Taija Kolehmainen Maha Sroor Anssi Sorvisto Teemu Autto Petteri Palojärvi Marianna Jantunen Erika Halme Gabriella Laatikainen Pekka Abrahamsson (Eds.)

Simply Member

A human-centric digital membership solution based on Self-Sovereign Identity

Results of JYU TJTS570 Course on Blockchain in Digital Business , spring 2021

SimplyMember
a human-centric digital membership solution based on self-sovereign identity

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Startuplab JYU LabStartup

JYU AI ethics Lab

Foreword

The master-level course “Blockchain in Digital Business” is an optional, topical course at the Faculty of Information Technology, University of Jyväskylä, Finland. The objective of the course has been to provide an in-depth understanding of the fundamentals of distributed ledger technologies while critically evaluating their feasibility, benefits, and pitfalls. The course has been unique in many ways. First, besides providing tacit knowledge, a special emphasis has been made on developing essential skills needed in today's work, such as complex problem solving, critical thinking, creativity, coordination with others, judgment and decision making, and service orientation. In particular, we put theory into practice and developed a digital membership solution from a business idea to an early proof-of-concept as a collaborative effort.

Blockchains and distributed ledger technologies are related to concepts of decentralization, consensus, voting, and collaborative governance. In line with these concepts, in this course the students could choose which business idea to develop further collaboratively, they could choose between a theoretical and an empirical individual task, and they were able to select the team according to their interest in service development.

Spring 2021 has been a special time in the history of Self-Sovereign Identity. Due to the pandemic, the regulatory changes, and the increasing privacy and security concerns, the technology has been under development. While, undoubtedly, the technology may provide outstanding opportunities for human value creation, there have also been several challenges to be addressed and research gaps to fill in. Thus, in this course, we experimented co-creation in educational settings where students and teachers worked together towards the same goal. With very different, complementary skills, roles, and tasks, we have been searching for answers to research questions and untacking the value of Self-Sovereign Identity solutions in practice - together.

This book is the outcome of the six-weeks intensive course, written by the course participants and edited by the teaching team. It provides a snapshot of a special, pre-chasm phase of adopting Self-Sovereign Identity innovations. Enjoy!

Gabriella Laatikainen
Postdoctoral researcher
StartupLab, Faculty of Information Technology,
University of Jyväskylä, Finland

Contents

List of Figures

List of Tables

1 Blockchain in Digital Business 2021, Course Description

In Spring 2021, a master level course in University of Jyväskylä, Finland, developed in a collaborative effort a digital membership solution from a business idea to an early proof-of-concept: *SimplyMember – a human-centric digital membership solution based on self-sovereign identity (SSI)*. The end product aims to demonstrate how blockchain and SSI promise to shape our digital world by, for example, allowing private persons to control their own data. This book summarizes the key findings of the participants in the course.

In the following section we will introduce the course lecturers, and the mentoring team. Next, we present an agile working method that guided more than 70 people to work on the same goal. The two last sections will give floor to the course itself through participants' eyes (in a form of a blog post) and introducing the final event that wrapped up and celebrated the hard work of 6 weeks.

1.1 Lectures From Academy and Industry

Associate Prof. Juho Lindman
Director of the Blockchain Lab Sweden
University of Gothenburg

Associate Prof. Erol Kazan
IT University of Copenhagen
Denmark

Nicky Hickman
Innovation and identity specialist
United Kingdom

Ravikant Agrawal
Chief Strategy Officer
Blocksterlab, India

Markus Hautala
Head of Innovation Center & Chairman of Findy
TietoEvry, Finland

Mikko Ohtamaa
Author & entrepreneur in FinTech/blockchain
Gibraltar

Gabriella Laatikainen
Postdoctoral researcher, StartupLab
University of Jyväskylä, Finland

Prof. Pekka Abrahamsson
Professor of Information Systems and Software Engineering
University of Jyväskylä, Finland

Lecturers' topics are the following:

Gabriella Laatikainen: *Introduction to the course. Blockchain and distributed ledger technologies. ICOs as a special type of crowdfunding*

Juho Lindman: *The Uncertain Promise of Blockchain for Government*

Erol Kazan: *Value creation within blockchain systems*

Nicky Hickman: *Self-Sovereign Identity: A human and business perspective*

Marianna Jantunen and Erika Halme: *Designing ethically aligned blockchain systems and organizations: A method and an organizational model*

Mikko Ohtamaa: *Evolution of blockchains and cryptocurrencies: History and today*

Markus Hautala: *Findy – A Finnish verifiable data network for individuals, organizations, and things*

1.2 Mentoring Team

The iterative development work and collaborative decision making was overviewed by five mentors who coached and managed the work of 13 teams. In addition, there was a product manager who directed the project and product development.

Taija Kolehmainen, lead mentor and product manager, is a master's degree student in Information Systems at JYU and developes a tool for designing and governing collaborative ecosystems based on domain-specific modeling.

Anssi Sorvisto, mentor, is a master's degree student in Information Systems at JYU focusing on e.g., revenue logic and blockchain. Currently Anssi is also connected to Finnish software industry.

Petteri Palojärvi, mentor, is a Master of Science in simulation and optimization. Recently his interest has been in data analysis.

Teemu Autto, mentor, is a master's degree student in computer science at JYU advocating open source. Most recently Teemu works on Internet of Behavior and develops a code base.

Marianna Jantunen, mentor, is a doctoral researcher at JYU, studying the ethics and quality of AI systems and their development.

Erika Halme, mentor, is a doctoral researcher at JYU, studying Ethical User Stories, building an AI ethics maturity model and tools for software engineers to consider ethics in AI/S systems.

1.3 Agile Proof-of-Concept Development in Large-Scale

In the beginning of the course, participants voted for a business idea. In just six weeks the teams validated the idea of a digital membership solution based on self-sovereign identity and created a proof-of-concept to see whether it would be feasible to be commercialized.

The development process applied LeSS[1] (large-scale scrum) working methods. The LeSS framework was chosen as it allows lean and agile development in a large-scale context. Developing the SimplyMember solution involved more than 80 individuals with varying backgrounds. The framework provided principles for transparent, customer-centric, lean, and continuously improving development of the SimplyMember solution.

The proof-of-concept was developed in an iterative, incremental manner with 13 teams who worked in 1-week sprint cycles see Figure 1. Each of the cross-functional teams was responsible for developing the product and delivering in self-managing manner. Their work was supported by mentors whose responsibility was to remove obstacles and improve team capabilities. The product manager directed the project and ensured that the goals were met, and the vision stayed clear. The mentors supported the product manager in e.g., assessing the teams' performance. Additionally, the mentoring team received coaching and feedback from experienced field and topic experts to improve the product development quality.

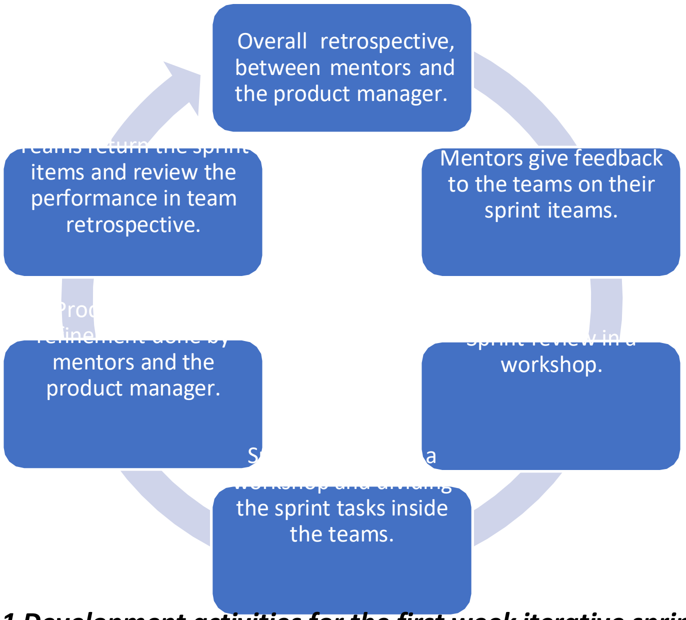

Overall retrospective, between mentors and the product manager.
Mentors give feedback to the teams on their sprint iteams.
workshop.
the sprint tasks inside the teams.
mentors and the product manager.
items and review the performance in team retrospective.

Figure 1 Development activities for the first week iterative sprint cycles

[1] https://less.works/less/framework/index

The teams and mentors participated in five remote workshops (15.3.–26.4.2021) that served as a forum for reviewing the previous sprint and planning the next one. The teams presented their work and had a chance to give and receive peer-feedbacks. Each 2-hour-long workshop included a specific lecture on a topic related to the SimplyMember solution. The participants learned about the basics of SSI technology and heard an introduction to ICOs and ERC20 tokens. In one of the workshops field expert Ravikant Agrawal from Blockster Labs presented SSI-based solutions in practice, and in the last workshop Team 3 issued verifiable credentials for one of the use cases for SimplyMember. The course participants were able to gain hands-on experience how SSI works in practice using the platform provided by the Blockster Labs.

The course followed the idea of collaborative governance, and the participants took part in making decisions over the development of the SimplyMember solution. There was a cooperative peer relationship between the teams, mentors, product manager and coaches. Valuing decentralized, self-organized coordination in a large-scale context required good communication and support for self-managing teams while providing enough boundaries and acceptance criteria to keep the vision clear. In the end, the single most important aspect was the participants' willingness to frequently reassess their work and respond to change rapidly. The 6 weeks development period required embracing agile way of thinking for everyone involved in the process the workshop schedule shown in Table 1.

