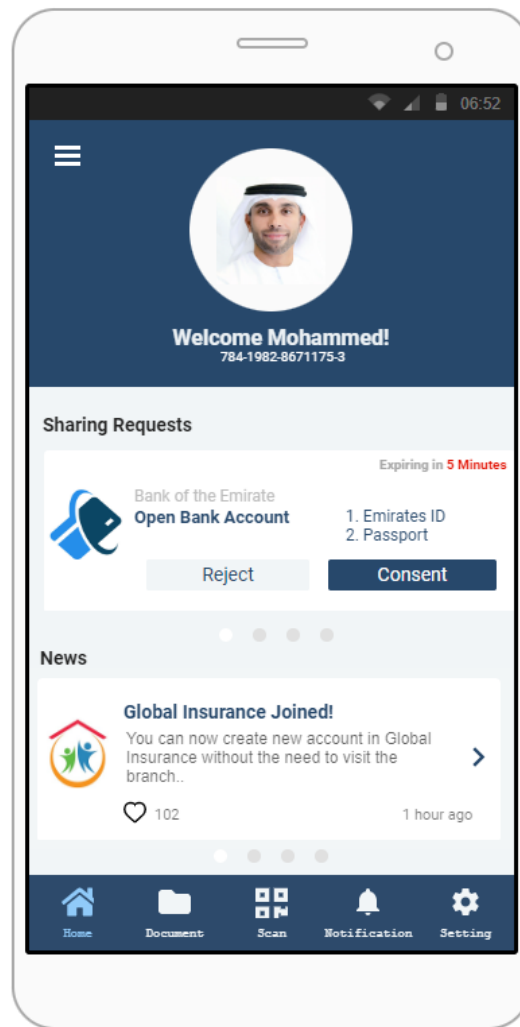


Figure 32: Home screen

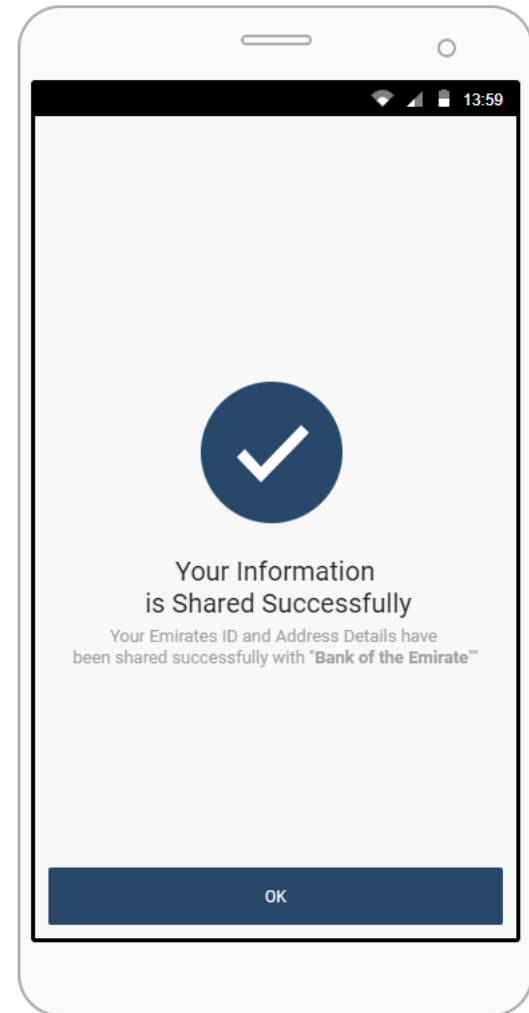
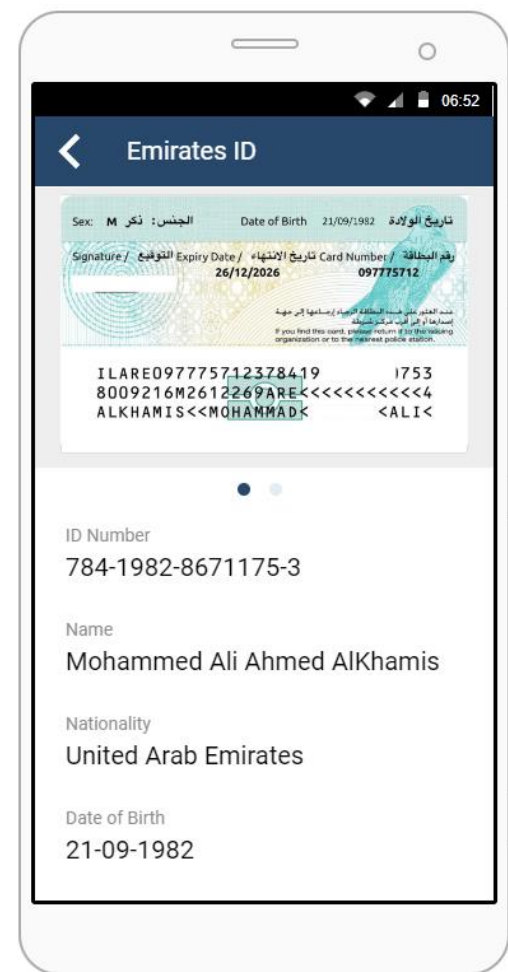
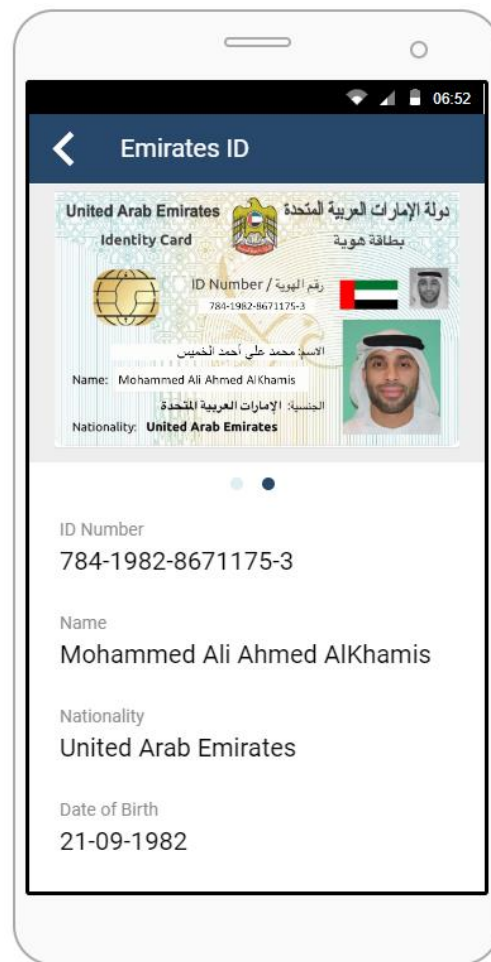
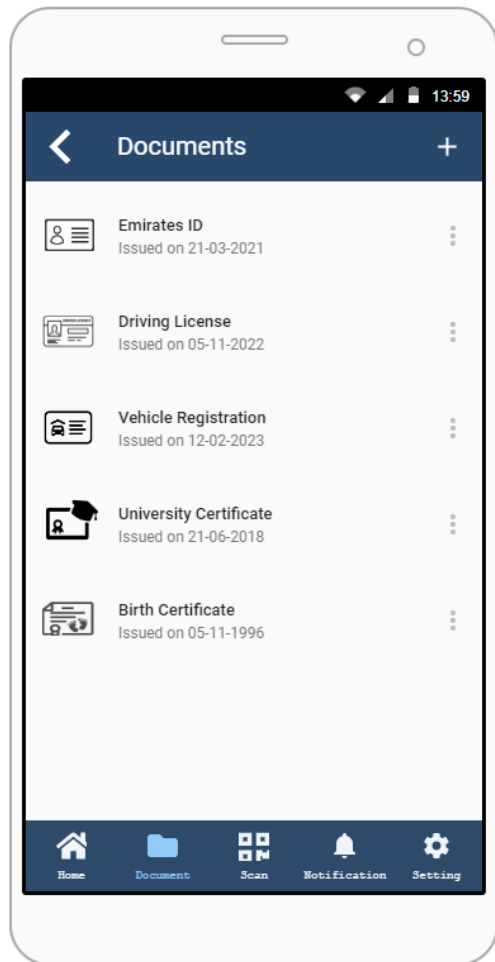


Figure 33: User consent to share successfully screen



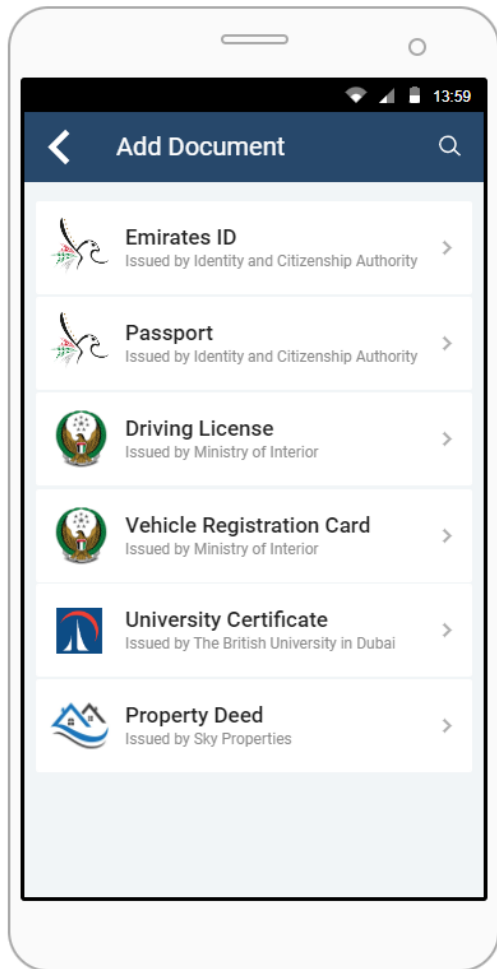


Figure 37: Adding document screen

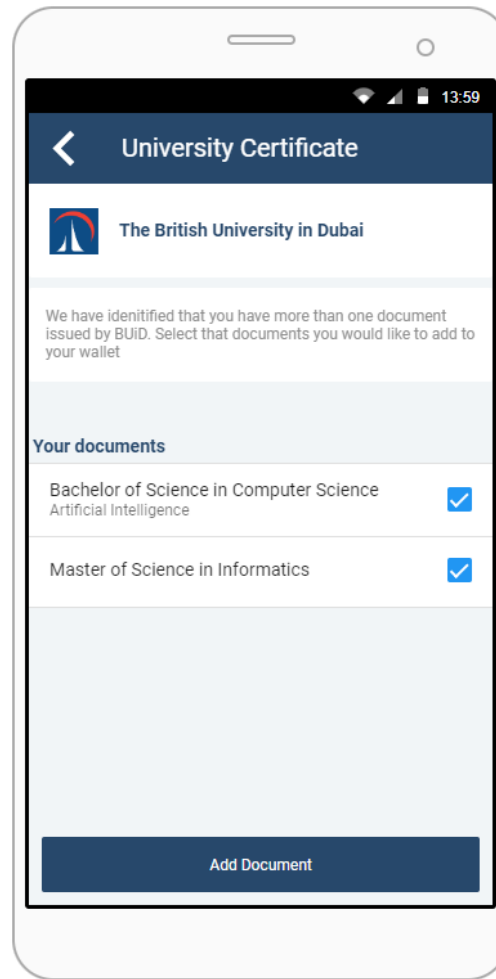


Figure 38: Selecting documents from the Issuer screen

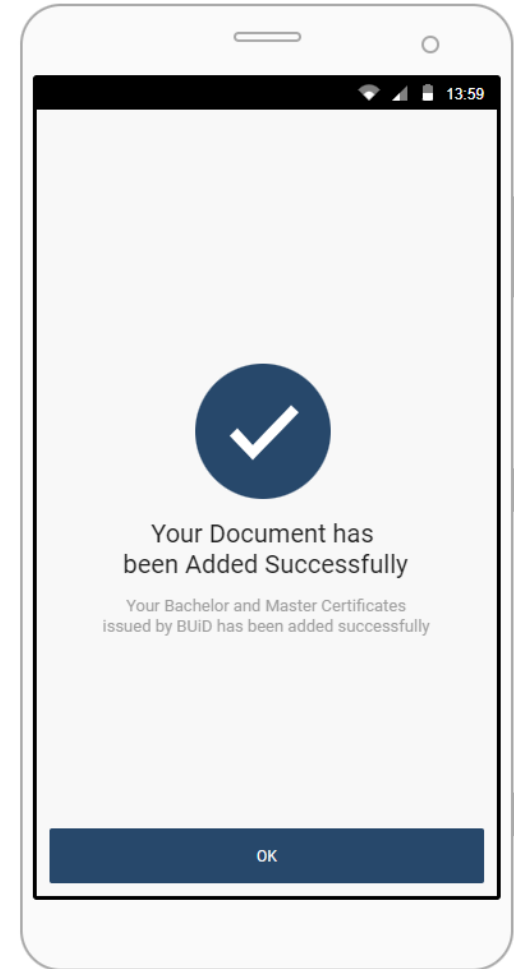


Figure 39: Documents added successfully screen

6.5 Evaluation

The Digital Trust Framework developed in this thesis was evaluated using a criteria-based evaluation to assess its applicability in providing value and improving the efficiency of the current KYC process in the UAE (March and Smith, 1995). The evaluation was conducted through interviews and focus group sessions with experts and surveys with end users. Experts' backgrounds and expertise and end users' demographics are described in Chapter 4. The evaluation was based on the design objectives and associated requirements detailed in Chapter 5. Below is the evaluation of each objective.

6.5.1 Experts' Feedback

Efficiency

Expert G emphasized that the proposed framework would enhance the efficiency of the KYC process by streamlining the individual account opening journey for Citizens (R 1.1). Expert G stated that through API integration, customers would no longer need to provide physical copies of their identity documents (R 1.4). Instead, the bank could automatically retrieve the digital data, such as the Emirates ID and passport, at the start of the customer journey, eliminating the manual process of document handling and verification while reducing the burden and processing time for clients and banks. Focus Group 1 also supported this view, acknowledging that the proposed architecture and capabilities would alleviate Citizens and bank processing time.

Expert H stressed the potential of the proposed KYC flows to improve efficiency. Expert H emphasized that the proposed framework could reduce verification costs, enhance

transparency, improve data accuracy and increase trust (R 1.1). Expert H highlighted that the Citizens' ability to submit their documents digitally would enable a streamlined and automated process. SPs would benefit from reduced manual processes while accessing up-to-date data (R 1.2 and R 1.3). Focus Group 2 emphasized the importance of the design element where the Digital Trust Framework would not hold data copies, always presenting the latest information directly from the Issuer. Focus Group 3 highlighted the need for notification in case of document status changes.

Expert G emphasized the importance of retrieving digital data directly from Issuers to ensure accuracy and reduce restrictions and delays during onboarding (R 1.4). With the proposed processes, the reliance on manual checking mechanisms and agents could decrease, allowing manpower to focus on critical tasks like due diligence and transaction analysis. Expert G stressed that the Digital Trust Framework would reduce the information-gathering phase by relying on government-provided data, minimizing the bank's need for separate data collection. However, the review phase would remain crucial, especially for high-risk customers requiring additional documentation. Expert G highlighted that the framework would minimize the need for a full-fledged review for standard risk customers, constituting a significant portion of the customer base (R 1.2).

Expert G stressed that implementing the proposed KYC processes for onboarding and continuous updates would benefit financial institutions. A monitoring mechanism would track document expiry and status changes, promptly notifying the financial institution and customers. The proposed Digital Trust Framework could ensure up-to-date information before reaching the financial institution, reducing the need for manual updates. This streamlined

process would involve API calls to retrieve updated information from the government, ensuring the timely completion of KYC reviews (R 1.3, R 1.4).

Expert H referred to the World Economic Forum's five critical elements for an efficient digital identity system (i.e. fit for purpose, inclusivity, usefulness, offering choices and security). According to Expert H, the proposed framework would satisfy these elements by ensuring accurate information, unique identity, sustainability, scalability, inclusivity, utility, transparency, privacy, user control and security. The proposed design would provide a standard integration means for Issuers and SPs, following open and widely adopted standards. Adopting recognized industry standards like W3C, VCs would enhance sustainability and ease of acceptance within the ecosystem (R 1.4).

Regulation Compliance

Expert H mentioned that the UAE's digital transformation is supported by updated laws and regulations, including the digital signature law, which now covers advanced signatures, identity establishment and qualified digital signatures (R 2.3). Hence, the legal framework provided by this updated law supports the implemented identity system. Additionally, there are national PKI policies and guidance for establishing digital identities, ensuring compliance with best practices. Expert I noted that the proposed design of the Digital Trust Framework aligns with the law, as a trustworthy and audited entity issues certificates. The law requires entities providing trust services to be licensed and accredited (R 2.3). Focus Group 5 also emphasized the importance of the framework adherence to the highest level of

security standards by utilizing the national PKI for issuing digital certificates to all actors in the ecosystem (R 2.3).

Expert H highlighted that the proposed design of the Digital Trust Framework would integrate privacy and data protection laws, ensuring compliance with existing regulations (R 2.2). Expert I noted that the proposed framework would support key principles of data privacy law, including transparency in data processing and obtaining user consent for data sharing (R 2.2). Expert I added that while the presented design and flow may not cover all aspects of the privacy law, such as the user's right to amend data, the main principle of user awareness and consent would be satisfied.

Expert G stressed central bank regulations emphasizing validation and verification controls for data. Banks must obtain data from authentic and verified entities, and customers must agree to the verification process. Expert G highlighted that the proposed Digital Trust Framework could fulfil local bank needs if the central bank were aligned (R 2.4). The expert added that international banks could have additional regulations based on their jurisdictions but still follow the central bank's regulations.

Focus Groups 1 and 2 highlighted the requirement for regulatory changes to support the success of the proposed Digital Trust Framework. They also stressed the need to include images as part of identity proof. Focus Group 4 supported the idea of the proposed framework and highlighted the possibility of regulation amendments to consider the framework on par with existing ID document verification processes. They also highlighted the possibility of waiving physical visits for new or updated KYC processes using the Digital Trust Framework

(R 2.4). Focus Groups 4 and 5 emphasized that aligning the Digital Trust Framework with UAE laws and regulations and international regulations such as data protection and eIDAS would provide a solid regulatory foundation and increase trust (R 2.4). Expert C also highlighted the importance of compliance with local regulations, guiding compliance with other industry bodies, such as AML (R 2.1).

Decentralization

Expert I mentioned ongoing debates about the best methods for data storage, highlighting the high risk of storing data in centralized storage. Experts I and H agreed that data storage risks should not be delegated to the user and emphasized the need to balance protecting user data while providing a seamless user experience. They highlighted that storing data on the cloud could offer a better user experience but raised privacy and security concerns. Expert H suggested that data should be stored with the issuer entities who originally issued them, maintaining the data with each issuer instead of distributing it across a decentralized system. Focus Group 6 also stressed the importance of not storing data in a centralized system, including during transit, and found the current design regarding on-chain data storage and data flow acceptable (R 3.1). Focus Groups 2 and 3 acknowledged and appreciated the ability to independently verify the documents shared by the user (R 3.2).

While no interviews directly addressed the balance between centralization and decentralization in governing the ecosystem and ensuring the trustworthiness of key operations, such as identity claim issuance, lookup and data storage, they emphasized the importance of certificates issued by audited, certified entities, the need for governing entities

onboarding the framework, the need for reliance on a National Digital Identity, the importance of independent verification of credentials and the requirement of the data remaining with the government that issued it (R 3.3).

Trust Establishment

Expert H confirmed that trust would be established in the Digital Trust Framework through multiple factors. First, the government's involvement in implementing the framework would bring trust, ensuring the safety and protection of Citizens' rights. Second, the framework could ensure the uniqueness of digital identities by adopting the national PKI policy and biometric validation (R 4.5). Focus Group 3 emphasized the importance of the framework design consideration in terms of identity authenticity in protecting personal data, while Focus Group 4 highlighted the importance of establishing identity credentials based on valid, not expired documents (R 4.1).

Expert H mentioned that trust would be further strengthened in the framework by the Issuer issuing identity documents to authenticated, authorized users in real time. Expert H stated that by using the digital identity to retrieve the document from the issuer, the framework would ensure that only the rightful user could access it (R 4.4). Focus Group 4 stressed that retrieving the document as a trusted document from the issuer, with only the owner retrieving and sharing it, would be a key factor in considering the proposed framework acceptable from a regulatory perspective (R 4.1). The up-to-date nature of the data was also highlighted as an important element by Focus Group 4. Moreover, Expert H confirmed that the framework would enable validity checks as the user would authenticate and authorize the sharing process

so that the SP could verify the data's authenticity and identity through digital signature and blockchain capabilities (R 4.3). Expert H added that compliance with existing regulations and legal requirements could further enhance trust in the proposed framework and include mechanisms such as an audit trail to ensure the framework's integrity and liability (R 4.2). Focus Groups 3, 4 and 5 stressed the importance of the audit trail capability in governing any dispute and compliance with regulators' requirements.

According to Focus Group 6 and Expert I, trust in the framework would be based on technology and process. The framework should satisfy basic security measures (e.g. authentication, authorization and accountability), and robust procedures should be in place to ensure the identity of users and entities. The framework could be trusted if these factors were implemented according to best practices.

Privacy Protection

Expert G noted that customer consent would be a crucial part of the data-sharing process in the proposed Digital Trust Framework (R 5.3). Data shared would remain within the bank, not accessible to third parties without explicit customer consent (R 5.1). Privacy policies within the organization would govern data management. Expert G added that prior to any data exchange between the bank and the Digital Trust Framework, customer consent would be obtained, ensuring a solid level of privacy protection. Expert I emphasized that the proposed framework would ensure user awareness of the requested data and the entities requesting it, as users would receive notifications about sharing data (R 5.2). Expert H mentioned that the proposed framework would offer choices to users, promoting transparency

and privacy as users could see who is collecting and using their data, giving them control and the ability to manage it.

Expert I highlighted that the proposed framework would align with the data privacy law principle of obtaining user consent for data sharing. The framework would not store personal data and minimizes its processing (R 5.4 and R 5.5). Focus Groups 4 and 5 stressed the importance of user consent for regulated sectors, allowing users to control their data while aligning with local and international data protection regulations.

Focus Group 3 highlighted the importance of the design element. Data sharing would be customer-driven and associated with the customer profile, preventing anonymous sharing requests. Focus Group 6 noted the alignment of the proposed framework with the required privacy law.

User Experience

Expert H emphasized that the proposed Digital Trust Framework would improve the efficiency of the KYC process through the integration and exchange of documents within the ecosystem. Expert H highlighted that users accessing their documents through a mobile application provided by the Digital Trust Framework would eliminate the need for manual digitization and submission to SPs. Expert H also highlighted that the framework could ensure the integrity of the documents by registering their footprint on the blockchain (R 6.1). Expert H added that the framework would enable users to choose the services they want and consent to share their data with the SP, enabling the pre-filling of forms to reduce manual data entry. Moreover, Expert H highlighted that the framework enablement of data verification and

validation automation would reduce processing time while enhancing efficiency for Citizens and SPs (R 6.2).

Experts G and H confirmed that the proposed Digital Trust Framework could improve the user experience by automating processes, ensuring data integrity and transparency while streamlining the experience for customers and SPs (R 6.1, R 6.2). Focus Groups 2 and 6 emphasized the need to merge the proposed Digital Wallet mobile application with the national identity mobile application to simplify the customer journey and reduce the number of applications involved. They also highlighted the importance of not sharing expired or revoked documents.

