Maha Sroor

MODELING SELF-SOVEREIGN IDENTITY GOVERNANCE FRAMEWORK

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION TECHNOLOGY
2022

ABSTRACT

Sroor, Maha
Modeling Self Sovereign Identity governance framework
Jyväskylä: University of Jyväskylä, 2022.
Major subject, type of the publication (e.g., Information Systems, Master's Thesis)
Supervisor(s): Gabriella Laatikainen(first supervisor), Pekka Abrahamsson(Second supervisor).

Digital identity has become a topic that attracts the attention of researchers due to the enormous number of digital services that have been provided online recently. Researchers face many obstacles regarding the security, privacy, and utility of digital identity. Self-Sovereign Identity (SSI) ecosystems provide a solution for digital identity and provide a decentralized human-centric paradigm that enables users to own and control their identity. The governance framework (GF) is a crucial challenge in building SSI ecosystems for two reasons. Firstly, the governance framework needs to address various aspects such as user needs, standards, laws, and business requirements in the ecosystem. Secondly, the ecosystem consists of a diverse, dynamic, and distributed group of stakeholders. This work adopts a new methodology for developing a governance framework by providing a visual view of the SSI ecosystem. In addition, it seeks to highlight the importance of domain-specific modeling in developing governance frameworks. It also addresses empirical observations from a real case study and the modeling journey that supported the creation of the governance framework. The advantages, challenges of modeling, and the modeling tool used are discussed based on the evaluation from the case feedback and conclude with future work.

Keywords: Self- sovereign Identity, Governance framework, Modeling.

FIGURES

TABLES

TABLE OF CONTENTS

1 INTRODUCTION

Digital identity has become an important area of interest(Ante et al., 2022). After the COVID pandemic, most regular human activities had to be suspended physically as a way to avoid the consequences of the pandemic. Researchers, companies, and governments collaborated to find a way to proceed with regular daily activities. The best option was to rely on the internet space. All activities that do not need physical presence turned out to be online. Employees worked remotely. Students go to virtual schools in many countries, and many people start shopping online.

One of the significant problems of replacing physical activities with online activities is digital identity usability and security(Feher, 2021). Digital identity is a way to prove who the user is and verify his claims about the information he/she provides about himself. It reflects a digital presentation of the physical user to perform online activities. Digital identity is usually stored on iCloud or digital wallets, making the user exposed to identity theft the same as in real life.

On some level of online interactions, people need a secure and trustable connection, especially if they provide sensitive information about their lives, bank accounts, or identity numbers. One solution to have a secure connection is the centralized identity management model. The centralized model provides authentication using a username and password. This solution force users to register with a user name and password for every Service Provider(Cao & Yang, 2010). This model has security, privacy, and usability drawbacks. For example, using the same password for multiple Service Providers results in security and usability threats. If the password is revealed, multiple accounts will be threatened. It also leads to usability issues because the user needs to change the password for all accounts with the same password. Many users use the same password for multiple services, and they do not realize the importance of having a strong and unpredictable password (Talib et al., 2010).

The next step towards a trusted and secure connection is the federated model. Users register with an identity Service Provider (IdSP) who is responsible for hosting, securing, storing, and authenticating the user's information(Hommel & Reiser, n.d.). The user can use it to register himself to many online services. For example, users can register to Amazon by using a google account or Facebook account(Google and Facebook are the IdSP). Although the federation model is more accessible for users, it exposes users to privacy and security risks. In fact, it exacerbates Service Providers' privacy and liability risks because users do not know how their information could be utilized by the IdSP (Schardong & Custódio, 2021).

An evolution in online self-authentication and identity management models is the decentralized model. This model uses distributed ledger technologies (DLT) to verify a user's identity using cryptographic keys. Identity verification happens without exposing unnecessary personal data or using the services of IdSP. The decentralized model, or Self-Sovereign Identity (SSI), enables users to authenticate themselves using verifiable credentials stored in a personal wallet rather than with an identity Service Provider. Also, it enables them to select which information to expose(Trust over IP Foundation, 2020). This model grants accessibility, portability, and security. In addition, it gives all the rights to the credential owner to use and control his credentials.

One of the critical challenges in SSI ecosystems is the governance framework. The Trust over IP Foundation defined a governance framework as "A set of business, legal, and technical [definitions], [policies], [specifications], and contracts by which the members of a trust community agree to be governed in order to achieve their desired objectives." (Trust over IP Foundation, N.D) In a centralized or federated model, the Service Provider or IdSP is responsible for writing and enforcing the system's governance, whereas, in a decentralized model, the governance framework must be agreed upon by many different Service Providers and credentialed issuers. The governance framework results from long discussions and analyses of many stakeholders from legal, business, technical, and financial perspectives.

Studying the SSI ecosystem and digital identity is essential for its relevance. Many governments and private sector organizations are migrating to digitalization. They have a big challenge with identity management and governance to build a timely trustworthy ecosystem. SSI support trustworthiness in digital interaction through innovative technology utilizing inherited trusted mechanism and a framework that enforce policies and standards among the participants(Laatikainen, Kolehmainen, & Abrahamsson, 2021).

Digital Identity is crucial because it is a key enabler of automating business decisions by providing means to verify data (its actual state, its provenance, and history). Many organizations tend to put digital identity at the center of their business model. Organizations create digital identities for themselves, their employees, partners, and service users (Wyatt et al., n.d.). It helps to have identity mapping to provide a full history of each identity, its related data, business activities, and financial position on the market(GLEIF, n.d.). It helps predict the business direction and automate the business decisions, a definite advantage for the business processes and decisions.

SSI addresses the privacy and security concerns related to controlling, collecting, and analyzing users' personal data by third parties. Third parties can be a target for cyber-attacks and data misuse that make it an indirect threat to users. By offering the users control over their identity and associated data, protection against cybercrime and identity theft would increase.

Identity is a core component of digital services, and it is accelerating over time. The Finnish government started a project to develop digital identities for all Finnish citizens and people who live in Finland due to the high demand for digital services. The project takes place from 8 October 2020 to 30 June 2023. According to the Finnish Ministry of finance, digital services are the fastest and the easiest way to contact Finnish authorities(Digital Services, n.d.).

According to Juniper Research Limited-the leading forecasting markets company-SSI is expected to open a new market forecasted to be a billion-dollar business by the end of 2024. The market operates in many areas all over the world. Also, it forecasts that the revenues growth to be 1000% over the next four years. Juniper expects that SSI benefits appeal to businesses in the long run due to the immutability of blockchain records and large data repositories(Juniper, n.d.).

1.1 Research objective and research question

This thesis investigates the SSI development process and how modeling can improve it by developing an SSI governance framework. Also, this research aims to help different stakeholders groups to be on the same level of understanding of the business function and process. The thesis helps to present how different aspects of the ecosystem could be interrelated. The thesis aims to provide practitioners with a systematic base to facilitate and professionalize the development of a governance framework. Finally, the thesis aims to answer the research question: What role could modeling play in developing SSI governance frameworks?

1.2 Thesis structure

The first chapter represents the recent work related to digital identity, SSI ecosystems, governance framework, real-world examples of SSI governance framework, and software ecosystem modeling, including different modeling approaches. The second chapter introduces the case" Yoma" and the modeling language used to create models " Ecosystem Governance Compass (EGC)." The third chapter covers the research methodologies, data collection, and model creation. The fourth chapter lists the Findings, including the models, lessons learned, and future development. Next, the main findings, discussion, and thesis conclusion are presented in the fifth, sixth, and seventh chapters.

2 THEORETICAL BACKGROUND

This chapter describes the recent work related to digital identity, SSI, Governance framework, and software ecosystem modeling. The first section introduces digital identity and its importance. The second section explains SSI as a governance ecosystem and as a technology solution. Also, it addresses the SSI principles and the evaluation specifications for SSI. The third section introduces governance and how it can be viewed in the SSI context. The third section also presents the governance frameworks, their requirements, and some real examples of the SSI governance framework. The fourth section introduces software ecosystem modeling and its options with the limitations of each option

2.1 Digital Identity

Identity is one of the main attributes that distinguish one person from another. Psychologists define identity as a mix of beliefs, personality, and expressions(Ishola, 2019). Technology provided a new scope of identity that could be utilized in cyberspace. In the last few years, many people have spent much time online doing their work, reading news, shopping, and interacting with other people using different social media applications. Relying on online activities highlighted the need to define and manage a new identity scope to distinguish one user from another online (Mühle et al., 2018). This new scope is called digital Identity.

Digital Identity is defined as a way for people to prove who they are and what they say online(Cameron, 2005; Mühle et al., 2018). It is also defined as a digital copy of a person's physical identity that is used to validate the claims of who he/she is. Digital identity has two main parts: First is the data stored and transferred online; second is the digital persona and presence of an entity or a person (Feher, 2021). Digital identity is not only for people. It is also used to identify organizations. Digital organization identity represents an organization's existence, vision, mission, interactions, culture, and sense of action(Whitley et al., 2014). In a general scope, it determines an online snapshot of an entity's characteristics to distinguish it.

Having a Digital Identity can be done in two simple steps: registration and transaction. The first step is identity creation or registration. It is the static part of the process. In registration, the user starts to add his real or fake personal data that he/ she wants to present, like name, date of birth, place of birth, and more identifying information. All data goes into data storage or data registry. The second step is the identity transaction. It is the dynamic step when the user data is verified at the transaction time. The verification happens when the data entered into the system matches the data stored on the data storage during the registration process (Step 1 identity creation)(Sullivan, 2018).

Digital Identity has become a powerful tool to identify users when accessing online services. It is usually used for particular purposes and in specific contexts, which means that users can choose the presented details of their identity when accessing different online services (Der et al., 2017). For example, some governmental services require the user's name and social number, while the same user does not need to provide them in online shopping. The identification process happens by authenticating users' attributes (Schardong & Custódio, 2021).

Digital Identity and physical identity are at the same level of importance. Digital identity gives the users the right to reflect their persona based on their interests and the context of practices, the same as physical identity. In other words, each person can have many digital identities and leave a different digital footprint based on how he/she wants to represent himself. It also gives the users the right to anonymity in online activities, making users more active participants (Costa & Torres, 2011).In an organizational context.

Digital identity is related to cost-saving. Online services are cheaper than human services(Sullivan, 2018). For sure, the implementation of digital services, including software innovation, is high initially, but in the long run, it saves costs related to human activities in business and makes the work more efficient(Rahimi, 2019)

Risks related to digital identity attract the researchers' attention. Digital Identity must resist forgery, fraud, and personal information leakage (Schardong & Custódio, 2021), so the most common risks related to digital identity are privacy breaches and identity theft. A privacy breach happens when the identity data is disclosed intentionally or unintentionally to a third party. The third-party can access the user's identity, and it could accelerate identity theft. Identity theft means that the user loses access to his identity and can be used by someone else. Identity theft could take the owner to court or destroy his reputation (Ayaburi & Treku, 2020; Ben Ayed, 2011).

Recently many public and private organizations have become interested in Digital Identity, like digital identity workgroups and digital identity community groups. Digital identity organizations aim to find solutions for Digital identity trustworthiness and security issue. It also aims to facilitate digital identity in the organizational context. The latest research for the DGX digital identity workgroup [1]about digital identity is the COVID environment and how it could be utilized to develop the trading and traveling sector. Identity and digital identity are the main concepts of the SSI ecosystems.

2.2 Self Sovereign Identity

Self-Sovereign Identity(SSI) is an identity management model that can also be seen as a technology. In SSI, governance plays an equally important role as the technological solution. The first section presents SSI as an identity ecosystem and how governance regulates the interaction among the players. The second section is the technological solution that ensures trustworthiness using blockchain technology and messaging protocols to secure data transactions among network nodes. The third section addresses the SSI principles and the metrics used to evaluate SSI.

2.2.1 Self-Sovereign Identity ecosystems

SSI emerged strongly in the last few years(Wang & De Filippi, 2020a). Although SSI does not have a specific definition, it is described as a form of identity management that allows users to own and manage their digital identity (Mühle et al., 2018). Also, it is described as a further evolution of non-centric identity management models that give complete control of data to users. SSI does not rely on a central trusted authority, and credential owners are granted selective credentials disclosure (Abraham et al., 2021).

The credentials used to present the digital identity are different from the claims. Claims are statements about a subject, while credentials are claims with some metadata like the issuer and the validity period. The metadata provides the utility conditions for the claims (Mühle et al., 2018).

Verifiable credentials are the digital form of the documents used as credentials in everyday life like passports, identification cards, birth certificates, university certificates, and more(Lux et al., 2020). Like real-life, verifiable credentials are like legal documents that need to be protected by their owners. Verifiable credentials are stored on digital wallets, mobile phones, or iCloud (Sporny et al., 2019). Credentials are disclosed upon their owner's choice (Wang & De Filippi, 2020b).

SSI provided a different model for users; it differentiates itself by being a non-centric identity management model. Previous identity management models made the Service Provider the center of the model, and the user has only the license to use his identity (Abraham et al., 2021; Laatikainen, Kolehmainen, & Abrahamsson, 2021). Users see SSI ecosystems as a system that gives them control over the digital copy of their data and lets them decide what level of infor-

[1] https://www.tech.gov.sg/files/media/corporate-publications/FY2021/dgx_2021_digital_identity_in_response_to_covid-19.pdf

mation they want to share and for whom they would like to share (Schardong & Custódio, 2021).

Abraham et al. described SSI as a human-centric paradigm, meaning that the user is the center and the main initiator for the authentication process(Abraham et al., 2021). Furthermore, it ended the ownership and control of the identity providers on the users' credentials(Naik & Jenkins, 2020), meaning the roles acting in the verification process changed and did not include Service Providers anymore.

SSI ecosystems' have prominent roles, and the verifiable credentials are exchanged between these roles to achieve a trusted transaction. The prominent SSI roles are the Holder, Issuer, Verifier, and governance authority(Laatikainen, Kolehmainen, Li, et al., 2021b). Literature and organizations -like E-SSIF lab, Sovrin Foundation, and TrustOverIP Foundation- provided definitions to the holder, issuer, verifier, and governance authority. FIGURE 1 shows the Trust diamond that explains the relationship among Holder, Issuer, Verifier, and Governance authority.