	Speaker	Progress presentations
Workshop 1, 15.3.2021	Have you heard about Initial Coin Offerings? Gabriella Laatikainen	
Workshop 2, 22.3.2021	SSI ecosystems, Gabriella Laatikainen. Live demo: What are ERC20 tokens? Teemu Autto	
Workshop 3, 12.4.2021	An SSI-based solution in practice & proof-of-concept platform for SimplyMember, Ravikant Agrawal	TEAM 1: Value Creation, TEAM 3: Business Activities, TEAM 6: Token & Launching, TEAM 7: Wallet Design, TEAM 9: ICO Webmasters
Workshop 4, 19.3.2021	SimplyMember proof-of-concept. From an idea to reality! Taija Kolehmainen	TEAM 2: Value Capture, TEAM 4: Governance & Risk Identification, TEAM 12: Blockchain Legislation, TEAM 13: Project Coordinators
Workshop 5, 26.4.2021	SimplyMember in Practice. It is now possible to receive VCs for gym membership! TEAM 3 Business Activities	TEAM 5 On-Chain (Technical) Governance, TEAM 8 Marketing & Promoting, TEAM 10 User Experience, TEAM 11 Trustworthy Blockchain System

Table 1Workshop schedule and presentations for the course Blockchain in Digital Business

1.4 Team Members

The course participants formed the teams during the first workshop of the course. There were altogether 13 teams with varying responsibilities such as revising the business model (value, costs, activities), identifying risks, understanding the SSI principles, assuring the trustworthiness of the system, looking to the legal and regulatory aspects, forming a project road map, analyzing the solution functional and non-functional requirements, creating a plan for an Initial Coin Offering (ICO), creating a market strategy and so on. Team responsibilities and team members are listed in Table 2.

Team name	Team responsibility	Team members
Team 1 Value creation	The team portrayed how the value is created in the SimplyMember ecosystem by presenting the value proposition for the ecosystem. They also assessed the current market as the for base the proposition and created a market share forecast.	Daria Vaganova, Santeri Tammisto, Matilda Mäkitalo and Mabindra Rai. Responsible mentor: Taija Kolehmainen.
Team 2 Value capture	The team developed a set of suitable revenue models for the ecosystem by describing how the value could be translated into incoming money streams. They identified the customers for verifiable credentials and created optional pricing models.	Joonas Kartano, Aleksis Virtanen, Joona Tasanen, Henri Krats, Tuula Taponen and Tuukka Nyrhinen. Responsible mentor: Taija Kolehmainen.
Team 3 Business activities	The main task for the team was to identify the roles for the key actors in the ecosystem and configure the SimplyMember proof-of-concept demonstration accordingly.	Aleksi Saarinen, Mikael Mäntylä, Mikko Kyyrö, Juho Pulkkinen, Joonas Jaatinen and Milka Schüler. Responsible mentor: Anssi Sorvisto and Taija Kolehmainen.
Team 4 Governance and risk identification	The team created a risk analysis for the actors in the digital membership ecosystem. Based on that knowledge they designed ways to mitigate the identified key risks.	Saku Sikiö, Heikki Pesonen, Valtteri Siitonen, Rasmus Aumakallio and Joonas Lähde. Responsible mentor: Taija Kolehmainen.
Team 5 On-chain (technical) governance	Understanding the technical aspects of the ecosystem, the team explained the underlying technical aspects of the SimplyMember solution. They consulted the other teams on the fundamentals of blockchain and SSI and how they assure trust in SimplyMember.	Milan Bratu, Juuso Kuisma and Jaakko Saha. Responsible mentor: Teemu Autto.

Team 6 Token and launching	The team was responsible for designing blockchain-based crowd funding called Initial Coin Offering ICO. This also included creating a token strategy for the SimplyMember ecosystem.	Team members: Henrik Seppänen, Valtteri Kinnunen, Aatu Savolainen, Ilkka Itkonen, Eemil Ahonen, and Tatu Rimpiläinen. Responsible mentor: Petteri Palojärvi.
Team 7 Wallet design	Identifying the key functional requirements for the digital identity wallet was their main task. The team carried out a requirement analysis for the wallets from the holder's perspective and created an initial development plan for its technical implementation.	Jussi Kauppinen, Maha Sroor, Joose Tikkanen and Elias Päivinen. Responsible mentor: Petteri Palojärvi.
Team 8 Marketing and promoting	They created a strategic marketing plan for the early adoption phase of the project and were responsible for creating all the marketing material including a poster, a blog post, a marketing video, and social media posts. The team also created the visual brand design for SimplyMember.	Mikke Bergström, Heikki Hanhijoki, Jenny Hornborg, Ella Nissinen, Roosa Holopainen and Henrik Luostarinen. Responsible mentor: Responsible mentor: Taija Kolehmainen and Anssi Sorvisto.
Team 9 ICO webmasters	The team was responsible for designing and executing an easy-to-use website for the project's launching phase and managing the content on the site.	Md Rayhan Al Islam, Aatu Liimatainen, Sasu Ilmo, Juuso Koistinen and Panu Porki. Responsible mentor: Teemu Autto.
Team 10 User experience	Based on the findings of their conducted user research, the team collected user requirements for the solution. They collected data on user perceptions and analyzed the data into non-functional and functional requirements.	Mikael Ovaska, Ari Perälä, Tomi Tonteri and Elmeri Karnasaari. Responsible mentor: Petteri Palojärvi.
Team 11 Trustworthy blockchain system	The team considered ethical aspects of developing technological system based on the emerging technologies. They analyzed and assessed ethical, social and societal impacts of the SimplyMember solution.	Juho Koivula, Linda Holma, Siiri Lassila and Elias Laine. Responsible mentor: Marianna Jantunen and Erika Halme.
Team 12 Blockchain legislations	The role of this team was two-fold: they defined the current legal and regulatory context for the solution and next identified possibilities for expanding SimplyMember into international markets based on their chosen factors.	Kristiina Kronholm, Erno Pajala, Mayura Selvarajah, Elina Takamäki and Niko Kuokkanen. Responsible mentor: Taija Kolehmainen.

Team 13 Project coordinators	The coordinators' team created a roadmap for SimplyMember beyond the proof-of-concept stage and was managed reporting the results for the course.	Joel Holappa, Tiitus Kivikangas, Arttu Laukkanen, Anssi Pulkkinen and Joel Hiltunen. Responsible mentor: Anssi Sorvisto.

Table 2Teams responsibilities and participating members

In this course, the participants gained more than just an in-depth understanding of the fundamentals of blockchain and DLT. They put the theory in practice and validated the feasibility of the SSI technology that have potential to change the future of our digital world.

To avoid overlapping work or conflicting results, the teams worked closely together. This book especially, is the result of every team input to the service design process of SimplyMember as shown in Figure 2.

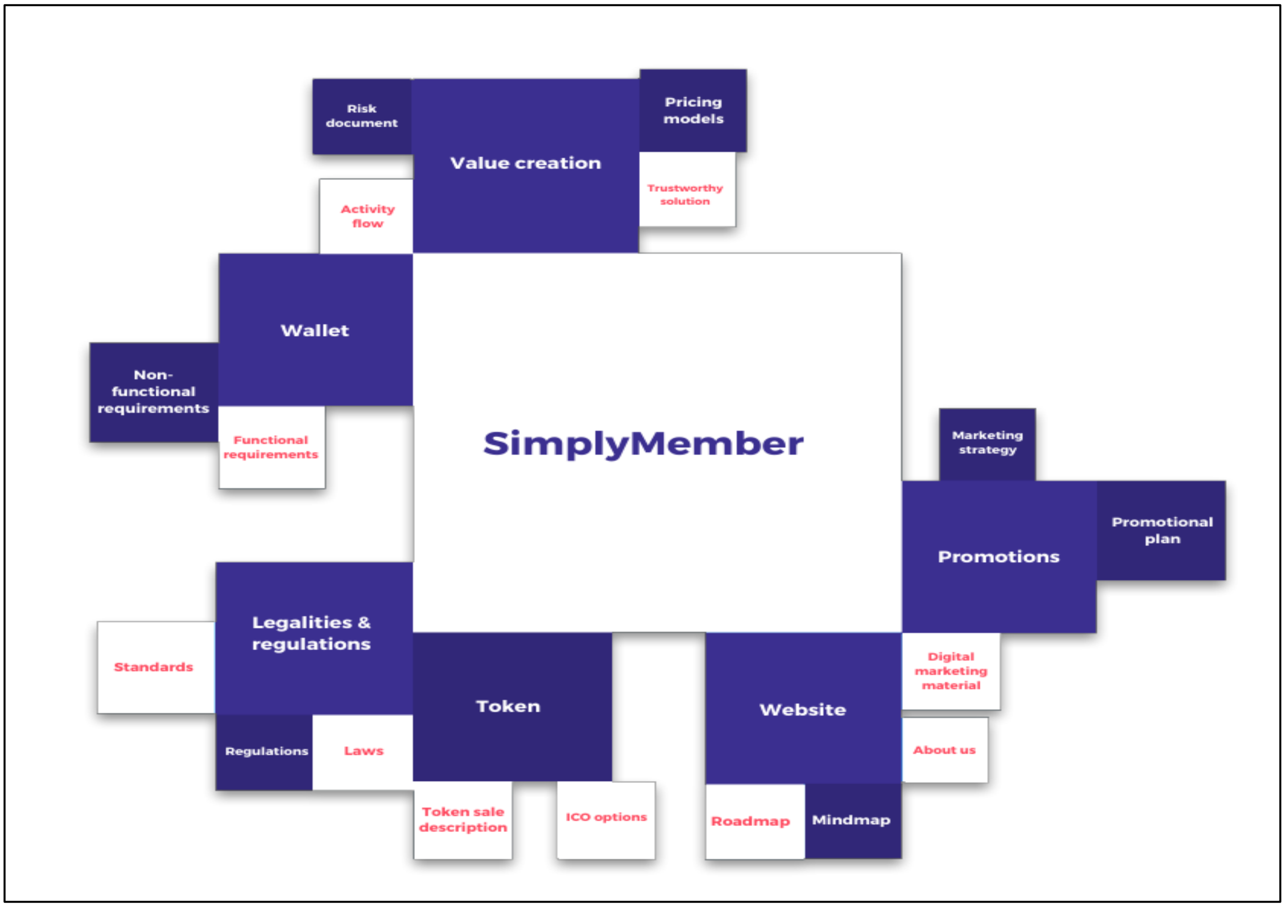


Figure 2 SimplyMember tasks as a mindmap

1.5 Blog Post: The Inaugural Course on Blockchain in Digital Business

The team responsible for marketing wrote a blog post and interviewed both the course participants, lecturers, and teachers about the course Blockchain in Digital Business.