Expert H mentioned that the proposed design would ensure that users' identities are not lost if they lose their mobile devices or delete the application. Expert H added that the design of the Digital Trust Framework would hide the technical complexities, providing a seamless user experience for all ages and education levels. Expert H stressed that the framework would ensure compliance with international standards, regulatory trust and legal standards related to digital identity, data protection and privacy (R 6.4).

Sustainability

Expert H highlighted that the proposed design of the Digital Trust Framework could benefit various sectors by improving their KYC processes, providing scalability, a homogeneous user experience and sustainability (R 7.1). Expert I confirmed that the proposed framework would be applicable in scenarios where SPs, such as banks, require user consent to obtain data and comply with central bank regulations. Expert I added that the framework

would give Citizens the right to grant or deny consent. Focus Group 6 emphasized that the framework should only contain relevant identity data, excluding transactional data like utility bills.

Expert G emphasized that implementing the KYC processes proposed as part of the Digital Trust Framework would reduce the need for many agents and the reliance on checker mechanisms. Expert G added that this model would free up manpower for tasks like conducting due diligence on customers and analyzing transaction patterns, allowing banks to focus on essential activities beyond document authenticity verification and supporting the goal of streamlining processes (R 7.2). Expert E stated that banks would be willing to pay for the information provided through the Digital Trust Framework and proposed sharing the fund between government and private entities (R 7.2).

Focus Group 4 mentioned the need for certified technology and banking experts in court cases.

Technological Advancements

According to Expert H, the Digital Trust Framework would provide a standard integration means for Issuers and SPs. The framework could adopt recognized standards such as W3C VCs for data structure, making it easier for ecosystem partners to understand and integrate with the framework. Using international standards like SSI and VCs would enhance sustainability and ease of acceptance within the ecosystem (R 8.1). Expert H also highlighted the scalability aspects of the Digital Trust Framework designed as a decentralized system.

Moreover, Expert E added utilizing Ethereum. Blockchain technology would add to scalability since a proven blockchain network could handle millions of transactions globally (R 8.2).

Focus Group 6 emphasized the importance of leveraging government initiatives such as the digital signature platform, the government cloud and network security.

6.5.2 End User Concept Testing

The prototype was designed to be used by end users representing Citizens in the UAE, so it was important to evaluate the concept from their perspectives. A digital survey was developed and shared with a population sample, as seen in Appendix 3. Moreover, the details of the concept testing and the participants' demographic information are highlighted in Chapter 4. Based on the demographic information of the participants, it was noticed that approximately 85% of the participants were between 20 and 49, a fair distribution considering the eligibility factor to apply for services from an age perspective and digital literacy level. Moreover, the sample size aligned with the distribution percentage of the UAE population distribution⁸ in terms of age and gender, but from a nationality perspective, the sample did not match the UAE population distribution. However, the nationality distribution should consider blue-collar workers in the UAE: 2.2 million, representing 52% of the workforce.⁹ This category has challenges in terms of education and digital literacy. However, they are not the targeted audience for the Digital Wallet application. Thus, despite the sample not matching the

⁸ <https://www.globalmediainsight.com/blog/uae-population-statistics/>

⁹ <https://sustainabledevelopment.un.org/partnership/?p=29886>

UAE population distribution percentage, it gathered the point of view of UAE nationals and ex-pats, which can be considered sufficient. The ex-pat sample size was approximately 51%, slightly higher than UAE nationals at 47%, while the sample size of the GCC was 1.75%.

The survey was designed with eight Likert-scale and three open-ended questions. The Likert scale is a commonly used survey question format that presents respondents with an odd number of options, usually five, ranging from “strongly agree” to “agree somewhat”, “neither agree nor disagree”, “disagree somewhat” and “strongly disagree”. Likert scales generate quantitative data. In contrast, open-ended questions enable respondents to respond in their own words. Respondents can provide more insights about a specific question or aspect. Open-ended questions generate qualitative data. Responses provided to open-ended questions can be used for follow-up inquiries enabling respondents to elaborate more on the reasoning behind their answers. The questions in the survey have been developed based on industry guidelines of concept testing (Maze, 2023; *Concept Testing: Methods, examples & best practices*, 2022).

The overall feedback provided by the respondents indicated that the concept was well-received, with respondents appreciating its uniqueness, relevance in addressing a need, ease of use and time-saving aspect. This section provides more details regarding the responses to each survey question. In response to the first question on the initial reaction, 98% were either extremely or somewhat positive. None of the respondents had a negative reaction. Moreover, regarding the concept being different from what is currently available, all respondents confirmed that it provides uniqueness. Of the total respondents, 6% highlighted it as a little unique. The open-ended questions were analysed to gather insights regarding user feedback in this regard. Based on the analyses, respondents compared the concept with a similar product,

such as the built-in document vault in smartphones and government applications in the UAE displaying documents they issue to end users. However, there was no comparison to the uniqueness of the concept in terms of the unification of a document wallet and the ability to share documents to avail services. Respondents highlighted these as some of the most important aspects they liked about the concept.

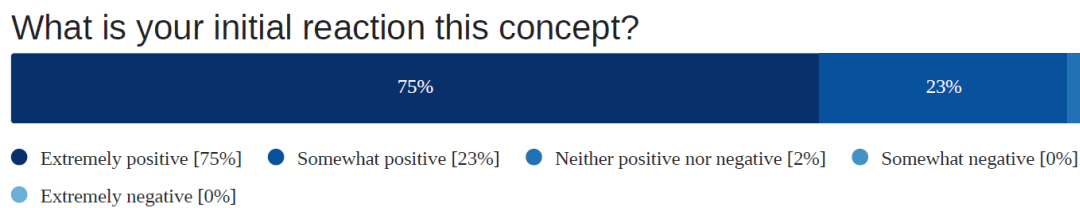


Figure 40: Concept testing results – Impression

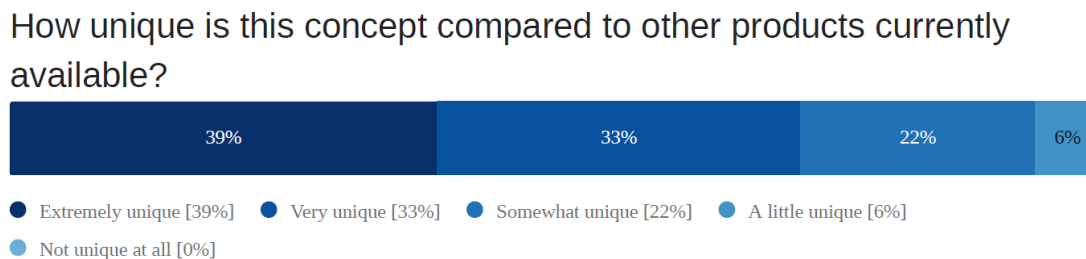


Figure 41: Concept testing results – Uniqueness

In terms of the concept's attractiveness, all respondents responded positively. Approximately 80% highlighted that the concept was either extremely appealing or very appealing, while none found it a little or not appealing. Regarding the 22% respondents who stated the concept was somewhat appealing, 64% of the total respondents were UAE nationals. Hence, there may be a need for more in-depth design sessions in this category. Similar to the results of the first impression question, where 98% of the respondents provided a very positive

response, the results of the likability question were quite positive: 91% provided positive feedback while none disliked it, confirming the consistency of responses and the overall positive response to the concept.

How appealing is this concept compared to other products currently available?

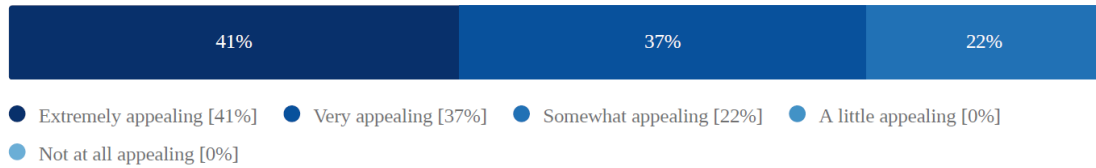


Figure 42: Concept testing results – Appeal

How much do you like or dislike this concept?

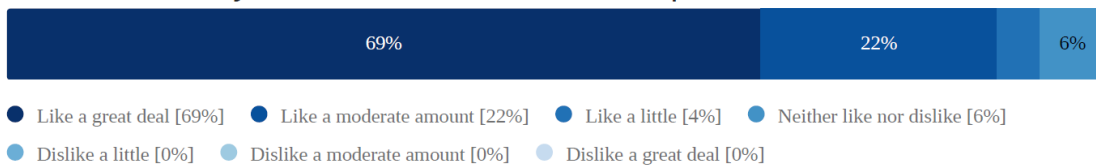


Figure 43: Concept testing results – Likability

The survey questions investigated how much respondents trusted the claims about the concept and its feasibility. The responses indicated a high level of trust in the concept and its feasibility, with 96% choosing extremely or moderately believable. No respondents found it unbelievable, while 2% found it slightly believable, and 2% responded with neither believable nor unbelievable. These respondents were all ex-pats, so the responses may be influenced by the leadership in the UAE that encourages the thinking that nothing is impossible and the demonstration of it with success stories, quotations and the creation of the Ministry of Possibility. Moreover, regarding the concept's relevance and alignment to the lives of the

target audience and its fulfilment of a need, responses indicated the concept highly relevant in addressing an existing gap. Approximately 90% highlighted that the concept was either extremely or moderately relevant, emphasizing that it addresses a need that is personally relevant to them. None found it irrelevant, while the 2% of respondents who highlighted the concept as neither relevant nor irrelevant were below 20 years old, an expected response since this category does not necessarily apply for services.

In terms of addressing a gap, 57% confirmed that nothing is currently available to solve the problem, while 37% indicated the concept as slightly better than existing methods. This response was positive, as overall, 94% considered the concept the only solution to the problem or one that could provide a better solution than existing methods. The overall average response regarding trust in the concept, personal relevance and fulfilment of the gap was 93%.

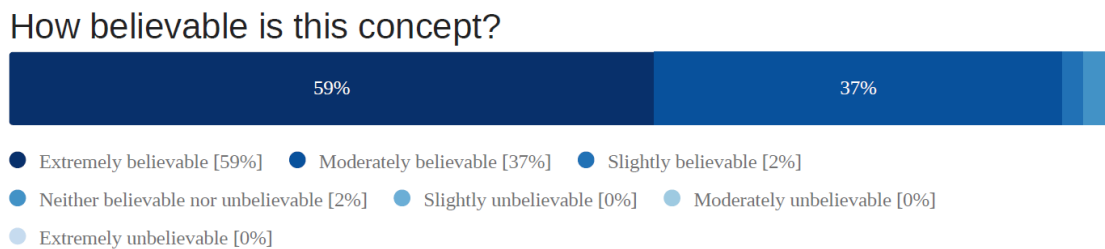


Figure 44: Concept testing results – Believability

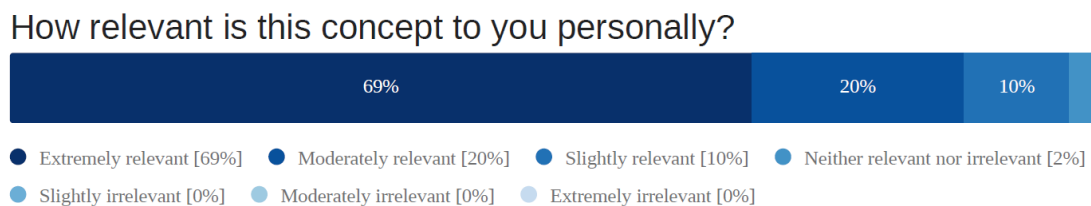


Figure 45: Concept testing results – Relevance

From the list below, which best describes your thinking about this concept?

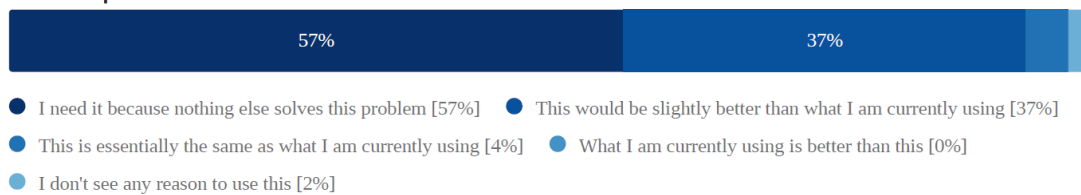


Figure 46: Concept testing results – Demand

Given that the concept revolves around trust, security and privacy, the survey had two questions to gauge end users' points of view. One question was in the form of a Likert scale, while the other was open-ended to acquire in-depth information. The Likert-scale security question was the only question where respondents were evenly distributed across levels of concern, with 45% very or somewhat unconcerned, 24% neutral and 32% somewhat or very concerned. The open-ended question dug deeper to understand respondents' concerns about security, as 58% answered the optional open-ended question, "How important is the security and privacy of your personal documents to you? What would make you feel confident about this app?" The main concern from the end user perspective was driven by the application being related to their personal documents and enabling them to share them to conduct transactions. Notably, 21% used words related to compromise, such as "misuse" and "fraudulent".

From a privacy perspective, limited feedback was provided. One of the respondents highlighted sharing limited information in the form of tokenization, while another respondent highlighted that the application should not store data. The respondents highlighted two main factors to increase their confidence in the application. The first was the involvement of a

trusted entity in the application. Of the total respondents, 33% highlighted that the application should be backed by the government or a trusted authority using keywords like “government”, “public authority”, “trusted authority”, and “well-known firm”. Approximately 73% suggested government involvement to increase confidence in the application. The second factor that respondents highlighted to increase their confidence was ensuring robust security measures for authentication and authorization, as 21% highlighted the need for secure access, recommending the usage of 2FA and Face ID. Respondents also recommended the usage of encryption, blockchain and a page describing the application’s safety and privacy.

Overall, 21% were confident in the proposed application. Moreover, the 90% who highlighted being very concerned about the security of the application as a response to the question, “How concerned are you about the security of sharing official documents through an app?” highlighted that they would be confident about the application if the government backed it, while 33% who were somewhat concerned provided very positive feedback about their confidence in the application. These levels indicated a high possibility that the Likert-scale question related to the application’s security was not understood, so the answers were provided from a general concern about the security of their personal data. With these insights, the response to the Likert-scale security question in Figure 44 as very or somewhat unconcerned could increase to 67%. In summary, security and privacy were paramount to end users. End users viewed the government as a trust anchor, aligned with the feedback provided by the experts during the interviews and focus groups.

How concerned are you about the security of sharing official documents through an app

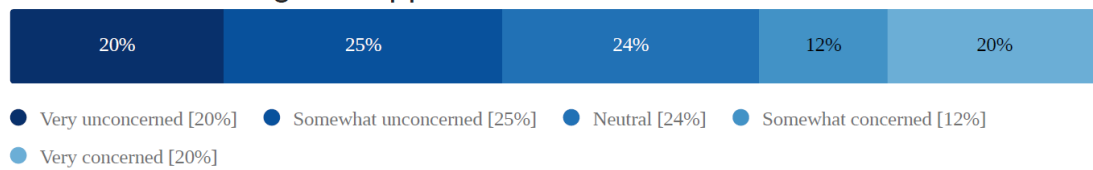


Figure 47: Concept testing results – Security

The last two open-ended questions were optional. For the question “What do you like most about this concept?”, 65% had positive feedback concerning the convenience and ease of use, efficiency and timesaving and unification of the document repository. Approximately 43% highlighted ease of use, while 35% highlighted efficiency and timesaving, emphasizing how it would make life easier by eliminating the need for physical documents while speeding up processes by reducing steps in sharing documents. Approximately 43% expressed satisfaction with having all documents in one place to share with multiple entities for various purposes. A few respondents also highlighted the application’s uniqueness and security as elements they liked.

In contrast, for the question “What do you like least about this concept?”, only 49% answered. However, many respondents stated that there was nothing they disliked or did not provide a specific aspect they disliked. After removing those responses, the total responses were lowered to 28%. Due to minimal responses, it was difficult to generalize them. The main three categories that users liked the least were 1) security (31% with no details), 2) the look and feel (19% highlighting colors, elderly usage and having “Add Documents” on the home screen and 3) the need for more information (19% highlighting how to add a document and

where to use it). One respondent highlighted other items worth mentioning: the acceptance of documents by other entities, the time required to integrate it with all entities, accessibility if the user is out of service, minimal information to be shared instead of documents and the need for the application to perform.

Overall, the concept testing survey results suggested that the respondents well-received the concept of a digital identity wallet application for sharing official documents. The concept's uniqueness, appeal and personal relevance were highlighted as strong points. However, security concerns must be addressed to increase user confidence and acceptance. The concept is also perceived as easy to use, a positive sign for user adoption. The feedback provided by respondents offered valuable insights for further improvements and development of the application.

6.6 Design Principles

As mentioned in Section 6.5, the proposed framework could significantly enhance the financial KYC processes. Specifically, blockchain-based SSI architecture offers efficiency, trust and privacy advantages. However, many of these improvements extend beyond the financial KYC use case. The trust relationship between the actors of the Digital Trust Framework involving the Holder of identity attributes, the Issuer of digitally trusted documents and the Verifier is applicable in various domains. Therefore, the proposed architecture, associated processes and prototype could provide insights into the general design of artifacts in the emerging field of blockchain-based SSI. The insights gathered from interviews with SSI experts and focus groups suggested that similar benefits could be realized in other areas where concerns about centralized SPs have hindered cross-organizational IdM

efficiency, transparency, compliance in regulated environments and privacy preservation in sharing confidential user data. To facilitate further theoretical discussion, the researcher derived three DPs that abstracted the findings and aimed to guide future research and practical implementations in blockchain-based SSI (Gregor and Hevner, 2013). The researcher analyzed interview codes related to technical building blocks of the proposed architecture, such as distributed ledgers, blockchains, VCs and storage, to identify commonly proposed design patterns and their justifications, formulating these three general principles.

Design Principle 1: Utilize Blockchain Storage for Traceability and Verification

The research identified that for regulators to accept and trust a digital platform on par with existing physical mechanisms, they must be able to trace any digital transaction for any dispute with the assurance of its authenticity. An immutable footprint of minimal data that does not reveal Citizen identity information is required, which can act as an audit trail for regulators. Moreover, from SPs' perspectives, they desire a platform that verifies Citizen data without lock-in effects or dependencies. They need up-to-date data with high quality and accuracy from a reliable platform. SPs never want to have information about their customers available publicly. Security agencies and government authorities would prevent creating honeypots of customer data.

In this context, a distributed ledger is suitable for transparently displaying public information due to its transparency, redundancy and tamper-resistant properties. Information stored in this case should not directly reveal any actors' identity or private data. No personal data should be stored, even if encrypted (Finck, 2018; Zhang, Xue and Liu, 2019). Mühle *et*

al. (2018) and Soltani, Nguyen and an (2018) suggested storing credential hashes and peer DIDs on a distributed ledger. However, experts interviewed as part of Schlatt *et al.* (2022) argued that this approach would not offer apparent advantages while posing performance challenges and regulatory risks. The same was also highlighted by Toth and Anderson-Priddy (2019). Per Schlatt *et al.* (2022), trust in the interaction with a DID is established through a VP, while the tamper resistance of VCs is ensured through the Issuer's digital signatures, making on-chain hashes unnecessary. However, per Focus Groups 3, 4 and 5, having an audit trail is required by regulators, deriving the need to store hashes of the VP, VCs and DIDs to trace the sequence of transactions through the blockchain events registered with timestamps that can be cryptographically verified ensuring their tamperproof nature and non-repudiation. Storing the hashes of VCs also enables the SP to independently verify the validity status of the VCs at the time of verification while having the digital signature on the VCs and VP ensures data integrity through off-chain verification. The hashes of the VP, VCs and DIDs on their own do not contain PII and cannot be directly linked to any legal person or entity without having the VP and VCs to map them. This safeguard prevents any correlation of the data stored on the blockchain while eliminating privacy issues aligning with the seven laws of identity defined by Cameron (2005). The blockchain can be designed to be a permissioned network to reduce data exposure.

Per Expert I, since the proposed framework does not store personal data on-chain or process it, it can aid blockchain use cases in complying with regulations related to data protections, such as the GDPR and addressing privacy concerns. The proposed framework shares user data based on user consent as only data in transit.

The original data forming the VC should remain off-chain. Per Experts A and H and Focus Group 6, it should remain with the issuing entity. They recommended not storing this data in the cloud or edge devices to avoid data centralization, shifting the responsibility in terms of data storage and user protection.

Design Principle 2: Instil Trust with a Balance of Decentralization

The actor identity cannot be completely anonymous for a blockchain-based SSI solution to be trusted (Expert A). The legal entity (i.e. Issuer and Verifier) and legal person (i.e. Holder) should be registered in the framework through a governed process with the highest LoA. There is a need to issue digital certificates for these actors from a CA audited and accredited by an authorized entity in the country so that their identities can be mapped to real-world identities and can be considered legitimate by the court. The user's or Holder's digital identity should be created with the highest LoA, such as using biometrics (Experts I and H, and Focus Groups 3 and 5).

The integrity of the data exchanged between the actors can be ascertained by a digital signature that uses public-key cryptography (Experts A, H and I). Therefore, the public key of an actor is the only information required to verify its footprints. The signature is applied to the off-chain data and is used to sign it to ensure its integrity, authenticity and non-repudiation. Indeed, introducing certificate authorities and digital identities introduce centralized systems, which are important in increasing trust (Experts A, H and I).

Moreover, registering the sequence of transactions through blockchain events with timestamps enables end-to-end traceability. With a decentralized and distributed ledger and

immutable and irreversible properties, blockchain instils trust and independent verification. The ability to correlate identity, data and digital signatures in off-chain data with the on-chain data of Proof-of-Issuance and Proof-of-Process containing hashes ensures that the framework meets five important goals: 1) data integrity, as the message received by the recipient is exactly the same message sent by the sender; 2) authenticity, as the message is received from the intended sender; 3) non-repudiation, as the sender cannot disown sending the message; 4) traceability, as every phase of the credential's lifecycle can be traced from blockchain starting from the issuance of a credential; 5) data validity, as up-to-date credential status is always maintained on-chain by the Issuer; and 6) decentralization with distributed blockchain node does not create a centralized personal data honeypot (Experts A, and H and Focus Group).

Per Expert I, the framework needs to satisfy the AAA framework, a three-process framework referring to authentication (to prove identity), authorization (to give permission) and accounting (to log an audit trail). The process should be well-governed, including creating and storing identities and keys.

Finding the right balance between decentralized and centralized solutions is crucial (Experts A and I). Cloud storage can offer recovery, availability and security advantages. However, Expert I believed this storage could eventually be prone to cyber risks, while Experts A and D considered cloud storage viable and essential for delivering a positive user experience as long as the data remains encrypted and inaccessible to cloud providers and cloud providers offer the highest level of security and privacy measures. Experts A and D believed that the architecture should ensure that users can store their VCs on the storage of their choice.

Design Principle 3: Build a Sustainable Platform

Per Experts A and D, technologies evolve. Thus, designing a modular architecture is a key factor for adaptability and sustainability. Components should be designed as standalone or a microservice that can be easily scaled or replaced. There should be standard interfaces between the components. Moreover, the design should adhere to industry standards currently being developed by organizations such as the W3C (Sporny, Longley and Chadwick, 2022).

Expert A believed there is a paradigm shift towards modular and application-specific blockchain architecture, allowing developers to focus on specific layers and application logic. Expert A stated that interoperability has improved with the development of bridge solutions and advancements in scalability. Expert A believed future projects should consider application-specific blockchain, citing Cosmos and Polkadot as examples of offering software development kits and interoperability features.

Experts A, D and H stated that the complexity of the technology and SSI should be hidden from the user. Consolidating all identity-related data in a single app could simplify the management of identity documents and enhance authenticity through hardware binding or credential linking. However, self-management could introduce various hurdles. For instance, users could require assistance if their devices were lost or stolen, necessitating a shift from the current reliance on centralized systems as users need to understand their responsibility for their data and learn how to store them appropriately (Wagner *et al.*, 2018), as highlighted by Experts A and D.