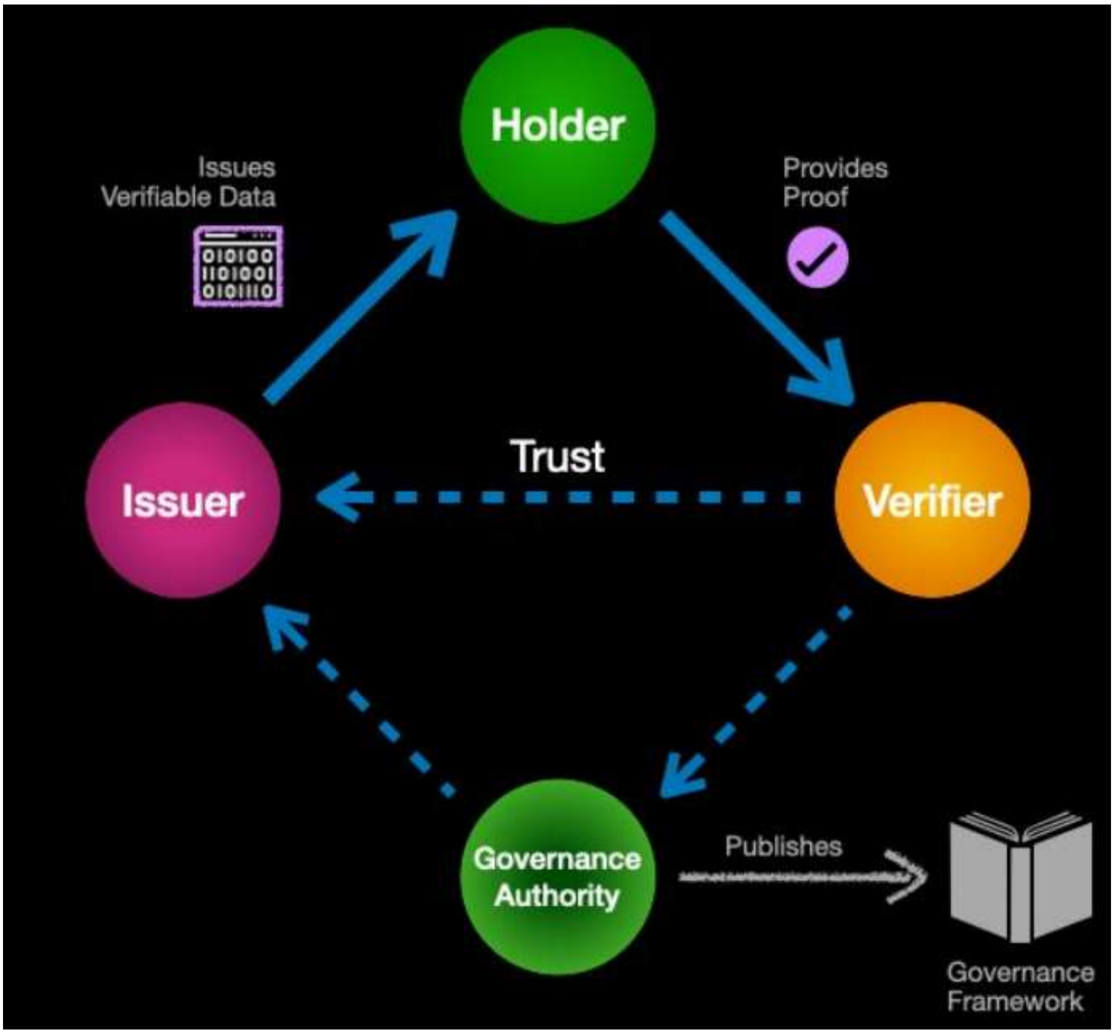

FIGURE 1 Trust Diamond in TrustOverIP Foundation (Trust over IP Foundation, 2020

The TrustOverIP Foundation glossary provided a detailed description of SSI roles. The issuer is an organization or entity that creates or releases the credentials. Credentials could be governmental documents like a passport or driving license or non-governmental documents like a gym card or library card. Holders are the credential owner and the primarily responsible actor for credentials security and keeping it in a digital wallet. Holders also are responsible for presenting the credentials when needed. Verifiers are anyone authorized to validate the holder's claims about who he/she is(Trust over IP Foundation, n.d.). The governance authority is responsible for governing the ecosystem and publishing the governance framework. In some ecosystems, governance authority can also operate as administrative authority.

2.2.2 Self-Sovereign Identity as an emerging technology

SSI uses an emerging technology that supports decentralization. SSI uses a decentralized identity model to build a digital Trust mechanism (Davie et al., 2019a). The decentralized model depends on a trusted peer-to-peer relationship among the system actors to enable the actors to exchange credentials without control from a third party (Preukschat & Reed, 2021). The Trust in SSI starts with a technological cryptographic trust layer and extends to the human interaction trust layer (Sovrin-Glossary-V2.Pdf, n.d.). FIGURE 2 shows the trust layer in the Sovrin stack

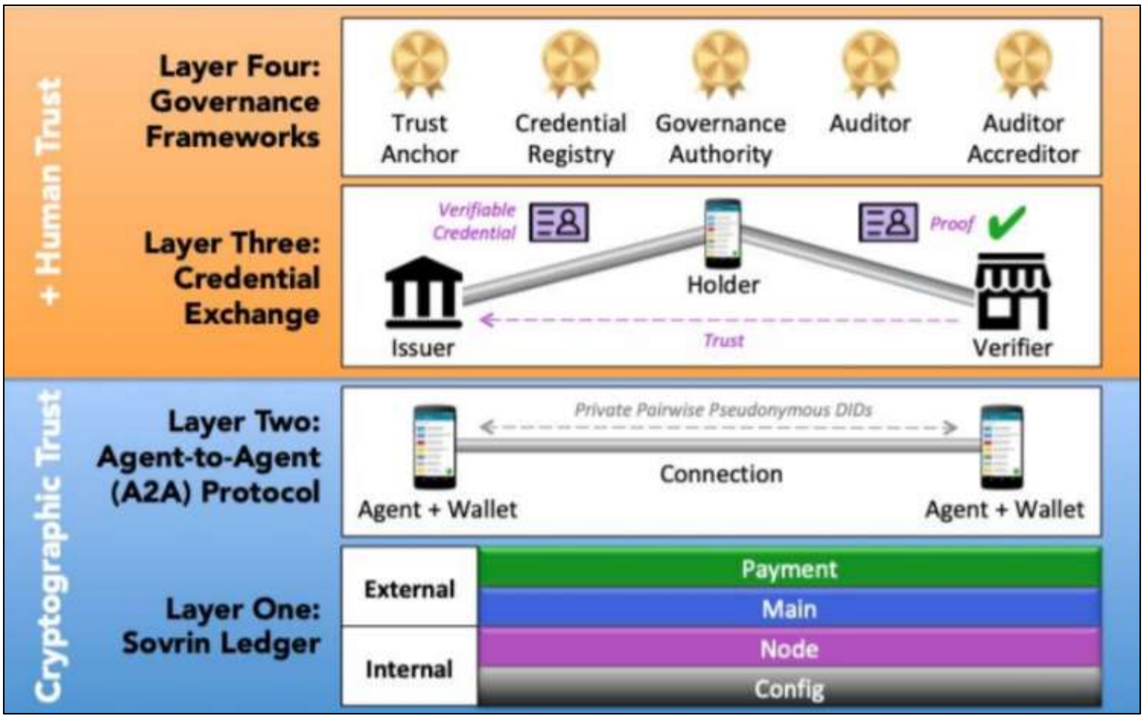

FIGURE 2 Sovrin stack representing the trust layers in SSI (Sovrin-Glossary-V2.Pdf, n.d.).

Trust in SSI is built using Decentralized Identifiers (DID). DIDs are unique web addresses that refer to a DID subject fully controlled by its owner (Sghaier Omar & Basir, 2020). The DID subject has information about DID document, the verification method, and the service endpoints. DID document works on providing information about how to use the DID. Verification method used for the authentication. Service endpoints are necessary for a trusted connection and cryptographic material (Wang & De Filippi, 2020a). DIDs use a messaging system called DIDComm. DIDComm generates the DIDs, key pairs, subsequent key rotation or revocation, and the DID document. All the generated elements are essential to establishing the connection(Davie et al., 2019). DIDs need to work together with verifiable credentials to support the holder's selective data disclosure within SSI ecosystems.

Verifiable credentials(VCs) are the data describing identification attributes stored in distributed ledgers. VCs should include the credential type, subject, issuing authority, constraints, and physical attributes(Sporny et al., 2019). VCs exchange within the ecosystems must be protected and ensure selective disclosure. It is protected with a digital signature using public and private cryptographic keys. Selective disclosure has zero-knowledge proof to ensure minimum data disclosure to the verifier(Sedlmeir et al., 2021).

Distributed ledgers are verifiable data registries that enable data encryption, provenance, timestamping, and immutability in the ecosystem network(Yu et al., 2018). They replicate, share and synchronize DIDs across ledger nodes with no central administration. If any changes occur on the ledger and the consensus algorithm is satisfied, The change reflects across all nodes.

The verifiable credential exchange on SSI ecosystems begins when the holder asks the issuer for credentials. The issuer creates the credentials, sends them to the holder to keep them in his digital wallet, and writes a DID on the verifiable data registry so that the verifier can use the DID in the verification process. When the holder wants to use his credentials, he needs to present his VCs to the verifier. The holder should show credentials issued from a trusted source, and the issuer has not revoked them. The verifiable presentation of the credentials enables the holder to prove specific claims or attributes to the verifier. The verifier can ensure the accuracy and authenticity of the credentials from the verifiable data registry(Mühle et al., 2018; Schardong & Custódio, 2021).

2.2.3 Main principels of SSI

Researchers developed principles to govern and manage SSI ecosystems. Kim Cameron was one of the first researchers who wrote principles for identity in his "laws of Identity" (Cameron, 2005). According to Schardong & Custódio, The "laws of Identity” influenced Christopher Allen's proposal on SSI principles(C. Allen, 2016). These principles were categorized into three main categories: security, controllability, and portability. Security: includes the principles that guarantee the security of the user information. Controllability: includes the principles that guarantee users full control over their credentials and what attributes to show and what to hide. Portability: includes principles that guarantee users can use their credentials anywhere and not be restricted to one provider(Tobin et al., 2017). TABLE 1 list of the SSI principles categorized into security, controllability, and portability principles.

TABLE 1 SSI basic Principals (Naik & Jenkins, 2020).

Security	Controllability	Portability
Protection	Existence	Interoperability
Persistence	Control	Transparency
Minimisation	Consent	Access
		Portability

These principles ensure control over self-sovereign identity systems by balancing transparency, fairness, and support. For example (C. Allen, 2016; Cameron, 2005; Naik & Jenkins, 2020; Schardong & Custódio, 2021).

- Control refers to the holders' ability to control their identities; they can choose what attributes they want to show and what should be updated.
- Existence ensures that the digital identity of the actor should refer to a physical person, organization, or entity. It cannot refer to a virtual actor
- Access refers to users' ability to access their identities anytime, anywhere.
- Transparency means identity administration and operation should be open source and transparent to all users.
- Persistence should be forever or upon users' request.
- Portability makes sure that identity and its related credentials can be easily transferred from one device to another and from one platform to another, which requires standardization in structure.
- Interoperability does not limit identity to a single environment and enables different identity solutions to communicate on some scale.
- Consent refers to users' consent on their identity usage is mandatory.
- Minimization Portability makes sure that identity and its related credentials can be easily transferred from one device to another and from one platform to another, which requires standardization in structure.
- Protection means to protect the identity by using an independent authentication system and prioritizing the individual rights on the network identity rights.

In researchers' and practitioners' trials to evaluate SSI ecosystems, They set metrics to evaluate the SSI ecosystem's performance. Metrics mainly include the SSI main principles and considered more aspects (Naik & Jenkins, 2020). The proposed metrics are :

- Storage control gives the identity holder the control over the device and the digital wallet used to store his credentials.

- Verifiability is to ensure that identity can be verified. The verification happens using the identity credentials and with no direct connection between the issuer and the verifier.
- Recovery is to have various mechanisms to restore or recover the identity if the digital wallet keys are lost or the holding device breaks down.
- Cost-free is to provide the identity free of charge for everyone.
- Availability is to make the identity services and solutions available for everyone with no discrimination on any basis.
- Scalability is to make sure that identity solutions are capable of providing any identity requester to encourage governments and organizations to expand SSI utility.

2.3 Governance and governance framework

The governance framework is the most crucial element in the SSI ecosystem because it provides information about the ecosystem's rules, goals, drivers, and elements. The first section discusses governance and SSI governance. The second section investigates the governance framework and its requirement. The third section shows real-world examples of SSI governance frameworks with different goals.

2.3.1 Governance and SSI governance

The Oxford dictionary defines governance as "having the right and the authority to control something." In SSI ecosystems, governance has a similar meaning to the Oxford dictionary. Essif lab defined governance in the SSI context as "the act or process of governing or overseeing the realization of (the results associated with) a set of objectives by the owner of these objectives."(ESSIF lab, n.d.)

Many pieces of literature define governance in SSI ecosystems. Some literature sees it as a process that addresses the needs of ecosystems. Other literature sees it as actors' collaboration management. Different definitions of governance are listed in TABLE 2

TABLE 2 Governance definitions and how it is viewedTABLE 2

Governance view	Governance definition
Process	“It is the process of governing, whether undertaken by a government, market, or network, whether over a family, tribe, formal or informal organization, or territory, and whether through laws, norms, power, or language.” (Pelt et al., 2020)
Process/Actor management	“It is governance as decision rights placement

	and enactment. Also, it is a description of responsibilities and power assigned to actors, who and how decisions are made"(Ziolkowski et al., 2019)
Process	"Governance describes the processes by which individuals and groups with ongoing relationships bargain about how to adapt to changes within an institutional environment—such as the firm, a political or community organization, or in market contracting"(D. W. E. Allen & Berg, 2020)
Actor management /process	"Governance refers to the way rules, norms, and actons of how people interact with each other are structured, sustained, regulated, and held accountably. It is about regulating decision-making processes among actors involved in a collective problem, leading to the creation, reinforcement, or reproduction of social norms" (Shermin, 2017)

SSI governance enables holders to govern their credentials. The credentials are owned by the holders who have full control over them. Holders decide who can verify credentials when to use them, and where (Abraham et al., 2020; Laatikainen, Kolehmainen, Li, et al., 2021a; Naik & Jenkins, 2020; Schmidt et al., 2021). Governance is not limited to holders only, but also it is owned by a governance authority that controls and organizes the whole ecosystem's activities. Also, it controls the actors' interaction, including the credential holder. According to the Sovrin organization, governance authority is responsible for "issuing Trust Anchor Credentials, Credential Registry Credentials, Auditor Credentials, or Auditor Accreditor Credentials"(Sovrin Foundation, 2019b). In addition, it is responsible for publishing the Governance frameworks.

2.3.2 The governance framework and its requirements

There are various types of governance frameworks- sometimes called 'trust frameworks'- such as the security governance framework, IT governance framework, and SSI governance framework.

A security governance framework defines guidelines, and implements controls used as a reference for governing information security in all aspects of the organization's environment (Veiga & Eloff, 2007). An IT governance framework provides guidelines to clarify decisions, rights, and accountabilities to encourage desirable behavior redeemed for incentives (Beck et al., 2018). The SSI Governance framework has the same goals as security, and the IT governance framework is to "provide guidelines". SSI governance framework is still different due to its unique nature. It includes all the guidelines and standards that direct the ecosystem in multiple aspects like business, governance, technology, and legal aspects(Laatikainen, Kolehmainen, Li, et al., 2021a).

According to TrustOverIP foundation [2] and cheqd [3], SSI governance frameworks have standard requirements. It should be understandable and straightforward. Also, the language should be plain and not too formal to educate the reader about the principles. It should spell out the aspects that credentials operate. The governance framework should deliver value by specifying the rules and policies while considering the governance framework principles. It should be rigorous, and its outcomes should have the authority and mechanisms to be achieved within the ecosystem scope(cheqd, n.d.; Sovrin Foundation, 2019a).

2.3.3 Real-world examples of SSI Governance framework

2.3.3.1 Sovrin Governance Framework

The most common example for the SSI ecosystem is the Sovrin Governance Framework. It includes the principles, policies, terminology, and standards that enable different trust communities to define their digital credentials and address their specific needs, scope, and outcomes. Sovrin governance framework is a document that presents the ecosystem, direct principles, list agreements, and terminology explicitly used in the ecosystem domain, in addition to technical specifications, standards, policies, and more about the ecosystem. The Sovrin Governance Framework document consists of three documents: (1)the primary document, (2)the legal agreements, and (3) and policies. The primary document has the master document, the glossary, and the trust assurance report. The legal agreements cover the steward agreement, data processing agreement, transaction author agreement, and transaction ending data processing agreement. The third part is the policies; it includes the governance policies, ledger access policies, business policies, technical and organizational policies, economic policies, and trust mark policies (the Sovrin Governance Framework Working Group, 2018).