The Inaugural Course on Blockchain in Digital Business, spring 2021 Student & Teaching Staff Perspective

The University of Jyväskylä offered an action-packed 6-week course on Blockchain in Digital Business for master's level students who are interested in blockchain technology and SSI ecosystems. Because of the ongoing COVID-19 pandemic and the consequent restrictions, the course was organized in an online format, commencing on the 15th of March 2021. An overarching theme for the course was collaboration between students and a co-creationary approach to learning and teaching.

The aim of this 5 ECTS intensive course was to give the students an understanding of blockchain and Distributed Ledger Technologies: key concepts, benefits, challenges, and practical applications. The participants also gained hands-on experience in developing an SSI-based business and launching an Initial Coin Offering. The course included both individual and team assignments and deliverables were expected on a weekly basis. There were weekly lectures and workshops but, to the delight of at least some students, no exam. The responsible teacher for the course, Gabriella Laatikainen, said that the students were given a lot of control over what they wanted to study and focus on. "*We wanted to give the students choices on many things*," said Laatikainen, "*As an example, they could vote on the business idea that we have been developing further collaboratively, they could choose between a theoretical and an empirical individual task, and they were able to choose the team according to their interest.*"

There were approximately 70 students participating in the course work. The students had the chance to put themselves in any of the 13 groups, each of which had a different task. A common goal for the groups was to develop a Proof of Concept and facilitate the ICO of the SimplyMember ecosystem, which is an SSI based universal membership card solution aiming to create an easy way to manage gym cards, bonus cards etc. The groups collaborated closely, asking each other for advice in order to make sure that everyone was on the same page at all times. Each group also had its own mentor, who provided weekly feedback and was available for meetings, if a team needed more guidance. The mentoring team consisted of Taija Kolehmainen, Anssi Sorvisto, Petteri Palojärvi, Teemu Autto, Erika Halme and Marianna Jantunen.

The teams used a special reflective learning diary concept called the scratchbook, developed by prof. Pekka Abrahamsson, to document the process of learning and discovery. These collections of charts, meeting notes, chat logs, lecture notes, screenshots etc., were more than 100 pages long and the students were encouraged to put every course related item and thought into the scratchbook. *"If it's not in the scratchbook, it doesn't exist"* was the mentality.

Many of the students brought up teamwork and learning a new technology as big motivating factors during the course. Studying something so current also brought its own challenges. *"Personally, I feel like the biggest motivating factor for this course was also one of the biggest challenges and that was the fact that I was completely unfamiliar with blockchain technology prior to this course,"* commented one student, *"It has been fun, and hard, to study a completely new technology."* Efficient and fair distribution of work between group members as well as good communication was mentioned by most of the groups. *"The workload between our team members was divided evenly and none of us were left behind or without responsibilities,"* another student said.

The groups also benefited from the expertise of multiple blockchain and SSI experts with different backgrounds. Lectures were given from all over the world by both academic researchers (Juho Lindman and Erol Kazan) and field experts (Nicky Hickman). A special role had Ravikant Agrawal, an SSI expert and an entrepreneur, who is involved in a digital identity product startup based in Pune, India. He found it exciting that SSI was taught in the University of Jyväskylä and wanted to help the students convert their acquired knowledge into a viable product. *"We offered our SSI products, CREDEBL and ADEYA, so that students could configure their use cases and touch and experience such a solution,"* said Agrawal, *"We hope that students actually realize the value from this solution development exercise and get encouraged to explore SSI stream in their future career."*

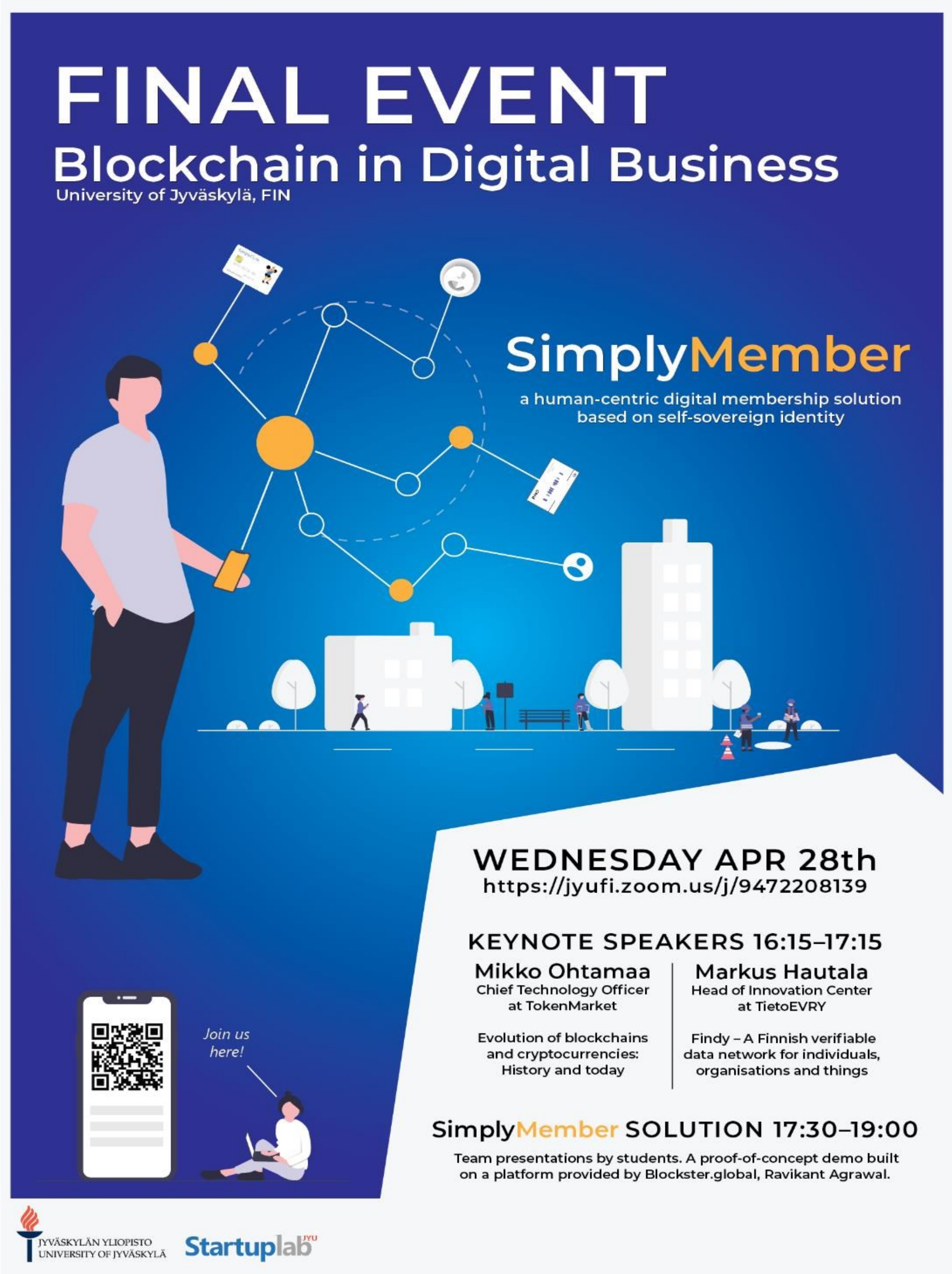
Gabriella Laatikainen, the teacher responsible for the course, emphasizes that putting the course together required a great deal of effort from a lot of people and praises the way everyone involved worked towards a common goal.

“Developing a business idea into a proof of concept requires lots of work, a great teaching team and great course participants. At this point I would like to thank everyone for the great work and effort put in this course. First of all, I would like to thank Taija Kolehmainen, who put her heart into this course, and did an excellent work in coordinating the teams and leading the workshop. Furthermore, we had the best mentoring team ever–thank you for all your effort and great job for everyone! I also would like to thank the insightful and high-quality lectures from all the lecturers, and Ravikant Agrawal for providing his insights into our service development and for the SSI platform to build our PoC on. Last but not least, we are grateful for Prof. Pekka Abrahamsson for continuous support during this course in many different ways. Finally, the greatest amount of work has been done by the students–thank you all for participating in this course and your positive attitude during this whole exciting, but sometimes challenging journey!”

The course concluded with a final event on the 28th of April, where the students presented the results of the course to the audience and visiting field experts. Mikko Ohtamaa, a decentralized finance investor and developer, and Markus Hautala, the chairman of the Findy Cooperative board, delivered keynote speeches at the event.

1.6 The Course Final Event, Wednesday April 28th 2021

How much data do you hand over for free as an exchange for bonuses or discounts? What if you could be in control over your own data? Come and see how we built a human-centric digital membership service with self-sovereign identity technology. The final event poster is shown in Figure 3.



FINAL EVENT

Blockchain in Digital Business

University of Jyväskylä, FIN

SimplyMember

a human-centric digital membership solution based on self-sovereign identity

WEDNESDAY APR 28th

https://jyufi.zoom.us/j/9472208139

KEYNOTE SPEAKERS 16:15–17:15

Mikko Ohtamaa	Markus Hautala
Chief Technology Officer at TokenMarket	Head of Innovation Center at TietoEVRY
Evolution of blockchains and cryptocurrencies: History and today	Findy – A Finnish verifiable data network for individuals, organisations and things

SimplyMember SOLUTION 17:30–19:00

Team presentations by students. A proof-of-concept demo built on a platform provided by Blockster.global, Ravikant Agrawal.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Startuplab JYU

Figure 3 Poster for the course final event in April

The final event of the Blockchain in Digital Business course offers insights on a human-centric, SSI-based digital membership solution, SimplyMember, that was built collaboratively by the course participants. The event started with keynote speeches from real field experts. First, Mikko Ohtamaa, a decentralized finance investor and developer, talked about blockchains and cryptocurrencies, and then, Markus Hautala, the chairman of the Findy Cooperative board, introduced Findy, which is the ongoing initiative for the Finnish SSI Infrastructure founded by several organizations and public institutions.