According to Experts A, D and H, the platform should take care of the key management, DID and VC storage, data representation, backup and recovery. This idea builds on DP 1, where VC is recommended to be stored in the issuing entity SOR, while VP can be stored in the SP system as long as required. Moreover, to build upon DP 2, the user key management should be managed centrally by the platform to ease the backup and recovery processes for the user.

6.7 Summary and Conclusion

This chapter detailed the IT artifacts constituting the Digital Trust Framework: architecture, processes and a user experience prototype of a Digital Wallet application. The IT artifacts were designed based on the design objectives and requirements described in Chapter 5. Experts evaluated the Digital Trust Framework architecture and processes through interviews and focus groups. It was well-received by the experts in general. Citizens evaluated the Digital Wallet application prototype in the form of a digital survey. The prototype was also well-received by the Citizens. Both experts and Citizens emphasized the government's role as a trust anchor.

The IT artifacts of the Digital Trust Framework provide a basis for the implementation phase. The next chapter describes the proof-of-principle prototype implementation of the framework. The proof-of-principle prototype implementation is used later in this research to demonstrate the feasibility and performance of the implementation of the framework in efficient KYC process.

Chapter 7: Implementation of Prototype System

7.1 Introduction

This chapter describes the implementation of the Digital Trust Framework aiming at improving the efficiency of the KYC process into a prototype system. The prototype implementation serves as a proof-of-principle of the feasibility and performance of the framework which will be evaluated in the next chapter. Moreover, the prototype implementation addresses the fourth objective of this thesis. The chapter presents the functionality of the prototype. It then illustrates a high level design and a layered modular architecture pattern of the Digital Trust Framework. It highlights the technology choices used to develop the prototype system. In addition, it describes the core API developed for each function of the prototype and provides sample request and response of these APIs.

7.2 Prototyping

The implementation phase objective is to produce a prototype system in order to validate the feasibility of the architecture of the proposed framework as described in Section 4.4.3. The researcher can gain insights from system prototyping in term of how well the actual system supports the framework. The system prototyping can also help in term of identifying additional requirements and understanding the strength and weakness of the system which, can lead to further refinements and improvement of the framework (Sommerville, 2011).

The prototyping process starts with defining the objectives of the prototype and the type as illustrated in figure 11 in Section 4.4.3. The objective of developing a prototype in this thesis is to provide a proof-of-principle for the proposed framework which serves as evidence

of the feasibility of the design of the framework and enables its extendibility to other areas apart from what it is been tested (Kendig, 2015). The functionalities of the prototype are defined based on the use cases of the system and considered as part of the formation of the architecture of the prototype. The next section describes the core functionalities of the prototype system.

7.3 Prototype Functionalities

The objective of the implementation of the prototype is to deliver the required functionalities to conduct a KYC process. This includes all the tasks related to the identification of the Citizen, sharing of credentials and verification of the credentials by Service Provider or for audit trail purposes by regulators in case of dispute. The implementation of these functionalities in a prototype can be considered as initial steps towards the realization of the proposed Digital Trust Framework. The functionalities identified for the implementation of the prototype are described below:

- The prototype should register the identity of every actor in the framework in the Blockchain which includes Issuer, Citizen and Service Provider.
- The prototype should enable the Citizen to request their credentials from the authorized entities i.e. issuers.
- Any credential issued by an issuing authority registered in the ecosystem, should be registered in the Blockchain.
- Citizen should be able to avail services from the service provider, which initiates a request to the Citizen to share required credentials.

- Any request made by the service provider registered in the ecosystem for the citizen to share credentials should be registered in the Blockchain.
- Citizen should be able to share credentials with the service provider after providing a consent.
- The sharing of the credentials by the Citizen should be registered in the Blockchain.
- The prototype should be scalable to allow multiple sharing from different Citizens with an acceptable response time.
- The prototype should enable the service provider and regulator to verify the credentials shared and validate any dispute.

The next section describes the key technology choices, the Blockchain implementation considerations, and the core APIs.

7.4 High Level Design

This section provides details of the high level design of the Digital Trust Framework. The below figure represents the logical decomposition of the framework.

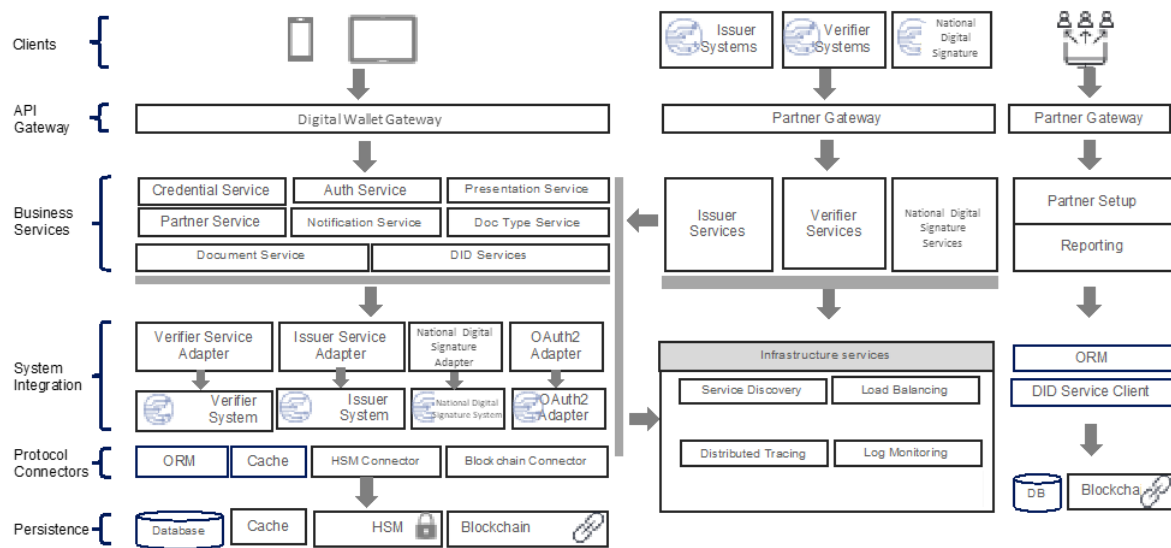


Figure 48: Logical View of the Digital Trust Framework

As illustrated in the above diagram, the prototype is implemented in a layered and modular architecture pattern to ensure its adaptability and sustainability. The Clients represents variety of client integrations which include Digital Wallet mobile application to allow citizen to use its services, the Issuer Systems which represents the owner of the credentials system of records, and the Verifier systems which represents the service providers that request for citizen credentials to provide them with services. The API gateway is the layer responsible for routing the calls to the appropriate service group and performs security checks. The Business Services implements the business services of the Digital Trust Framework. These services could be internal or external. The System Integration layer represents the different external system that Digital Trust Framework integrates with. Digital Trust Framework provides standard integration such as REST based. Protocol Connectors connect different systems using ORM for databases, IPC for blockchain, object caching abstraction for

distributed caching, and HSM native connection wrappers for HSM. Finally Digital Trust Platform uses relational databases, distributed cache, HSM and blockchain as persistence data stores.

The Digital Trust Framework is decomposed based on functional and data isolation principles in order to allow utmost reuse and independent scalability of each component. The figure below illustrates the each deployment unit.

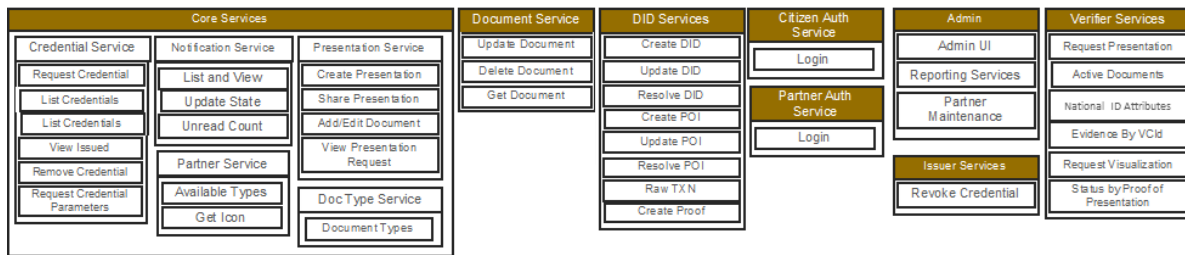


Figure 49: Digital Trust Framework Functional Decomposition

The relationship between these services in runtime is illustrated in the below figure as such the green lines represent external call while the blue lines represent the inter service communication.

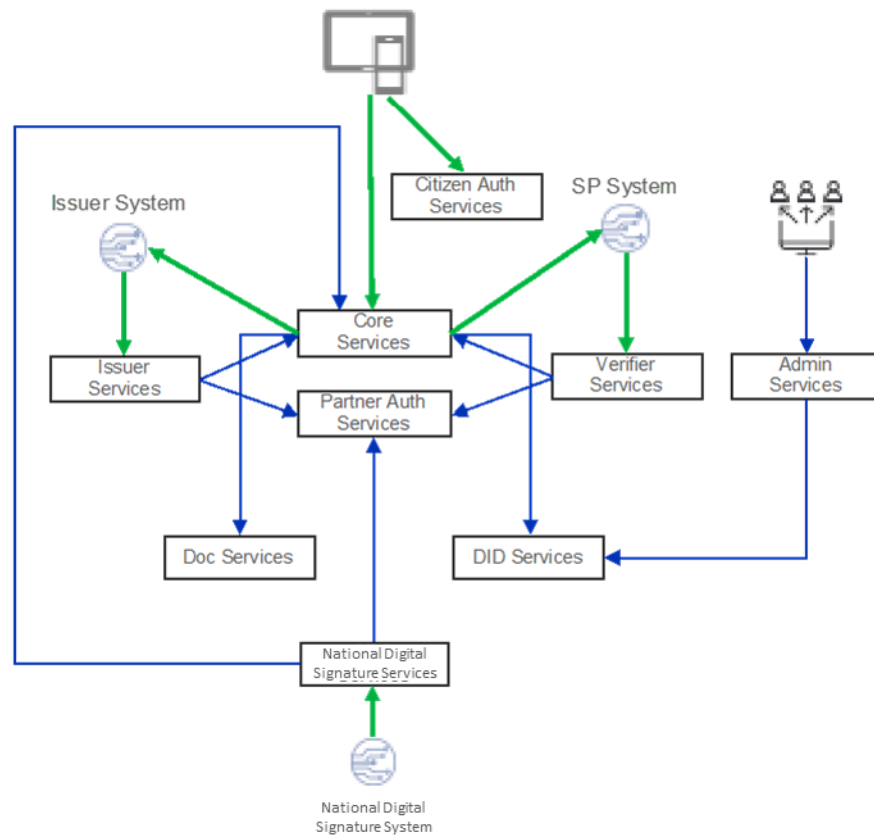


Figure 50: Service Orchestration

7.5 Technology Stack

Open source technologies were used for the implementation of the proof-of-principle. It was based on Spring cloud¹⁰ architecture. Only the database and HSM were not an open source. These persistence stores were provided by the researcher organization. Moreover, the infrastructure were also provided by the researcher organization given the case study would

¹⁰ <https://spring.io/cloud/>

connect to other government entity systems. The table below lists the technology stack used to implement the prototype.

Table 14: Technology Stack of the proof-of- principle

Layer	Technology
Gateway	Netflix Zuul
Service Registry	Netflix Eureka
Service Client	Feign Client
Client Load Balancer	Netflix Ribbon
Configuration Server	Netflix Archais
Distributed Tracing	Spring Cloud Sleuth and Zipkin
Business Services	Spring Boot
REST API	Spring MVC
ORM	Hibernate JPA 2.2
Blockchain Connector	Web3J
Caching library	Spring Data Redis
Connection Pool	Hikari Pool and Commons pool
Database	Oracle 12g
Distributed Cache	Redis
Blockchain	Quorum Geth
HSM	Safenet Luna
Log Collector	FileBeat
Log Aggregator	Logstash and Elasticsearch

As illustrated in the above table, Quorum was chosen as Blockchain technology due to the fact that it can be deployed as private permissioned network, the ease of managing a

progressively growing network and ability to support key externalization, thereby enabling secured key storage. The consensus model chosen is RAFT. All of the nodes have equal access, which means any node can write transaction. RAFT is a consensus model for faster block times, transaction finality, and on-demand block creation. The choice of a private permissioned network and a lightweight consensus model contribute to improving the performance of Blockchain implementation. The Blockchain integration adapter uses the Web3J abstraction which uses JSON-RPC to interact with the blockchain node. The application maintains the list of Geth node IPs and can failover to a node which is available.

7.6 Main APIs

This section provide details regarding the main APIs that addresses the functionalities of the prototype. These APIs also serve as implementation of the Digital Trust Framework described in Chapter 6.

7.6.1 Authentication

The Digital Trust Framework APIs are stateless services. It uses Spring security filter chain to authenticate users and entities. There are two types of authentication that are supported by Digital Trust Framework based on the type of user. These types are citizen authentication and partner authentication.

7.6.1.1 Citizen Authentication

The digital wallet gateway acts as a gatekeeper. It routes the calls to the appropriate service implementation. The Citizen Authentication API authenticates the citizen by passing the access token acquired from the National Digital ID, validating the token, and issuing a

JWT with limited validity. All subsequent calls to the Digital Trust Framework REST interfaces requires passing this JWT token in the Authorization header. The figure below demonstrates the authentication flow while the table represents the structure of the JWT issued.

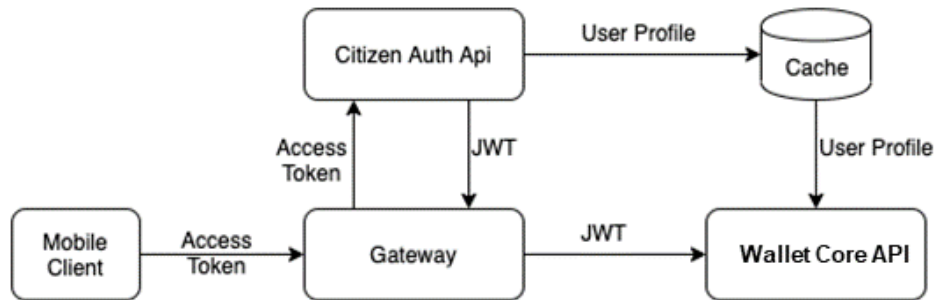


Figure 51: Citizen Authentication Flow

Table 15: The structure of the JWT token issued

Field	Description	Section
Alg	Algorithm used to sign the payload	Header
Sub	Subject of the claim, in case of digital wallet this would be the DID of the citizen	Body
Authorities	Array of permissions granted to the subject	Body
Iat	Unix epoch time at which the token was generated	Body
Exp	Unix epoch time at which the token will expire, typically 10 minutes from Iat	Body

7.6.1.2 Partner Authentication

During the on boarding process of a partner which could be an issuer or service provider, Digital Trust Framework shares a secret with the partner. The partner system can

then generate an authentication token which can be verified independently by Digital Trust Framework. The figure below demonstrates the flow of the partner authentication.

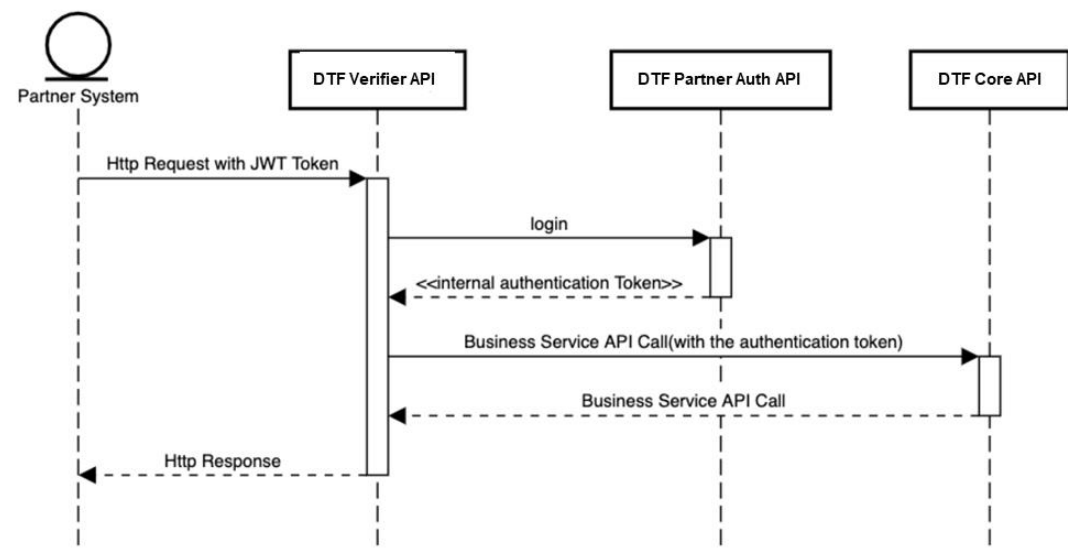


Figure 52: Partner Authentication Sequence Diagram

7.6.2 Create DID Document

As described in section 6.2, the first step to add any actor to the Digital Trust Framework is to register their identity. Thus, every actor, including the Issuer, Holder and Verifier, has a unique DID to identify their DID information. The Create DID document API, generates a DID document and persists it in Blockchain using DID Registry smart contract. While generating the DID document object, it uses Web3j library to generate asymmetric key-pair for the DID and set the DID public key and DID authentication attributes of the DID document object. This API accepts valid JWT token as Authorization header that has been acquired by the Authentication API.

```
curl --location --request POST 'http://10.254.0.8:9009/api/v1.0/did/' \
--header 'Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWUiOiJkaWQ6dWFOmV0aDo2YWNoOWE4NWYwNjcwMTk4ZTk4YzFjOGU3MGU2YzJkNm1Mj13MjRliiwiYXV0aG9yaXRpZXMlOlsiQ2l0aXplbiJlCjpwYXQlOiE1Nz1MTA5NzYslmV4cCl6MTU3MjU5Nz1M3Nn0.999DWu_476AyyAluntXc1AiLxW9h_VZmmbOC0vk1GG13Z15pW8zRVyI7AtYo0HckN2BnGVWwFkHYbc-wpL0THQ'\
--header 'Content-Type: application/json' \
--data-raw ""
```

```
{
  "@context": [
    {
      "value": "https://w3id.org/uaec/v1"
    }
  ],
  "id": "did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8",
  "publicKey": [
    {
      "id": "did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8#key-1",
      "type": "Secp256k1VerificationKey2018",
      "controller": "did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8",
      "publicKeyBase58": "2fdSgreLLmrBNvhGATkj1knXu6TvSzA7M7jAPzEsZy3YgxnDLWpB2CpVqT9fUMW3Y7wxn3LizATDWZotWTdV7R2zdNQtpPeHAhUdtq4t9q52HYSJ5i7Q8Ez27zYUqSwCUrZGVSR6GEkGju4oBDmTz9scJrSMdHAMhUTE6wxxDcxVexHb4p",
      "expiredOn": null
    }
  ],
  "authentication": [
    {
      "type": "Secp256k1SignatureAuthentication2018",
      "publicKey": "did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8#key-1"
    }
  ]
}
```

Figure 53: Create DID Document - Sample Request/Response

7.6.3 Request Credential

This API allows a citizen using Digital Wallet mobile application to request for a credential from an issuer. The API accepts valid JWT token as Authorization Header that has been acquired by the Authentication API. It calls the issuer service (REST/ SOAP) to retrieve the claim data corresponding to the requested document type. Then, it generates the Proof of Issuance for the claim data and persists it on chain. After that, it invokes the issuer service (REST/ SOAP) in order to update the VCID at the issuer SOR. Finally, it generates a corresponding push notification for the citizen.

```
Request:

curl -X POST \
  https://apitest.dv.government.net.ae/api/v1.0/credential-requests/ \
  -H 'Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJkaWQ6dWFlOmV0aDo4Zjc3YjliYzdlMjFiMjY4ZGU5NTY1OTI1YjMwNDEzNzNjZjA0ZmQ4IiwiaXV0aG9yaXRpZXMiOiQ2I0aXplbiJdLCJpYXQiOiJlE1NzcwODU5MzIsImV4cCI6MTU3ODc3MjMzLn0.oE868x-tqKkh4YJf7jeHHnctZ8Uczya6HZrW7C5RARYqLXsltScAwJU2viyYv17P-ZpnwVGC5pNlsdpq5THxtg' \
  -d '{
    "requestedData": {
      "emiratesId": "784198906873744"
    },
    "issuer": {
      "partnerId": "did:uae:eth:33da8bc524b7a62478eb0a7740d1f21f4421f9"
    },
    "credentialDocumentType": {
      "id": 3
    }
  }'

Response:

{
  "id": "CR1YXHMxSO1C",
  "status": "SENT"
}
```

Figure 54: Request Credential - Sample Request/Response

7.6.4 Create Proof of Issuance Document

This API is an internal API, which is consumed by Request Credential. It generates Proof of Issuance of the document and persists it on chain. The API accepts valid JWT token as authorization header that has been acquired by the authentication API. This API uses asynchronous method, which first generates the hash of the DID document object, then signs the hash string using the DID key-pair using Web3j library and generates the signature string. These information is used to generate the DID proof object and sets it in the DID document object. The DID document is serialized into encoded hex string, which acts as input parameter for the 'DID Registry' smart contract. Then, it calls the Blockchain using web3j library in order to send raw transaction to the 'DID Registry' contract address using the signing key as DID most active key pair. The raw transaction returns the transaction hash.

```
Request:
curl --location --request POST 'http://10.254.0.8:9009/api/v1.0/proof-of-issuance/?ownerDid=did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8' \
--header 'Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJkaWQ6dWFIOmV0aDo2ZWYyY2NmMTA5NjlmYjk2ZWYxODQ1NTVhZTJhOGU1ZmI0ZDAwYWlyliwiYXV0aG9yaXRpZXMiOiJQZl0aXplbiuldCjPpYXQlOiE1NjksNDE4OTksImV4cCI6MTU2OTIyODI5OX0.Fp4uuKau9trQliicxawnqnKztZoV343qQhxxuFD6Dqic5scF707S79MdyFVq_Uji4-5wh1Xsw8L4H-vSjLpaxg' \
--header 'Content-Type: application/json' \
--data-raw '{
  "@context": {
    {
      "value": "https://w3id.org/uaec/v1"
    }
  },
  "claimAnchor": "e1a334000461002b3f2d6eb7085fe50332f1142e088f5ee25a533e21bdbed79a",
  "status": "ACTIVE",
  "sharedOn": "2024-01-05T10:57:21Z"
}'
```

Figure 55: Create Proof of Issuance Document - Sample Request

Response:

```
{
  "@context": [
    {
      "value": "https://w3id.org/uac/v1"
    }
  ],
  "id": "did:uae:eth:0x0e30bbf99511e3ef8b2b42046b632cbaf554d4ec",
  "publicKey": [
    {
      "id": "did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8#key-1",
      "type": "Secp256k1VerificationKey2018",
      "controller": "did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8",
      "publicKeyBase58":
"2fdSgreLLmrBNvhGATkj1knXu6TvSzA7M7jAPzEsZy3YgxnDLWpB2CpVqT9fUMW3Y7wxn3LizATDWZotWTdV7R2zdNQtpPeHAhUdtq4t9q52HYSJ5i7Q8Ez27zYUqS
wCUrZGVSR6GEkGju4oBDmTz9sclrSMdHAMhUTE6wxzDcxVexHb4p",
      "expiredOn": null
    }
  ],
  "authentication": [
    {
      "type": "Secp256k1SignatureAuthentication2018",
      "publicKey": "did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8#key-1"
    }
  ],
  "claimAnchor": "e1a334000461002b3f2d6eb7085fe50332f1142e088f5ee25a533e21bdbed79a",
  "status": "ACTIVE",
  "sharedOn": "2024-01-05T10:57:21Z",
  "statusUpdateDate": "03 JAN 2024 15:59:46",
  "proof": {
    "signatureType": "EdDsaSASignatureSecp256k1",
    "createdOn": "2024-01-05T15:59:45Z",
    "creator": "did:uae:eth:12b184a074d65a7912c9ff8a3e3745a4cb53f1e8#key-1",
    "signature":
"fa4788533a1f61dca535b4ebffc5fe696ce9fc2802c69a05d2b4983764725dfa2f1797f9f751b74ba9606b7a7e053c92eda6c1a4598683d1fc8bc53b9b6611db1c",
    "nonce": "EX6OUCoCqoJtL5Sg5RuQbSEfKYvm95mL"
  },
  "createdAt": "05 JAN 2024 15:59:46",
  "updatedAt": "05 JAN 2024 15:59:46",
  "version": 2
}
```

Figure 56: Create Proof of Issuance Document - Sample Response

Request:	
Curl-X	
POST	'http://10.254.0.8:9009/api/v1.0/native-txns/?dataHash=0xe99fe4fad4c8c3078bf5ef20b6848660e963ed7cb718c70f0596ef8953ea99f&toDIDId=did:uae:eth:b953a76dbdef75262488cb8017d6cd35753e6679&fromDIDId=did:uae:eth:24ae9c8faa899e6dfca7f3a2813d809c9d3bbbe8&'
HTTP/1.1	
Host: 10.254.0.8:9009	
Authorization:	Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJkaWQ6dWFlOmV0aDo2ZWYyZmMTA5NjlmYjk2ZWYxODQ1NTVhZTJhOGU1ZmI0ZDAwYWlyIiwiaXV0aG9yaXRpZXMiOiVkfVtFRFVVNFUiJdLCJpYXQ0IjE1NjYwNjg4NjYslmV4cCI6MTU2NjE1NTI2Nn0.vGSuTaNNmFVSXSJ2j2WtKRozopZkPIYJwCdsk7LTq-gH9jaYWE7mMqmVhCEK1PAMnqqI58b0KKQuDGuQAtVobg
cache-control: no-cache	
Postman-Token: 4b9de774-6293-4bea-ac60-be42cd1bb6bd	
Response:	
0x1b384a37ee0b51a371ea4e1796b98acaa44e513d244b727fb8cf84e249576e81	

Figure 57: Send Raw Transaction – Sample Request/Response

7.6.5 Receive Presentation Request from Service Provider

This API is an external API, which is consumed by the Service Provider to request the Citizen to share the credentials required to avail a service like opening a bank account. The API accepts valid JWT token as authorization header that has been acquired by the authentication API. The API validates the JWT token and the Secret Shared. Then, it resolves the DID of the Citizen and the DID of the Service Provider from the Blockchain. After that, it creates proof of presentation request in the Blockchain and sends a push notification to the Citizen.