2.3.3.2 Cheqd governance framework

One other example of the SSI governance framework is the Cheqd governance framework. Cheqd governance framework focus on creating a new business model for verifiable credentials. Its core is understanding the acknowledgment of how the system runs. In addition, it demonstrates accessible and democratic ways to influence decisions, clear communication, transparency, and inclusivity. Cheqd governance framework presents the principles in the Cheqd network and how the network was built to be more decentralized over time. It explains their view of governance in the form of laws and guidelines, principles, social norms, markets, and economic architecture. Cheqd view of governance can be detected clearly in its rules, boundaries, missions, rewards systems, and pun-

[2] https://wiki.trustoverip.org/display/HOME/ToIP+Governance+Metamodel+Specification

[3] https://docs.cheqd.io/governance/

ishments. Cheqd network governance can be impacted by off-chain forums or on-chain proposals.

2.3.3.3 The Good Health Pass Interoperability Blueprint.

Another example is the Good Health Pass (GHP) interoperability blueprint[4]. It is a document issued and approved by the Interoperability Working Group for Good Health Pass. The document describes the main goal for the ecosystem. It reopens global traveling after the covid pandemic. It provides solutions for interoperability challenges in a distributed and decentralized ecosystem. It spans the health and travel sectors; The document lists the principles and norms that drive the blueprint, like restoring confidence, promoting equity, building trust, and data control. GHP contains the terminologies used to differentiate the credentials from the pass, the design choices like being human-centric, equity and inclusion, and decentralization. It describes the ecosystem and its integration with open standards. The GHP interoperability blueprint includes a detailed description of the standards, data models, credentials format and protocols, data privacy regulations, and public health policies in different legal jurisdictions. It also lists recommendations on the user experience, security privacy, data protection, and identity binding.

2.4 Software Ecosystem Modeling

Software ecosystem modeling is an old trend in presenting software ecosystems. Modeling is a way to analyze and view software ecosystems (Jansen et al., 2015). It is a vital factor in developing the software ecosystem; it supports a good understanding of principles, analysis of design, and construction activities(France & Rumpe, 2005). It aims to present the activities within the ecosystem, the sequence of these activities, the actors doing those activities, and for a deeper level of modeling, it represents the ecosystem entity details(Giaglis, 2001; Hong & Bae, 2000). Modeling software ecosystems is essential because it decreases the ecosystem's complexity by developing the communication between various actors' categories (technical, business, legal, managerial)within the same ecosystem (Barclay et al., 2020). The following sections explain different options for software modeling and their basic features.

2.4.1 Options for Modeling Software Ecosystems

Modeling software ecosystems was the interest of researchers over time. It developed and improved over time to create more value for and satisfy the needs of software practitioners. Modeling software ecosystems have different approaches like UML, MDA, Istar, ArchiMate, and DSM. All these approaches will be presented in this section.

[4] https://www.goodhealthpass.org/blueprint

UML is one of the earliest modeling languages supported in the software industry. It is an object-oriented language that uses classes, methods, attributes, and relationships to visualize models. It can model both static and dynamic software systems. It was widely used among information system users in the nineties for its simplicity compared to KIF. It facilitates the decisions related to concepts. It helps provide a visual view of the ecosystem, but it does not support decision-making, automation, or object reuse (Cranefield & Purvis, 1999; Kelly & Tolvanen, 2008a).

MDA is an approach for modeling software ecosystems. It supports software design, specification, and development. Its technique is to detach the logical side from the platform technology to create model series of models according to three views: Computation Independent Model (CIM), Platform Independent Model (PIM), and Platform Specific Model (PSM). CIM, PIM, and PSM models represent the same idea from different views, but each model exists independently and is not linked by any means to other models (Abdelhedi et al., 2017; OMG standards development organization, n.d.). The main disadvantage of MDA is that the codes are generated directly from the models. For every change or any maintenance for codes or models, all the series of models and codes need to be refined, making it an eliminated option for agile ecosystems (Kelly & Tolvanen, 2008a).

ArchiMate is a modeling approach developed to model enterprise architectures. It has the ability to analyze and visualize the relationships within a specific domain. It can present information flow, organization structure, and business process. This research is interested in ArchiMate's ability to model IT systems, infrastructure, and business components. It supports the visualization of IT systems with their relations and dependencies. Also, It supports agility(Josey et al., 2016). Despite that, it is not the best option for modeling all software ecosystems for two reasons. The first reason is the limited availability of human-centric vision in the governance layer and the lack of data storage objects in the technology layers. The second reason is the absence of legal and regulatory objects like laws, acts, agreements, standards, and much more.

Istar is the first modeling language used for modeling SSI ecosystems. It is an actor-based modeling approach. It takes the user to a different level of detail. It does not describe only the basic structure and activities of the ecosystem, but it also goes deeper into the main actors of the ecosystems and their goals. It can describe the main resources and needs. Istar provides two perspectives for the models. First is the dependencies and relations among actors. Second is the justification for the actor behavior like goals, tasks, activities, and resources. one of its main advantages is its focus on a specific domain and its flexibility(Dalpiaz et al., 2016). The main disadvantages of Istar are that it can not produce codes and has no guidelines for the modeling process. (Handoyo, 2017)

Domain-specific modeling is a modeling approach used to design and develop software systems. It supports agility and can be developed for specific domains like SSI ecosystems. It will be explained in more detail in the following section.

2.4.2 Domain-Specific Modeling (DSM)

DSM is a modeling approach that makes the development process fast and easy. DSM works to solve a specific domain problem. The resulting solution can be customized to the organization's rules, concepts, and culture. Non-technical users could utilize it because coding is not needed anymore (Kärnä et al., 2009). According to Steven Kelly and JP Tolvanen, DSM does two important things" First, raise the level of abstraction beyond programming by specifying the solution in a language that directly uses concepts and rules from a specific problem domain. Second, generate final products in a chosen programming language or another form from these high-level specifications."

For any domain, the development process in DSM aims to create three primary outcomes: the modeling language(DSL), the code generator, and the framework (Kelly & Tolvanen, 2008a). DSL is a way or a method to describe and generate a series of programs on a specific domain. It has syntax and semantics to represent objects' properties and connections. It has graphical and textual features for better representation (Van Deursen & Klint, 2002). Code generators are responsible for transforming the models into written codes. This process is automated and does not need any editing or inspection from a human actor, but it can also be edited manually. The framework is a layer that works as a median between the code generator and the platform to avoid complexity and repetition.

One of the most important advantages of DSM is that it supports agility. It supports agility and reusability not only from the business perspective but also from the language definition itself. If the customer asked for improvement to the language body, like changing symbols, the changes are only done on the code generator, and no updates need to be made to the models. From the business perspective, if the customer wants to update the models, they can be easily modified and reflect on reused elements at once.

Organizations consider DSM is a successful approach for many reasons. It enabled organizations to develop in-house business solutions without outsourcing or hiring developers. It increases business productivity and agility. In case Organizations need extra features for their modeling language, Users can use a visual interface to be part of the production process; hence, users can easily guide the developer to the production-specific requirements. It facilitates the interactions between the developers and the non-technical user. It saves money and effort(Kärnä et al., 2009; Kelly & Tolvanen, 2008a).

Developers also consider DSM a successful approach for many reasons. DSM constructs are easily communicated with users from the domain because they are extracted from the domain, making them familiar. DSM operates in a limited scope which makes the framework building less challenging. The DSM component reusability is very high within the same business disciplines, making the delivery faster and more efficient.

According to this research scope, the most important outcome of DSM is the domain-specific language(DSL). DSL is the first and most critical part of the

DSM solution. The goal of DSL is to produce a software product to model systems with a higher-level language. It takes many steps to have a DSL. It starts with defining the language. Defining a DSL is not as complex as defining a general language because it focuses on the small scope with a specific concept and specific vocabulary for the language. Defining DSL takes many phases that are described in the following points(Kelly & Tolvanen, 2008a; Van Deursen & Klint, 2002)

- The first phase in defining the language is identifying the language concepts. In this phase, the language developers need to understand the domain to map its main concepts. Concepts can be identified from the problem domain concepts and/or by consulting the problem domain experts. In addition, the concept identification can be supported by the business architecture, existing products, business specifications, and business patterns. This can not be done in one iteration; it takes many iterations to define the concepts. The number of iterations depends on multiple factors like the domain size and the extent to which the developers understand the domain. Let us note that The language definition process is iterative and can be changed with the requirements changes. The changes can take place at any phase.
- The second phase is to map the identified domain concepts into modeling concepts. In this phase, developers think about how the domain concepts can be utilized in the DSL in symbolic presentation. The primary domain concepts are usually mapped into modeling objects. Other domain concepts are mapped as roles, relationships, and properties. Developers should create the language definitions guidelines at this phase, like creating naming policies, keeping the language simple, minimizing the modeling work, adding definitions for each element, and considering the extension possibilities.
- The third phase is formalizing the language with metamodeling. The main goal of this phase is to make the modeling language guide the modeling work. The metamodeling process begins with drawing the modeling concepts and their possible connections. Developers start to create objects, properties, relationships, and roles. Developers should make sure after the language implementation that the models are understandable by the domain users and decision-makers even if the modeling concepts are not familiar to them.
- The fourth phase is defining the modeling rules. It provides guidance for the users on the best way to use the modeling language. Defining the language rules helps prevent errors, have a design pattern, identify missing concepts, and ensure language specification consistency. The rules are domain and modeling rules. The domain rules include the uniqueness of object names, forcing some properties to objects, connection rules, setting default values, and structuring hierarchies. The modeling rules prevent modelers from making mistakes. For example, prevent the mod-

elers from establishing a new relationship before deleting the old relationship or adding two objects with the same name.

- The fifth phase is creating the language notations. Notations give a visualization of the modeling concepts. To ensure good presentions for the DSL elements, the notions should be graphical, textual, or a mix of both. The graphical notions add symbols to give the user a hint of what that object could be. The textual notations enable adding text to name or explain.

The main advantage of DSM is that agility is one of its constructs, This theory is built on the fact that all ecosystems can not still be the same, and it is customary to change over time. It also supports code generation without any human refinement, decision making, object reuse, and flexibility in creating new domain objects when needed.

3 Introduction to Case Study and the Modelling Language

This chapter introduces the case study and the new modeling language used in this study field. The following sections present the case study(Yoma) as an organization, its goals, business process, and technologies Yoma relies on. The second part introduces the modeling language (Ecosystem Governance Compass), the mental model behind it, and its definition.

3.1 Yoma

Yoma[5] (youth agency and a marketplace) is a digital platform that enables youth participants to create a digital CV. Yoma platform provides participants with educational opportunities. Participants had to pass educational challenges or impact task challenges to find employment paths. Yoma rewards youth participation with tokens (ZLTO) to be spent on goods and services such as mobile network airtime or premium education opportunities in the Yoma marketplace. Yoma uses AI to build personalized learning pathways for youth and impact tasks as challenges to engage youth in activities that have a positive environmental or social impact on their communities. In addition, Yoma helps youth to find jobs that match their aspirations and psychometric profile. Yoma also aims to build self-confidence and trust within local communities. The Yoma ecosystem has been built using a value-based engineering methodology in which youth defined their core values as privacy, personal self-development, trust, community, fairness, and inclusion. It is an ecosystem solution that links youth participants with opportunities provided by a wide range of partners, such as private enterprises, Social Impact Organizations, and future employers.

Yoma uses verifiable credentials to help youth build their digital identity in a digital CV. They can find new experiential learning opportunities by com-

[5] https://www.yoma.africa

pleting impact tasks or 'challenges'; then, they are awarded a verifiable credential added to their digital CVs. Youth can use their digital CVs to find jobs on the same platform where employers verify using SSI. Youth are also awarded digital tokens for completing impact tasks or challenges. Tokens can be redeemed in physical or intellectual marketplace awards(Johnson, 2020).

Yoma has the general governance framework requirements like simplicity, understandability, plain language, and delivering value. At the same time, it has its own requirements due to operating in specific business disciplines(educational and environmental sectors). Yoma governance framework's particular requirements are to follow the TOIP foundation governance metamodel. Yoma chose TrustOverIP governance framework because it is based on open standards that enable Yoma to operate across different sectors (education, environment) and put the holder (youth participants) at the center of the ecosystem design. In addition, as Yoma is still in an early innovation phase, it does not yet have a legal entity that can act as a governing authority.

3.2 Ecosystem Governance Compass

Yoma models were built using a new modeling tool called Ecosystem Governance Compass [6](EGC)(Kolehmainen et al., To be submitted). EGC is a new tool developed based on domain-specific modeling theory(Tolvanen & Rossi, 2003). It is developed by the Startuplab at the University of Jyvaskyla. EGC aims to build and manage blockchain governance and satisfy the unique requirements for SSI ecosystems. The domain EGC operates on is the SSI ecosystems. It helps ecosystem practitioners to plan and automatize governance frameworks. It provides actions, system methods, and processes to make different ecosystem layers for different stakeholders.

EGC's mental model describes the language constructs. It handles four aspects: Governance, business, legal and regulatory context, and technology. The objects of the governance aspect are actors in the ecosystem and their roles. It also identifies the rights, rules, and responsibilities per actor/role. It explains the incentives that each actor/ role would gain for participating in the ecosystem. The business aspect identifies the main business activities per actor/role. The Business aspect shows the revenue models and the costs for each actor/role with business activities. The legal and regulatory context identifies the laws, regulations, legal, and technology standards the ecosystem requires to comply with. It also identifies the legal agreements or contracts that control the interaction among different actors. The technology aspect identifies the technical services, the technology components, data objects, and data storage.

EGC has supportive relationships and properties that the modeler can customize according to case needs. EGC formalizes itself with a color code to distinguish each aspect. The governance layer color is purple, the business layer

[6] https://gitlab.com/jyu-startup-lab/ecosystem-governance-compass-jyu

color is yellow, the technology layer color is green, and the legal and regulatory layer color is orange. The user can quickly notice that the objects used on models belong to which layer. Also, it uses different shapes(notions) to represent the objects rectangles, triangles, cylinders, ovals, and hexagons to represent the objects. It also uses main containers and sub-containers for better object grouping and representation.

EGC sets many language rules to avoid modeling mistakes and has a good model presentation. The domain rules are general rules like the naming starts with capital letters, objects can not duplicate names have the same names, set default values for the properties, and many more rules. The modeling rules in EGC are left as comments to give the modelers the freedom to present the mods

The notions in EGC are graphical and textual. Each object has a symbol on the upper right side that tells about the object's activity. All objects have a space for names and a description area where the modelers can add a detailed description for the object.

4 Research Method

In this chapter, the research methodology is explained. Also, it explains the work procedure in Yoma, including the data collection and data analysis and the main milestones in the model creation.

This research work is a field study that aims to help SSI practitioners develop the governance framework using modeling. The research was done in collaboration with the Yoma task force. The research uses an exploratory qualitative approach. The exploratory qualitative approach helped the data collection process be unbiased toward the expected research results (Edmondson & McManus, 2007).

4.1 Data collection

The data collection method in this research is active participant observation(Takyi, 2015). Active participation observation helped collect the empirical data during the task force meetings, value-based engineering workshops, risk assessment workshops, technology team meetings, business team meetings, and legal and regulatory team meetings.

The collaboration with Yoma started in May 2021. It took about two months with the task force meeting to overview the project and the key players and their responsibilities. After that started to work on Yoma layers one by one. First started with a governance layer, then the business layer, after that the technology layer, and finally the legal and regulatory layer

The empirical data was collected as notes during the meetings and coded on a predefined spreadsheet. The spreadsheet was designed according to the requirements for the EGC mental models. Building Yoma models took place in accordance with writing the Yoma governance framework.

EGC and the governance framework development had two evaluation phases. The first phase of evaluation was in a meeting with the Yoma project managers. The second evaluation phase was with the Yoma task force, which combines all the stakeholders together. FIGURE 3 shows the timeline for the collaboration with Yoma.