Mikko Ohtamaa: *"Evolution of blockchains and cryptocurrencies: History and today"*

Markus Hautala: *“Findy – A Finnish verifiable data network for individuals, organizations and things"*

Next each team presented their work in a three-minutes talks. The course participants introduced the audience how SimplyMember was developed collaboratively from a business idea to a proof-of-concept stage.

I What has been done in the course, where to look for more information?

Team 13 Project coordinators
Team 9 SimplyMember webmasters

II Problem & value proposition

Team 1 Value proposition – What do we offer?
Team 3 Demo of Proof of Concept

II Underlying Magic

Team 5 How SSI enables trustful digital interactions (technical aspects)

IV Pricing Model

Team 2 Alternatives for Value Capture

V Behind the scenes–value creation

Team 10 User experience key findings
Team 7 SimplyMember wallet design
Team 11 Trustworthy solution
Team 4 Risk Identification & management

VI Future plans

Team 8 Marketing and promoting SimplyMember
Team 12 Legal aspects & internationalization
Team 6 Role of a token & plan for launching an ICO

2 Introduction to SimplyMember

The emerging technologies, blockchain and self-sovereign identity (SSI), have the potential to enable trustful digital interactions in a human-centric manner. In the topical course “Blockchain in Digital Business, 2021” at University of Jyväskylä, Finland, participants gained an in-depth understanding of the technologies and put theory in practice by designing a digital membership ecosystem. In the ecosystem, trust among actors could be established in a decentralized manner and the identity holders own and are able to control their confidential data.

The solution called SimplyMember was developed from an idea to proof-of-concept in workshops in 6-weeks period. The course consisted of 70+ participants and 13 teams who developed a digital service in an iterative manner with weekly deliverables. At the beginning of the course, all teams were given tasks to familiarize themselves with relevant concepts such as SSI, distributed ledger technologies and the SimplyMember business idea. After getting teams up to date, they started working on their respective areas introduced below.

SimplyMember is currently in the early proof-of-concept stage. The demo was built using a credential platform called CREDEBL[2], and an identity wallet ADEYA[3] by Blockster[4] Global. The solution was first developed for two chosen digital membership use cases: retail membership and gym membership representing SMEs. The retail use case includes two largest retail chains in Finland, Kesko Corporation and S Group cooperative.

In this white paper, we will cover:

- The Building Blocks of an SSI-based digital membership – portraying how we create value and assure trust in the SimplyMember ecosystem while developing and ethically aligned SSI-solution.
- Competition and risks in the developing the SimplyMember solution – identifying the field that SimplyMember targets from the point of view of current competition as well as risks and their management.

[2] https://blockster.global/products/credebl/

[3] https://blockster.global/products/adeya/

[4] Blockstar Labs is the product-based startup founded in 2019 by the technocrats behind Ayan works Technology Pvt Ltd. Since its establishment, Blockster Labs specializes in emerging technologies such as blockchain and Internet of things (IoT) and others with key functional areas like data privacy and self-sovereign identity. Homepage: https://blockster.global/

- Pricing of a digital membership solution based on SSI – describing alternative ways of value capture.
- Designing an easy-to-use membership solution – introducing the requirements for frictionless user experience and how to consider the holder’s point of view in developing the solution.
- The legal and regulatory context for developing SimplyMember – analyzing the current legal and regulatory settings that determine how the proof-of-concept could be implemented.
- The marketing strategy and measuring the impact in digital membership markets – describing how we are going to penetrate the digital identity market and setting goals to the ecosystem growth.
- The roadmap to the future growth – illustrating the steps for realizing the proof-of-concept in terms of raising funds and gaining ground in the international markets.

SimplyMember

a human-centric digital membership solution
based on self-sovereign identity

3 An SSI-Based Digital Membership Solution

In this section we describe how SimplyMember creates value in the current digital identity market, and how we can assure trust in the digital membership ecosystem while developing an ethically aligned SSI-solution.

3.1 Value Proposition for SimplyMember

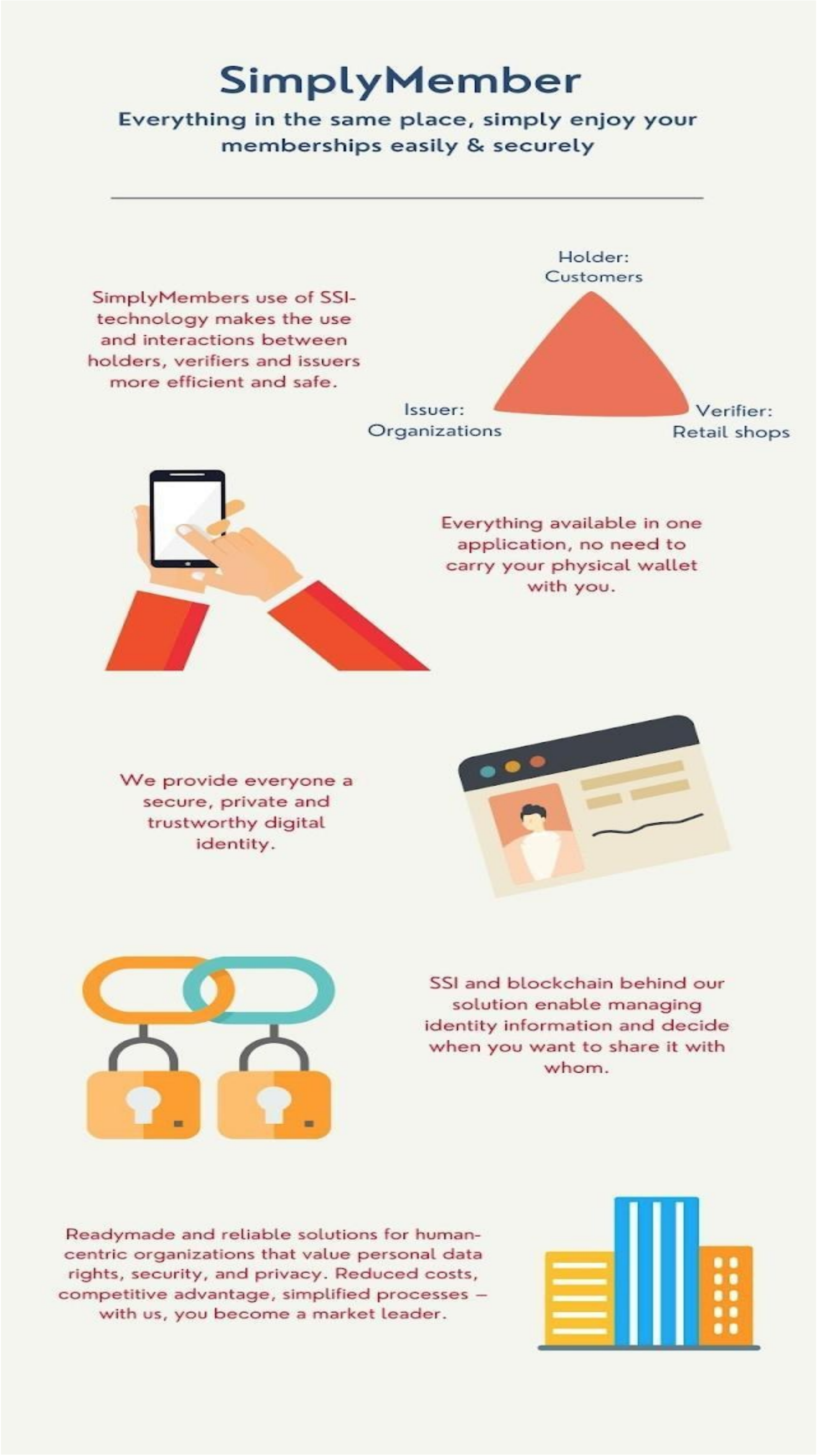
"SimplyMember. Everything in the same place, simply enjoy your memberships easily & securely."

SimplyMember provides everyone a secure, private, and trustworthy digital identity. It is a digital membership solution that is based on Self-Sovereign Identity (SSI). The solution is designing with a human-centric approach focusing on user experience and requirements as well as trustworthiness of the system. SSI and blockchain technology behind our solution enable managing identity information and decide when the user want to share it and with whom.

3.1.1 Value in the SimplyMember Solution

SimplyMember provides secure, private, and trustworthy digital identity to the holders and gives the control over data to the user in the context of digital membership. Our solution eliminates the need for wallets by decentralizing all users' memberships conveniently on one platform, securely with SSI-technology that gives users' the power to decide and control their own data. Manage and use all their memberships faster through one application without worries.

SimplyMember provides a user with a simplified SimplyMember provides a user with a simplified way to live and allows them to carry on with their daily life without worrying about managing their memberships or data security. SSI-technology behind our solution allows us to secure and decentralize data safely and transparently without third parties and gives a user an option to see and decide how and by whom their personal information is being used. SimplyMember value proposition can be seen in Figure 4.



SimplyMember

Everything in the same place, simply enjoy your memberships easily & securely

SimplyMembers use of SSI-technology makes the use and interactions between holders, verifiers and issuers more efficient and safe.

Everything available in one application, no need to carry your physical wallet with you.

We provide everyone a secure, private and trustworthy digital identity.

SSI and blockchain behind our solution enable managing identity information and decide when you want to share it with whom.

Readymade and reliable solutions for human-centric organizations that value personal data rights, security, and privacy. Reduced costs, competitive advantage, simplified processes – with us, you become a market leader.

Figure 4 SimplyMember value proposition

SimplyMember is a readymade and reliable solution for human-centric organizations that value personal data rights, security, and privacy. Reduced costs, competitive advantage, simplified processes enable organizations to become a market leader in an emerging field of digital identity. The SSI-based solution enables new innovations such as utilizing tokens for discount vouchers or data buying.