Request:

```
curl -X POST \
https://apistage.dv.government.net.ae/papi/v1.0/presentation-requests/ \
-H 'Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJkaWQ6dWF0aDphOGY5YzNzIiwuZWQ2NzIhIiwiaXNzIjoizGikOnVhZTpdGg6N2I3NTBlyZQ5YTU5mODg5MzIjMDI2YWQ5YTU5YmM2MjdlOWI1MjA3ZSIsImhhdCI6MTU3MTU0OTM4MCwiZXhwIjoxNTcyNTQ5MzgwfwQ.sHD8ZRhP89DLoS07llsZcMXWr1yvQkYhccZhtizvn-70TmLD12jDqnDUflkZhKTWb7tvloZtqV4Ca4Y9nDk2Zw' \
-H 'Content-Type: application/json' \
-H 'Postman-Token: 8679b439-0d95-45c6-a2a5-a3d8aa513b1e' \
-H 'cache-control: no-cache' \
-d '{
  "partnerId": "did:uae:eth:7b750ec49a5f88932b026ad9a59bc627e9b5207e",
  "purposeEN": "Applying for Standard Current Account",
  "purposeAR": "\u0627\u0644\u062a\u0642\u062f\u0627\u062f \u0639\u0644\u0649 \u0627\u0644\u062d\u0633\u0627\u0628 \u0627\u0644\u062c\u0627\u0631\u064a \u0627\u0644\u0642\u064a\u0633\u064a",
  "requestId": "1571549462",
  "expiryDate": "2014-01-12 12:12:12",
  "origin": "WEB",
  "requestedDocuments": [
    {
      "documentType": "EmiratesId",
      "required": true,
      "selfSignedAccepted": false
    },
    {
      "customDocumentType": "Utility Bill",
      "required": false,
      "selfSignedAccepted": true
    }
  ],
  "requestedVerifiedAttributes": ["mobile", "email"]
}'
```

Response:

```
{
  "proofOfPresentationRequestId": "0x27e1f5d2684c07ec5ad6e3c2a2b163ceaa0d42d0f8cfdc9c827536719f6c5ea"
}
```

Figure 58: 7.4.5 Receive Presentation Request – Sample Request/Response

Based on the push notification sent to the Citizen Mobile Wallet, this API creates the presentation to be shared with the Service Provider. The API accepts valid JWT token as authorization header that has been acquired by the authentication API. The API validates the JWT token and the Secret Shared. Then, it fetches the presentation request that was trigger based on the Service Provider request and matches the available credentials with requested credentials where possible. Upon Citizen consenting to share the credentials with the service provider, it encodes the presentation in Base64, generates SHA256 hash, signs the presentation, send proof of presentation raw transaction to blockchain, retrieves the Service Provider end point, sends presentation to Service Provider and returns the confirmation status to Citizen.

```

Request:
curl -X POST \
  'http://192.168.0.4/api/v1.0/presentations/share?uaePassDocumentID=8hbgsbs8h43ejdbhcn72o2mrd99bfusn&status=finished' \
  -H 'Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWUiOiJkaWQ6dWFlOmV0aDpmOTAwNjY5Mjg4MDFiOGI5MzU1YTlhNGNmZGY3NDI1YTg3Mjg2ZDhhliwiYXV0aG9yaXRpZXMiOiSiQ2I0aXplbiJdLCJpYXQjOiE1NzA3ODE1ODMslmV4cCI6MTU3MDg2Nzk4M30.rchXgkHvrYxe39iz34FnM1Cbpm8r22KS-I0B6ubD_B6a8oXMkiwPd4zK67bXGw7NWgvJTzJuaXMMsVauwGn4iQ'\'
  -H 'Postman-Token: e778f90e-2a33-494b-8a0d-7d58f56d94d9' \
  -H 'cache-control: no-cache'

Response:
{
  "status": "SHARED",
  "message": ""
}
```

230

7.6.7 Credential Verification API

This API allows Service Provider to validate the status of any credential shared by the Citizen through Digital Wallet. The API accepts valid JWT token as authorization header that has been acquired by the authentication API. The API validates the JWT token, validates the Service Provider in the Blockchain, validates the proof of presentation and the proof of issuance, retrieves the credential status from the Blockchain and responds back to the Service Provider.

```
Request:

curl -X POST \

https://apistage.dv.government.net.ae/papi/v1.0/presentations/credential-status \

-H 'Authorization: Bearer eyJhbGciOiJIUzUxMiJ9.eyJzdWIiOiJkaWQ6dWFIOmV0aDpkNzFmOGI5NmFhNmE4OTg3NGI2YjZlOWJmYWFiZDlmMzgwYTM1MmFliiwiaXNzIjoizGkOnVhZTpdGg6ZDVINGViZmUxZGkYzQ3MjBjNDVkdMDM3Yjk5MTJkZDk3MWU4YjJhNCIsImhhdCI6MTU3MDYwMDMzOSwiZXhwIjoxNTgyNjAwMzM5fQ.HSDPw2o1EHfGn9MDYkhWRntFXsI4W_s7IUE4u5K5_zn4ydVMdRSoFASyJ4InsgHJ_dmxL8kWIT2madIYCvR06A' \

-H 'Content-Type: application/json' \

-H 'Postman-Token: 98cdf08d-0488-4154-9d72-4d487844b4b1' \

-H 'cache-control: no-cache' \

-d '{

    "proofOfPresentationId": "0x1d7c44d222d48326476bf3159b1b59ff60dfe5c034a96f58e148e55764de5a67",

    "requestId": "1578384657"

    "proofOfIssuanceId": "did:uae:eth:706aa9a748a9d35ed2928da750d942db2830f00423b9f7f47"

}'

Response:

{

    "proofOfCredentialValidation": " did:uae:eth:476bf3159b1b59ff60dfe5c034a96f58e148e55764de5a67",

    "status": "active"

    "lastStatusUpdateDate": " 08-JAN-24 01.53.28.845000000 AM"

}
```

Figure 60: Credential Verification API – Sample Request/Response

The below figure demonstrates step by step the verification process that a Service Provider can follow to validate the credential shared to ensure its been issued by the issuer and

shared with consent from the Citizen. The same process can be used by the regulator for audit trail purposes for any dispute case.

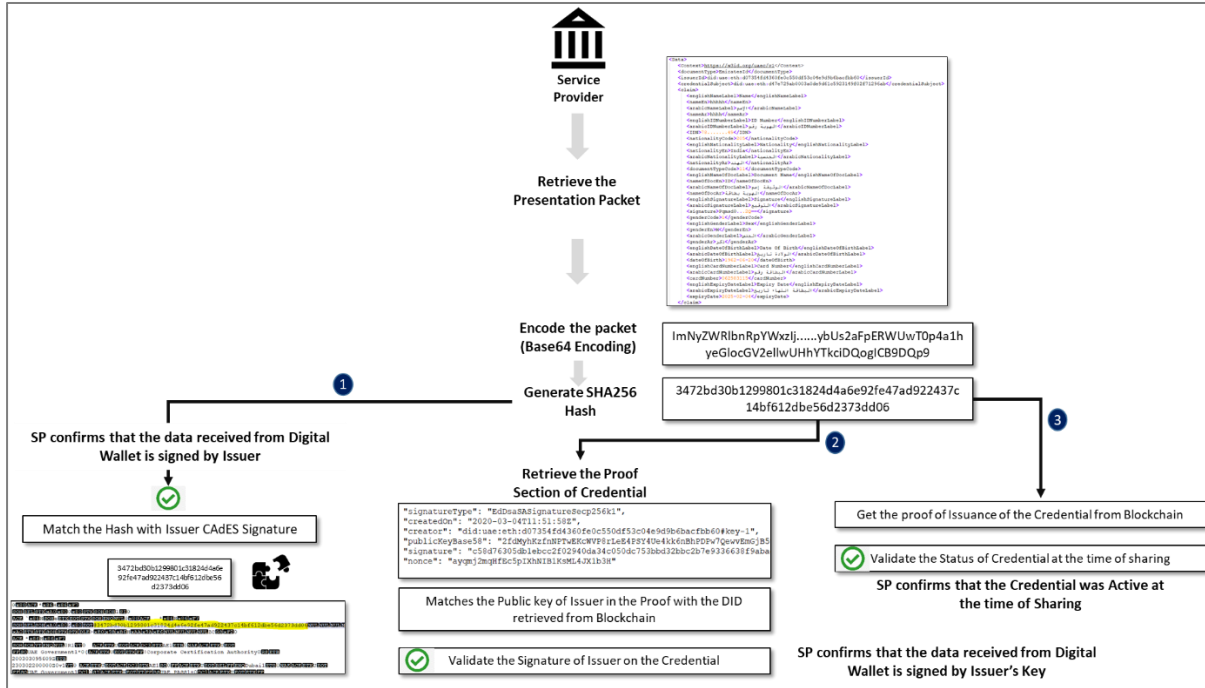


Figure 61: Service Provider Stepwise Verification

7.7 Chapter Summary

This chapter demonstrated the implementation of the prototype of the Digital Trust Framework to be used in KYC process. The prototype development serves as proof-of-principle of the design of the Digital Trust Framework which was presented in Chapter 6. The required functionalities of the prototype were defined and the layered architecture was presented. The chapter also highlighted the technology choices for the implementation of the prototype and the main APIs with a sample request and response.

The next chapter will demonstrate the feasibility of the prototype system by integrating it with issuer and service providers to conduct a KYC process. It will then evaluate the prototype using a set of performance metrics.

Chapter 8: Prototype Demonstration and Evaluation

8.1 Introduction

This chapter presents the prototype evaluation results. It addresses the fifth objective of this thesis. In order to evaluate the prototype and as highlighted in section 4.4.4, a case study is used to demonstrate the feasibility of the developed prototype. The case study includes the integration with a government as an issuer and two financial institutes as service providers. A sample of real customers' data from production is migrated to the system prototype and used after obtaining the users consent. The performance of the prototype system was empirically evaluated through the prototype demonstration results. Different performance metrics and graphical representations are calculated and developed when required to evaluate the performance of the prototype in term of KYC efficiency and overall system efficiency. The KYC efficiency is measured through sample dataset while the overall system efficiency is measured by exposing the prototype system to a larger dataset. The summary of the evaluation findings is presented at the end of this chapter.

8.2 Evaluation Settings

The evaluation of the Digital Trust Framework starts with the demonstration of the feasibility of the implemented prototype in the form of a real case study as highlighted in section 3.4.4. The results of the demonstration phase are used to evaluate the performance of the Digital Trust Framework. The details of the case study demonstration is described in this section.

8.2.1 Case Study Selection

The KYC process is explained in details in section 6.3.5. The fundamental document for any KYC process is the identity document which is represented in UAE by the Emirates ID card which is issued by the Federal Authority for Identity, Citizenship, Customs and Port Security (ICP). Thus, ICP was integrated as an issuer to the Digital Trust Framework and the emirates ID was implemented as verifiable credential. Moreover, two national banks were integrated as service providers to conduct a KYC process for opening a bank account service.

8.2.2 Sampling

Sampling is the process of selecting a subset from the population. In this thesis a sample is representation of individuals with different demographics in UAE as well as different scenarios for the bank e.g. new customer vs existing customer. The sample should be small enough to be able to identify real users who would like to participate in the case study yet it should be sufficient to evaluate the prototype system.

In order to determine the size of the sample, the pre-calculated table that determines the sample size based on set of sampling criteria such as the population, confidence level, and margin of error is used (Krejcie and Morgan, 1970). Krejcie and Morgan (1970) created a table to determine the sample size without the need for any calculation to use it. This table has been widely adopted (Hill and Hamilton, 1998). A simple form of the table is illustrated below with confidence level as 95% and margin of error as 5%.

Table 16: Required Sample Size

(Source: Krejcie and Morgan, 1970)

Population Size	Sample Size	Population Size	Sample Size	Population Size	Sample Size
10	10	2,500	333	75,000	382
50	44	5,000	357	100,000	383
100	80	7,500	365	500,000	384
250	152	10,000	370	1,000,000	384
500	217	15,000	375	1,000,000	384
750	254	25,000	378	2,000,000	384
1,000	278	50,000	381	10,000,000	384

As illustrated in the table above, as the population size increases the sample size increases at a declining rate and eventually remains slightly constant at around 380 as per the calculation conducted by Krejcie and Morgan (1970). The population size of UAE is around 10 million¹¹ and a subset of those estimated as 5.8 million would open a bank account in bank. The subset includes age group from 21 to 64 and exclude blue-collar worker. Thus a sample of size 384 would be sufficient for this thesis. A sample size of 400 real users were randomly selected similar to demographic distribution described in section 6.5.2. The users were selected based on convenience sampling (Shaughnessy, Zechmeister and Zechmeister, 2016). Users who accepted to participate, their real Emirates ID profile were migrated from

¹¹ <https://www.globalmediainsight.com/blog/uae-population-statistics/>

production to test environment after obtaining their consent to have real simulation. The table below illustrates the demographic distribution of the participants.

Table 17: Case study participants' demographics

CATEGORY	SUB-CATEGORY	FREQUENCY (N)	PERCENT (%)
AGE	20 to 29	79	19.75%
	30 to 39	132	33%
	40 to 49	105	26.25%
	50 to 59	63	15.75%
	60 and above	21	5.25%
GENDER	Male	238	59.5%
	Female	162	40.5%
NATIONALITY	UAE National	113	28.25%
	GCC	13	3.25%
	Expat	274	68.5%

8.2.3 User and Scenario Preparations

All the 400 users were provided with Digital Wallet Test Application. The users were divided into two groups. First group was given one of the URLs of the financial institutes test website URL, while the second group was given both of the financial institutes test website URLs. This enables the simulation of three test scenarios 1) completely new onboarding where the customer does not have a wallet, 2) new to KYC where the customer has a wallet and the required VCs to conduct a KYC process, and 3) fast onboarding where the customer has a wallet and VCs and previously completed KYC process. The testing was conducting remotely at the user convenient time and location.

8.2.4 Service Providers on Boarding

The case study was conducted with two major national financial institutes in UAE. These two financial institutes were part of this thesis since the initiation of the DSR process. These financial institutes developed a new flow for opening a bank account and therefore on boarding customer. In this new flow, the KYC process in term of customer identification, data verification and identity authentication is automated through the integration with Digital Trust Framework. The screens below demonstrate the integration of these financial institutes without the identification of their brands.

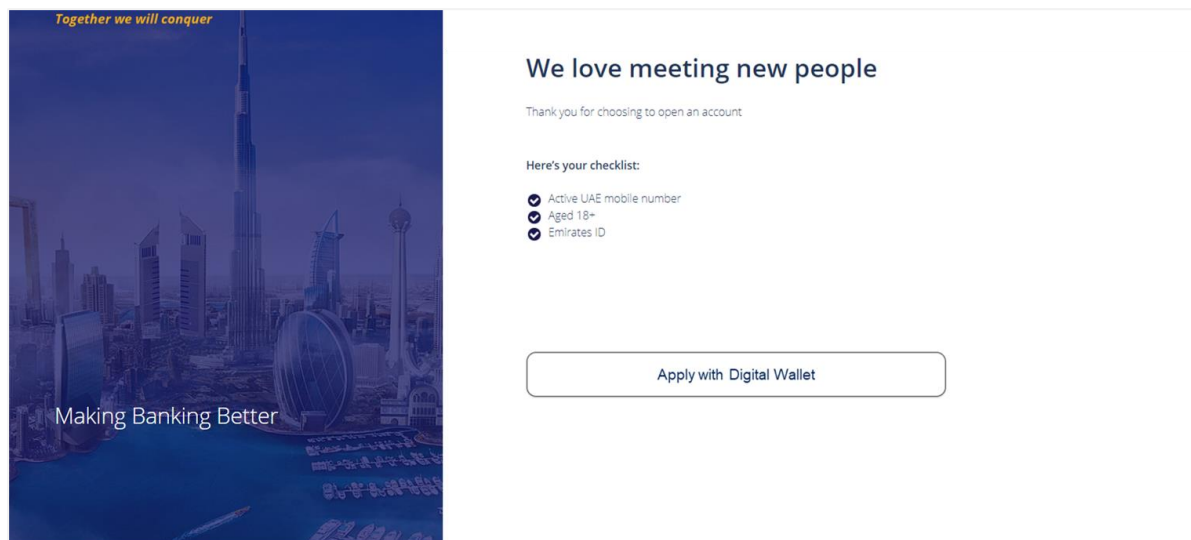


Figure 62: Case Study Financial Institute A – Initiation

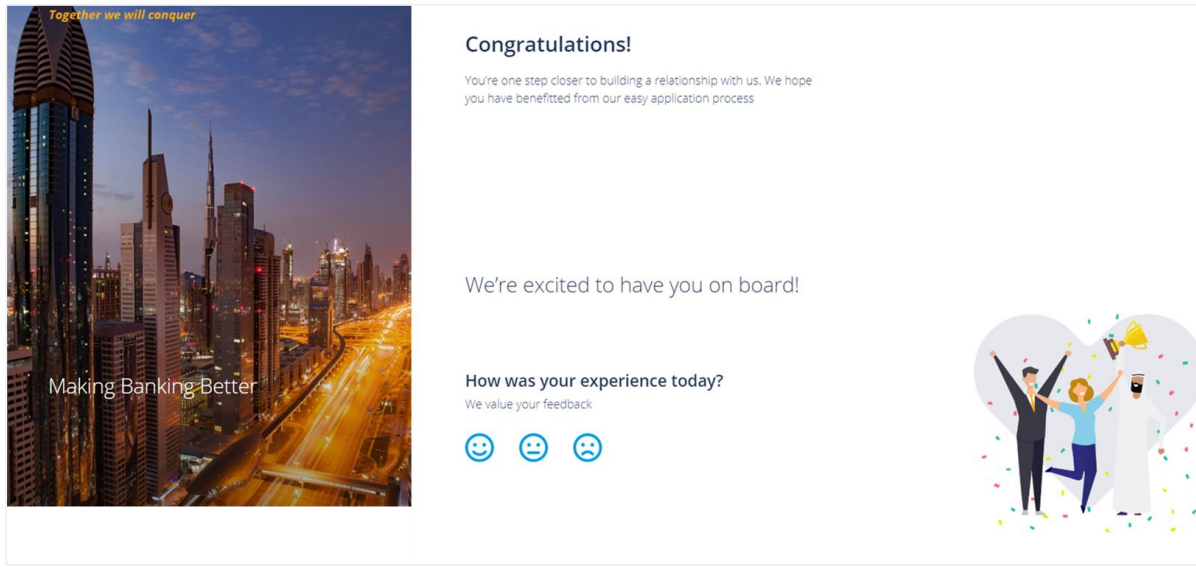


Figure 63: Case Study Financial Institute A – Completion

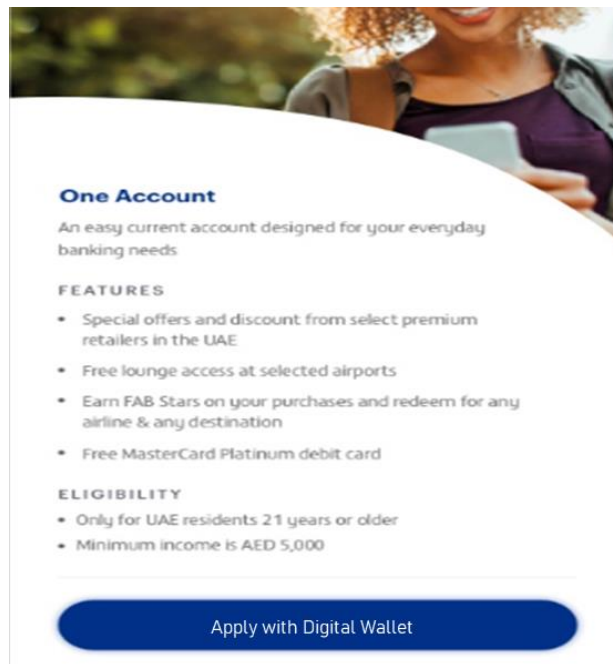


Figure 64: Case Study Financial Institute B – Initiation

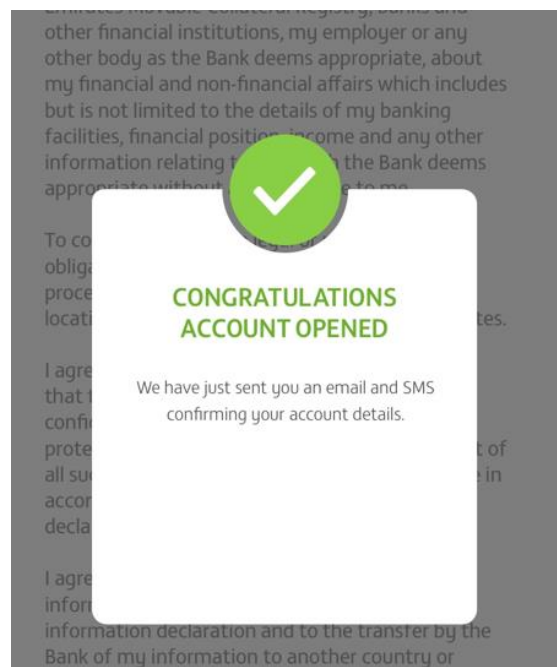


Figure 65: Case Study Financial Institute B – Completion

8.3 KYC Process Efficiency

As highlighted previously in section 4.4.4, the KYC process efficiency is evaluated through three performance metrics which are processing time, accuracy of verification, and cost per KYC. In order to evaluate the KYC processing time, the 400 participants were requested to apply for an account opening for at least one of the financial institutes. The total number of applications submitted were 538. The total number of applications received for financial institute A was 276, while the total number of applications received for financial institute B was 262. As per the experts from both the financial institutes, the total time for service fulfillment to open a bank account used to be between 7 to 15 days however, with the new flow it reduced to 1 day for standards cases in which additional due diligence is not required. The experts from the financial institutes highlighted that the saving in term of cost per application for new KYC is around 78.3% which is equal to 245 USD dollar per application.