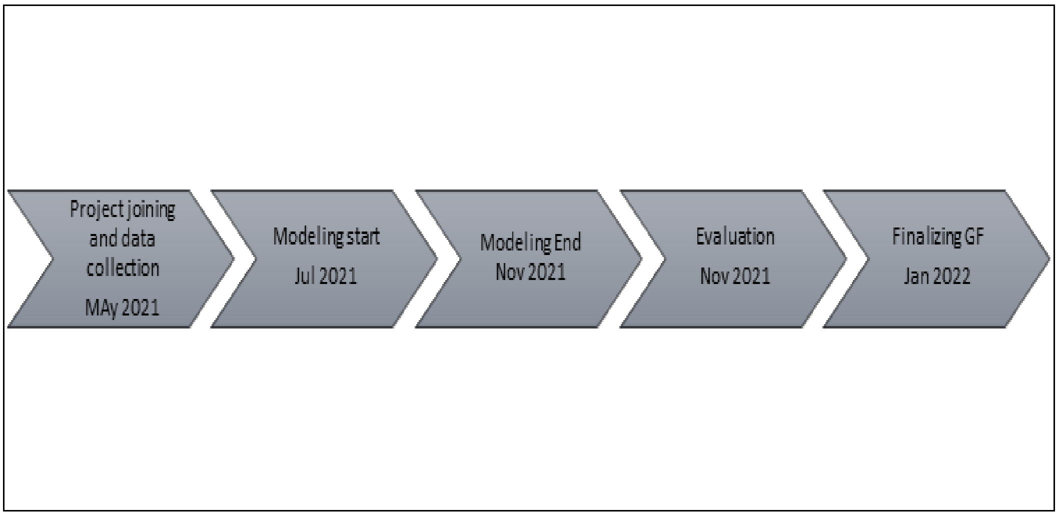

FIGURE 3 Yoma Participation Timeline

The meetings started in May 2021 with the Yoma project manager. The main goal of the meeting is to introduce the tool and discuss what aspects EGC can help Yoma's governance framework. The governance layer modeling is discussed with the Yoma project manager and the Yoma task force. The business layer modeling is discussed with the Yoma project manager and the business team. The technology layer modeling is discussed with the technology team. The legal layer modeling is discussed with the legal team. TABLE 3 shows the Yoma meeting table.

TABLE 3 Yoma Meeting Table

Meeting objective	Date	Duration in minutes	Participants
• introduction to Ecosystem governance compass and how it is going to help Yoma	7-May-21	30	Yoma Project manager
• discussion about the technical team expectation from the Ecosystem Governance Compass and how to fulfill it	13-May-21	60	Yoma Technology team
• Review requirements for Interim Governance Authority	18-May-21	60	Yoma Task Force

• Get support from the task force to find the Interim GA. • Get feedback from the Ecosystem governance compass Exercise.			
• Addressing requirements for the governance model	7-Jun-21	30	Yoma project manager
• looking into the technical side of modeling • Creating meta-models and new objects to fit the Yoma case	8-Jun-21	60	Block chain and Digital Identity Research Team (Startup lab) at University of Jyvaskyla
• EVR specification workshop YOMA | Value-based Engineering	9-Jun-21	120	Yoma Task Force
• How will the Yoma process work.? • Target achievement as outlined in the straw man process. • What are key sources for UNICEF Policies and Best Practice links Sovrin Ecosystem GF for Requirements, Layer 1 Requirements, and Custodian Rules & Policies? • Ecosystem governance compass feedback.	15-Jun-21	60	Yoma Task Force
• Collecting the technology needs of the technical team to update EGC	17-Jun-21	60	Yoma Technology team
• Addressing and implementing the technical requirement for the Yoma technology model	18-Jun-21	60	Blockchain and Digital Identity Research Team (Startup lab) at the University of Jyvaskyla
• EVR specification workshop YOMA |	18-Jun-21	120	Yoma Task Force

Value-based Engineering (2)			
• addressing Governance incentives and Risks	24-Jun-21	30	Yoma project manager
• Business requirements preparation (1)	24-Jun-21	30	Yoma business team
• updating the governance model requirements (1)	29-Jun-21	60	Yoma project manager
• Risk assessment process. • Ecosystem governance compass discussion feedback. • Custodianship Discussion Document	29-Jun-21	60	Yoma Task Force
• Risk assessment workshop explaining the Yoma risk assessment approaches. • Ecosystem governance compass feedback.	30-Jun-21	60	Yoma task force
• Business requirements preparation(2)	30-Jun-21	60	Yoma business team
• EVR specification workshop YOMA | Value-based Engineering (3)	2-Jul-21	120	Yoma Task Force
• updating the governance model requirements (2)	6-Jul-21	60	Yoma project manager
• discussion about the motivation of each actor to share on Yoma • Addressing the revenue model and costs	21-Jul-21	60	Yoma Business Team
• Antitrust Policy Notice. • Ecosystem governance compass feedback. • Custodianship conversation de-	27-Jul-21	60	Yoma Task Force

veloped with support from Sovrin's Guardianship WG. • ESSIF Lab Mental Models and Glossary.			
• Ecosystem governance compass updates. • Risk Assessment updates. • Reviewing and adding to the Governance Framework Terminology • Changes in Yoma Scope	10-Aug-21	60	Yoma Task Force
• Introducing Ecosystem governance compass • presenting how it helped to develop the Yoma Governance framework	2-Sep-21	60	DIF Africa call Audience
• Updates on Ecosystem governance compass and risk assessment. • Reviewing the Governance Framework. Need for Interim GA. • Yoma next Steps	7-Sep-21	60	Yoma Task Force
• Collecting the technology requirements (1)	21-Sep-21	60	Yoma Technology team
• Collecting the technology requirements (2)	30-Sep-21	60	Yoma Technology team
• Human Experience WG has agreed to support Yoma in developing the HX Controlled Document plan with Yoma's UX team Finalising the GF	5-Oct-21	60	Yoma Task Force
• Collecting the legal and regulatory requirements	11-Oct-21	60	Yoma project manager
• Discussion on building Yoma eq-	18-Oct-21	60	Yoma task force

uity among youth. • Ecosystem governance compass feedback.			
• proposed 'Interim Youth Council.' • Finalizing the glossary with CTWG • Discussion on the human experience of Yoma governance • Ecosystem governance compass feedback.	25-Oct-21	60	Yoma task force
• Evaluation session for the Ecosystem governance compass	26-Oct-21	60	Yoma project manager Blockchain and Digital Identity Research Team (Startup lab) at the University of Jyvaskyla
• Evaluation session for the Ecosystem governance compass	16-Nov-21	60	Yoma task force

4.2 Model creation

Model creation took place in four phases accordingly to data collection. Data were extracted from the meeting minutes and the initial document for the governance framework undergoing continuous development during all four phases.

Phase one: Governance models, the key actors were modeled and their roles in the ecosystem, then linked each actor/role to their rights, responsibilities, and incentives gained from being part of the ecosystem, considering each actor could have only one role or multiple roles; for example, Education Opportunity Provider had two roles the first is Youth Credential Issuer, and the second is a Yoma Organizational Member.

Phase two: Modeling business aspects. The primary concern was the business activities of each actor/role. They were linked to their revenue model and to the expected costs, including cost type (fixed or variable).

Phase Three: Technology model. The technology model represents Yoma's services, for example, Employment Provider Onboarding, Notifications, and Credentialing. It also represents technology components, for example, the Yoma platform, framework, applications, and middleware. Lastly, data objects and data storage, Indy ledger, Aries wallet, and different data storage components.

Phase four: Legal and regulatory aspects. The legal and regulatory model represents all the agreements that control actors'/roles' interaction. It also represents all relevant standards for the ecosystem, for example, GDPR, VC, DID, DIDComm.

4.3 Evaluation

The participation in the Yoma task force helped to study the effect of modeling in developing the Yoma governance framework. The feedback and evaluation were based on a discussion with the Yoma task force that belongs under Trust Over IP Foundation's Ecosystem Foundry Working Group [7]and the project manager of the Yoma. The discussions focused on two areas. First, Does building the models help achieve Yoma governance framework requirements like simplicity and understandability? Second, how Yoma helped EGC identify its strength points and Yoma's view of the changes that need to be done to develop EGC further and provide value for ecosystems.

[7] https://wiki.trustoverip.org/display/HOME/YOMA+Ecosystem+Task+Force

5 FINDINGS

5.1 Yoma models

Building the Yoma model happened in four phases. Each phase is concerned with one model, and each model provides a visual view of an aspect of the ecosystem (governance, business, legal, technology, legal and regulatory). Model creation started with collecting and analyzing data, then implementing the models. Each model has all the related details about the aspect. As Yoma is a human-centric SSI ecosystem and its primary concern is the credential holder, EGC followed the same perspective in its way. EGC's primary concern is actors/roles. Actors/roles are the starting point for the model creation; then, all other details are organized around them. The following sections explain each model, followed by the model picture—the overall picture of the whole ecosystem in Appendix1. For a bigger model picture, please visit the startuplab GitLab[8].

5.1.1 Governance

The governance model's primary concern is to list the actors participating in the Yoma ecosystem. The actor is an entity capable of performing behaviors or activities in Yoma. The governance model attaches a role to each actor. The role is the characteristic set of behaviors or activities undertaken by Yoma actors. Multiple actors can share the same role if they perform the same activities. For example, Guardian and Youth share the role of Educational Credential Holders. Social Impact Organization, Education Opportunity Provider, and Youth Credential Verifier also share the same role as Yoma Organizational Member. The governance model presents actors/roles with essential details like the rights, responsibilities, rules, and incentives. Rights are a privilege to perform a partic-

[8] https://gitlab.com/jyu-startup-lab/ecosystem-governance-compass-jyu/-/tree/main/models/Yoma%20v3

ular behavior or activity. Responsibility is a behavior or action that actors or roles can be held accountable for. The rule is a regulation or principle that governs conduct in Yoma. The incentives are the motivational factor of the actors or roles to take action. The governance model is shown in FIGURE 4

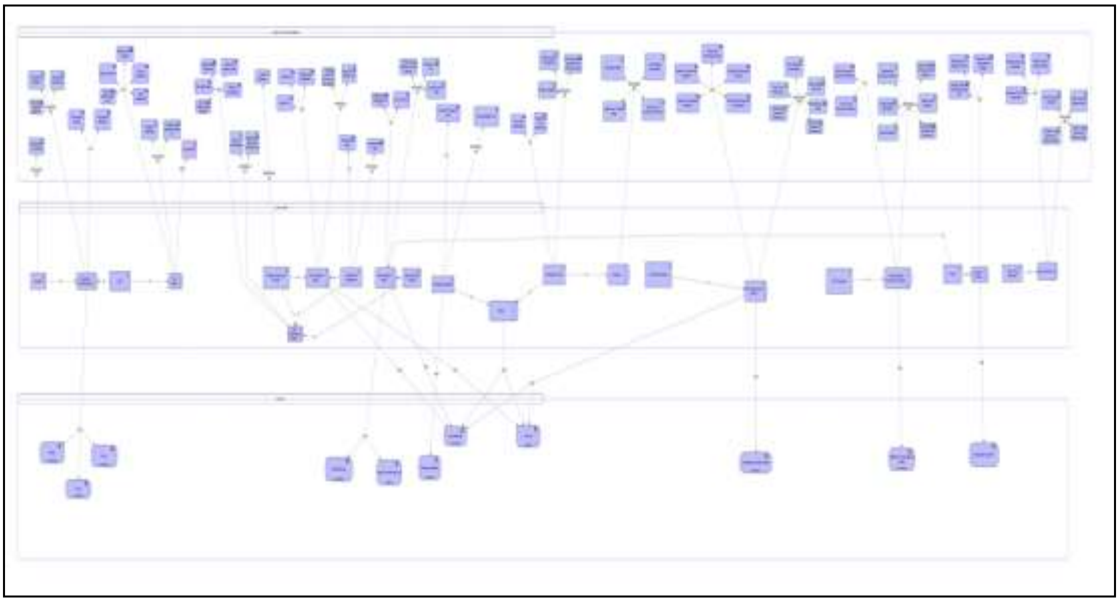

FIGURE 4 Yoma Governance Model

The first actor in Yoma ecosystem is the youth. Youth have two roles at Yoma: a Yoma Member and an Educational Credential Holder. Youth as Yoma Members are responsible for completing and updating the digital CV and completing educational challenges. They have rights like ceasing their membership, revoking Guardianship when they reach 18 years old, appointing a Guardian if youth under 18 years old, requesting credential issuance when he/she is eligible for it, and using the Yoma Member badge on the CV. Yoma Member has a rule that youth should meet the age constrain of 18 years old. If the youth is 16, he/she can register to Yoma, but he/she should appoint a Guardian.

As Educational Credential Holders, youth responsibilities are to ensure the VCs are updated to digital CV, use the VCs' selective disclosure, and check their VCs' accuracy. Credential holders have the right to choose the party they want to share their credentials with and what to share. Also, they can ask for VCs issuance. The credential holder gains multiple incentives from Y, such as growing their experience and skills, the personal and social impact from the learning experience, and thriving by having better job opportunities.

The second actor is the Guardian. The Guardian role is an Educational Credential Holder. Guardian is responsible for legally representing youth under 18. Guardian is not the actual credential holder, but his role is to support youth under 18 to be part of the ecosystem, meaning that Guardians do not have any rules, rights, or incentives.

The third actor is the Education Opportunity Provider. Its role is Yoma Organizational Member. Yoma Organizational Member is responsible for maintaining and updating the company profile. Also, it is responsible for guiding the actions of legal delegates (lawyers or employees). Yoma Organizational Member has the right to post and remove educational opportunities, create and edit company profile, appoint a delegate, and use the Yoma Member badge or branding.

Education Opportunity Provider has another role as youth Credential Issuer. The Credential Issuer is responsible for notifying the Incentive Provider of Zlto youth recipients and issuing VCs for eligible youth (Zlto is a digital token awarded for passing challenges in addition to the credentials). Education Opportunity Provider has the right to issue and revoke VCs and specify youth qualification. Their incentive to be a Yoma Member is to gain a good reputation and have a paid fee for courses.

The fourth actor is Social Impact Organization. It has two roles; Yoma Organizational Member and youth Credential Issuer. It shares the same responsibilities, rights, and incentives as an organizational member with the third actor (Education Opportunity Provider). In addition, it is responsible for generating impact tasks and has the right to post them on the Yoma platform in cooperation with the Education Opportunity Provider.

The fifth actor is the job opportunity provider. Jobs opportunity provider role is a Youth Credential Verifier. The Youth Credential Verifier is responsible for adding and removing the job offers, verifying the Youth VCs, and ensuring employment policies are followed. Youth Credential Verifier has the right to accept or reject VCs after verification and request proof of qualifications on the CV. The Youth Credential Verifier incentives to be part of Yoma include having skilled employees and reducing recruitment costs. Jobs opportunity provider has another role as Yoma Organizational Member. It has the same rights and responsibilities as (Social Impact Organizations and Education Opportunity Providers).

The sixth actor is Marketplace Participant. The Marketplace Participant role is a Business Partner. Business Partners do not have shared responsibilities or rights at Yoma because they do different business activities. On the other hand, Business Partners have shared incentives: to get a paid fee and have a good reputation. Marketplace Participants as an actor has their responsibilities like rewarding eligible youth. It has the right to check ZLTO credit for youth. It also has its incentive, which is customer acquisition.

The seventh actor is the Technology Provider. The Technology Provider's role is a Custodian. Custodian is responsible for hosting the digital wallets, executing digital transactions, complying with the governance framework general principles, and supporting the VC holders offline. It has another role as a Business Partner, so it has the same incentives as the Marketplace Participant. Technology Provider has other responsibilities as an actor, like writing documentation associated with services provided, building and developing a Yoma platform, and providing consultation when needed. It also has its own rights, like ceasing youth accounts using Yoma infrastructure.