3.1.2 Value for Different Ecosystem Actors

With SimplyMember, it is important to recognize that it brings value and solves problems considering all actors, including Issuers, holders, and investors. This human-centric solution gives the data control to the one that it truly belongs to, the holder.

It is important to understand the factors that make SimplyMember better than traditional digital membership solutions. SSI enables SimplyMember to be easier and more reliable to issue, manage and present when it comes to the identity of the holder. Also, SimplyMember privacy can be seen to be higher and more secure than in traditional digital solutions and the fact that holders are in control of their own data makes a significant difference. Important factor is also that their data will not be shared with third parties. Of course, another practical benefit for a solution that provides centralization of memberships is that it makes everyday life of the holder easier. There would no longer be need for multiple cards and apps for membership programs.

If we look at the issuers and verifiers side, we can look at the cost structure. We can see that the decentralization of the core infrastructure means that costs are shared.

Also, it could be pointed out that the holder’s data security would no longer be a burden of the issuer and verifier. Due to the solution’s strong bond to identity, misuse of memberships could also be prevented with SimplyMember. Issuers may also gain competitive advantage from providing new innovative memberships solutions and acquire new customers. Verifies benefit from the simplicity of the use as holders can be verified quickly.

3.1.3 Market Analysis for SimplyMember

Digital memberships allow companies to advertise online and make people subscribe right from home via websites and landing pages.

The Current Market

More and more businesses are developing digital memberships and digital cards to make people join their communities. One of the biggest communities in Finland’s market is H&M membership that provides special offers and tailored newsletters. Being a member requires installing a mobile application but logging in online through the website is also available, though less convenient.

There are some local solutions that provide benefits for students. They are JAMKO[5] for the students of JAMK University of Applied Sciences. Frank App[6] is available to all students. Both offer many discounts, special offers, access to services, events and even gifts.

Elixia gym[7] net has digital membership offering and heavily advertises it on YouTube and Facebook.

Espresso House membership is very much like H&M. Customers have to download an application where they get and use coupons, collect loyalty points and know about new beverages, desserts and pastry products.

Market Share Forecast

The base for this market forecast is the existing size of the membership programs for the biggest companies and the amount of smartphone users in Finland. We see that the two biggest membership providers in Finland are the S Group (a Finnish retailing company. it is engaged in groceries, consumers durables, service stations, hotels, and restaurant services) and Kesko (a Finnish retailing company. It is engaged in food trade, the building and home improvement trade, and car and machinery trade) and decided to use their membership counts as the key figures for our possible market share. There are approximately 3,6 million K-Plussa card holders (K-Plussa8,) and S Group has 2,4 million customer-owners (S group, 2020).

There are some overlaps in these figures since it is very common to have both membership cards. The market share for SimplyMember could cover anywhere from 2 million to 4 million users according to these figures of S Group and Kesko. Another point of view for the market share forecast could be that 96% of Finnish population owns a smartphone which means that there are nearly 5.3 million potential users for SimplyMember (puhelinvertailu[9]) (Yli-Korhonen, 2020)It is basically impossible to cover the whole base but if SimplyMember would gain great popularity among customers perhaps it could be possible to cover around 70-80% of them. We have to take in account that part of the 5.3 million smartphone users is underage and due to this not included in our customer segment.

[5] https://kide.app/en/community/9475b554-bf26-41f8-907f-b0923ff5639a
[6] https://www.frank.fi/
[7] https://beta.elixia.fi/
[8] https://plussa.fi/
[9] https://www.puhelinvertailu.com/

If we think about gaining global market share with SimplyMember the estimations become even more challenging. According to a research by (maximize market research, 2019) the value of Global Membership Management programs was US$ 4.39 Bn in 2019 and it is expected to exponentially grow in the following years. The need for this kind of solutions is growing and the market is yet open for new companies since no one has not yet emerged as a permanent market leader. Globally there are currently around 3.8 billion smartphone users. The most ideal market areas to cover could be Europe, North America, and Asia to begin with. The developing countries are still too big of a leap.

3.2 Underlying Magic: An Ethically Aligned SSI Solution

In the following two sections we describe how the different components of Self-Sovereign Identity (SSI) ensure maintaining a secure and anonymous ecosystem. We give a short overview of SSI's key components and how its principles are applied in the SimplyMember's ecosystem. Then in the next three sections we introduce how SimplyMember is designed to be an ethically aligned SSI-solution and how we can ensure trustworthiness of the solution.

3.2.1 Trust Assurance with SSI Technology

Trust is an essential part of an SSI ecosystem. Digital identity is the representation of an entity in a specific environment or context. It consists of unique identifiers, descriptive attributes and data claims related to the system for which it is issued. For a digital identity to be trustworthy, the information provided must be verified or checked for authenticity. All of the key components enable trust, but the approach is a user-focused one in terms of identity, favoring the rights of the end-user. In SSI, the individual has full control and autonomy over their identity and its data.

SimplyMember is designed to provide a cryptographic trust. Together the issuers, holders, verifiers and DID's form the verifiable credential trust triangle by IdRamp, as shown in Figure 5. In the picture below it is shown how the verifiable credentials work. First the issuer writes a DID together with its public key to a blockchain. Secondly the issuers the issuer uses its private key to sign the credential. Thirdly the verifier requests digital proof for the credentials from the holder. At last, the verifier uses the issuer's public key to verify the credentials are valid. No matter what type of credential the triangle involves the three primary roles: Issuer, holders, and verifiers.

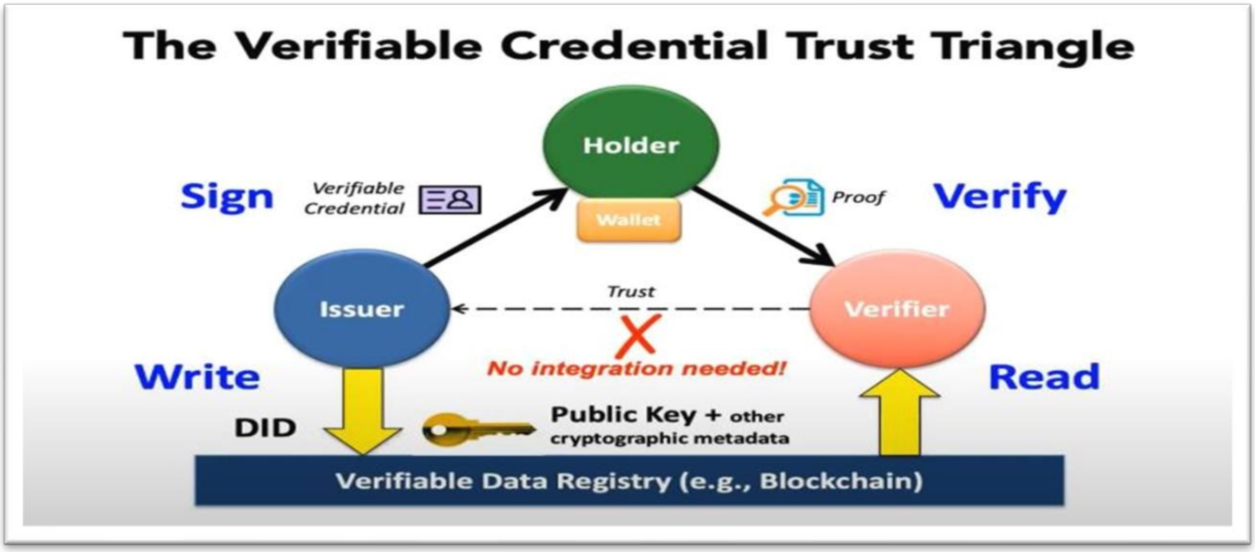

The Verifiable Credential Trust Triangle
Holder
Wallet
Sign
Verifiable Credential
Proof
Verify
Issuer
Trust
Verifier
No integration needed!
Write
Read
DID
Public Key + other cryptographic metadata
Verifiable Data Registry (e.g., Blockchain)

Figure 5: The Verifiable Credential Trust Triangle (Trust Over IP, 2020)

Decentralized Identifier (DID)

DID is a type of identifier which enables verifiable, decentralized digital identity which can identify any subject (e.g., organization, person, data model, abstract entity etc.) if the controller of the DID decided that this should be identified. This differs from federated identifiers in a sense that DIDs can be decoupled from any certificate authorities and centralized registries. DIDs are a component within larger systems such as Verifiable Credentials.

DID documents are able to express verification methods and other cryptographic material, which provides mechanisms for the DID controller in order to prove control of the DID.

DID design goals can be summarized with 10 points:

- Decentralization – Eliminating the need of centralized authorities and minimizing the risk of single point failure in identifier management.
- Control – Human and non-human entities have a direct power to control their own digital identifier without participation of external authorities.
- Privacy – Entities control the privacy of their information
- Security – Entities that depend on DID documents have sufficient security.
- Proof-based – DID controllers have the possibility to provide cryptographic proof when interacting with other entities.
- Discoverability – Entities have possibility to discover DIDs for other entities

- Interoperability – DID infrastructure can use existing tools and software libraries
- Portability – DIDs should be independent from systems and networks allowing entities to use their digital identifier with any supporting system
- Simplicity – Technology is easier to understand, implement and deploy due to reduced set of simple features
- Extensibility – Provided when it does not hinder interoperability, portability, or simplicity.

Verifiable Credentials

Verifiable Credentials are a technological counterpart to physical credentials, and they can represent all the same information, such as:

- Information identifying the subject (photo, name, ID-number)
- Information issuing authority (national agency, certification body)
- Information related to the type of credential (driver's license, passport, insurance card)
- Information about specific attributes or properties (classes of vehicle entitled to drive, date of birth)
- Information about constraints of the credential (expiration date, terms of use)

Addition of technologies, such as digital signatures to what is mentioned above grants verifiable credentials more security against tampering against their physical counterparts. Entities that hold verifiable credentials can generate verifiable presentations and share these with verifiers, which works as a proof that they possess the presented credentials with their characteristics. Transporting these presentations is fast, making it much more convenient to establish trust from a distance, compared to the physical counterparts.