In order to evaluate the accuracy of verification of the application submitted, a manual verification is required. One expert from each financial institute was assigned to review a sample of 50 different applications comparing the original documents with information received digitally. Due to the fact that it is a lengthy process to review the applications manually, not all applications were reviewed. Experts reported that the 100 applications that were reviewed were 100% accurate.

8.4 Overall System Efficiency

The overall performance of the prototype system efficiency was evaluated to ensure its robustness with growing number of transactions. The evaluation was conducted through

performance metrics targeting the Blockchain APIs such as DID creation and send transaction as well as business services such as credential service and presentation service. The Digital Trust Framework was deployed on a private cloud as it had to integrate with government entity. The Blockchain nodes were deployed on four virtual machines each with 8 vCPU and 16 GB of memory while the business services were deployed on two virtual machines with 16 vCPU and 30 GB of memory.

In order to evaluate the overall performance, there is a need to define the expected performance results to be used as reference. Table 18 highlights the business considerations that were used as input to calculate the required performance. The citizen on boarded and nationality were derived based on the information available online¹²⁻¹³. The newly on boarded users were assumed to be 10% of the populations considering the growth and new expats visiting the country. The credentials issued considers either newly issued or renewed credentials. These numbers are considered at very high-end of the utilization as it assumes the whole eligible population is using it. Table 19 illustrates the operational window parameters to calculate the expected transaction per second.

Table 18: Performance Metrics Input

Business Scenario - Consideration/Assumption	Values
Citizen on boarded <i>The whole population from age 21 to 64 except blue-collar workers</i>	5,828,160
UAE National	669,073

¹² <https://www.globalmediainsight.com/blog/uae-population-statistics/>

¹³ <https://sustainabledevelopment.un.org/partnership/?p=29886>

Expat	5,159,087
New users (Yearly)	582,816
No of Issued Credential per UAE National (Yearly)	3
No of Issued Credential per Expat (Yearly)	2
No of services consumed per Citizen per year	3

Table 19: Performance Metrics - Window Input

Operational Window Parameters	Values
Working days in a Year	251
Working window (in hours) for Service Provider	10

Based on these input, the performance metrics expected results in term of the total number of transactions, average TPS and peak TPS were calculated and presented in table 20. The calculation is highlighted for both the business service including credential service and presentation service and the underlining Blockchain API including Send Transaction API, Create POI API and Create DID API.

Table 20: Performance Metrics Expected Results

Presentation for Citizen		
Business Service	Presentation Service	17,484,480
	Average TPS	1.21
	Peak TPS	1.9
Blockchain API	Send Transaction API <i>Proof of presentation Request and Proof of presentation</i>	34,968,960
	Average TPS	2.42

	Peak TPS	3.83
Credential for Citizen		
Business Service	Credential Service	12,325,392.77
	Average TPS	0.85
	Peak TPS	1.36
Blockchain API	Create POI API	12,325,392.77
	Average TPS	0.85
	Peak TPS	1.36
New Citizen on Boarded		
Blockchain API	Create DID API	582,816
	Average TPS	0.04
	Peak TPS	0.07

The performance metrics of the Blockchain to be evaluated included throughput, response times (average and 90th percentile), error rates, CPU utilization, and memory utilization. The performance metrics were evaluated for core functionality of the Blockchain, including creating DIDs, sending raw transactions, and creating Proofs of Issuance (POIs). The APIs were evaluated individually as well as combined together. The test methodology involved simulating increasing virtual users (VU) and concurrent threads to mirror real-world scenarios. Multiple test runs were conducted for each scenario with increasing load parameters to determine the maximum attainable throughput. The load parameter for each API was different to represent real world scenario as illustrated in table 20, as such the load on Send Transaction API which registers proof of Presentation Request and Proof of Presentation was

the highest followed by Proof of Issuance API and Create DID API. The load was generated using JMeter¹⁴. The test scenarios were run for durations ranging from 10 minutes for the individual APIs test scenarios and two hours for the combined test scenario.

The first Blockchain API that was tested was "Create DID API". The "Create DID API" test scenario demonstrated good scalability, with throughput increasing from 4.2 to 10.3 transactions per second as the concurrent threads were scaled up from 10 to 40. This is higher than the expected throughput which ranges between 0.04 and 0.07 per second. The sample transaction ranged between 2,506 and 6,235 with a 100% success rate that was achieved across all test runs, demonstrating the system's reliability in fulfilling DID creation requests. The response times remained consistently below established thresholds as highlighted in the figure 66, signifying stability under increasing pressure. Additionally, figure 67 illustrates the CPU and memory utilization which also remained within manageable levels, indicating efficient resource usage. The cache memory represents the allocated memory to the application in this case it's the JVM heap memory. The memory allocated for Quorum Geth is higher as it heavily rely on RAM for efficient operation.

¹⁴ <https://jmeter.apache.org/>

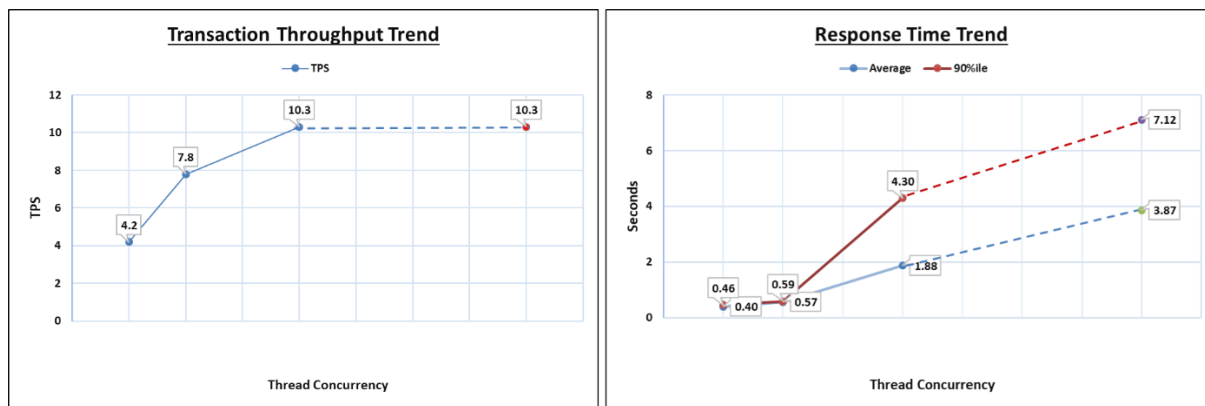


Figure 66: Create DID API Throughput and Response Time

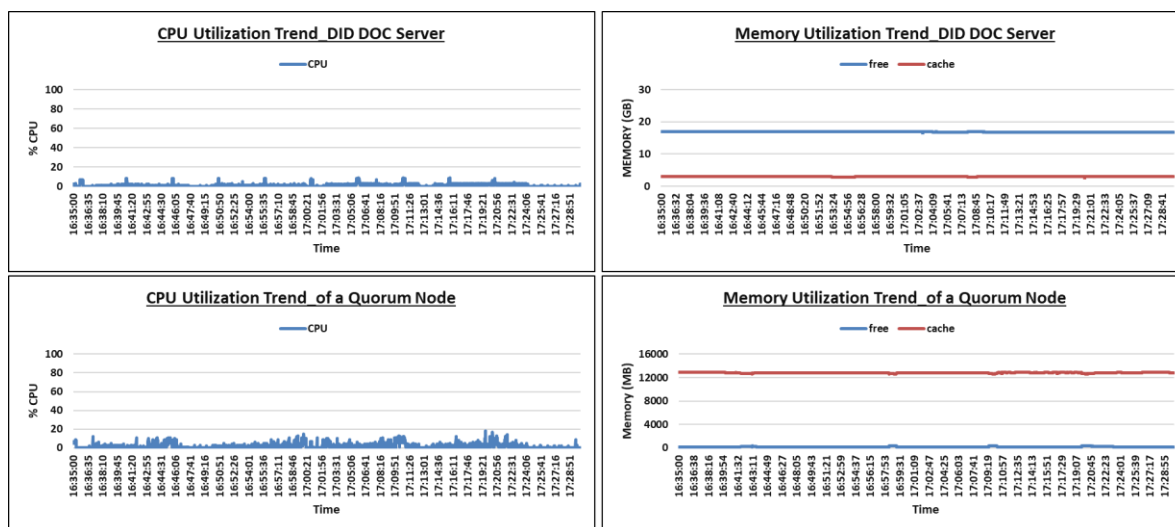


Figure 67: Create DID API Resource Utilization

The second test was for "Send Transaction API". The "Send Transaction API" test runs demonstrated the highest throughput, achieving a maximum of 143.1 transactions per second. . This is higher than the expected throughput which ranges between 2.42 and 3.87 per second. The sample transaction ranged between 53,233 and 86,543 with a 100% success rate that was achieved across all test runs. Response times was the lowest with an average of 0.207 seconds

and a 90th percentile of 0.217 seconds for the test scenario which had the highest number of transaction. Figures 68 and 69 illustrate the performance metrics results of "Send Transaction API" throughput, response time, CPU utilization and memory utilization.

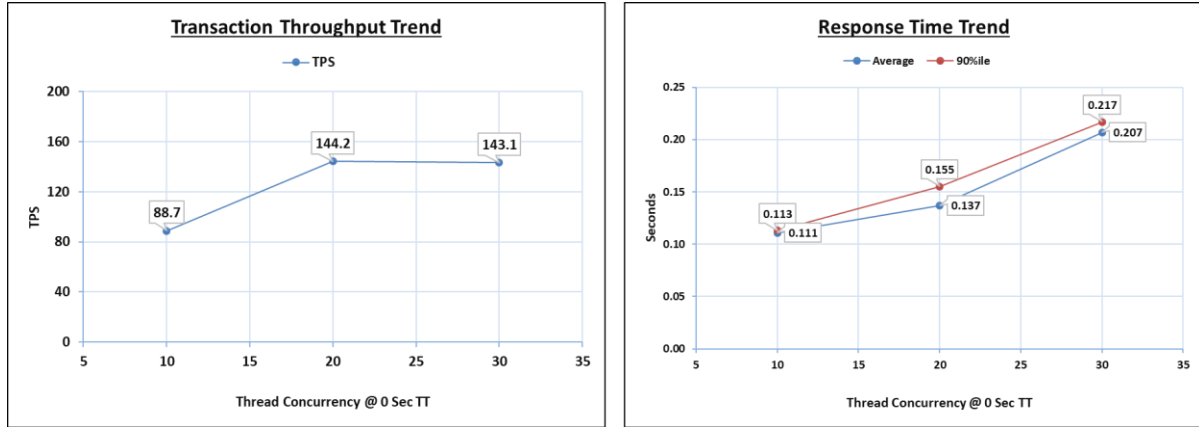


Figure 68: Send Transaction API Throughput and Response Time

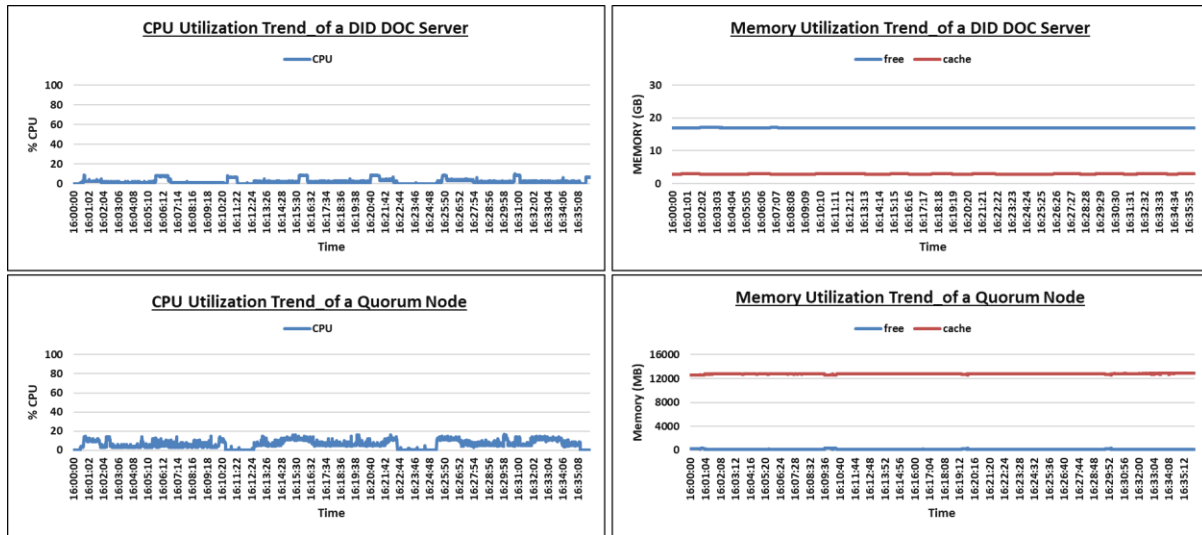


Figure 69: Send Transaction API Resource Utilization

The third test was conducted for "Create POI API". The "Create POI API" test results demonstrated that the throughput increased from 6.7 to 19.7 transactions per second as the concurrent threads were scaled up from 10 to 40. This is higher than the expected throughput which ranges between 0.85 and 1.36 per second. The sample transaction ranged between 4,039 and 11,859. A minor issues was observed with load increasing to 30 and 40 concurrent threads. Some of the requests were not completed successfully resulting into error rates of 0.34% and 1.23%. These errors were attributed to transaction receipts not being generated. The error occurred when the same issuer is issuing multiple VCs concurrently at a high load. These transactions are posted on the Blockchain with the issuer account. Each transaction posted into the Blockchain has a nonce associated with it. The nonce needs to be unique for all transactions posted from the same account. This is achieved with the web3j library by requesting the nonce from the Blockchain and passing this nonce into the transaction. However, under heavy load from multiple machines the atomicity of these operations cannot be ensured, thereby associating same nonce value with two transaction and causing one transaction to fail to be written in the Blockchain. This can be resolved by having an asynchronous process that picks up the failed transactions and posting them again. The response times remained consistently below established thresholds as illustrated in figure 70, signifying stability under increasing pressure. Additionally, the CPU and memory utilization were efficient as indicated in figure 71.

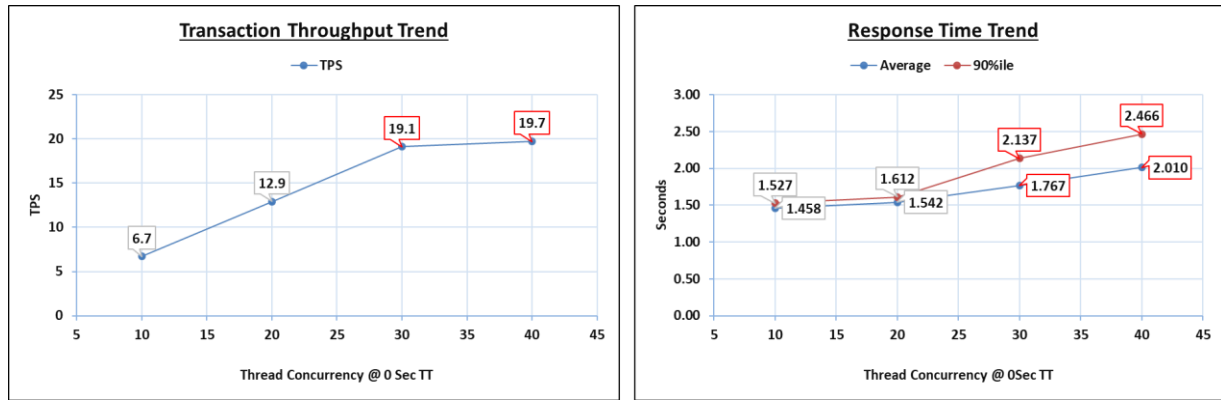


Figure 70: Create POI API Throughput and Response Time

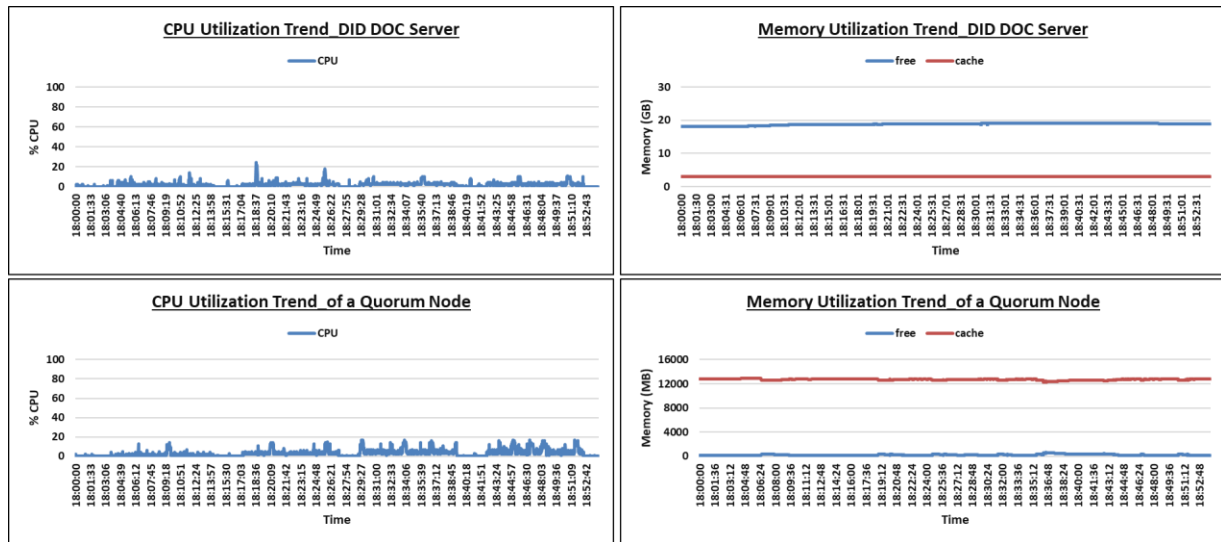


Figure 71: Create POI API Resource Utilization

In order to simulate a real world scenario, a test was conducted combining different Blockchain APIs running simultaneously for a period of two hours. The 30 concurrent threads were set in this test with 10 threads simulated for each type of API. The total throughput per second was 78.1. Moreover, a 100% success rate was achieved across all APIs. The response

times remained consistently below established thresholds, signifying stability under increasing pressure. Additionally, the CPU and memory utilization remained within manageable levels, indicating efficient resource usage.

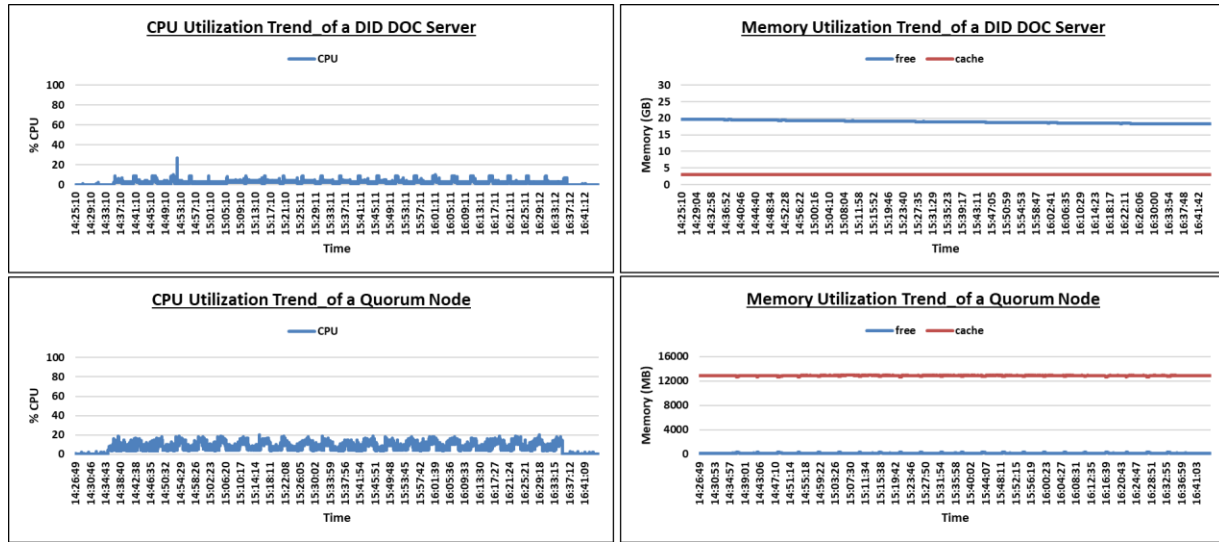


Figure 72: Combined Blockchain APIs Resource Utilization

The performance of the business services were also measured through performance metrics including throughput, response times (average and 90th percentile), and error rates. The performance metrics were evaluated for core business services which are credential service and presentation service. Each service was evaluated individually with all APIs related to it as well as combining the two services together. This test had a dependency on the external partner systems which are the issuer entity and the service provider entities. Thus, the load generated was less considering it was a test environment for the external systems. The test scenarios were run for durations ranging from 10 minutes for the individual service test scenarios and one hour for the combined test scenario.

For the presentation service test, the average and 90th percentile response times for all the APIs was under 0.5 second from a total of around 770 samples of each API. The throughput was 1.3 per second which is slightly higher than the average TPS expected. The success rate was 100% which was achieved across all APIs demonstrating the system's reliability and stability in fulfilling presentation service requests. For the credential service test, the average and 90th percentile response times for all the APIs was under 0.3 second from a total of around 60 samples for each API except for “Credential Request” service and “View Credential” service which are dependent on response from ICA, external system, which was around 3 to 4 seconds. The throughput was less than the expected measure. The success rate was 100% which was achieved across all APIs demonstrating the system's reliability and stability in fulfilling credential service requests.

The combined test was conducted with 10 concurrent threads for all services. The sample ranged from 305 to 9,800 transactions with less load been passed to external partners. The throughput ranged between 1 and 3 per seconds. The average and 90th percentile response times was under 0.5 second for all the APIs except for “Credential Request” service and “View Credential” service which are dependent on response from ICA, external system, which was around 3 to 5 seconds. All APIs had 100% success rate expect one of the APIs related to “Credential Request” had an error of 14% which was attributed to it been an external test environment.

The performance of the overall prototype system of the Blockchain API and business services showed satisfactory performance across various metrics indicating the system stability and reliability in handling expected growing load. The overall performance metrics in

term of throughput, response times (average and 90th percentile), error rates, CPU utilization, and memory utilization were all within expected thresholds. There were valuable insights in term of its transactional capabilities and areas for improvement. The "Create POI API" testing highlighted stability issue that warranted further investigation and optimization. A batch processing with asynchronous call can address the issue observed. Future testing can be considered simulating higher realistic loads and addressing dependencies on external systems to further measure the system performance.