The eighth actor is Yoma Social Enterprise. Yoma Social Enterprise's role is Yoma Infrastructure Operator. Yoma Infrastructure Operator is responsible for administering and operating the infrastructure, building Yoma infrastructure, Yoma commercial sustainability, monitoring compliance with SLA's, managing the Yoma brand, and providing Yoma Members & organizational members with technical support. It has the right to manage Yoma's business operations, manage Yoma technical operations, and contract with (Technology Providers, opportunity providers, and Social Impact Organizations). Its incentive to be a Yoma Member is to increase the reach of the impact mission.

The ninth actor is the Yoma Foundation. Yoma Foundation's role is Yoma Ecosystem Governance Authority. Yoma Ecosystem Governance Authority is responsible for administering the governance framework, monitoring compliance with the governance framework, maintaining Yoma's reputation, opening transparent and democratic governance, updating regulatory requirements, and resolving disputes. It has the right to write and change the governance framework and enforce the Yoma governance framework. Its incentive is to fulfill Yoma's purpose & mission.

The tenth actor is RLabs. RLabs' role is Incentive Provider. The Incentive Provider has the right to contract Yoma Organizational Members, refuse Zlto to be assigned to a task, and request credential proof before issuing Zlto. The incentive Rlabs aim for is to ensure the success of their research work on token (Zlto). RLabs also have another role as a Youth Credential Verifier; it has the same rights, responsibilities, and incentives.

The eleventh actor is the Local Yoma Ecosystem. The Local Yoma Ecosystem role is a Service Provider. The Service Provider is responsible for maintaining the Yoma governance framework locally, arranging Yoma local operations, deciding Yoma local policies and acts, and enforcing the Yoma governance framework locally. It has the right to assign Yoma local policies and acts, organize Yoma local operations, and make use of local Yoma infrastructure.

5.1.2 Business

The model of business aspects represents the activities and financial aspects of the actors/roles. Business activities are a collection of business behavior that an actor or role can perform to create and capture value. The financial aspects show the money flow in Yoma; it includes the revenue model and the costs. The revenue model is the incoming money stream and the related pricing elements through which an actor or a role captures value, and the costs are a financial representation of a cost incurred due to an asset, resource, activity, or service necessary for value creation or capture. The business model is shown in FIGURE 5

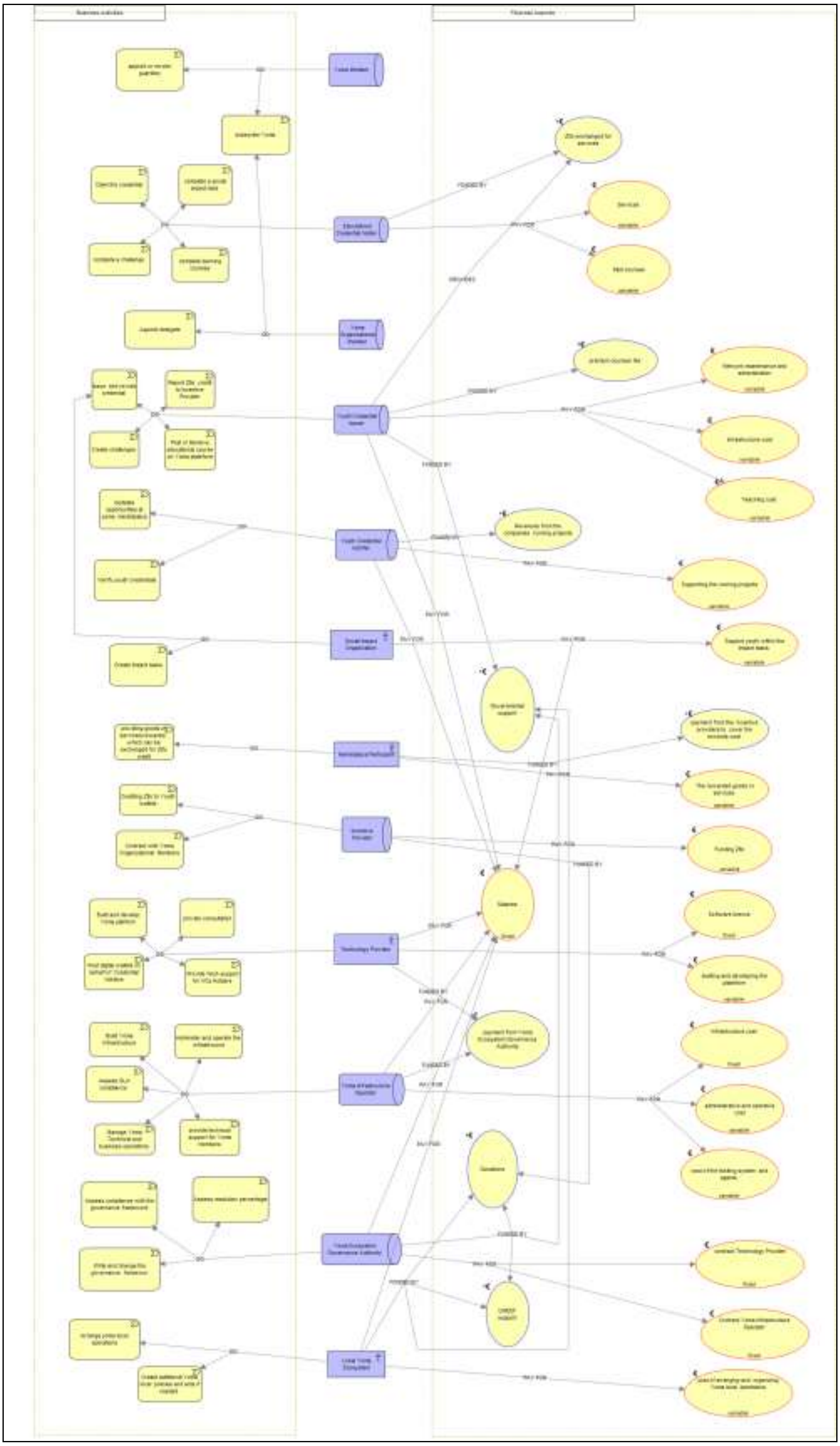

FIGURE 5 Yoma business Model

The first actor/role in the business model is a Yoma Member. Yoma Members do business activities like subscribing Yoma platform and appointing or revoking Guardians. Yoma Member role business activities do not reflect any costs or any revenue.

The second actor/role in the business model is the Educational Credential Holder. Educational Credential Holder does business activities like claiming the credential, completing a social impact task, completing a challenge, and completing learning courses. Educational Credential Holder funded by Zlto that exchanges for services. Educational Credential Holder costs in the ecosystems are requesting services and paid courses.

The third actor/role in the business model is Yoma Organizational Member. Yoma Organizational Member is doing business activities like appointing a delegate and subscribing Yoma platform. Yoma Organizational Member has no revenue and does not reflect any costs or revenue.

The youth Credential Issuer is the fourth actor/role in the business model. Youth Credential Issuer is doing business activities like issuing and revoking credentials, reporting Zlto credit to the Incentive Provider, posting or removing educational courses on the Yoma platform, and creating challenges. Youth Credential Issuer is funded by the premium courses fee and funds from the government. The costs are network maintenance and administration, infrastructure, salaries, and teaching costs.

The business model's fifth actor/role is the Youth Credential Verifier. Youth Credential Verifier does business activities like updating Yoma marketplace opportunities and verifying youth credentials. Youth Credential Verifier funded by running projects. The costs are supporting the Yoma credential verification process and salaries.

The sixth actor/role in the business model is Social Impact Organization. Social Impact Organization does business activities like creating impact tasks and issuing and revoking credentials. The Incentive Providers fund Social Impact Organization to cover the rewards. Social Impact Organization costs are supporting youth within the impact tasks and salaries.

The sixth actor/role in the business model is the Marketplace Participant. Marketplace Participant business activities are to provide goods or services(rewards) that can be exchanged for Zlto credit. The Incentive Providers' payment funds Marketplace Participants, and its costs are the payment of rewarded goods or services that are redeemed with Zlto.

The seventh actor/role in the business model is Incentive Provider. Incentive Provider business activities are crediting Zlto to Youth wallets and contracting Yoma Organizational Members. Donations fund Incentive Provider and Incentive Provider costs are funding Zlto.

The eighth actor/role in the business model is a Technology Provider. Technology Providers' business activities are building and developing the Yoma platform, providing consultation, hosting digital wallets on behalf of credential holders, and providing technical support for VCs holders. Technology Provider funded by Yoma Ecosystem Governance Authority. Technology Provider costs are Salaries, software licenses, and the building and development of the platform.

The ninth actor/role in the business model is the Yoma Infrastructure Operator. Yoma Infrastructure Operator's business activities provide technical support for Yoma Members, manage Yoma technical and business operations, assess SLA compliance, build Yoma infrastructure, and administer and operate the infrastructure. The government fund Yoma Infrastructure Operators, and the costs are salaries, infrastructure cost, administrative and operative cost, and cost of the ticketing system and agents.

The ninth actor/role in the business model is the Yoma Ecosystem Governance Authority. Yoma Ecosystem Governance Authority's business activities are writing and changing the governance framework, assessing compliance with the governance framework, and assessing resolution percentage. Yoma Ecosystem Governance Authority is funded by governmental support, donation, and UNICEF support, and the costs are salaries payments to the Technology Provider and Yoma Infrastructure Operator.

The tenth actor/role in the business model is the Local Yoma Ecosystem. Local Yoma Ecosystem business activities arrange Yoma local operations and create additional Yoma local policies and acts if needed. The local Yoma ecosystem is funded by governmental support, donation, and UNICEF support, and the costs are salaries and organizing Yoma local operations.

5.1.3 Technology

The technology model represents the technologies used and applied in Yoma. Technologies elements can be categorized into three main categories: technology architecture and infrastructure, services, and data. The technology architecture comprises platforms, applications, frameworks, software, and middleware. Platform refers to (tools, libraries, and reusable components) that facilitate value creation, applications that encapsulate the Yoma web application. Frameworks are software libraries (components, interfaces, and tools) that enable the development of a technological solution. Software facilitates the integration of different components within a unified interface. Middleware facilitates the integration of different Yoma components within a unified interface. Services in the Yoma context are user notifications, educational and job onboarding, and a trustful connection. Data do not include the collected information only but also present different varieties for data storage (database, indy ledgers, user wallets). The technology model is shown in FIGURE 6

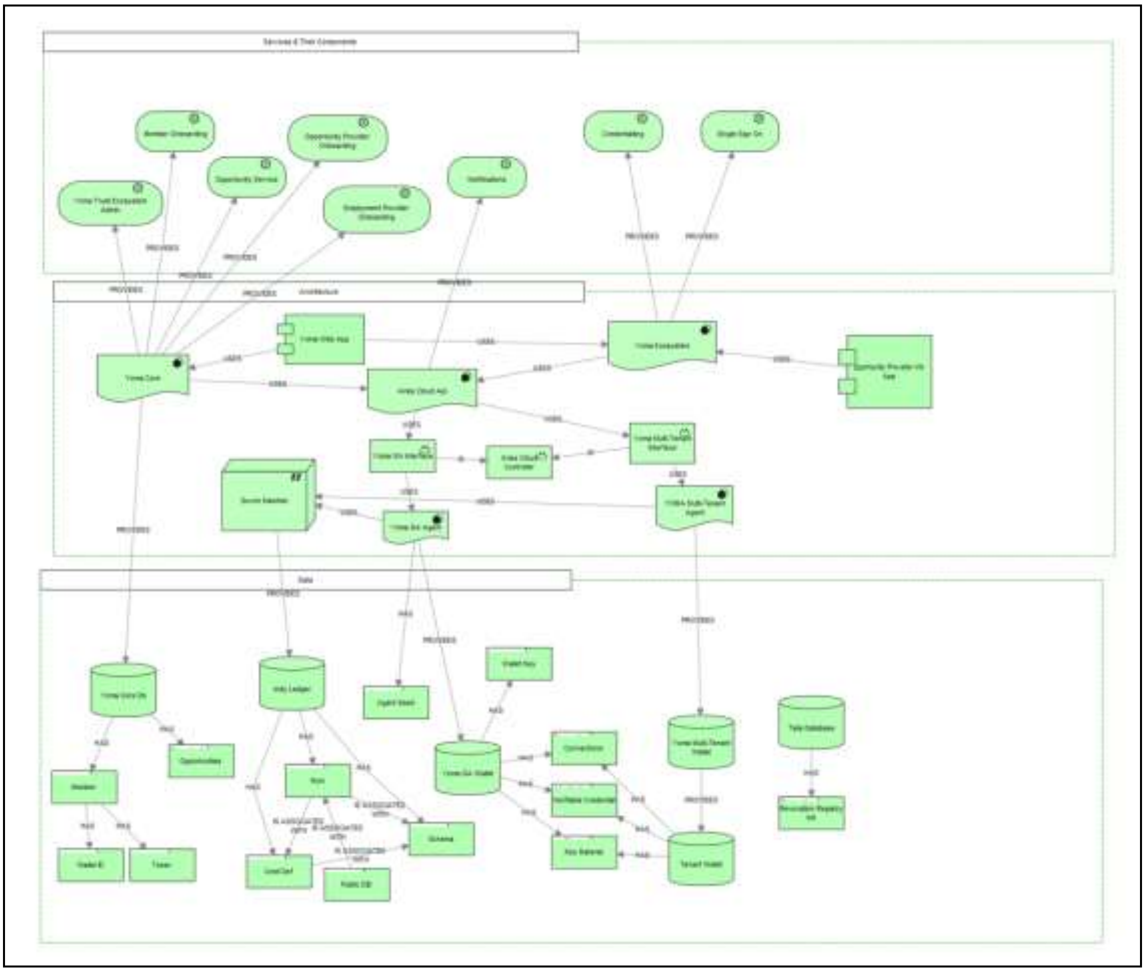

FIGURE 6 Yoma Technology Model

The infrastructure of the Yoma technology layer is modeled in the middle container. The upper container shows the services Yoma provides and their components. The down container shows the Yoma data objects and their components.

The infrastructure layer has the Sovrin MainNet it is the platform Yoma operates on. The Sovrin MainNet stores data on the indy ledger. The data types saved on the indy ledger are Nym, credentials, public DID , and the Schemas.

Yoma has five frameworks: Yoma Core, Yoma Ecosystem, Aries Cloud, Yoma Agent, and Yoma Multi-Tenant Agent. Aries Cloud is the center of technology architecture. It connects the Yoma external operation frameworks to Yoma internal operation frameworks. The Aries Cloud links and organizes external operations in the Yoma core with the Yoma ecosystem(the Yoma ecosystem control the users' activities).

For the internal Yoma operation, Aries Cloud connected to Yoma Multi-Tenant Agent with Yoma Multi-Tenant Interface middleware. AriesCloud connected to Yoma Agent with Yoma interface middleware. Both middleware(Yoma Multi-Tenant Interface and Yoma Multi-Tenant Interface) are linked together with another middleware(Aries Cloud Controller) to facilitate their integration.

Yoma Multi-Tenant Agent and Yoma Agent frameworks are connected directly to the central platform (Sovrin MainNet). Yoma web applications are connected to Yoma Core and Yoma Ecosystem frameworks to provide the required information. Also, the Yoma Ecosystem framework is linked to Opportunity Provider Web Application.