Verifiable Claims

A verifiable claim, VC, is a machine-readable statement made by an entity that is cryptographically authentic and verified by a 3rd party. These can be e.g., banking account information, education qualifications, healthcare data etc. The strength of claims is dependable on the degree of trust between verifier and issuer.

Public Key Infrastructure (PKI)

PKI consists of a set of roles, policies, hardware, and software needed to create, manage and use digital certificates and manage public-key encryption with the purpose of facilitating secure electronic transfer of information for a range of network activities. PKI can be considered as a more secure authentication method than simple passwords.

PKI system requires certificate authorities (CA) as their root of trust. PKI system works in a way that an owner of a private key (e.g., a website) gives their public key to a CA who can sign it with their own private key and issue a public key certificate. When using this website, the browser checks this certificate with every connection and this is how the user knows that they are connected to a website with encrypted HTTPS connection, meaning that the website is exactly what it claims to be.

Main problem with the PKI system is that it is centralized. Inserting a third party (CA) to the digital trust infrastructure is a security risk. If the CA makes a humane mistake or their service becomes unavailable for one reason or another, the whole system is in danger of falling apart.

Zero Knowledge Pool (ZKP)

Method allowing to prove to another party about having a certain piece of knowledge without revealing what that knowledge is. In the cave door analogy this is shown as a circular cave with one exit. In the back of the cave is a door which is locked with a keypad code, meaning that if one would want to walk around the cave and return to the cave entrance, they must know the code for the keypad. If two people enter the cave and one of them walks around the cave, they have proven that they know the code for the door, without revealing the code itself.

In blockchains this similar method can be used when agreeing upon money transactions between two actors. For this transaction to happen, the blockchain needs to be able determine if the one paying this transaction has in fact enough money to send, without knowing who the user is and how much money they exactly have.

These components grant multiple tools for maintaining secure and anonymous ecosystems enabling network members to pick and choose the amount of information they are willing to share. For example, should some service require some specific credentials in order to accept participants, verifiable credentials grant an opportunity to send only relevant parts of a user’s credential information. This is a huge advantage compared to physical credentials, considering that with physical credentials it is basically with “all or nothing” principle. For example, let's consider a truck rental system, where you would need to prove that you are certified to operate the selected vehicle. Presenting your driver’s license gives this information, but it also tells your name, picture, social security number etc. whereas with an electronic verifiable credential you could send only the relevant information.

Only problematic part of these tools is the Public Key Infrastructure (PKI) which is in direct conflict with the SSI principle of decentralization. As stated in sovrin.org *"An SSI ecosystem shall not require reliance on a centralized system to represent, control, or verify an entity's digital identity data."* This problem is solvable with decentralized public key infrastructures (DPKI), where every identity is controlled not by a trusted third-party, but by its principal owner.

In the SimplyMember idea these tools can be utilized in at least following ways:

- Platform providers work as DID Controllers
- Payment of subscription fees to the customer organizations can be ensured with ZKP method
    - The system ensures that the End Users have sufficient funds to pay for the services they require, without telling the Customer Organizations their names or information about their financial situation as a whole
    - This also ensures that members who do not have sufficient funds aren't able to purchase services they cannot afford during that time
- All the membership information and credentials can be stored within Verifiable Credentials
    - Most membership-based services require information about some credentials (age, membership status etc.) but with Verifiable Credentials it is possible to only present the relevant credentials

3.2.2 Principles of SSI in the SimplyMember Ecosystem

We list the foundational principles of SSI in Table 3 SSI principles in SimplyMember context. These principles are part of the digital identity ecosystem governance framework of SimplyMember. We give a global description of the principles followed by a description of how the principle is applied to the SimplyMember solution.

PRINCIPLES OF SSI	DESCRIPTION	SIMPLYMEMBER
Representation	The SSI-ecosystem should provide the means for any entity (human, legal, natural, physical, digital) to be represented by any number of digital identities.	Customers (entities) can have multiple digital identities as they are able to have multiple memberships in different services
Interoperability	SSI-ecosystem enables digital identity data for an entity to be represented, exchanged, secured, protected, and verified interoperability using open, public, and royalty-free standards	This overlaps with portability and is similarly achieved with the app
Decentralization	The ecosystem does not rely on a centralized system to represent, control, or verify an entity's digital identity data	End users' data is not shared to third parties

Control & Agency	Identity rights holders have the power to control usage of their digital identity data and exert this control by employing and/or delegating to agents and guardians of their choice, including individuals, organizations, devices, and software	Is there a possibility for the customers to prevent their data being used for e.g., market research or marketing etc.? Customers have access to their own data via app
Participation	Participation is not required from identity rights holders	Customers are not required to participate in any manner
Equity and Inclusion	SSI ecosystem shall not exclude or discriminate against identity rights holders within its governance scope	Identity rights holders are not discriminated
Usability, Accessibility and Consistency	SSI ecosystem shall maximize usability and accessibility of agents and other SSI components for identity rights holders	SimplyMember aims for maximum usability and accessibility
Portability	Identity rights holders have the ability to move or transfer a copy of their digital identity data to the agents or systems of their choice	All the required information can be presented within an app
Security	Identity rights holders have the power to secure their digital identity data at rest and in motion, to control their own identifiers and encryption keys and to employ end-to-end encryptions for all interactions	Customers are in control of their own data and decide with who their data is shared.
Verifiability and Authenticity	Identity rights holders have the power to provide verifiable proof of the authenticity of their digital identity data	SimplyMember's solution uses verifiable credentials.
Privacy and Minimal Disclosure	Identity rights holders have the power to protect the privacy of their digital identity data and to share the minimum digital identity data required for any particular interaction	The data shared is always only the required minimal data, e.g., when participating in age restricted event, age is the only information presented (ZKP)
Transparency	Identity rights holders have the power to access and verify information necessary to understand the incentives, rules, policies and algorithms under which agents and other components of SSI ecosystems operate	Is there a possibility for customers/members to receive this information?

Table 3 SSI principles in SimplyMember context

3.2.3 Developing an Ethically Aligned Solution

We used a method called ECCOLA to support our work on potential ethical issues in a digital identity system that is based on SSI and blockchain and is supposed to have less decision-making by human on-chain. Finally, we form requirements for the trustworthy SimplyMember solution.

Introduction to ECCOLA Method

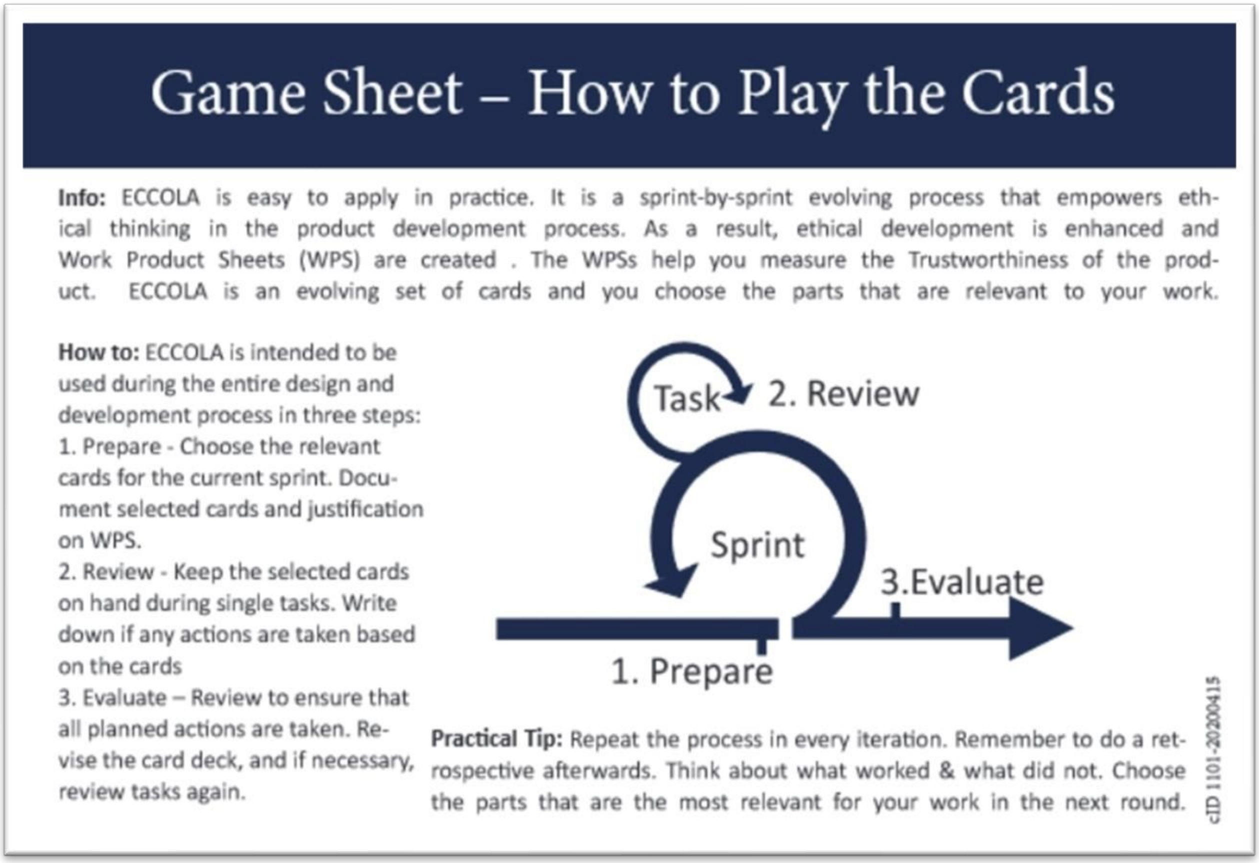
In our project we have used ECCOLA: a Method for Implementing Ethically Aligned AI Systems, developed in the University of Jyväskylä, Finland. ECCOLA aims to help organizations develop more ethical AI systems by providing tools for developers to implement AI ethics in a practical manner. The method has been developed iteratively with a cyclical action design research approach (Vakkuri et al., 2020).