8.5 Chapter Summary

This chapter described the evaluation of the Digital Trust Framework by demonstrating case study of the prototype system and examining the obtained results. First, it described the case study settings which includes the selection of the case study, the sampling, the user and scenarios preparation, and the service providers on boarding. The case study included the on boarding of two major national finance institutes as service providers, an identity entity as issuer and 400 users as citizen.

The chapter then describes the evaluation of the prototype system through defined performance metrics. The chapter outlines two sets of evaluation. The first one was business focused in which the KYC process efficiency was examined through standards performance metrics which included processing time, accuracy of verification, and cost per KYC. The second one was technical focused to examine the robustness of the prototype system by evaluating the overall system efficiency through standards performance metrics which included throughput, response times (average and 90th percentile), error rates, CPU

utilization, and memory utilization. The technical evaluation investigated the performance of the Blockchain APIs as well as the business services.

The next chapter will provide final conclusions, discuss results, limitations, and implications of the Digital Trust Framework. It will also present the overall findings and achievements of this thesis addressing the research questions and objectives. Moreover, it will outline future research directions.

Chapter 9: Conclusions and Recommendations

9.1 Introduction

This chapter represents the communication phase which is the last phase of this thesis. As highlighted in Section 4.4.5, the communication phase reviews and consolidates the outcomes of the development of the Digital Trust Framework and communicates the main findings to diverse interested audiences. Thus, this chapter provides a summary of the results of this thesis. It also describes the significance and research limitations. Moreover, it highlights the key contributions to the knowledge. Finally, it highlights areas for future work.

9.2 Research Aim and Objectives

The primary aim of this thesis is described in Section 1.4 as:

“design, develop, and evaluate a new framework using SSI and blockchain to improve the KYC process which:

- a) automates the initial verification of the customer through digital identity in which the identity and its credentials can be verified independently,*
- b) instills trust and ensure privacy through the utilization of blockchain and SSI capabilities, and*
- c) operates in a timely manner.”*

The main challenges related to the adoption of emerging technologies, Blockchain and SSI, were identified through the study of the technology capabilities and concepts described in Chapter 2. Moreover, the challenges related to the existing KYC process were identified

through the review of related literature in Chapter 3. As a result, the main aspects of this thesis were identified as the initial identity verification step of the KYC in which the customer data is collected and verified, and the establishment of trust between different parties.

In order to respond to the aim of the thesis and achieve the main aspects, three IT artifacts were designed to form the Digital Trust Framework as described in Chapter 6. Blockchain and digital signatures using public-key cryptography are used as core components to establish trust. The design of the framework considered four key functionalities which are identity registry of each actor, issuance and revocation of verifiable credential, sharing and verification of the credential, and audit trail for any dispute. The functionalities enabled the framework to effectively handle all tasks associated with KYC processes in any domain. The design of the IT artifacts provided the foundation for the implementation of the prototype system described in Chapter 7. The implemented prototype system was validated successfully through the demonstration of real life case study described in Chapter 8. Moreover, the performance of the implemented prototype system was evaluated in Sections 8.3 and 8.4.

The solution architecture artifact described in Section 6.2 focused on achieving the aim of this thesis by designing the identity registration and verification of every actor in the system using established standards. While some of the research described the registration of the issuer and verifier, none of the research to the knowledge of the researcher addressed the issue of registering the Citizen identity with the assurance of the identity vetting process or the authenticity check in a digital form (see Section 3.2). Moreover, the solution architecture addressed the initial document submission authenticity which was not addressed by any of the research (see Section 3.2). The solution architecture used the National Digital ID to derive the

Citizen DID digitally unlike existing frameworks which either require the citizen to visit for the first time or register online and upload the documents without any authenticity check. Moreover, the solution architecture proposed having the credentials been issued and managed by issuing authority in form of verifiable credentials to ensure the authenticity and validity of the documents. Unlike existing methods which depends on the submission of the documents manually and issuance of KYC verification document in form of verifiable credentials that is not managed in case of any future changes. These two design aspects of the framework corresponds directly to point (a) of the aim. These capabilities were implemented in the prototype system as described in Sections 7.6.1 and 7.6.2. Leveraging both Blockchain and digital signatures enabled the verification of each transaction which instill trust among various parties involved in the ecosystem. This design aspect of the framework corresponds directly to both points (a) and (b) of the aim. These capabilities were also implemented in the prototype system as described in Section 7.6.3 to Section 7.6.7. Moreover, defining governance framework to manage the network in term provisioning of partners and node hosting contributed to the trust in the network. Empirical evaluation of the prototype system demostarted that the derived digital identity, issuance of verifiable credentials and utilizing Blockchain and digital signatures reduced the total time to conduct KYC to 1 day instead of 7 to 15 days with traditional methods and saved around 78.3% in term of cost per application. Moreover, experts reported that applications that were reviewed were 100% accurate. The achievement represents a significant improvement and suggests that the framework is able to effectively automate the initial verification of the customer. None of the existing research have demostarted the frameworks proposed by them nor evaluated them (see Section 3.2).

Moreover, in an interview conducted with experts, 67% of the interviewees highlighted the challenge of establishing trust between banks and customer which indicates that the proposed frameworks were not acceptable (Schlatt et al., 2022). In the contrary, in the interviews conducted in this thesis with experts, the results showed that 100% of the experts confirmed the trust instilment in the proposed framework in this thesis (see Sections 5.3 and 6.5).

The KYC process and user experience prototype were developed as IT artifacts of the Digital Trust Framework as outlined in Sections 6.3 and 6.4. The key processes are related to VC issuance and revocation by the Issuer, VP sharing by the Citizen and verification by Verifier and can be applied to any KYC process. The KYC process was developed to illustrate end-to-end digitization of the KYC process without the need for manual intervention. It was intended to ease the understanding of the solution architecture in form of sequence diagram which facilitated the evaluation of the framework by experts as described in Section 6.5.1. The development of the user experience prototype of the Digital Wallet on the other hand eases the evaluation of the Digital Trust Framework by end users. No former research paper had an end-user prototype designed and presented. The evaluation of these two artifacts has been included as part of the KYC process efficiency performance metrics as described in Section 8.3.

Point (c) of the research aim is addressed through the evaluation of the overall prototype system efficiency described in Section 8.4. The outcomes of the evaluation showed satisfactory performance across various metrics indicating the system stability and reliability in handling expected growing load. In a combined test with different APIs been executed simultaneously to simulate real world scenario, in which the sample ranged from 305 to 9,800 transactions per API, the throughput ranged between 1 and 3 per seconds and the average and

90th percentile response time was under 0.5 second for all the APIs except for “Credential Request” service and “View Credential” service which were dependent on a response from external system, which was around 3 to 5 seconds. All APIs had 100% success rate except one of the APIs related to “Credential Request” which had an error of 14% which was attributed to it been an external test environment. The challenges faced were mainly attributed to it been an external test environment. Further tests can be conducted in future work with more reliable test environments from external partners.

The following sections will review and discuss the research objectives and their related outcomes.

9.2.1 Objective One

The first objective of this thesis was described as:

“understand and analyze the characteristics and capabilities of blockchain, SSI and digital identities”

In order to address the first objective of the thesis, Chapter 2 focused on exploring concepts related to this research which includes digital identity in general, SSI in specific and blockchain. It described the concept of identity and provided an overview of the evolution of identity management system from isolated use identity model to Self-Sovereign Identity (SSI) model. It also investigated SSI design patterns defined by widely adopted international technical organizations which can be used to design SSI systems. These design patterns were leveraged during the design of the Digital Trust platform in specific the Qualified Electronic Certificates (QEC) design patterns to instill trust in regulated domains. Moreover, the chapter

highlighted few challenges to consider when implementing SSI model. These challenges have been addressed in the design and the implementation of the Digital Trust Framework.

Moreover, the chapter described the concept of Blockchain, and its key characteristics, properties, types and its implementation in different domains. It highlighted the importance of Blockchain in realizing SSI implementations. It investigated existing solutions of Blockchain based SSI implementations. The challenges and constraints of Blockchain were also highlighted. The chapter emphasized on the importance of balancing between centralized and decentralized models. Finally, it provided a summary on privacy frameworks internationally and in UAE that need to be considered during the design and implementation of identity related solutions.

The information achieved at the end of this stage served as foundation to guide the definition of design objectives as well as the design and development of the Digital Trust framework as part of addressing objectives 2, 3 and 4.

9.2.2 Objective Two

The second objective was described as:

“study the underlying concepts, requirements and existing methods and current state of the use of blockchain and SSI in KYC”

In order to address the second objective of this thesis, a review of existing research related to implementing decentralized digital identity, SSI, and blockchain to improve the KYC process efficiency in the financial was presented in Chapter 3. The financial sector was selected due to the fact that it is the most restricted domain in term of KYC processes. The

chapter described the main gaps in the existing blockchain implementation specific to KYC, which are the regulatory support, ID verification during the initial document validation phase, the storage of data and scalability impact for on-chain data and the security and privacy impact for off-chain data, and the scalability of the network versus the security and privacy of data. The challenge related to initial identity verification was identified as the most critical phase, which is inefficient and inaccurate phase in KYC process. This is due to the fact that this challenge prevented having end-to-end digital processing and automation of manual processes of the KYC. This served as justification for focusing on the initial identity verification and confirmed the need of the research as described in Section 1.4.

In addition, the chapter reviewed the usage of Blockchain in Digital Identity since none of the research related to KYC investigated that. The review highlighted the advantages and challenges of blockchain implementations in IdM. Moreover, the chapter presented eID and SSI implementations in governments worldwide, highlighting lessons learnt. The core lessons highlighted included the need for easy to use solution with availability of services, modular architecture solution, and the security and privacy aspects to be by design.

The knowledge gained at the end of Chapter 3 greatly influenced the requirements of the Digital Trust Framework and the identified design objectives which were described in Chapter 5. The design objectives focused on streamlining the KYC process in the financial sector through automation and digitization. The objectives included efficiency, regulatory compliance, trust establishment, privacy protection, user experience, sustainability and technology advancement. Experts evaluated the design objectives in one-on-one interviews. They represented various expertise and organizations with experience working locally and

internationally. Their selection ensured diversity and coverage of all involved stakeholders from a wide range of entities. The evaluation's key insights capitalized on trusted digital identity and having government as a trust anchor.

The outcomes of Objectives 1 and 2 significantly contributed to the design and implementation of the Digital Trust Framework in response to the aim of this thesis.

9.2.3 Objective Three

The third objective of this thesis was to design a KYC framework fulfilling below aspects:

- a) Digital identity establishment, management and verification to enable the automation of the initial customer identification and verification, and continuous monitoring*
- b) Trust instilment to be accepted by participants in KYC process through blockchain, and*
- c) Regulatory and legal acceptance*

Designing a new framework to improve the KYC efficiency and user experience in financial sector in Chapter 6 of this research was considered as part of the aim of this thesis. The design of the Digital Trust Framework was formulated based on the concepts drawn from investigating recent existing characteristics and capabilities of technology and design patterns in response to Objective 1 and reviewing current approaches to improve the KYC efficiency in response to Objective 2.

The Digital Trust Framework artifacts consisted of architecture, processes and a user experience prototype of the Digital Wallet application. The IT artifacts were designed based

on the design objectives and requirements defined earlier. The design of the framework directly addresses the challenges identified earlier. The solution architecture leveraged Blockchain and digital signatures to establish trust in the new framework. The processes of the framework were defined as general processes that can be applied to any KYC process. The development and evaluation of the architecture and processes were conducted iteratively with experts through interviews and focus groups, while the Citizens evaluated the Digital Wallet application prototype in the form of a digital survey. The survey aimed to evaluate the digital wallet concept concerning different aspects, including user experience, relevance and acceptance.

The outcome of the third objective contributed in addressing the fourth and fifth objectives in specific in term of creating the foundation for the prototype system implementation.

9.2.4 Objective Four

The fourth objective was described as:

“implement a prototype system for blockchain-based SSI and KYC use cases”

The implementation of a prototype system described in details in Chapter 7, addressed the fourth objective. It was based on the design of the new framework in response to Objective 3. The implementation assisted in the realization and validation of the new designed framework. The functionalities of the framework were specified in Section 7.3, to ensure efficient implementation.

After the definition of the prototype system functionalities, the prototype system was implemented in a layered and modular architecture pattern which was detailed in Section 7.4. The Business Services layer implemented the business services of the Digital Trust Framework which encompass its core functionality in term of issuing and sharing credentials. Open source technologies were used for the implementation of the prototype system except for the database and HSM. It was based on Spring cloud¹⁵ architecture. Quorum was chosen as Blockchain technology to implement private permissioned network. Moreover, RAFT was chosen as consensus model as it enables faster block times, transaction finality, and on-demand block creation. The prototype system enabled the demonstration of the framework through case study and the evaluation of the framework to achieve Objective 5 of this thesis.

9.2.5 Objective Five

The last objective of this thesis which is the fifth objective, was to evaluate the new proposed framework through the evaluation of the implemented prototype system and to identify any improvement areas. Chapter 8 presented the details of the prototype evaluation. The evaluation was conducted in two steps. The first step was to validate the feasibility of the prototype system through a real life case study demonstration. A number of steps were taken to fulfill the requirements of the case study demonstration. This include case study selection, sampling, user and scenario preparations, and service provider on boarding. The case study included the on boarding of two major national finance institutes as service providers, an

¹⁵ <https://spring.io/cloud/>

identity entity as issuer and 400 users as citizen. This was followed by the evaluation of the prototype system through defined performance metrics. The prototype system was evaluated in term of KYC process efficiency this included processing time, accuracy of verification, and cost per KYC, and robustness of the prototype system which included throughput, response times, error rates, and CPU and memory utilization. In order to be able to evaluate the overall performance of the prototype system to ensure its robustness, a reference performance results were defined based on the expected utilization of the system in real world setting.

The outcome of the evaluation enabled the researcher to verify the feasibility and performance of the proposed system. It also enabled the researcher to identify areas of improvement which can be addressed through an iteration of the design process or the communication of the limitation in the thesis. This research was conducted in an iterative manner with various improvements been implemented based on the results of the evaluations throughout the research process. However, due to the time and resources constrains, a number of improvement areas were not implemented and left for future work. The limitations and recommendations for future work are highlighted in Section 9.5.

The findings of the fifth Objective as well as the findings of the third and fourth objectives contributes to responding to the research problem.

9.3 Conclusion on Research Problem

The research problem is stated in Section 1.2 as:

“Despite the recognized potential of blockchain and SSI to improve the efficiency of KYC processes, current approaches in blockchain research:

- a) *do not efficiently digitize the initial customer identification and verification as well as continuous monitoring*
- b) *do not accurately identify the authenticity and integrity of the customer during the initial customer identification and verification*
- c) *do not incorporate regulatory, servicer provider, document issuer, and customer requirements for the initial customer identification and verification as well as continuous monitoring in a unified accepted framework*

As a result, current approaches cannot provide a comprehensive and trusted foundation for the adoption of blockchain in regulated environment that requires a thorough KYC.”

The research problem stated above was addressed through a new framework that was designed, implemented and evaluated. The framework was capable to create a seamless digital service that includes submitting and processing relevant documents end-to-end with high-level assurance of the authenticity of the customer’s digital identity and its association with the digital documents submitted, without needing a physical presence or manual intervention. The implementation of the proposed framework in form of prototype system and the demonstration of the prototype in a real life case study provided clear indication of the feasibility of the framework and effectiveness in improving the efficiency of the KYC process. The performance evaluation of the prototype system demonstrated significant improvement in the efficiency of KYC process in term of time, cost and accuracy in comparison to existing approaches in related areas. Moreover, as far as the researcher is aware, it is the first attempt to examine the relevance in real environment settings where business needs from all stakeholders were evaluated in a unified framework. It includes individuals, government, regulatory,

technology and private sector. The study ensures that stakeholders are included in the design process since it is important to provide them with solutions that serve their needs to ensure user satisfaction while increasing the intention to adopt the proposed solution (Wagner *et al.*, 2018).

9.4 Implications and Contributions

The successful development and deployment of a framework that improves the KYC efficiency in financial sector, contributes to an ongoing research of the utilization of digital solutions to instill trust in regulated domain. The framework can assist financial institutes in reducing the time and cost of the KYC processes in onboarding new customers and ongoing monitoring, eliminating the need for manual processes while improving the quality and accuracy of the data gathering. The proposed framework can also eliminate the manual verification of standard risk customers, which covers a significant percentage of financial institutions' customer bases. It takes around 7 to 14 days to onboard new customer based on existing approaches. The proposed framework in this thesis can be used to digitize the initial customer identification and verification and automate the process. The framework can also be used to provide instant updates for the ongoing monitoring process.

This thesis proposes a novel design of a framework that instills trust in regulated domain and enables the digitization and automation of end to end KYC process. First of all, getting the requirements from all different stakeholders to form the design objectives is an essential knowledge to design any framework. Second designing the IT artifacts addressing well-known challenges with technologies and KYC process, and deriving three design principles, is an essential knowledge that allows the IT artifacts developed in this research to be evaluated for

more abstract and generalizable theoretical discussion. The design principles also provide guidance for blockchain-based SSI design alignment considering businesses' and regulators' needs. The findings of the evaluation in a form of case study suggested that the framework performs all the tasks related to the initial identification and verification in a reliable and timely manner. The performance level of the proposed framework can be considered as baseline as no other research to the knowledge of the researcher have published any results. These results have been evaluated against expected real performance and found satisfactory (see Section 8.4).

The design of the Digital Trust Framework has been developed and evaluated by experts from financial and telecom domains. However, the financial sector evaluated the framework in depth. The telecom sector was evaluated at a high level during the design phase. Evaluating the framework by different domains is subject to future research. Moreover, the targeted audience representing the end users using the proposed framework was diverse. Due to the **fact that the** feedback collected from end users in **the form of** a quantitative study indicated security as a key factor for the acceptance of the proposed framework, a qualitative study is needed to validate the results, understand their needs further and confirm that the proposed framework addresses them. Further studies would need to evaluate data storage design choices and **to** define guiding principles on data storage and the roles and responsibilities of the data custodians as the current design choice has implications in terms of performance on the issuer system and high dependency on the availability of their systems.

9.5 Recommendations for Future Work

A number of further research directions were identified based on the research conducted. The future work can be relevant to existing limitation of the framework or possible extensions to the framework. The research presented in this thesis intended to lead to deeper and more robust utilization of technology to create a digitally trusted framework to enable critical domains and services to transact digitally without the need to manual or physical intervention to be able to have continuity of business during crisis like COVID-19.

1. Smart contract was used to create the proof of issuance. At very high load from multiple machines the atomicity of these operations cannot be ensured, thereby associating same nonce value with two transactions and causing one transaction to fail to be written in the Blockchain. This has caused a minor error rate in term of failed transactions. A proposed solution is suggested in term of having asynchronous process that picks up the failed transactions and posts them again. Further research can be conducted to investigate alternative solutions.
2. Readiness of external partner test environment have impacted the ability to conduct an extensive test on APIs that had dependencies on these environments. While the test was satisfactory on lower sample, a larger volume might be required to be test to ensure the robustness of the proposed framework.
3. Maintaining the data with each issuer instead of distributing it across a decentralized system may have implications in terms of performance on the issuer system and the high dependency on the availability of their systems. The evaluation results highlighted the ongoing debates about the best methods for

data storage, emphasizing the high risk of storing data in centralized storage. In addition, they stressed that data storage risks should not be delegated to the user and emphasized the need to strike a balance between protecting user data and providing a seamless user experience. Storing data on the cloud may offer a better user experience but raises privacy and security concerns. Further studies would need to evaluate data storage design choices and define guiding principles on data storage and the roles and responsibilities of the data custodians.

4. Citizens highlighted requirements such as sharing minimal data instead of documents and sharing tokenized information, suggesting further study potential in terms of feasibility and acceptance of data minimization and ZKPs.

References

- Aberdeen, T. (2013) 'Yin, R. K. (2009). Case study research: Design and methods (4th Ed.). Thousand Oaks, CA: Sage.,' *The Canadian Journal of Action Research*, 14(1), pp. 69–71. <https://doi.org/10.33524/cjar.v14i1.73>.
- Abraham, A. *et al.* (2020) 'Privacy-Preserving EID derivation for Self-Sovereign Identity Systems,' in *Lecture Notes in Computer Science*, pp. 307–323. https://doi.org/10.1007/978-3-030-41579-2_18.
- Abraham, A., Theuermann, K. and Kirchengast, E. (2018) 'Qualified eID derivation into a distributed ledger based IdM system', *2018 17th IEEE international conference on trust, security and privacy in computing and communications*. New York, NY, USA, 2018, pp. 1406–1412. doi:10.1109/trustcom/bigdatase.2018.00195.
- Ahn, G. -J., Ko, M. K. W. and Shehab, M. (2009) 'Privacy-enhanced user-centric identity management', *2009 IEEE international conference on communications*. Dresden, Germany, 2009, pp. 1–5. doi:10.1109/ICC.2009.5199363.
- Aken, V.J.J. (2007) 'Design science and organization development interventions,' *The Journal of Applied Behavioral Science*, 43(1), pp. 67–88. <https://doi.org/10.1177/0021886306297761>.
- Akkermans, H. and Gordijn, J. (2006) 'What is This Science Called Requirements Engineering?,' *14th IEEE International Requirements Engineering Conference (RE'06)*, pp. 273–278. <https://doi.org/10.1109/re.2006.73>.

- Al Tamimi & Company (2020) *UAE central bank: Modernisation of identification procedures*. Available at: <https://www.tamimi.com/law-update-articles/uae-central-bank-modernisation-of-identification-procedures/>.
- Al Tamimi & Company (2021a) *UAE issues new federal electronic transactions and trust services law*. Available at: <https://www.tamimi.com/news/uae-issues-new-federal-electronic-transactions-and-trust-services-law/>.
- Al Tamimi & Company (2021b) *UAE's new federal data protection law*. Available at: <https://www.tamimi.com/news/uaes-new-federal-data-protection-law/>.
- Allen, C. (2016) 'The path to self-sovereign identity', *Life with alacrity*, 25 April. Available at: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html>.
- Anthony, B. (2022) 'Toward a collaborative governance model for distributed ledger technology adoption in organizations,' *Environment Systems and Decisions*, 42(2), pp. 276–294. <https://doi.org/10.1007/s10669-022-09852-4>.
- Arner, D. W. *et al.* (2018) 'The identity challenge in finance: From analogue identity to digitized identification to digital KYC utilities', *European Business Organization Law Review*, 20, pp. 55–80. doi:10.1007/s40804-019-00135-1.
- Arner, D. W., Barberis, J. N. and Buckley, R.P. (2016) 'The emergence of Regtech 2.0: From know your customer to know your data', *Regulation of Financial Institutions eJournal*. doi:10.2139/SSRN.2676553.