Yoma provides many digital services. The provided services are related to Yoma Core, Yoma Ecosystem, and Aries Cloud API framework. Yoma services related to the Yoma core framework are Yoma trust ecosystem admin, member onboarding, opportunity service, and employment provider onboarding. Notifications services are linked to the Aries Cloud API framework. Credentialling and Single Sign-On services are linked to the Yoma Ecosystem framework.

Yoma has multiple data storages (databases, digital wallets, and Indy ledger). Yoma core Database collects data about Yoma Members and the opportunities (educational and job opportunities). Yoma Members' data are the digital wallet Id and the awarded tokens. Yoma Wallet is a digital wallet that stores data about the Wallet Key, member connections, verifiable credentials, and key material. It also provides agent seeds but does not store them on any system data storage. The user has to save the seeds somewhere else on email or on an external paper. Agent Seeds are the only way to recover the wallet in case the user is going to install it on another device or the device with the wallet is stolen. YOMA multi-tenant Agent framework is connected to YOMA multi-tenant Wallet. YOMA Tenant Wallet store shared information with Yoma Wallet. The shared information is about the member connections, verifiable credentials, key material.

5.1.4 Legal and regulatory

The legal and regulatory model is concerned with the agreements between Yoma actors, the standards Yoma follows, and the (laws, acts, and regulations)Yoma complies with. Agreements comprise the agreements' parties' terms, conditions, rights, and obligations. Yoma operates in multiple African countries, so laws, acts, and regulations would differ from one country to another in Yoma's case. Yoma laws, acts, and regulations are not decided yet, and it is left for the next iteration. FIGURE 7 shows the Yoma legal and regulatory model.

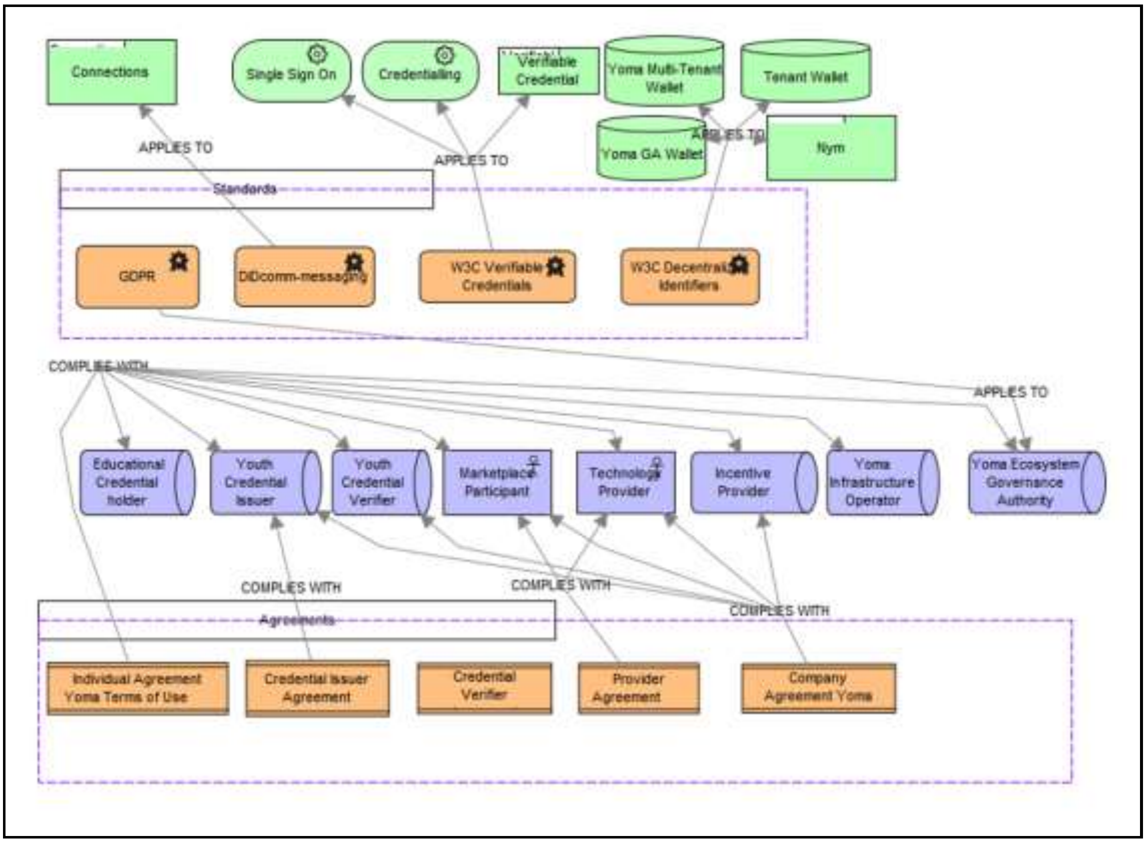

FIGURE 7 Yoma legal and regulatory Model

Yoma has five agreements. The first agreement is the individual agreement Yoma Terms of Use. It includes all details related to terms of use for the Yoma platform or Yoma resources. The second agreement is Credential Issuer Agreement. The agreement between the Youth and the Credential Issuer includes the requirements for issuing the credentials. The third agreement is the Credential Verifier Agreement. The agreement between the Youth and the credential verifier includes the requirements for the credentials verification. The fourth agreement is Provider Agreement. The agreement between the Marketplace Participant and Yoma Ecosystem Governance Authority; includes the requirements for redeeming the Zolto token with goods or services. The fifth is a Company Agreement Yoma Terms of Use. The agreement includes data about the financial obligation between the companies.

Yoma ecosystem complies with many standards. Yoma Ecosystem Governance Authority must comply with the General Data Protection Regulation(GDPR)[9]. GDPR ensures data protection in the European Union and the data transaction from European Union to other countries. It supports individual control over their own data. The second standard is DIDcomm-messaging[10]. It helps to have a secure and private connection for the DIDs.The third standard is

[9] https://gdpr.eu/

[10] https://identity.foundation/didcomm-messaging/spec/

W3C Verifiable Credentials [11]which controls the credential transaction on the network to be verified by the issuer. The fourth standard is W3C Decentralized Identifier[12]. It is a standard that controls the generation of the DID subject, DiD control, and the DID document.

5.2 Empirical Findings resulted from modeling.

Models were not the only results from the case study, but empirical findings were noticed during the modeling process. The empirical findings are summarized in TABLE 4 and described next.

TABLE 4 summary of empirical findings (EF)

Activity	Key experience
Governance framework perspective	
EF1:Uniting viewpoints	Different stakeholders have different views on the ecosystem. Modeling made different views into one united view on the GF.
EF 2:Depth of details	Deeper details create a better understanding of the governance framework and help to formulate better.
EF3:Systematic and structured base.	Governance frameworks need a systematic base to produce a comprehensive framework.
EF4:Visualization influences understandability	visualization helps to have a holistic view of the Governance Framework.
Modeling language perspective	
EF5:Reports facilitate taking a decision	Models can give details about the ecosystem elements and relationships in the form of reports.
EF6:Flexibility and the ability to Customize is a need to fit the business needs	modeling language flexibility help to cover all the aspects of the business domain and the organizations' specific requirements
EF 7:Establishing new relations	Actors' incentives need to be justified by the actors' objectives
EF8:Consider new perspectives to keep ecosystem unity	All member of any business environment has typical shared roles and responsibilities towards this environment to keep it running.

[11] https://www.w3.org/TR/vc-data-model/

[12] https://www.w3.org/TR/did-core/

First, modeling brought various stakeholders together in discussions about the governance framework because their cooperation was a need to build the models. Stakeholder groups have different perspectives on the ecosystem, and modeling helped unify their view of the governance framework.

Second, modeling helped the stakeholders to have more informative discussions about ecosystem details; they had to dig deeper into each layer and make more decisions about the ecosystem workflow. For example, in the governance model discussions, stakeholders decide the main responsibilities of each actor and their role in the ecosystem? Do they need Custodians' and Guardians' roles in the ecosystem? Furthermore, why would each actor be motivated to share in this ecosystem? Such questions helped direct the governance framework, made it more understandable for non-technical readers, and justified why the Yoma ecosystem runs this way. The Yoma project manager said, "*it helped filter out the extra bits because we were forced to specify things and answer questions.*"

Third, modeling provides a systematic, structured base for developing a governance framework. EGC's mental model provides a preliminary structure for building the model, and the stakeholders need to build over this structure. The structure requires details about each aspect. The governance model requires information about actors, roles, responsibilities, incentives, rights, and rules. The business model requires information about actors/roles who have business activities, costs, and revenue, models. The technology model requires information about the technology architecture, technology services components, and data storage. The legal and regulatory model requires information about laws, acts, regulations, agreements, and standards that actors need to comply with.

Fourth, modeling enables visualizing all the elements in the governance framework. It helped to view each layer separately and a holistic view of the whole ecosystem, enabling more understanding of the ecosystem elements and how they are connected. EGC used a color code for each layer to distinguish layers. Visualization provided a base for discussion, brainstorming, and development.

Fifth, modeling has clear and detailed information for each aspect of the ecosystem. These details could be translated into output reports. Reports provide an informative summary of the ecosystem. Reports are helpful for decision-making. The decision-maker can extract various reports about the ecosystem, individual layers, or even on a specific element of the ecosystem. It also helps people who joined the task force later to find a clear definition and description for each element. For example, the age limitation for youth was discussed in the early Yoma task force sessions. People who joined the Team later were able to find descriptive details about the age limitation and justifications for making it 16 years old and explained why the task force included the role of the Guardian in this iteration.

Sixth, EGC enables flexibility and customization. Yoma was able to customize the modeling language to fit its purposes. Ecosystems do not have to stick to the available objects only, and they create their domain objects. New stakeholders can add or remove objects and have their version of EGC. Adding new objects is not limited to the early planning phase of the project; the language could be updated at any project iteration, and elements could be added when needed. For example, Yoma added a new object (Risk) and new relationships in the second iteration. Also, New properties were added to the language in different project phases.

Seventh, EGC establish new relationships to keep the ecosystem analysis realistic. It is commonly known that incentives are an essential part of any SSI ecosystem; it reflects the motivation for each actor to participate in the ecosystem and evaluate their satisfaction with participants. It should be linked to objectives for each actor to justify provided incentives and evaluate incentives' influence on participants to achieve their objectives. For example, one of the incentives for youth participants in Yoma is earning digital tokens (ZLTO) to spend in the Yoma marketplace. Would it be enough to encourage youth to proceed with accepting new opportunities? Youth objective will answer that question. Objectives are also essential in risk modeling. Risks primarily prevent actors from achieving their objectives, leading to reduced incentives or penalties.

Eighth, EGC needs to consider new perspectives to keep the ecosystem unity. The rights, rules, responsibilities, and incentives are addressed based on the actors/ roles perspective, while in real-life ecosystems, some of the rights, rules, responsibilities, and incentives are shared among all ecosystem participants. Building trustworthiness, keeping ecosystem data privacy, and accessing the infrastructure are examples of objects that need to be shared among all actors to keep the analysis realistic

5.3 Challenges For Ecosystem Governance Compass

Although the modeling process was mainly considered to develop the Yoma-governance framework, the modeling process directed attention to new ideas for EGC value creation and development.

First, The modeling language is implemented on a licensed tool metaEdit+[13]. Any user who wants to build or access the model needs to have a paid license. Modeling and models updating are only available for specific resources that have the license; this creates time delay, complexity, and limits the utility of EGC. This disadvantage could be overcome if EGC were implemented on an open-source tool.

Second, The Essif-lab mental model [14] guided the Yoma governance framework. At some points, the modeling language mental models did not match the Essif- lab mental model. In the Essif lab, there is a distinction between actors and parties, and no separation between actors and roles, unlike the mod-

[13] https://www.metacase.com/store/

[14] https://essif-lab.github.io/framework/docs/essifLab-pattern-list

eling language. Some terms like actors have different definitions, and some concepts are not included in both models (for example, Essif focuses on 'objectives' as the primary motivator for actors, whereas the modeling language focuses on 'incentives. Understanding these differences helped to raise some key questions about the ecosystem needs and think of new ways to develop EGC to satisfy new needs.

Third, The modeling process has many details that need to be presented in two different ways: as a visual model and as a text report. In Large organizations and ecosystem of ecosystems, the number of details added to the models is massive. So, a new way for data categorization needs to be developed to avoid congested models and reports.

Fourth, The legal and regulatory model has many laws, acts, and (business, technical)standards that the ecosystem needs to follow. Top management and quality assurance teams need to have a trust assurance document indicating that different ecosystem aspects comply with the laws, acts, and standards.

6 DISCUSSION

This chapter discusses the role of modeling in developing the SSI identity governance framework and what value EGC added to the Yoma governance framework. The second section discusses the value of co-creation for EGC. The third section compares EGC to other modeling approaches.

6.1 The role of modeling in developing the SSI governance framework

The thesis used a domain-specific modeling language (EGC) developed explicitly for SSI ecosystems. The findings from that research describe how modeling made the development process of the Yoma governance framework more accessible and helped focus on the deep discussions between different stakeholder groups. The stakeholders' groups presented different views of the ecosystem working processes, motivations, expectations, and other details.

The findings show that modeling is a new technique in the governance framework development process. It is observed that modeling could fulfill the general requirements of the governance framework in Yoma's case and extend new processes to achieve these requirements and increase its efficiency level. a summary of the findings aligned with literature and the new findings that participate new findings knowledge.TABLE 5 shows the findings aligned with the literature and new findings for this research

TABLE 5 Findings aligned with literature and the new research findings

Findings aligned with the literature	**New research findings**
Uniting different viewpoints	Systematic, structured base
Depth of details	Visualization influences understandability
	Distinguishable ecosystem layers

	Support for output reports
	Flexibility and ability to customize
	Establishing new relations
	Consider a new perspective to keep ecosystem unity

According to literature and practitioners, the general requirements for a governance framework are providing guidelines, specifications, definitions, and contracts to make the governance framework clearer, usable, and more understandable (cheqd, n.d.; Sovrin Foundation, 2019a; Veiga & Eloff, 2007; Weill & Ross, 2005). The research findings approved that these findings were achieved at a more efficient level using modeling, and it shows in lessons learned :

- (EF1 [Uniting different viewpoints])The EGC provides a visual view for creating the governance framework, and all stakeholders groups are at the same level of understanding. Thus, the creators can ensure that all the stakeholders' groups are on the same level of understanding and awareness of the governance framework details.
- (EF2 [Depth of details]) modeling was helpful in decision-making related to the ecosystem. Decisions were made in the presence of various stakeholder groups as creating the models needs stakeholders' cooperation. All stakeholders groups added their views on guidelines, specifications, definitions, and contracts, making the ecosystem details deeper and more informative.

This study reveals the advantages of modeling that existing literature has not identified yet and helped create and develop the governance framework.

- Modeling provides a systematic and structured base that ensures all the needed information is included in the governance framework (EF3 [Systematic, structured base]). The systematic, structured base was not available before the modeling, and the discussion flow guided the content of the governance framework. After modeling, the details of the predefined layers are considered first. Then, the discussion details are also included in the governance framework documentation.
- Modeling provides a visual view of the ecosystem elements and relatedness (EF4 [Visualization influences understandability]). Visualization provided stakeholders and governance framework developers with a better understanding of how the ecosystem operates. Also, it assisted in distinguishing layers by using color codes that presented how ecosystem layers are interrelated and elements affect each other. Before modeling, The layer, elements, and relationships are described in the governance framework in text only. Reading a long text can confuse readers and lead to losing focus on the essential details. The difference between the texted description and models can easily be noticed in the FINDINGS chapter of this thesis. The models were presented in two different ways in Yoma

models section. It was easier to follow the ecosystem elements and relationships from the models' pictures than read the text describing them.