In practice, ECCOLA is a deck of 21 cards that are split into 8 themes with 1-6 cards in each theme. The themes are AI ethics themes that are found in different ethical guidelines, for example fairness and transparency. Each card then deals with a more specific aspect of the theme, such as accessibility or communication.

Each individual card is divided to three parts:

- Motivation – why is this topic important
- What to do – how to resolve the issue?
- A practical example – to make the issue more tangible

In addition to the cards there is also a game sheet that explains how to use the ECCOLA method.



Game Sheet – How to Play the Cards

Info: ECCOLA is easy to apply in practice. It is a sprint-by-sprint evolving process that empowers ethical thinking in the product development process. As a result, ethical development is enhanced and Work Product Sheets (WPS) are created . The WPSs help you measure the Trustworthiness of the product. ECCOLA is an evolving set of cards and you choose the parts that are relevant to your work.

How to: ECCOLA is intended to be used during the entire design and development process in three steps:
1. Prepare - Choose the relevant cards for the current sprint. Document selected cards and justification on WPS.
2. Review - Keep the selected cards on hand during single tasks. Write down if any actions are taken based on the cards
3. Evaluate – Review to ensure that all planned actions are taken. Revise the card deck, and if necessary, review tasks again.

Practical Tip: Repeat the process in every iteration. Remember to do a retrospective afterwards. Think about what worked & what did not. Choose the parts that are the most relevant for your work in the next round.

cID 1101-20200415

Figure 6 ECCOLA method

The ECCOLA works well in the forethought of potential ethical issues in blockchain-related systems that are supposed to have less decision-making by human on-chain. When in the creative and innovative phase ECCOLA method gives food for thought on ethical issues but it works afterward also when making changes to the system. Cards help to encounter a lot of blind spots ethically wise. ECCOLA Method can be shown in Figure 6.

People working in the department of trustworthiness do not need to be ethics experts. They do not have to think of Kantian imperatives, but they can involve themselves directly in blockchain-related system planning with help of this ethically aligned method. Method helps to think of many perspectives that stakeholders could expect from this blockchain-related system. These perspectives include for example, data privacy, system safety, accountability issues and possible impacts on environment and society.

Working with the ECCOLA Cards

We had two sessions with our team mentors: one a workshop with a tutorial to see how the cards are meant to be used in action and another one choosing the cards for our project. We chose thirteen cards: Types of Transparency, Communication, Traceability, System Reliability, Privacy and Data, Access to Data, System Safety, Accessibility, Stakeholder Participation, Societal Effects, Auditability, and Ability to Redress and Minimizing Negative Impacts. The rest of the cards were discarded mainly because most of them did not seem relevant to a project that was not concerned with artificial intelligence.

We worked on and reviewed the cards from an ethical perspective but also had trustworthiness of the system in mind. Our focus was especially on non-functional requirements. Based on our work and reviewed work of other teams we formed four categories for trustworthy system requirements: 1. Transparency, 2. Data & Safety, 3. Fairness & Wellbeing and 4. Accountability. Then we added our findings based on our work with the cards to applicable themes.

3.2.4 Trustworthy System Requirements

Transparency

- Reasons behind decision making to stakeholders and end-users
- Documentation of code and progress
- Open communication of successes and failures
- Clear and concise communication for stakeholders about the essential features, purposes, benefits, costs, data collection, partners, changes, and appliances
- Account for potential vulnerabilities and threats via multiple scenario generation

Summary: Document code & progress, Communicate relevancies to stakeholders, Account for vulnerabilities and threats.

Data and Safety

- Have a data privacy and protection policy
- Inform users of the data policies (who, what, how, why)
- Take steps to ensure data privacy (e.g., encryption)
- Make sure that the data regulations and laws concerning the company (e.g., GDPR) are followed
- Take steps to ensure that only the right people have access to the data
- Keep log of who accesses the data.
- Follow information security standards and make continuous risk assessments

Summary: Form a data privacy and protection policy, follow regulations and laws on data, Relevant access to data, Record accesses, Assess risks

Fairness & Wellbeing

- Assess the environmental impact of the system as a whole, from development to use
- Consider the environmental impact when choosing technical solutions
- Take measures to reduce the environmental impact of the system
- Make sure that stakeholders are not in unfair positions and that there are no unethical trade-offs in commercialization of end-user or user data.
- Discuss: Whom is the system for? Who benefits the most and on whose cost? Do the users have higher priority?
- Make an analysis of potential end-user groups
- Account for possible downside of unequal access to SimplyMember application
- Make sure that application is not discriminatory against people with disabilities. If it is, how would it be countered?
- Involve stakeholders in the system development process
- Assess the societal impact of the system.

Summary: Assess environmental impact, Assess the societal impact, ensure equal priority between stakeholders, analyze potential end-user groups, Account for unequal accesses, Involve stakeholders in development.

Accountability

- Consider if the system is auditable
- Follow financial laws
- Have an audit mechanism in place
- Have a redress plan
- Inform the stakeholders of the redress plan
- Follow laws concerning redress such as consumer protection rights acts
- Renew the stakeholder analysis when considering any improvements or changes
- Check that the risk-analysis is not out-of-date
- Make re-evaluations when there are changes to laws and regulations that are in force or when new laws or regulations are introduced
- Consider ways how stakeholders can inform about possible threats
- Have a dialogue with relevant stakeholders about possible ethical issues. F. ex., end-users must know if their data is collected

Summary: Ensure auditability, follow laws and regulations, have a redress plan, renew stakeholder analysis and risk-analysis periodically, inform stakeholders of possible threats, Inform end-users on ethical questions.

3.2.5 Implementing the Trustworthiness in SimplyMember

The issues concerning data privacy and access in the SimplyMember solution are not the most pressing ones because of the technology with which the system is being developed such as Verifiable Credentials. SSI and blockchain guarantees that the end-user is in control of most of the data concerning them, and that they regulate who can access the data and when. And ensure that when it is accessed, only the relevant information is shown. However, no system is foolproof, as was displayed by one user's concern of losing their phone in the interview conducted by group 10, so of course these matters still need to be paid attention to and to ensure that no one's identity is compromised and ends up in the wrong hands, especially as it is a big concern for potential users as per group 10's findings.

In addition to that communication with end-users can heighten the adoption of new technology when they have understood well all significant and relevant information provided by SimplyMember. Also, open communication of failures and success make a good reputation to the system and its developers. Clear and concise communication for stakeholders about the essential features, purposes, benefits, costs, data collection, partners and appliances of the system is essential for transparency and comprehension.

There's also the fact the system uses customer registries from many retail stores, gyms, libraries, universities, etc. For example, the biggest grocery stores in Finland, S Group and Kesko, have their own memberships and according to their data protection policies, they collect personal information such as names, addresses, phone numbers, emails, dates of birth, gender, language preference, permissions given, customer interactions such as feedback or customer service calls, digital service use, data collected via cookies, information about targeted marketing and information about the membership and the card, such as expiration dates, and card use, such as what groceries the customer has bought from K-Plussa[10]. S Group also collects information about the family members of their customers if the customer has signed up for a shared membership(S group, 2019). Another example of the information various services collect is Keski-kirjastot (libraries of Central Finland), that collects usernames, emails, names, card number and pin code, and home library (Keski-kirjastot, 2021).

[10] https://plussa.fi/

From the examples, we can see that the participants in the system collect various levels of personal information. The question would be if these stakeholders would still collect this data on the new system or if they would remain in control of it, outside the system. Some personal data such as names, usernames or addresses etc. would be collected by SSI for the purpose of verification.

Another aspect that could be considered is the end-user's willingness to control their own data. Would the appeal of being in control of their own data be enough, or would people still have no enthusiasm for it? If not, would some sort of data controllers be necessary as is the case in some developing countries where the level of technology and technical knowledge is not high enough (Wang & De Filippi, 2020).

The matter of environmental impact has to be given some thought when developing the system as mining in a blockchain can consume much energy, depending on how it is executed. This is important not only for the sake of the environment and the people who are harmed when the climate crisis gets worse but also it is smart from an economic point of view because consumers nowadays pay more attention to the sustainability of their services/products.

Ability to redress and possibility for auditability are important to be present for the sake of the trustworthiness of the system and for making certain the system follows regulations and financial and consumer protection laws. As Team 12 has made notice of the unrelatedness of blockchain, it is important to stay on forefront as an SSI service provider to keep compliance risks at minimum. As Team 4 has identified many types of risk, it is high priority to ensure trustworthiness of the system by assessing and identifying threatening unknowns. "Ecosystem risks, verifier risks, holder risks, issuer risks, provider risks" have to be accounted for. Account for potential vulnerabilities and threats via multiple scenario generation periodically. When threats and vulnerabilities are made aware, it is good to communicate to reduce risks in the ecosystem.

With periodical threat and vulnerability assessment potential issues are known to self. Make that known to stakeholders. Ethical value creation and business model ensures trustworthiness. Seek foresight about future impact on environmental and societal level. Let no trade-offs be made on detriment of stakeholders. With legality, transparent communication and redressability accountability is ensured. In SSI trustworthiness is a valuable asset.

4 Competitive Analysis and Risks

In this section we identify the competitive field that SimplyMember targets and the key risks and their management for our solution. We conducted an initial analysis that identifies our major competitors and their products as well as marketing strategies. Next, we describe the results of our study on key risks that could negatively affect developing an SSI solution. Our risk assessment also includes managing and mitigating the risks.

4.1 Competitive Analysis

Are there any other SSI-based solutions for digital membership already in the global market? Who are the SimplyMember's competitors? What kind of services do they offer? What are the key strengths of the competitors?

With the introduction of the self-sovereign identity (SSI) technology, different companies are investing their time and resources to build digital wallets to store different kinds of identity-related data that is more secure and trustworthy.