- Azaria, A. *et al.* (2016) 'MedRec: Using blockchain for medical data access and permission management', *2016 2nd international conference on open and big data (BD)*. Vienna, Austria, 2016, pp. 25–30. doi:10.1109/OBD.2016.11.
- Au, Y.A. (2001) 'Design Science I: The role of Design Science in Electronic Commerce Research,' *Communications of the Association for Information Systems*, 7. <https://doi.org/10.17705/1cais.00701>.
- Baskerville, R. L. *et al.* (2018) 'Design science research contributions: Finding a balance between artifact and theory', *Journal of the Association for Information Systems*, 19(5), pp. 358–376. doi:10.17705/1jais.00495.
- Bathen, L.A.D. *et al.* (2019) 'SelfIs: Self-Sovereign Biometric IDs,' *In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)*, pp. 2847–2856. <https://doi.org/10.1109/cvprw.2019.00344>.
- Baxter, P. and Jack, S.M. (2015) 'Qualitative case study Methodology: study design and implementation for novice researchers,' *The Qualitative Report* [Preprint]. <https://doi.org/10.46743/2160-3715/2008.1573>.
- Beck, R. *et al.* (2017) 'Blockchain technology in business and information systems research', *Business & Information Systems Engineering*, 59(6), pp. 381–384. doi:10.1007/s12599-017-0505-1.
- Benbasat, I. and Zmud, R. W. (1999) 'Empirical research in information systems: The practice of relevance', *Management Information Systems Quarterly*, 23(1), p. 3. doi:10.2307/249403.

- Benbasat, I. and Zmud, R. W. (2003) 'The identity crisis within the IS discipline: Defining and communicating the discipline's core properties', *Management Information Systems Quarterly*, 27(2), p. 183. doi:10.2307/30036527.
- Bergeå, O. *et al.* (2006) 'Education for sustainability as a transformative learning process: a pedagogical experiment in EcoDesign doctoral education,' *Journal of Cleaner Production*, 14(15–16), pp. 1431–1442. <https://doi.org/10.1016/j.jclepro.2005.11.020>.
- Bhaskaran, K. *et al.* (2018) 'Double-blind consent-driven data sharing on blockchain', 2018 *IEEE international conference on cloud engineering (IC2E)*. Orlando, FL, USA, 2018, pp. 385–391. doi:10.1109/IC2E.2018.00073.
- Bolderston, A. (2008) 'Writing an effective literature review,' *Journal of Medical Imaging and Radiation Sciences*, 39(2), pp. 86–92. <https://doi.org/10.1016/j.jmir.2008.04.009>.
- Bowen, G. A. (2009) 'Document analysis as a qualitative research method', *Qualitative Research Journal*, 9(2), pp. 27–40. doi:10.3316/qj0902027.
- Brocke, J.V. *et al.* (2020) 'Special issue editorial – Accumulation and evolution of design knowledge in design science research: A journey through time and space', *Journal of the Association for Information Systems*, 21(3), pp. 520–544. doi:10.17705/1jais.00611.
- Butijn, B. -J., Tamburri, D. A. and Van Den Heuvel, W. -J. (2020) 'Blockchains', *ACM Computing Surveys*, 53(3), pp. 1–37. doi:10.1145/3369052.
- Bunge, M. (1967) *Scientific Research: The search for system*. Berlin ; New York : Springer-Verlag.

- Bunge, M. (1985) *Epistemology & Methodology III: Philosophy of Science and Technology Part I: Formal and Physical Sciences*. Springer Science & Business Media.
- Cahill, C. P. (2007) 'Liberty ID-WSF provisioning service specification', *Liberty alliance project*. Available at: <https://www.projectliberty.org/liberty/content/download/3915/25672/file/liberty-idwsf-prov-v1.0.pdf>.
- Calmeyer, T. *et al.* (2011) 'How to succeed in your master's and doctoral studies: A South African guide and resource book, Johann Mouton : book review,' *New Voices in Psychology*, 7(2), pp. 148–152.
<https://journals.co.za/content/unipsyc/7/2/EJC119602>.
- Cameron, K. (2005) 'The laws of identity', *Kim Cameron's identity weblog*, 5 November. Available at: <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>.
- Cantor, S. *et al.* (eds.) (2005) 'Assertions and protocols for the OASIS security assertion markup language (SAML) V2.0', *Security Services Technical Committee*. Available at: <https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>.
- Casino, F., Dasaklis, T. K. and Patsakis, C. (2019) 'A systematic literature review of blockchain-based applications: Current status, classification and open issues', *Telematics and Informatics*, 36, pp. 55–81. doi:10.1016/j.tele.2018.11.006.
- Central Bank of the UAE (2018) *Chapter 16 of the standards for the regulations regarding licensing and monitoring of exchange business, Version 1.20 of November 2021 amending Version 1.10 of February 2018* (2021). Available at:

<https://www.centralbank.ae/media/5ghbiokx/chapter-16-of-standards-version-1-20-of-nov-2021-amending-version-1-10-of-feb-2018.pdf>.

Chadwick, D. R. (2009) 'Federated identity management,' in Aldini, A., Barthe, G. and Gorrieri, R. (eds.) *Foundations of security analysis and design*, Berlin: Springer, pp. 96–120. doi:10.1007/978-3-642-03829-7_3.

Charmaz, K. (2006) *Constructing grounded theory: A practical guide through qualitative analysis*. Newberry Park, CA: Pine Forge Press.

Chatterjee, S. (2006) 'The role of theory and theorising in design science research', *First international conference on design science research in information systems and technology*, 24 February. Claremont, CA: Claremont Graduate University.
doi:10.1.1.110.2475.

Checkland, P. (1999) *Systems thinking, systems practice*.

Cleven, A., Gubler, P. and Hüner, K. (2009) 'Design alternatives for the evaluation of design science research artifacts,' *DESRIST '09: Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology* [Preprint]. <https://doi.org/10.1145/1555619.1555645>.

Cole, R.E. *et al.* (2005) 'BEING PROACTIVE: WHERE ACTION RESEARCH MEETS DESIGN RESEARCH,' *Proceedings of the International Conference on Information Systems, ICIS 2005* [Preprint]. <http://dblp.uni-trier.de/db/conf/icis/icis2005.html#ColePRS05>.

- Colladon, A. F. and Remondi, E. (2017) 'Using social network analysis to prevent money laundering', *Expert Systems With Applications*, 67, pp. 49–58.
doi:10.1016/j.eswa.2016.09.029.
- Concept Testing: Methods, examples & best practices (2022).
<https://www.qualtrics.com/uk/experience-management/product/product-concept-testing/?rid=ip&prevsite=en&newsite=uk&geo=AE&geomatch=uk>.
- Creswell, J. W. (2014) *Educational research: Planning, conducting, and evaluating quantitative and qualitative Research* (5th edn.). New York: Pearson Education.
- Čučko, Š., Keršič, V. and Turkanović, M. (2023) 'Towards a catalogue of Self-Sovereign identity design patterns,' *Applied Sciences*, 13(9), p. 5395.
<https://doi.org/10.3390/app13095395>.
- Cucko, S. and Turkanović, M. (2021) 'Decentralized and self-sovereign identity: Systematic mapping study', *IEEE Access*, 9, pp. 139009–139027. doi:10.1109/access.2021.3117588.
- Decentralized Identity Foundation. (2022) *Together We're Building a New Identity Ecosystem*. Available at: <https://identity.foundation/>.
- Deng, Q. and Ji, S. (2018) 'A review of design science research in information systems: Concept, process, outcome, and evaluation', *Pacific Asia Journal of the Association for Information Systems*, pp. 1–36. doi:10.17705/1pais.10101.
- Denyer, D., Tranfield, D. and Aken, V.J.J. (2008) 'Developing Design Propositions through Research Synthesis,' *Organization Studies*, 29(3), pp. 393–413.
<https://doi.org/10.1177/0170840607088020>.

- Dhamija, R. and Dussault, L. (2008) “The seven flaws of identity management: Usability and security challenges,” *IEEE Security & Privacy*, 6(2), pp. 24–29. Available at: <https://doi.org/10.1109/msp.2008.49>.
- Domeyer, A. *et al.* (2020) ‘How governments can deliver on the promise of digital ID’, *McKinsey & Company*. Available at: <https://www.mckinsey.com/industries/public-and-social-sector/our-insights/how-governments-can-deliver-on-the-promise-of-digital-id>.
- Dong, C. *et al.* (2020) ‘BBM: A blockchain-based model for open banking via self-sovereign identity’, in *Lecture notes in computer science*. Cham: Springer Science+Business Media, pp. 61–75. doi:10.1007/978-3-030-59638-5_5.
- Dresch, A., Lacerda, D.P. and Antunes, J.A.V. (2014) *Design Science Research: A Method for science and Technology Advancement*. <http://ci.nii.ac.jp/ncid/BB1882021X>.
- Dubé and Paré (2003b) ‘Rigor in Information Systems Positivist case Research: Current practices, trends, and recommendations,’ *Management Information Systems Quarterly*, 27(4), p. 597. <https://doi.org/10.2307/30036550>.
- Dunphy, P., Garratt, L.W. and Petitcolas, F. (2018) ‘Decentralizing digital identity: Open challenges for distributed ledgers’, *2018 IEEE European symposium on security and privacy workshops (EuroS&PW)*. London, UK, 2018, pp. 75–78. doi:10.1109/eurospw.2018.00016.
- Dunphy, P. and Petitcolas, F. (2018) ‘A first look at identity management schemes on the blockchain’, *IEEE Security & Privacy*, 16(4), pp. 20–29. doi:10.1109/msp.2018.3111247.

- EBSI. (2022) *EBSI Specifications*. Available at: <https://ec.europa.eu/digital-building-blocks/wikis/display/EBSIDOC/>.
- European Union (2014) *Regulation (EU) No 910/2014 of the European Parliament and o... - EUR-Lex* (2014) *Official Journal of the European Union*. 910/2014. Available at: https://eur-lex.europa.eu/legal-content/EN/LSU/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG.
- Eyerman, S. and Eeckhout, L. (2008) 'System-Level Performance Metrics for multiprogram workloads,' *IEEE Micro*, 28(3), pp. 42–53. <https://doi.org/10.1109/mm.2008.44>.
- Fan, K. *et al.* (2018) 'MedBlock: Efficient and secure medical data sharing via blockchain', *Journal of Medical Systems*, 42(8). doi:10.1007/s10916-018-0993-7.
- Ferdous, S., Chowdhury, F. and Alassafi, M.O. (2019) 'In search of self-sovereign identity leveraging blockchain technology', *IEEE Access*, 7, pp. 103059–103079. doi:10.1109/access.2019.2931173.
- Finck, M. (2018) 'Blockchains and data protection in the European Union', *European Data Protection Law Review*, 4(1), pp. 17–35. doi:10.21552/edpl/2018/1/6.
- Fuller, R.B., Inventory, S.I.U. at Carbondale.W.R. and Architects, I.U.O. (1965) *World Design Science Decade 1965-1975: Five Two-year Phases of a World Retooling Design Proposed to the International Union of Architects for Adoption by World Architectural Schools. Comprehensive thinking ; [by R. Buckminster Fuller ; selected and edited by John McHale].. Phase I, doc. 3.*

- Geerts, G.L. (2011) 'A design science research methodology and its application to accounting information systems research,' *International Journal of Accounting Information Systems*, 12(2), pp. 142–151. <https://doi.org/10.1016/j.accinf.2011.02.004>.
- Gibbons, M. et al. (1994) *The new production of knowledge: The Dynamics of Science and Research in Contemporary Societies*. SAGE.
- Glaser, F. (2017) 'Pervasive decentralisation of digital infrastructures: A framework for blockchain enabled system and use case analysis', *ScholarSpace*.
doi:10.24251/hicss.2017.186.
- Grassi, P. (2017) 'Digital identity guidelines (revised draft)', *NIST Computer Resource Center*. Available at: <https://csrc.nist.gov/publications/detail/sp/800-63/3/archive/2017-03-31>.
- Gregor, S. (2006) 'The nature of theory in information systems,' *Management Information Systems Quarterly*, 30(3), p. 611. <https://doi.org/10.2307/25148742>.
- Gregor, S. and Hevner, A. R. (2013) 'Positioning and presenting design science research for maximum impact', *Management Information Systems Quarterly*, 37(2), pp. 337–355.
doi:10.25300/misq/2013/37.2.01.
- Gruner, A., Mühle, A. and Meinel, C. (2019) 'An integration architecture to enable service providers for self-sovereign identity', *2019 IEEE 18th international symposium on network computing and applications (NCA)*, 2019. Cambridge, MA, USA, pp. 1–5.
doi:10.1109/nca.2019.8935015.
- Hardman, D. H. et al. (2019) 'Using biometrics to fight credential fraud', *Using Biometrics to Fight Credential Fraud*, 3(4), pp. 39–45. doi:10.1109/mcomstd.001.1900033.

- Hardt, D. (2012) *The OAuth 2.0 authorization framework*. Available at:
<https://tools.ietf.org/html/rfc6749>.
- Hasan, H. R. *et al.* (2020) 'Blockchain-based solution for COVID-19 digital medical passports and immunity certificates', *IEEE Access*, 8, pp. 222093–222108.
doi:10.1109/access.2020.3043350.
- Hassenzahl, M. and Tractinsky, N. (2006) 'User experience - a research agenda,' *Behaviour & Information Technology*, 25(2), pp. 91–97.
<https://doi.org/10.1080/01449290500330331>.
- Herley, C. (2009) 'So long, and no thanks for the externalities, NSPW '09: *Proceedings of the 2009 workshop on new security paradigms workshop*, pp. 133–144.
doi:10.1145/1719030.1719050.
- Hevner *et al.* (2004) 'Design science in information systems research', *Management Information Systems Quarterly*, 28(1), p. 75.doi:10.2307/25148625.
- Hevner, A. R. and Gregor, S. (2022) 'Envisioning entrepreneurship and digital innovation through a design science research lens: A matrix approach', *Information & Management*, 59(3), p. 103350. doi:10.1016/j.im.2020.103350.
- Hill, R.J. and Hamilton, W.P. (1998) 'WHAT SAMPLE SIZE is 'ENOUGH' in INTERNET SURVEY RESEARCH?,' *Interpersonal Computing and Technology: An Electronic Journal for the 21st Century*, 6.
<http://cadcommunity.pbworks.com/f/what%20sample%20size.pdf>.

- Houtan, B., Hafid, A. and Makrakis, D. (2020) 'A survey on blockchain-based self-sovereign patient identity in healthcare', *IEEE Access*, 8, pp. 90478–90494.
doi:10.1109/access.2020.2994090.
- Hughes, P. J. (1988) 'The “need to know” principle of computer security', *Computer Law & Security Review*, 3(5), pp. 29–30. doi:10.1016/0267-3649(88)90114-8.
- Ja, H. (1989) 'Receiver operating characteristic (ROC) methodology: the state of the art,' *PubMed*, 29(3), pp. 307–35. <https://pubmed.ncbi.nlm.nih.gov/2667567>.
- Jain, H., Sinha, A.P. and Vitharana, P. (2011) *Service-Oriented perspectives in Design Science Research: 6th International Conference, DESRIST 2011, Milwaukee, WI, USA, May 5-6, 2011, Proceedings*. Springer.
- Jessel, B., Lowmaster, K. and Neil, H. (2018) 'Digital identity: The foundation for trusted transactions in financial services', *IDEAS, Research Division of the Federal Bank of St. Louis*. Available at: <https://ideas.repec.org/a/ris/jofitr/1607.html>.
- Jones, D. and Gregor, S. (2007) 'The anatomy of a design theory', *Journal of the Association for Information Systems*, 8(5), pp. 312–335. doi:10.17705/1jais.00129.
- Kallio, H. *et al.* (2016) 'Systematic methodological review: Developing a framework for a qualitative semi-structured interview guide', *Journal of Advanced Nursing*, 72(12), pp. 2954–2965. doi:10.1111/jan.13031.
- Kaminski, T. W. and Pitney, W. A. (2004) 'Strategies for establishing trustworthiness in qualitative research', *Athletic Therapy Today*, 9(1), pp. 26–28. doi:10.1123/att.9.1.26.

- Karame, G. (2016) 'On the security and scalability of Bitcoin's blockchain', *CCS '16: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security*. Vienna, Austria, 24–28 October. doi:10.1145/2976749.2976756.
- Kendig, C. (2015) 'What is Proof of Concept Research and how does it Generate Epistemic and Ethical Categories for Future Scientific Practice?,' *Science and Engineering Ethics*, 22(3), pp. 735–753. <https://doi.org/10.1007/s11948-015-9654-0>.
- Kokolakis, S. (2017) 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon', *Computers & Security*, 64, pp. 122–134. doi:10.1016/j.cose.2015.07.002.
- Kolb, J. *et al.* (2020) 'Core concepts, challenges, and future directions in blockchain,' *ACM Computing Surveys*, 53(1), pp. 1–39. Available at: <https://doi.org/10.1145/3366370>.
- Kothari, C. R. (2004) *Research methodology: Methods and techniques*. New Dehli: New Age International.
- Krejcie, R.V. and Morgan, D.W. (1970) 'Determining sample size for research activities,' *Educational and Psychological Measurement*, 30(3), pp. 607–610. <https://doi.org/10.1177/001316447003000308>.
- Lemieux, V.L., Voskoboynikov, A. and Meng, K. (2021) 'Addressing Audit and Accountability Issues in Self-Sovereign Identity Blockchain Systems Using Archival Science Principles,' *In Proceedings of the 2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, pp. 1210–1216. <https://doi.org/10.1109/compsac51774.2021.00167>.

- Lilja, D.J. (2005) *Measuring computer performance: A Practitioner's Guide*. Cambridge University Press.
- Lim, S. *et al.* (2018) 'Blockchain technology the identity management and authentication service disruptor: A survey', *International Journal on Advanced Science, Engineering and Information Technology*, 8(4-2), p. 1735. doi:10.18517/ijaseit.8.4-2.6838.
- Lincoln, Y. S. and Guba, E. G. (1986) 'But is it rigorous? Trustworthiness and authenticity in naturalistic evaluation', *New Directions for Program Evaluation*, 1986(30), pp. 73–84. doi:10.1002/ev.1427.
- Liu, G. and Haralick, R.M. (2002) 'Optimal matching problem in detection and recognition performance evaluation,' *Pattern Recognition*, 35(10), pp. 2125–2139.
[https://doi.org/10.1016/s0031-3203\(01\)00204-7](https://doi.org/10.1016/s0031-3203(01)00204-7).
- Liu, J. -W. *et al.* (2020a) 'An analysis of digital identity management systems – A two-mapping view', *2020 2nd conference on blockchain research & applications for innovative networks and services (BRAINS)*. Paris, France, 2020, pp. 92–96.
doi:10.1109/brains49436.2020.9223281.
- Liu, Y. *et al.* (2020b) 'Blockchain-based identity management systems: A review', *Journal of Network and Computer Applications*, 166, p. 102731.
doi:10.1016/j.jnca.2020.102731.
- Lootsma, Y. (2019) 'Blockchain as the newest regtech application – The opportunity to reduce the burden of KYC for financial institutions', *Banking & Financial Services Policy Report*, 36(8), pp. 16–21. Available at:

https://www.academia.edu/39393562/Blockchain_as_the_Newest_Regtech_Applicati
[on_the_Opportunity_to_Reduce_the_Burden_of_KYC_for_Financial_Institutions.](https://www.academia.edu/39393562/Blockchain_as_the_Newest_Regtech_Applicati)

Löwe, B. (2002) 'The formal sciences: their scope, their foundations, and their unity,'
Synthese, 133(1/2), pp. 5–11. <https://doi.org/10.1023/a:1020887832028>.

Lucking, M. *et al.* (2020) 'Decentralized identity and trust management framework for
Internet of Things', *2020 IEEE international conference on blockchain and
cryptocurrency (ICBC)*. Toronto, ON, Canada, 2020, pp. 1–9.
doi:10.1109/icbc48266.2020.9169411.

Lukka, K. (2003). The constructive research approach. *Case study research in logistics.*
Publications of the Turku School of Economics and Business Administration, Series
B, 1(2003), 83-101.

Lux, Z. *et al.* (2020) 'Distributed-ledger-based authentication with decentralized identifiers
and verifiable credentials', *2020 2nd conference on blockchain research &
applications for innovative networks and services (BRAINS)*. Paris, France, 2020, pp.
71–78. doi:10.1109/brains49436.2020.9223292.

Maler, E. and Reed, D. E. (2008) 'The Venn of identity: Options and issues in federated
identity management', *IEEE Security & Privacy*, 6(2), pp. 16–23.
doi:10.1109/msp.2008.50.

Malhotra, D., Saini, P. and Singh, A .K. (2021) 'How blockchain can automate KYC:
Systematic review', *Wireless Personal Communications*, 122(2), pp. 1987–2021.
doi:10.1007/s11277-021-08977-0.

- Maliki, T. E. and Seigneur, J. -M. (2007) 'A survey of user-centric identity management technologies', *The international conference on emerging security information, systems, and technologies (SECUREWARE 2007)*. Valencia, Spain, 2007, pp. 12–17. doi:10.1109/secureware.2007.4385303.
- Manson, N.C. (2006) 'Is operations research really research?,' *ORiON*, 22(2). <https://doi.org/10.5784/22-2-40>.
- Maramba, I., Chatterjee, A. and Newman, C. W. (2019) 'Methods of usability testing in the development of eHealth applications: A scoping review', *International Journal of Medical Informatics*, 126, pp. 95–104. doi:10.1016/j.ijmedinf.2019.03.018.
- March, S. T. and Smith, G. R. (1995) 'Design and natural science research on information technology', *Decision Support Systems*, 15(4), pp. 251–266. doi:10.1016/0167-9236(94)00041-2.
- March, S. T. and Storey, V. C. (2008) 'Design science in the information systems discipline: An introduction to the special issue on design science research', *Management Information Systems Quarterly*, 32(4), p. 725. doi:10.2307/25148869.
- Mason, R. A. (1986) 'Four ethical issues of the information age', *Management Information Systems Quarterly*, 10(1), p. 5. doi:10.2307/248873.
- Maze (2023) 'Concept Testing in UX: What it is + Concept Testing Examples | Maze,' Maze, 10 October. <https://maze.co/guides/concept-testing/>.
- Memminger, M., Baxter, M. and Lin, E. (2018) 'Banking regtechs to the rescue?', *Bain*. Available at: <https://www.bain.com/insights/banking-regtechs-to-the-rescue/>.

- Merkel, A., Hopf, H., and Müller, E. (2012). Accelerating the innovation process with the help of open source prototyping hardware. *Annals of the Faculty of Engineering Hunedoara*, 10(1), 105.
- Merriam, S. B. and Tisdell, E. J. (2015) *Qualitative research: A guide to design and implementation*. New York: John Wiley & Sons.
- Mishra, P. *et al.* (2021) 'Pseudo-Biometric Identity Framework: Achieving Self-Sovereignty for biometrics on Blockchain,' *2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC)* [Preprint]. <https://doi.org/10.1109/smc52423.2021.9659136>.
- Moor, J. H. (1997) 'Towards a theory of privacy in the information age', *Computers & Society*, 27(3), pp. 27–32. doi:10.1145/270858.270866.
- Morse, J. M. (1991) 'Strategies for sampling', in Morse, J. M. (ed.) *Qualitative nursing research: A contemporary dialogue*, pp. 127–145. New York: Sage.
- Morse, J. M. (2000) 'Determining sample size', *Qualitative Health Research*, 10(1), pp. 3–5. doi:10.1177/104973200129118183.
- Mougayar, W. (2016) *The business blockchain: Promise, practice, and application of the next internet technology*. New York: John Wiley & Sons.
- Müller, H. *et al.* (2001) 'Performance evaluation in content-based image retrieval: overview and proposals,' *Pattern Recognition Letters*, 22(5), pp. 593–601. [https://doi.org/10.1016/s0167-8655\(00\)00118-5](https://doi.org/10.1016/s0167-8655(00)00118-5).
- Mühle, A. *et al.* (2018) 'A survey on essential components of a self-sovereign identity', *Computer Science Review*, 30, pp. 80–86. doi:10.1016/j.cosrev.2018.10.002.