- Modeling provided clear and adaptable reports (EF5 [Support for output reports]). Without modeling, it was not possible to automate reports—an example of the automated output reports can be found in appendix1 page 62. Developers had to read the whole governance framework to collect the needed information about a specific operation. It is also possible to create one report about elements from different layers with their relationships. Such advantage was not accessible before modeling because each layer is described separately in the governance framework.
- Modeling language provided flexibility customization. It comes in the form of report customization and the flexibility in creating new objects to fit the business needs. Even the predefined objects could be customized by adding or removing properties. Objects can change shape or color if needed. It has been seen as an advantage of EGC as compared to most modeling languages that have predefined items (EF6 [Flexibility and ability to customize]).
- (EF7 [Establishing new relations]) EGC represents the actors/roles and their incentives in the models, but the motive behind incentives could not be understood. Modeling added that justification to the governance framework.
- Modeling provided another perspective for governance framework development (EF8 [Consider new perspectives to keep ecosystem unity]). Even stakeholders have different participation roles in the governance framework development, and they are not totally different as they have similar objectives, responsibilities, and rules. The similarities keep the ecosystem unity.

6.2 EGC value creation

Any domain-specific modeling language aims to increase business value for a specific business domain and support domain problem-solving. Also, it aims to increase productivity, improve quality, and provide economic benefits (Kelly & Tolvanen, 2008b). Modeling Yoma directs attention to the need for the development of EGC. It will help create more value for EGC to increase productivity, quality, and economic benefits.

EGC should consider replacing MetaEdit+(the modeling tool) with an open-source tool. MetaEdit+ is a licensed tool that costs 3,450 euros for the starter kit with licenses and services and 250 euros per month for additional licenses. Using an open-source tool will save money and provide an economic benefit.

The mental models for EGC should be updated to match the Essif lap mental models. Both mental models for the essif-lab [15]and EGC can deliver the same value, but the difference in naming and defining some of the objects in essif-lab mental models and EGC creates confusion for the stakeholders that decrease their productivity.

EGC should consider producing a trust assurance document to ensure that both technical and business standards are followed. In addition, EGC should do better categorization for data to avoid congested models and reports for big projects. Both the trust assurance document and a better data categorization will provide support for Ecosystem decision-makers that ensure better quality for the ecosystem.

6.3 EGC compared to other modeling approaches

Previous Software ecosystems modeling did not have uniform guidelines for the modeling process. (Handoyo, 2017). EGC provided systemization and guidelines that helped the models be accurate, informative, and uniform. At the same time, it also provides the flexibility of the details according to the business type and the customer's request.

6.3.1 EGC compared to UML

UML is a general-purpose modeling language. It does not support decision-making, automation, or object reuse. It does not upgrade the abstraction level above the concept, making it not support automation and decision making. In addition, it does not generate codes(Cranefield & Purvis, 1999; Kelly & Tolvanen, 2008a). On the other hand, EGC is an accessible language because the terminology used in the language and concepts are familiar to users. It supports automation. Generating the codes is available in EGC, and it is also an automated process that does not need any human inspection after generation. EGC highly supports decision-making; the implemented models include the project rules, vision, goals, and principles(Kolehmainen et al., To be submitted).

6.3.2 EGC compared to MDA

MDA is a general-purpose language that has the same problems as UML. It was explained in the previous section how EGC came over that issue. Another issue related to MDA is the codes are generated directly from the models. For any change in models or code maintenance, all the series of models and codes need to be refined(Kelly & Tolvanen, 2008a). EGC came over that problem. Models can copy objects from other models. Once the modeler makes changes for an

[15] https:// https://essif-lab.github.io/framework/docs/essifLab-glossary

object on a specific model, it reflects that object change on all other models using that object. Modelers do need to make an effort to refine other models, and it will not affect the code generation process(Kolehmainen et al., To be submitted).

6.3.3 EGC compared to ArchiMate

ArchiMate is developed for modeling enterprises architecture. It does not have the central SSI human vision for the models. Also, the legal and regulatory context, data storage, and cash flow are absent in the tool interface (Josey et al., 2016). ArchiMate editor window does not support code generation. All of these issues were covered on EGC. EGC has a human-centric view in all models, especially the governance model. All details go around the actors and roles. It has the human view like incentives, responsibilities, and rights. In the technical aspects, EGC provided options for data storage. In the legal and regulatory context, ArchiMate only provides contracts. Meanwhile, EGC has laws, acts, regulations, standards, and agreements(Kolehmainen et al., To be submitted).

6.3.4 EGC compared to Istar

Istart is mainly defined to model SSI ecosystems. It has two problems. First, it can give a visual model for the SSI ecosystem only and can not generates codes. (The same problem as UML and ArchiMate). The second problem is that it does not have modeling guidelines. Lack of guidelines increases the possibility of errors, loss of design pattern, missing concepts, and lack of language specification consistency(Handoyo, 2017). EGC considered those problems. It followed two types of rules to come over it. First, using language rules to ensure name uniqueness patterns, control reusability, relationships, and many rules. Second, EGC has modeling rules that regulate the domain concepts considerations in the models. The domain rules are not strict in EGC; they can be overridden if it helps implement the business better(Kelly & Tolvanen, 2008a; Kolehmainen et al., To be submitted).

7 CONCLUSION

This chapter summarizes the key findings in relation to the research scope. Also, it shows how the key findings helped answer the research question and outline the research contributions. After that, it discusses the limitations and future research related to the research process and the modeling tool.

The governance framework is a document that explains drivers, dynamics, goals, principles, legal agreements, standards, policies, values, norms, and the SSI ecosystems. Governance framework development is a problem that faces practitioners and decision-makers because it is a long document with technical details, and it is supposed to cover details related to different aspects. Developers from different backgrounds do not have the same level of understanding of the technical details, resulting in miscommunication between the stakeholders' groups. It causes a barrier to the governance framework development.

This research aimed to help practitioners and decision-makers from different backgrounds find a methodology to overcome the effort needed to develop a governance framework and solve the confusion due to various stakeholders groups' participation in the development process. The research suggested modeling to support the development process. Also, it aimed to highlight the advantages that modeling could provide to the SSI governance framework.

The key findings from this research are implementing four models(governance model, business model, technology model, and legal model) to represent the Yoma ecosystem. Also, there are many empirical findings from the modeling process like unifying the stakeholders' understanding level, adding more depth to the ecosystem details, providing a systematically structured base for the development process, distinguishing ecosystem layers and how they are interrelated, extracting reports, and provide flexibility on the customization of the report and the ecosystem elements.

The research findings exceeded the expectations from supporting the governance framework development process to developing the used modeling language(EGC). Modeling Yoma directed the attention to the need for using an open-source tool instead of Metaedit+, updating the mental models, efficient data categorization, and a trust assurance document.

7.1 Answer to the research question

This research is conducted to answer the question: what role could modeling play in developing self-sovereign identity governance framework aspects? The question could be answered that Modeling has two significant roles, a supporter of the governance framework and a developer of the governance framework:

In the first role(a supporter of the governance framework), Modeling works as a supporter to satisfy the essential requirements for the governance framework(understandability and value creation). It supports the unity of the ecosystem development teams allowing them to cooperate and exchange their thoughts about decisions. It made all stakeholders on the same level of understanding of different aspects of the ecosystem. Modeling made ecosystem development an easier task and provided more efficient results for the development process. Modeling helped SSI practitioners observe and interpret more about SSI with a decentralized human-centric paradigm that focuses on incentives. Modeling is able to create more value for the ecosystem by addressing stakeholders' objectives to evaluate the incentives' satisfaction to stakeholders.

In the second role(developer of the governance framework), Modeling provides new techniques to develop the governance framework. First, It provided a systematic base for the governance framework to build on. The systematically structured base is formed in predefined layers, and each layer includes a predefined object. Predefined layers and objects include all details that need to be addressed about the ecosystem. Second, Modeling provided visualization for the ecosystem. Visualization positively influenced the understanding of the ecosystem's stakeholders; furthermore, it provided more clarity on how the different layers of the ecosystem interact and what ecosystem elements are needed to make that interaction happen between the layers. Third, modeling facilitated decision-making by enabling report extracting. Fourth, Modeling enables flexibility and customization during the governance framework life cycle, meaning that it can reflect any new changes in the ecosystem and satisfy the need for report customization or the need for new reports.

Using the new technique provided by modeling to satisfy the requirements and enhance the development process resulted in more efficiency, understandability, and clarity of the governance framework. It makes the governance framework development more accessible, faster, and more regulated for the SSI practitioners.

7.2 Research limitation

This research has some limitations that may affect the validity of the results. One of the limitations are the discussions related to modeling are done with the Yoma task force as a group, but the notes are taken only by two members who have the license for metaEdit+(the modeling tool). To overcome that limitation , the produced models are reviewed regularly during the task force meetings to increase research validity.

Another lenition is that the research used qualitative methods and applied them to one case study(Yoma). The results reflect Yoma results only, and there is no insurance that the results are similar to other case studies. The results can not be generalized.

Using a new modeling language(Ecosystem governance compass) is another limitation. The mental models for the modeling language are explained to the Yoma task force, and training sessions are held to train the users to use the tool. The modelers' experience was only Yoma's case, and lack of experience might affect the work validity.

7.3 Future research

The thesis opens new scope for future research on the enhancement that modeling could achieve in other phases of the governance framework, like the creation and extension phase.

A new research scope related to the thesis is the development of the Ecosystem governance compass value creation, which could start from the challenges the language faced during modeling Yoma.

Another future research scope would help practitioners evaluate ecosystems development and the effectiveness of their development practices. Modeling might be helpful in tracking the weaknesses of current practices by comparing the optimal models and the current state models.

REFERENCES

Abdelhedi, F., Ait Brahim, A., Atigui, F., & Zurfluh, G. (2017). MDA-Based Approach for NoSQL Databases Modelling. In L. Bellatreche & S. Chakravarthy (Eds.), *Big Data Analytics and Knowledge Discovery* (pp. 88–102). Springer International Publishing. https://doi.org/10.1007/978-3-319-64283-3_7

Abraham, A., More, S., Rabensteiner, C., & Hörandner, F. (2020). Revocable and Offline-Verifiable Self-Sovereign Identities. *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1020–1027. https://doi.org/10.1109/TrustCom50675.2020.00136

Abraham, A., Schinnerl, C., & More, S. (2021). SSI Strong Authentication using a Mobile-phone based Identity Wallet Reaching a High Level of Assurance: *Proceedings of the 18th International Conference on Security and Cryptography*, 137–148. https://doi.org/10.5220/0010542801370148

Allen, C. (2016). *The Path to Self-Sovereign Identity*. http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html

Allen, D. W. E., & Berg, C. (2020). *Blockchain Governance: What We Can Learn From the Economics of Corporate Governance* (SSRN Scholarly Paper ID 3519564). Social Science Research Network. https://doi.org/10.2139/ssrn.3519564

Ante, L., Fischer, C., & Strehle, E. (2022). A bibliometric review of research on digital identity: Research streams, influential works and future research paths. *Journal of Manufacturing Systems*, *62*, 523–538. https://doi.org/10.1016/j.jmsy.2022.01.005

Ayaburi, E. W., & Treku, D. N. (2020). Effect of penitence on social media trust and privacy concerns: The case of Facebook. *International Journal of Information Management*, *50*, 171–181. https://doi.org/10.1016/j.ijinfomgt.2019.05.014

Barclay, I., Freytsis, M., Bucher, S., Radha, S., Preece, A., & Taylor, I. (2020). Towards a Modelling Framework for Self-Sovereign Identity Systems. *ArXiv:2009.04327 [Cs]*. http://arxiv.org/abs/2009.04327

Beck, R., Muller-Bloch, C., & King, J. L. (2018). Governance in the Blockchain Economy: A Framework and Research Agenda. *Journal of the Association for*

Information Systems, *19*(10), 1020–1034. https://doi.org/10.17705/1jais.00518

Ben Ayed, G. (2011). Digital Identity Metadata Scheme: A Technical Approach to Reduce Digital Identity Risks. *2011 IEEE Workshops of International Conference on Advanced Information Networking and Applications*, 607–612. https://doi.org/10.1109/WAINA.2011.118

Cameron, K. (2005). *The Laws of Identity*. http://myinstantid.com/laws.pdf

Cao, Y., & Yang, L. (2010). A survey of Identity Management technology. *2010 IEEE International Conference on Information Theory and Information Security*, 287–293. https://doi.org/10.1109/ICITIS.2010.5689468

cheqd. (n.d.). *Cheqd Governance Framework*. Retrieved November 1, 2021, from https://docs.cheqd.io/governance/

Costa, C., & Torres, R. (2011). To be or not to be, the importance of Digital Identity in the networked society. *Educação, Formação & Tecnologias*, *Specia*, 47–53.

Cranefield, S., & Purvis, M. (1999). *UML as an Ontology Modelling Language*. 10.

Dalpiaz, F., Franch, X., & Horkoff, J. (2016). IStar 2.0 Language Guide. *ArXiv:1605.07767 [Cs]*. http://arxiv.org/abs/1605.07767

Davie, M., Gisolfi, D., Hardman, D., Jordan, J., O'Donnell, D., & Reed, D. (2019). The Trust over IP Stack. *IEEE Communications Standards Magazine*, *3*(4), 46–51. https://doi.org/10.1109/MCOMSTD.001.1900029

Der, U., Jähnichen, S., & Sürmeli, J. (2017). Self-sovereign Identity $-$ Opportunities and Challenges for the Digital Revolution. *ArXiv:1712.01767 [Cs]*. http://arxiv.org/abs/1712.01767

Digital services. (n.d.). Valtiovarainministeriö. Retrieved February 12, 2022, from https://vm.fi/en/digital-services

Edmondson, A. C., & McManus, S. E. (2007). Methodological Fit in Management Field Research. *The Academy of Management Review*, *32*(4), 1155–1179. JSTOR. https://doi.org/10.2307/20159361

ESSIF lab. (n.d.). *ESSIF-Lab Glossary | eSSIF-Lab*. Retrieved January 15, 2022, from https://essif-lab.pages.grnet.gr/framework/framework/docs/essifLab-glossary

Feher, K. (2021). Digital identity and the online self: Footprint strategies – An exploratory and comparative research study. *Journal of Information Science*, *47*(2), 192–205. https://doi.org/10.1177/0165551519879702

France, R., & Rumpe, B. (2005). Domain specific modeling. *Software and System Modeling*, *4*, 1–3. https://doi.org/10.1007/s10270-005-0078-1

Giaglis, G. M. (2001). A Taxonomy of Business Process Modeling and Information Systems Modeling Techniques. *International Journal of Flexible Manufacturing Systems*, *13*(2), 209–228. https://doi.org/10.1023/A:1011139719773

GLEIF. (n.d.). *GLEIF and LEI News – News & Media – GLEIF*. GLEIF and LEI News - News & Media – GLEIF. Retrieved February 12, 2022, from https://www.gleif.org/en/newsroom/gleif-and-lei-news/

Handoyo, E. (2017). *Software Ecosystem Modeling*.

Hommel, W., & Reiser, H. (n.d.). *Federated Identity Management: Shortcomings of existing standards*. 4.

Hong, J.-E., & Bae, D.-H. (2000). Software modeling and analysis using a hierarchical object-oriented Petri net. *Information Sciences*, *130*(1), 133–164. https://doi.org/10.1016/S0020-0255(00)00090-6

Ishola, A. H. (2019). Identity Crisis Management and National Security. *Nigerian Journal of Social Psychology*, *2*(1). https://nigerianjsp.com/index.php/NJSP/article/view/29

Jansen, S., Handoyo, E., & Alves, C. (2015). Scientists' Needs in Modelling Software Ecosystems. *Proceedings of the 2015 European Conference on Software Architecture Workshops*, 1–6. https://doi.org/10.1145/2797433.2797479

Josey, A., Lankhorst, M., Band, I., Jonkers, H., & Quartel, D. (2016). *An Introduction to the ArchiMate® 3.0 Specification*. 20.