- Myers, M. D. and Newman, M. C. (2007) 'The qualitative interview in IS research: Examining the craft', *Information and Organization* 17(1), pp. 2–26.
doi:10.1016/j.infoandorg.2006.11.001.
- Myers, M. D. and Venable, J. R. (2014) 'A set of ethical principles for design science research in information systems', *Information & Management*, 51(6), pp. 801–809.
doi:10.1016/j.im.2014.01.002.
- Naik, N. and Jenkins, P. (2020) 'Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems', *2020 IEEE international symposium on systems engineering (ISSE)*. Vienna, Austria, 2020, pp. 1–6. doi:10.1109/isse49799.2020.9272212.
- Nakamoto, S. (2009) 'Bitcoin: A peer-to-peer electronic cash system', *ResearchGate*.
Available at: https://www.researchgate.net/publication/228640975_Bitcoin_A_Peer-to-Peer_Electronic_Cash_System.
- Nielsen, J. (2006) 'Quantitative studies: How many users to test?', *Nielson Norman Group*.
Available at: <https://www.nngroup.com/articles/quantitative-studies-how-many-users/>.
- Nobel, C. (2011) 'Clay Christensen's milkshake marketing', *Harvard Business School*.
Available at: <https://hbswk.hbs.edu/item/clay-christensens-milkshake-marketing>.
- Noizat, P. (2015) 'Blockchain electronic vote', in *Handbook of digital currency*. London: Academic Press, pp. 453–461. doi:10.1016/b978-0-12-802117-0.00022-9.

- Nunamaker, J.F. and Chen, M. (1990) 'Systems development in information systems research,' *Journal of Management Information Systems*, 7(3), pp. 89–106.
<https://doi.org/10.1080/07421222.1990.11517898>.
- OASIS Open (2020) *Web services federation language (WS-Federation) v1.2 - OASIS Open*.
Available at: <https://www.oasis-open.org/standard/ws-federation/>.
- Oates, B.J. (2006) *Researching information systems and computing*. SAGE.
- Ogwe, S.L. (2013) *An assessment of factors affecting quality customer care in the telkom industry - a survey of Telkom Kenya*.
- O’Leary, Z. (2017) *The essential guide to doing your research project*. New York: SAGE Publications Limited.
- OpenID Authentication 2.0 - Final* (2007). Available at: https://openid.net/specs/openid-authentication-2_0.html.
- Ørngreen, R. (2017) ‘Workshops as a research methodology’, *Electronic Journal of e-Learning*, 15(1). Available at: <https://academic-publishing.org/index.php/ejel/article/view/1820>.
- Ostern, N. and Riedel, J. (2020) ‘Know-Your-Customer (KYC) requirements for initial coin offerings’, *Business & Information Systems Engineering*, 63(5), pp. 551–567.
[doi:10.1007/s12599-020-00677-6](https://doi.org/10.1007/s12599-020-00677-6).
- Pahl, C., Bošković, M. and Hasselbring, W. (2008) 'Model-Driven Performance Evaluation for service engineering,' in *Birkhäuser Basel eBooks*, pp. 171–185.
https://doi.org/10.1007/978-3-7643-8864-5_12.

- Panamax Inc. (2021) ‘Why is digital KYC essential in telecom industry?’, *LinkedIn*. Available at: <https://www.linkedin.com/pulse/why-digital-kyc-essential-telecom-industry-panamax-inc-/>.
- Parra-Moyano, J. P. and Ross, O. (2017) ‘KYC optimization using distributed ledger technology’, *Business & Information Systems Engineering*, 59(6), pp. 411–423. doi:10.1007/s12599-017-0504-2.
- Peffers, K. *et al.* (2007) ‘A design science research methodology for information systems research’, *Journal of Management Information Systems*, 24(3), pp. 45–77. doi:10.2753/mis0742-1222240302.
- Perry, J.A. and Perry, E.K. (2015) *Contemporary society: An Introduction to Social Science*. Routledge.
- Pöhn, D., Grabatin, M. and Hommel, W. (2021) ‘eID and self-sovereign identity usage: An overview’, *Electronics*, 10(22), p. 2811. doi:10.3390/electronics10222811
- Rajput, A. and Gopinath, K. (2017) ‘Towards a more secure Aadhaar’, in *Lecture notes in computer science*. Cham: Springer Science+Business Media, pp. 283–300. doi:10.1007/978-3-319-72598-7_17.
- Pries-Heje, J., Baskerville, R. and Venable, J. (2008) ‘Strategies for Design Science Research Evaluation,’ *16th European Conference on Information Systems, ECIS 2008*, pp. 255–266. <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1214&context=ecis2008>.
- Rathee, T. and Singh, P. P. (2022) ‘A systematic literature mapping on secure identity management using blockchain technology’, *Journal of King Saud University* -

Computer and Information Sciences, 34(8), pp. 5782–5796.

doi:10.1016/j.jksuci.2021.03.005.

Romme, A.G.L. (2003) 'Making a difference: organization as design,' *Organization Science*, 14(5), pp. 558–573. <https://doi.org/10.1287/orsc.14.5.558.16769>.

Rose, K. H. (1995). A performance measurement model. *Quality progress*, 28(2), 63.

Rosemann, M. and Vessey, I. (2008) 'Toward improving the relevance of information systems research to practice: The role of applicability checks', *Management Information Systems Quarterly*, 32(1), p. 1. doi:10.2307/25148826.

Rowley, J. and Slack, F. (2004) 'Conducting a literature review,' *Management Research News*, 27(6), pp. 31–39. <https://doi.org/10.1108/01409170410784185>.

Runeson, P. and Höst, M. (2008) 'Guidelines for conducting and reporting case study research in software engineering,' *Empirical Software Engineering*, 14(2), pp. 131–164. <https://doi.org/10.1007/s10664-008-9102-8>.

Samir, E. *et al.* (2022) 'DT-SSIM: A Decentralized Trustworthy Self-Sovereign Identity Management Framework,' *IEEE Internet of Things Journal*, 9(11), pp. 7972–7988. <https://doi.org/10.1109/jiot.2021.3112537>.

Schardong, F. and Custódio, R.F. (2022) 'Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy,' *Sensors*, 22(15), p. 5641. <https://doi.org/10.3390/s22155641>.

Schlatt, V. *et al.* (2022) 'Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity', *Information & Management*, 59(7), p. 103553. doi:10.1016/j.im.2021.103553.

- Schwartz, D. (1987) *Concept testing: How to test new product ideas before you go to market*. Chicago, IL: American Association of Endodontists.
- Sedlmeir, J. *et al.* (2021) 'Digital identities and verifiable credentials', *Business & Information Systems Engineering*, 63(5), pp. 603–613. doi:10.1007/s12599-021-00722-y.
- Seuring, S. and Müller, M. (2008) 'From a literature review to a conceptual framework for sustainable supply chain management,' *Journal of Cleaner Production*, 16(15), pp. 1699–1710. <https://doi.org/10.1016/j.jclepro.2008.04.020>.
- Shamsi, K., Khorasani, K. E. and Shayegan, M. J. (2020) 'A secure and efficient approach for issuing KYC token as COVID-19 health certificate based on stellar blockchain network', *arXiv (Cornell University)*. Available at: <https://doi.org/10.22133/ijwr.2020.250275.1070>.
- Shaughnessy, J. D., Zechmeister, E. B. and Zechmeister, J. S. (2016) *Research methods in psychology*. Minneapolis: University of Minnesota. doi:10.24926/8668.2201.
- Shukla, A.K. and Saxena, A. (2013) 'Which Model is best for the Software Project? "A Comparative Analysis of Software Engineering Models"', *International Journal of Computer Applications*, 76(11), pp. 18–22. <https://doi.org/10.5120/13290-0806>.
- Simon, H. A. (1996) *The sciences of the artificial*. Cambridge, MA: MIT Press.
- Smith, C.U. and Williams, L.G. (2001) *Performance Solutions: A practical guide to creating responsive, scalable software*. <http://ci.nii.ac.jp/ncid/BA55360665>.
- Soanes, C. and Stevenson, A. (2004) *Concise Oxford English dictionary*. Oxford: Oxford Publishing.

- Sokolowski, J.A. and Banks, C.M. (2010) *Modeling and simulation fundamentals: Theoretical Underpinnings and Practical Domains*. John Wiley & Sons.
- Soltani, R. D. C., Nguyen, U. T. and An, A. (2018) 'A new approach to client onboarding using self-sovereign identity and distributed ledger', *2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCoM) and IEEE smart data (SmartData)*. Halifax, NS, Canada, 2018, pp. 1129–1136. doi:10.1109/cybermatics_2018.2018.00205.
- Soltani, R. D. C., Nguyen, U. T. and An, A. (2020) 'Decentralized and privacy-preserving key management model', *2020 international symposium on networks, computers and communications (ISNCC)*. Montreal, QC, Canada, 2020, pp. 1–7. doi:10.1109/isncc49221.2020.9297294.
- Soltani, R. D. C., Nguyen, U. T. and An, A. (2021) 'A survey of self-sovereign identity ecosystem', *Security and Communication Networks*, 2021, pp. 1–26. doi:10.1155/2021/8873429.
- Sommerville, I. (2011) *Software Engineering*, 9/e. Pearson Education India.
- Soni, A. and Duggal, R. (2014) 'Reducing risk in KYC (Know Your Customer) for large Indian banks using big data analytics', *International Journal of Computer Applications*, 97(9), pp. 49–53. doi:10.5120/17039-7347.
- Sonnenberg, C. and Brocke, J.V. (2012) 'Evaluations in the science of the Artificial – Reconsidering the Build-Evaluate pattern in design science research,' in *Lecture*

Notes in Computer Science, pp. 381–397. https://doi.org/10.1007/978-3-642-29863-9_28.

Sovrin. (2022) *Sovrin Specifications*. Available at: <https://sovrin.org/library/sovrin-governance-framework/>.

Sporny, M.; Longley, D.; Chadwick, D. (2021) *Verifiable Credentials Data Model 1.0*.

Expressing Verifiable Information on the Web.

Available at: <https://www.w3.org/TR/vc-data-model/>.

Sporny, M., Longley, D. and Chadwick, D. (2022) *Verifiable credentials data model v1.1*.

Available at: <https://www.w3.org/TR/vc-data-model/#what-is-a-verifiable-credential>.

Sporny, M.; Longley, D.; Sabadello, M.; Reed, D.; Steele, O.; Allen, C. (2022) *Decentralized Identifiers (DIDs) v1.0: Core Architecture, Data Model, and Representations*.

Available at: <https://www.w3.org/TR/did-core/>.

Squarepants, S. (2008) 'Bitcoin: A peer-to-peer electronic cash system', *Massachusetts Insitute of Technology*. doi:10.2139/ssrn.3977007.

Steele, O.; Sporny, M. (2022) *DID Specification Registries*. Available at:

<https://www.w3.org/TR/did-spec-registries/#did-methods>.

Takeda, H. *et al.* (1990) 'Modeling design processes,' *Ai Magazine*, 11(4), pp. 37–48.

<https://ir.cwi.nl/pub/5655/5655D.pdf>.

Tambe, P. and Tambay, P. Y. (2020) 'Reducing modern slavery using AI and blockchain', *2020 IEEE/ITU international conference on artificial intelligence for good (AI4G)*, pp. 22–27. doi:10.1109/ai4g50087.2020.9311031.

- Theodouli, A. *et al.* (2020) 'Towards a blockchain-based identity and trust management framework for the IoV ecosystem', *2020 global Internet of Things summit (GIoTS)*. Dublin, Ireland, 2020, pp. 1–6. doi:10.1109/giots49054.2020.9119623.
- Tobin, A. and Reed, D. (2017) 'Inevitable rise of self-sovereign identity', *Sovrin Foundation*. Available at: <https://sovrin.org/library/inevitable-rise-of-self-sovereign-identity/>.
- Toth, K. and Anderson-Priddy, A. (2019) 'Self-sovereign digital identity: A paradigm shift for identity', *IEEE Security & Privacy*, 17(3), pp. 17–27. doi:10.1109/msec.2018.2888782.
- Trætteberg, H. (2007) 'A hybrid tool for user interface modeling and prototyping,' in *Springer eBooks*, pp. 215–230. https://doi.org/10.1007/978-1-4020-5820-2_18.
- Trochim, W. M. K. (2007) 'What is the research methods knowledge base?', *Conjointly*. Available at: <https://www.socialresearchmethods.net/>.
- United Arab Emirates Telecommunication Regulatory Authority (2011) *Regulatory policy registration requirements for mobile consumers*. Available at: <https://tdra.gov.ae/-/media/About/regulations-and-ruling/EN/Registration-Requirements-for-Mobile-Consumers-Policy-pdf.ashx>.
- United Nations (2008) *Designing household survey samples studies in methods*. doi:10.18356/f7348051-en.
- Vaishnavi, V., and Kuechler, W. (2009). *Design research in information systems*. Available at: <http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf>

- Van Aken, J.E. and Romme, A.G.L. (2009) 'Reinventing the future: adding design science to the repertoire of organization and management studies,' *Organization Management Journal*, 6(1), pp. 5–12. <https://doi.org/10.1057/omj.2009.1>.
- Venable, J. R., Pries-Heje, J. and Baskerville, R. L. (2012) 'A comprehensive framework for evaluation in design science research', in *Lecture notes in computer science*. Cham: Springer Science+Business Media, pp. 423–438. doi:10.1007/978-3-642-29863-9_31.
- Veramo. (2022) *Veramo (v4.1.1) Specifications*. Available at: <https://veramo.io/docs/basics/introduction>.
- Voiskunskii, V.G. (1997) 'Evaluation of search results: A new approach,' *Journal of the American Society for Information Science*, 48(2), pp. 133–142. [https://doi.org/10.1002/\(sici\)1097-4571\(199702\)48:2](https://doi.org/10.1002/(sici)1097-4571(199702)48:2).
- Wagner, K. *et al.* (2018) 'Self-sovereign identity', *Blockchain Bundesverband*. Available at: https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity_-_Blockchain-Bundesverband-2018.pdf.
- Walls, J.G., Widmeyer, G.R. and Sawy, O. a. E. (1992) 'Building an Information System Design Theory for Vigilant EIS,' *Information Systems Research*, 3(1), pp. 36–59. <https://doi.org/10.1287/isre.3.1.36>.
- Wason, T. (n.d.) *Liberty ID-FF architecture overview*. Available at: <https://www.oasis-open.org/committees/download.php/4329/liberty-idff-arch-overview-v1.2.pdf>.
- Wazlawick, R.S. (2010) 'Reflections about Research in Computer Science regarding the Classification of Sciences and the Scientific Method,' *Sistemas De Informação*, (6), pp. 3–10. <https://doaj.org/article/5383f62e3c354d94aa938c1dc00766a7>.

- Wieringa, R. (2014) *Design Science Methodology for information systems and software engineering*, Springer eBooks. <https://doi.org/10.1007/978-3-662-43839-8>.
- Williamson, S.J., Stark, B.H. and Booker, J.D. (2014) 'Low head pico hydro turbine selection using a multi-criteria analysis,' *Renewable Energy*, 61, pp. 43–50.
<https://doi.org/10.1016/j.renene.2012.06.020>.
- Wind, Y., Mahajan, V. and Cardozo, R.N. (1981) 'New-product forecasting: Models and applications', *Journal of Forecasting*, 2(1), pp. 85–89. doi:10.1002/for.3980020109
- Zetzsche, D. A., Buckley, R. P. and Arner, D.W. (2018) 'Digital ID and AML/CDD/KYC utilities for financial inclusion, integrity and competition', *Journal of Financial Transformation*, pp. 133–142. Available at: <https://orbi.lu.uni.lu/handle/10993/38943>.
- Zhang, R., Xue, R. and Liu, L. (2019) 'Security and privacy on blockchain', *ACM Computing Surveys*, 52(3), pp. 1–34. doi:10.1145/3316481.
- Zhu, X. and Badr, Y. (2018) 'A survey on blockchain-based identity management systems for the Internet of Things', *2018 IEEE international conference on Internet of Things (iThings) and IEEE green computing and communications (GreenCom) and IEEE cyber, physical and social computing (CPSCoM) and IEEE smart data (SmartData)*. Halifax, NS, Canada, 2018, pp. 1568–1573.
doi:10.1109/cybermatics_2018.2018.00263.

Appendices

Appendix A: Expert's Consent Forms

Consent Form: Expert Research Participant

Dear Expert,

My name is Suaad Al Shamsi and I am a student in the British University in Dubai. I am currently exploring the implementation of decentralized identity and verifiable credentials leveraging blockchain infrastructure to create a Digital Trust Framework between government and private sector in UAE. This implementation addresses the challenges faced in KYC process while adopting Privacy by Design principles. As an expert working in either KYC domain, SSI or digital transformation, I would like to ask for your consent for your participation in this study.

If you choose to provide your consent, you would take part in an expert review in form of face-to-face one-on-one interview or focus group or workshop with the researcher to evaluate the problem relevance, objective relevance and completeness and evaluation of the framework. You will also be requested to fill a short questionnaire. All the collected data will be kept securely.

The results of the study may be published but your identity will remain confidential and anonymous. For example, we might refer to the organization as Organization A, and the expert as Expert A. Interviews might be audio-recorded, but all recordings will be deleted once transcribed. You may also request that no audio recording shall be used. Your answers to the questionnaire will be also anonymous.

Even though there may be no direct benefit to you from this study, a possible benefit for your participation is identifying possible ways of improving the efficiency of KYC among different parties involved in the KYC and SSI, which in return may improve the efficiency of KYC processes you might go through to avail services.

If you have any questions concerning the research study, please contact me. If you choose to provide your consent, you should note the following:

1. Your participation in this study is voluntary. If you choose not to participate or to withdraw from the study at any time, you can do so without any consequences to you.
2. Your identity will be reported anonymously.
3. The information from the interview recordings will be transcribed. The researcher will use a coding system to ensure your confidentiality is protected.
4. The research results will be used for publication.

By signing this form, you acknowledge that you understand the nature of the study, and the methods by which your identity will be kept confidential. Your signature on this form also indicates that you give your approval to voluntarily serve as a participant in the study described

Expert Name:

Expert Email:

Expert Phone number:

Expert Signature

Date

Suaad Al Shamsi

suad.alshamsi@gmail.com

050#####

Appendix B : Open-ended Interview Questions

Appendix B.1: Problem Identification

- (1) What do you think about the problem described in term of KYC efficiency?
- (2) How long does it take to complete a KYC process?
- (3) Would you be able to share the time it takes to complete the initial verification in specific and the ongoing monitoring?
- (4) What is the current customer satisfaction with KYC process?
- (5) Do you think there is a need to improve the efficiency i.e. reducing the human intervention and have an end to end automation?
- (6) What do you think about using an existing digital identity which has a sufficient vetting process during the registration to accelerate the KYC efficiency specifically the initial verification process?
- (7) Do you think the ongoing and periodical monitoring required to be addressed as part of the KYC efficiency?
- (8) Would you consider the below as important elements to be addressed during the KYC process improvement? Why do you think so?
 - a. Regulation Compliance
 - b. Privacy
 - c. Trust

d. Decentralization

e. User Experience

(9) Are there any other elements that should be considered as part of the KYC process efficiency?

Appendix B.2: Solution Evaluation

- (1) Do you think the framework will improve the KYC process efficiency?
- (2) What are the challenges that would be addressed by the framework?
- (3) What are the challenges that might result from using the framework that need to be addressed?
- (4) How much time do you think it would take to complete the KYC process using the framework in comparison to existing process?
- (5) Would you be able to share the expected time it would take to complete the initial verification phase and the ongoing monitoring in case of using the new process?
- (6) Would the framework fit the business requirements of your organization?
- (7) Would the framework be accepted by different stakeholders (government, private and regulators)?
- (8) Are the elements of Privacy by Design addressed by the framework?
- (9) What do you think about the user experience of the framework from end user perspective?
- (10) Is there any improvement that you would suggest related to the user experience or overall framework?

Appendix B.3: International Experts

- (1) Do you think the government should play a role in such framework? If so, why?
- (2) Are there any legal, regulatory and policy gaps that need to be addressed?
- (3) Can the framework be expanded to work cross countries?
- (4) What should be considered in such case?
- (5) Would interoperability be a challenge? how should it be addressed?
- (6) Where should identity information be stored?
- (7) What are the key elements that have to be considered in term of privacy?
- (8) Are there any other elements that should be considered for SSI blockchain-based implementation?

Appendix C : Concept Testing Survey Questions

Digital Identity Wallet

My name is Suaad Al Shamsi, I am a PhD Student. I am seeking your support to provide feedback on a product concept. Your answers will help me understand the strengths and weaknesses of my PhD idea. You will be able to view a prototype and then provide your feedback. It will not take more than 5 minutes of your time.

Please read about my concept below:

Concept Name: Digital Identity Wallet

Concept description:

A government mobile application that aims to streamline the process of sharing official documents for various services. The app allows users to request their official documents issued by the government, such as Emirates ID card, driving license and educational certificates. When a user needs to share these documents with a SP, such as a bank, they can do so directly through the app. The user receives a request to authenticate and then gives consent for the specific documents to be shared. This eliminates the need for physical documents and makes the process of opening a bank account, or accessing similar services, more convenient and efficient. The user can also show their documents in person when required at the counter e.g. hospital registration.

You can view the demo in this [link](#). You will be able to view document (Emirates ID), Add a document (University Certificate) and share a document

Can you tell us little bit about yourself before we start?

Q1: Which age group do you belong to?

- ☐ Below 20
- ☐ 20 to 29
- ☐ 30 to 39
- ☐ 40 to 49
- ☐ 50 to 59
- ☐ 60 and above

Q2: What's your gender?

- ☐ Male
- ☐ Female

Q3: What's your nationality?

- ☐ UAE National
- ☐ GCC
- ☐ Ex-pat

Q4: What is your initial reaction this concept?

- ☐ Extremely positive

- ☐ Somewhat positive
- ☐ Neither positive nor negative
- ☐ Somewhat negative
- ☐ Extremely negative

Q5: How unique is this concept compared to other products currently available?

- ☐ Extremely unique
- ☐ Very unique
- ☐ Somewhat unique
- ☐ A little unique
- ☐ Not unique at all

Q6: How appealing is this concept compared to other products currently available?

- ☐ Extremely appealing
- ☐ Very appealing
- ☐ Somewhat appealing
- ☐ A little appealing
- ☐ Not at all appealing

Q7: How much do you like or dislike this concept?

- ☐ Like a great deal
- ☐ Like a moderate amount
- ☐ Like a little
- ☐ Neither like nor dislike
- ☐ Dislike a little
- ☐ Dislike a moderate amount
- ☐ Dislike a great deal

Q8: How believable is this concept?

- ☐ Extremely believable
- ☐ Moderately believable
- ☐ Slightly believable
- ☐ Neither believable nor unbelievable
- ☐ Slightly unbelievable
- ☐ Moderately unbelievable
- ☐ Extremely unbelievable

Q9: How relevant is this concept to you personally?Extremely relevant

- ☐ Moderately relevant
- ☐ Slightly relevant
- ☐ Neither relevant nor irrelevant
- ☐ Slightly irrelevant
- ☐ Moderately irrelevant
- ☐ Extremely irrelevant

Q10: From the list below, which best describes your thinking about this concept?

- ☐ I need it because nothing else solves this problem
- ☐ This would be slightly better than what I am currently using
- ☐ This is essentially the same as what I am currently using
- ☐ What I am currently using is better than this
- ☐ I don't see any reason to use this

Q11: How concerned are you about the security of sharing official documents through an app

- ☐ Very unconcerned
- ☐ Somewhat unconcerned
- ☐ Neutral
- ☐ Somewhat concerned
- ☐ Very concerned

**Q12: How important is the security and privacy of your personal documents to you?
What would make you feel confident about this app?**

Q13: What do you like MOST about this concept?

Q14: What do you like LEAST about this concept?