Juniper. (n.d.). *Self-Sovereign Identity to be a Billion-Dollar Industry by 2024, but Monetisation will Remain a Stru*. Retrieved February 15, 2022, from https://www.juniperresearch.com/press/press-releases/self-sovereign-identity-to-be-a-billion-dollar

Kärnä, J., Tolvanen, J.-P., Kelly, S., & Karna, J. (2009). *Evaluating the Use of Domain-Specific Modeling in Practice*. 8.

Kelly, S., & Tolvanen, J.-P. (2008a). *Domain-Specific Modeling: Enabling Full Code Generation*. John Wiley & Sons.

Kelly, S., & Tolvanen, J.-P. (2008b). *Domain-Specific Modeling: Enabling Full Code Generation*. John Wiley & Sons.

Kolehmainen, T., Laatikainen1, G., & Abrahamsson, P. (To be submitted). *Ecosystem Governance compass*.

Laatikainen, G., Kolehmainen, T., & Abrahamsson, P. (2021). *Self-Sovereign Identity Ecosystems: Benefits and Challenges*. Scandinavian Conference on Information Systems. https://jyx.jyu.fi/handle/123456789/77892

Laatikainen, G., Kolehmainen, T., Li, M., Hautala, M., Kettunen, A., & Abrahamsson, P. (2021a). *TOWARDS A TRUSTFUL DIGITAL WORLD: EXPLORING SELF-SOVEREIGN IDENTITY ECOSYSTEMS*. 15.

Laatikainen, G., Kolehmainen, T., Li, M., Hautala, M., Kettunen, A., & Abrahamsson, P. (2021b). Towards a trustful digital world: Exploring self-sovereign identity ecosystems. *ArXiv:2105.15131 [Cs]*. http://arxiv.org/abs/2105.15131

Lux, Z. A., Thatmann, D., Zickau, S., & Beierle, F. (2020). Distributed-Ledger-based Authentication with Decentralized Identifiers and Verifiable Credentials. *2020 2nd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS)*, 71–78. https://doi.org/10.1109/BRAINS49436.2020.9223292

Mühle, A., Grüner, A., Gayvoronskaya, T., & Meinel, C. (2018). A survey on essential components of a self-sovereign identity. *Computer Science Review, 30*, 80–86. https://doi.org/10.1016/j.cosrev.2018.10.002

Naik, N., & Jenkins, P. (2020). Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology. *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 90–95. https://doi.org/10.1109/MobileCloud48802.2020.00021

OMG standards development organization. (n.d.). *Model Driven Architecture (MDA) | Object Management Group*. Retrieved February 22, 2022, from https://www.omg.org/mda/

Pelt, R. van, Jansen, S., Baars, D., & Overbeek, S. (2020). Defining Blockchain Governance: A Framework for Analysis and Comparison. *Information Systems Management*, 1–21. https://doi.org/10.1080/10580530.2020.1720046

Rahimi, K. (2019). Digital health and the elusive quest for cost savings. *The Lancet Digital Health*, *1*(3), e108–e109. https://doi.org/10.1016/S2589-7500(19)30056-1

Schardong, F., & Custódio, R. (2021). Self-Sovereign Identity: A Systematic Map and Review. *ArXiv:2108.08338 [Cs]*. http://arxiv.org/abs/2108.08338

Schmidt, K., Mühle, A., Grüner, A., & Meinel, C. (2021). Clear the Fog: Towards a Taxonomy of Self-Sovereign Identity Ecosystem Members. *2021 18th International Conference on Privacy, Security and Trust (PST)*, 1–7. https://doi.org/10.1109/PST52912.2021.9647797

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital Identities and Verifiable Credentials. *Business & Information Systems Engineering*. https://doi.org/10.1007/s12599-021-00722-y

Sghaier Omar, A., & Basir, O. (2020). Decentralized Identifiers and Verifiable Credentials for Smartphone Anticounterfeiting and Decentralized IMEI Database. *Canadian Journal of Electrical and Computer Engineering*, *43*(3), 174–180. https://doi.org/10.1109/CJECE.2020.2970737

Shermin, V. (2017). Disrupting governance with blockchains and smart contracts. *Strategic Change*, *26*(5), 499–509. https://doi.org/10.1002/jsc.2150

Sovrin Foundation. (2019a). Composition of the Sovrin Governance Framework V2. *Sovrin Governance Framework*. https://sovrin.org/library/sovrin-governance-framework/

Sovrin Foundation. (2019b). *Sovrin-Glossary-V2.pdf*. https://sovrin.org/wp-content/uploads/Sovrin-Glossary-V2.pdf

Sporny, M., Noble, G., & Longley, D. (2019). *Verifiable Credentials Data Model 1.0*. W3.Org. https://www.w3.org/TR/vc-data-model/

Sullivan, C. (2018). Digital identity – From emergent legal concept to new reality. *Computer Law & Security Review*, *34*(4), 723–731. https://doi.org/10.1016/j.clsr.2018.05.015

Takyi, E. (2015). The Challenge of Involvement and Detachment in Participant Observation. *Qualitative Report*, *20*, 864–872. https://doi.org/10.46743/2160-3715/2015.2164

Talib, S., Clarke, N. L., & Furnell, S. M. (2010). An Analysis of Information Security Awareness within Home and Work Environments. *2010 International Conference on Availability, Reliability and Security*, 196–203. https://doi.org/10.1109/ARES.2010.27

Tolvanen, J.-P., & Rossi, M. (2003). MetaEdit+: Defining and using domain-specific modeling languages and code generators. *Companion of the 18th Annual ACM SIGPLAN Conference on Object-Oriented Programming, Systems, Languages, and Applications*, 92–93. https://doi.org/10.1145/949344.949365

Trust over IP Foundation. (n.d.). *Glossary – General Trust Over IP Terms*. Retrieved January 15, 2022, from https://trustoverip.github.io/toip/glossary.html

Trust over IP Foundation. (2020). *Introducing the Trust over IP Foundation*. Trustoverip.Org. https://trustoverip.org/wp-content/uploads/2020/05/toip_introduction_050520.pdf

Trust over IP Foundation. (N.D). *GSWG Glossary*. https://trustoverip.github.io/gswg/glossary#trust-community

Van Deursen, A., & Klint, P. (2002). Domain-Specific Language Design Requires Feature Descriptions. *Journal of Computing and Information Technology*, *10*(1), 1. https://doi.org/10.2498/cit.2002.01.01

Veiga, A. D., & Eloff, J. H. P. (2007). An Information Security Governance Framework. *Information Systems Management*, *24*(4), 361–372. https://doi.org/10.1080/10580530701586136

Wang, F., & De Filippi, P. (2020a). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, *2*, 28. https://doi.org/10.3389/fbloc.2019.00028

Wang, F., & De Filippi, P. (2020b). Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Frontiers in Blockchain*, *2*. https://doi.org/10.3389/fbloc.2019.00028

Weill, P., & Ross, J. (2005). A Matrixed Approach to Designing IT Governance. *MIT Sloan Management Review*, *46*(2), 26.

Whitley, E. A., Gal, U., & Kjaergaard, A. (2014). Who do you think you are? A review of the complex interplay between information systems, identification and identity. *European Journal of Information Systems*, *23*(1), 17–35. https://doi.org/10.1057/ejis.2013.34

Wyatt, M., Vanhaecht, J., & van Es, G. (n.d.). *The future of digital identity*. 17.

Yu, F. R., Liu, J., He, Y., Si, P., & Zhang, Y. (2018). Virtualization for Distributed Ledger Technology (vDLT). *IEEE Access*, *6*, 25019–25028. https://doi.org/10.1109/ACCESS.2018.2829141

Ziolkowski, R., Parangi, G., Miscione, G., & Schwabe, G. (2019). *Examining Gentle Rivalry: Decision-Making in Blockchain Systems*. Hawaii International Conference on System Sciences. https://doi.org/10.24251/HICSS.2019.550

APPENDIX 1

FIGURE 8 shows a full view of the Yoma ecosystem with its four aspects in one model. The model includes the governance, the business, the technology, and the legal model in one picture.

FIGURE 8 Yoma Ecosystem models

The following report is an example of an automated produced report. The report shows all the objects used in the Yoma governance model with all available details.

Yoma [GOVERNANCE]: Blockchain Governance Compass

Graph properties:

Ecosystem Name	Yoma
Container Type	GOVERNANCE
Description	

Diagram picture: Yoma [GOVERNANCE]

Graph dictionary

Object	Type of Object	Documentation
Education Opportunity Provider	Actor	_
Guardian	Actor	An Individual or Organization that acts on behalf of Youth Participants who are unable to manage their digital credentials
Jobs Opportunity Provider	Actor	_
Local Yoma Ecosystem	Actor	_
Marketplace Participant	Actor	_

Labs	Actor	-
Social Impact Organization	Actor	-
Technology Provider	Actor	-
Yoma Foundation	Actor	-
Yoma Social Enterprise	Actor	-
Youth	Actor	The user is the person who wishes to join Yoma
Building Zlto ecosystem	Incentive	-
customer acquisition	Incentive	-
Fulfillment of Yoma's purpose & mission	Incentive	-
Good reputation	Incentive	-
Grow	Incentive	Building skills and experience learning, gain knowledge Earn Zlto
Impact	Incentive	Social Credit, psycho-social benefits of Trust and confidence in yourself, recognition from others
Increase Reach of Impact mission	Incentive	-
Paid Fee	Incentive	earn Income paid for courses
Reduce the recruitment cost	Incentive	-
Skilled employee	Incentive	the Employment opportunity provider makes sure that the employees are skilled due to the trustworthiness of Yoma awarding the VCs
Thrive	Incentive	Access Jobs and employment opportunities
Actions of legal delegates	Responsibility	Responsible for the actions of their delegates
Administer and operate the infrastructure	Responsibility	-
Administer the governance framework	Responsibility	-
Arrange Yoma local operations	Responsibility	-
Build and develop Yoma plateform	Responsibility	-
Build Yoma Infrastructure	Responsibility	-
checking the VCs accuracy	Responsibility	Checking the completeness and accuracy of verified credentials that are issued when they complete challenges, e.g., if the information is incorrect
Completing and updating the digital CV	Responsibility	Completing and updating self-asserted information in their Digital CV
Completing challenges	Responsibility	Youth is responsible for completing challenges
Comply with the Governance Framework	Responsibility	Comply with the Governance Framework
Create challenges	Responsibility	-
create the impact tasks	Responsibility	-
Decide on Yoma local policies and acts	Responsibility	-
Dispute Resolution	Responsibility	-
enforce the Yoma governance framework locally	Responsibility	-
Ensure the VCs updated to Digital CV	Responsibility	-
Execute digital transactions	Responsibility	Execute digital transactions only on the instruction of the Credential Holde
Host digital wallets	Responsibility	Host digital wallets on behalf of Credential Holders
Issuing VCs for eligible Youth	Responsibility	Responsible for issuing credentials to Youth Participants that have completed challenges and managing fraud
Maintain Yoma governance framework locally	Responsibility	-
Maintain Yoma reputation	Responsibility	-
maintaining and updating the company profile	Responsibility	Responsible for maintaining their company profile
Making sure employment poli-	Responsibility	Make sure the recruitment agents are following the em-

cies followed		ployment policies as agreed with Yoma
Managing the Yoma brand	Responsibility	_
Monitor compliance with SLA's	Responsibility	_
Monitor compliance with the governance framework	Responsibility	-
notifying Incentive Provider with Zlto recipient	Responsibility	Responsible for notifying Incentive Provider to load Zlto into the Youth Wallet following the issuance of the credential
Open, transparent, and democratic governance	Responsibility	-
Provide consultation	Responsibility	_
Providing Yoma Members & Organizational Members with Technical Suppor	Responsibility	-
Removing the job offers	Responsibility	Responsible for removing the job offer when they find a candidate or they do not need that job anymore
Representing Youth legally	Responsibility	_
Reward eligible Youth	Responsibility	provide rewards that are redeemed using ZLTO
Support the VC Holders offline	Responsibility	Offline and low-tech methods for Credential Holders to trigger digital transactions or provide instruction
Update regulatory requirements	Responsibility	Keeping up to date with legal and regulatory requirements and technical standards that require incorporation in the governance framework
VCs selective disclosure	Responsibility	Youth can choose to whom to present the credential to.
Verifying the Youth VCs	Responsibility	Responsible for verifying the Youth credentials
Write Documentation associated with services provided	Responsibility	-
Yoma commercial sustainability	Responsibility	Commercial sustainability of the Yoma ecosystem, build assets in the Yoma ecosystem
VCS selective disclosure	Right	Youth can choose to whom to present the credential.
Appoint a guardian	Right	The Youth has the right to appoint a guardian to manage the wallet.
appoint delegate legal actors	Right	The right to appoint delegate individuals or organizations to act on their behalf
Cease membership	Right	Cease membership (unsubscribe from Yoma)
Cease using Yoma Infrastructure	Right	_
check ZLTO credit For Youth	Right	_
Contract with Opportunity Providers	Right	-
Contract with Social Impact Organizations	Right	-
Contract with Technology Providers	Right	-
Contracting Yoma Organizational Members	Right	Contract with Yoma Organizational Members to assign Zlto to Opportunities or Impact Tasks
Create Yoma local policies and acts	Right	-
Create, edit company profile	Right	The right to create, edit and change their company profile
enforce the Yoma governance framework	Right	-
Issuing VCs	Right	The right to issue credentials
Make use of local Yoma infrastructure	Right	-
Manage Yoma business operations	Right	-
Manage Yoma technical operations	Right	-
Organize Yoma local operations	Right	_
Post opportunities	Right	The right to post opportunities to earn credentials in the

		Yoma marketplace
post the impact tasks	Right	-
Refuse Zlto to be assigned to a task	Right	-
Remove opportunities	Right	The right to remove opportunities to earn credentials from the Yoma marketplace
Request credential issuance	Right	The user has the right to request credential issuance following completion of a challenge
Request Credential Proof before issuing Zlto	Right	-
Request proofs of qualifications on a CV	Right	-
Revoke guardianship	Right	The Youth Has the right to revoke guardianship if he is over 18. if the user is under 18, he has the right to revoke it once he/she reaches 18.
revoking VCs	Right	The right to revoke credentials
Specify youth qualification	Right	The right to specify qualification criteria for youth participants to be accepted for opportunities to earn credentials
Use Yoma Infrastructure	Right	-
Use Yoma Member Badge / Branding	Right	-
Use Yoma Member Badge on CV	Right	-
VCs issuance request	Right	Youth has the right to request credential issuance following completion of a challenge
Verify Youth VCs	Right	-
Write and change the governance framework	Right	-
Educational Credential holder	Role	The credential holder is the person who legally can use the credentials, the user himself, guardian, or a delegated person
Custodian	Role	-
Incentive Provider	Role	-
Partner	Role	-
Service Provider	Role	-
Yoma Ecosystem Governance Authority	Role	-
Yoma Infrastructure Operator	Role	-
Yoma Member	Role	-
Yoma Organizational Member	Role	-
Youth Credential Issuer	Role	-
Youth Credential Verifier	Role	-
Age constrain	Rule	Age parameters from16 to 24. It might be a verification method in the future, but it is currently open to should not be accessible to under 16's, Debate. Should parental consent be required for 16 to18-year-olds? Depending on the jurisdiction, so dependent location and local law are contextual. If required and complicated, it would have to be over 18 only. GDPR compliance. Outside normal Unicef scope. Need to see in the s/w 's and C's may specify over 18 only.
Actors & Roles	Subcontainer	
Incentives	Subcontainer	
Rights, Rules & Responsibilities	Subcontainer	