SimplyMember is a membership card with SSI-based solutions and which focus is to integrate different companies' membership into applications such as S-Etukortti by S Group, K-Plussa by Kesko and membership programs offered by SMEs, such as gym membership cards. There are different kinds of membership applications available all over the world, but SSI-based solutions are very few. Most of the platforms focus on creating the digital identification wallets only few platforms focus on integrating different companies' membership or integrating similar kinds of company's membership. Since, SimplyMember is trying to integrate companies' membership into one platform using SSI based solutions and there are direct and indirect competitors globally for the SimplyMember.

4.1.1 Digital Membership Applications

There are very few platforms which are very similar to the idea of SimplyMember which helps to access the traditional membership cards through the mobile applications and store bonus, points system for shopping, card used, etc. These applications are listed below:

- Key ring [11]: This platform integrates loyalty cards like library cards and different stores such as Walmart, Target, CVS, Walgreens, Michaels, and more. Using this platform, customers can easily get the score bonus, coupons, manage shopping lists, etc. and backed up that information in the cloud. There are some features such as barcode scanner, weekly bonus and coupons can be accessed, loyalty card database, sharing loyalty cards, shopping lists among family members and friends, alert on new sales and bonus from the stores and so on.
- Stocard[12] : This platform helps to store all membership cards in one platform by scanning the barcode from the physical card and then store all the bonus and rewards in the Stocard application that customers receive by shopping from the stores. This application also helps to collect bonus from different stores in one application, show the received bonus from the stores, also alert any kind of offers, catalogues form similar products from different stores, and even show the different stores locations that are associated with the Stocard.
- LoyalMerchant[13]: This is a blockchain-based customer loyalty platform that is used to collect and store bonus and rewards from different stores in the form of LCredits and customers can use those LCredits to buy or exchange another product.

Moreover, these applications involve both companies and individuals' customers where companies can track their sales activities and bonus given to their customers, update information regarding store's discounts, coupons, and rewards through these platforms to their loyal customers and even market their membership campaigns to people using those platforms. For individual customers they can keep track of their buying activities, store bonus received from the shopping at different stores, and easy access of information about products discounts, catalogues from different stores and even share their shopping lists. The customers use these platforms to sell their data and even get the membership from the different stores. These platforms even have some additional features such as providing store locations, catalogues from different stores, sharing shopping lists among family and friends and so on which SimplyMember platform is not focused on developing at this initial phase.

[11] https://keyringapp.com/gdpr/

[12] https://stocardapp.com/en/de

[13] https://play.google.com/store/apps/details?id=com.appsolutely.aps&hl=en_AU

4.1.2 Digital Membership Platform

These platforms are at their initial stage of integrating different companies' membership into one platform and need some more improvement to work effectively.

The following are some of the direct competitors in the global market. Some of the indirect competitors in the global market for SimplyMember do not have a similar approach but they have developed platforms that either integrate different gym memberships into one platform or they have a platform that helps to store the customers information and use those platforms for membership management. These platforms manage different gym membership, or any kind of membership integrated into one platform. These platforms help companies to add, renew, upgrade, communicate and coordinate with members, track member's activities, and so on. Also, customers can integrate different company's membership into one platform which helps them to access easily using the same platform and store their bonus, rewards, or coupons from different companies into one platform.

Most of these platforms are open-source software, software as a service (SaaS), web-based, etc. based platforms but not SSI based solutions in the global market. These platforms are partially based on the ideas that SimplyMember is trying to develop and use different technology to develop these platforms.

The list of the platforms is:

- GYM Master https://www.gymmaster.com/
- My Member Software https://www.mymembersoftware.com/
- Glofox https://www.glofox.com/
- Aluminati https://www.aluminati.net/
- Maonrails https://www.maonrails.com/
- Raklet https://hello.raklet.com/
- Admidio https://www.admidio.org/
- Wild apricot https://www.wildapricot.com/
- Member planet https://www.memberplanet.com/
- Tendenci https://www.tendenci.com/
- Clubmaster https://www.clubmaster.org/

4.1.3 SSI-Based Solutions

There are some SSI-based platforms and other technology-based platforms that are developed to store digital identities of the people and these platforms can be identified as indirect competitors of the SimplyMember. These platforms are working to build more secure, reliable, and trusted digital wallets that help users to access their digital credentials easily through digital wallets.

- T-systems and multimedia solutions https://german-blockchain-ecosystem.t-systems-mms.com/en/hom
- Sovrin https://sovrin.org/
- Connect.me https://connect.me/
- Thales https://www.thalesgroup.com/en

These digital wallets are indirect competitors in such a way that customer information is already stored in the digital wallets and these platforms can add features like storing membership information of company and customers into digital wallets which is the main idea of the SimplyMember.

There are some companies like Tieto, Fujitsu who are working to develop SSI based digital wallets which could be indirect competitors for the SimplyMember in Finland. The target market for the SimplyMember platform is Finland so the SimplyMember direct competitors are the individual applications that companies such as S Group, Kesko and different SMEs' own membership application.

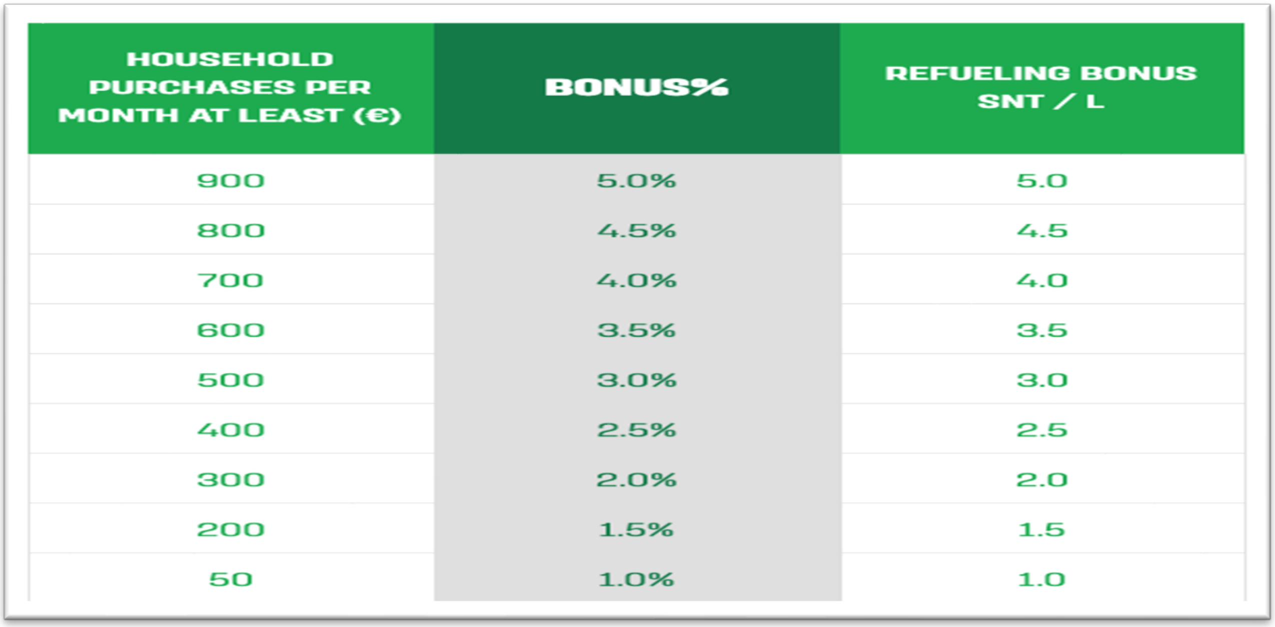
Use Case 1: Retail Memberships

The well-known green S Group membership card S-Etukortti is used to collect bonus and discount while shopping form the S Group associated stores like Alepa, Prisma, S-Market, S-Rauta, etc. and even in some restaurants, cafes and hotels that are associated with S Group as shown in Figure 7. The membership cards help to get 5% worth of the monthly purchase made by the customers and encourage members to use the cards even during small purchases. The bonus is made monthly and stored in member's account and designed for the benefits payments.

Figure 7 The S Group stores and associated business partners

The customers cannot get bonus for everything the buy or paid at stores, restaurants, and hotels the products which does not work get bonuses are invoices purchases, payment with company business card, brokerage sales such as lottery sales and tickets, beverage which is above 1.2% of alcohol, any tobacco related products or substitutes, tax-free purchase, recharging the travel cards at stores, refunds on bottle deposit and buying gift cards from the stores. After the bonuses are stored in the account of the customer then they stay until customer exchange or use it to make other purchases. The customers can track the bonus by using S-mobile phone applications which work with the bank's IDs credentials for IOS and Google Android phones and even access bonus information through S-bank's online service.

The bonus paid information is provided to customers through email. The bonuses are calculated based on the purchase made by the customers and below there is a table shown in Figure 8 which shows how much customers can get paid back on their purchase on the monthly basis.



HOUSEHOLD PURCHASES PER MONTH AT LEAST (€)	BONUS%	REFUELING BONUS SNT / L
900	5.0%	5.0
800	4.5%	4.5
700	4.0%	4.0
600	3.5%	3.5
500	3.0%	3.0
400	2.5%	2.5
300	2.0%	2.0
200	1.5%	1.5
50	1.0%	1.0

Figure 8 The S Group bonus returns to customers based on their purchase

Kesko's membership card (K-Plussa): This is also a membership card for the K Group which gives rewards for their customers while making purchase from their numbers of associates business with the K Group such as retail stores like K-Market, K-Citymarket, etc., restaurants, spas, and hotels. The maximum bonus percentage that customers can gain from their purchase is the same as the S Group. The customers can also gain rewards while renting cars, subscriptions of magazines, movies, and insurances. The customers' bonuses are stored in the Plussa accounts in the form of the points which are used as Plussa money, collected through purchases made from K Group business's partners.

The Plussa money information can be accessed by the customers through in-store payments terminals after making the payment for the purchase, by logging into Kesko's member site at www.plussa.com, Plussa statement provided by K-Plussa, K-Food mobile application, and through email from K Group with Plussa money information. Below there are the lists of the main K Group stores and business partners where customers can gain Plussa points through their purchases as shown in Figure 9

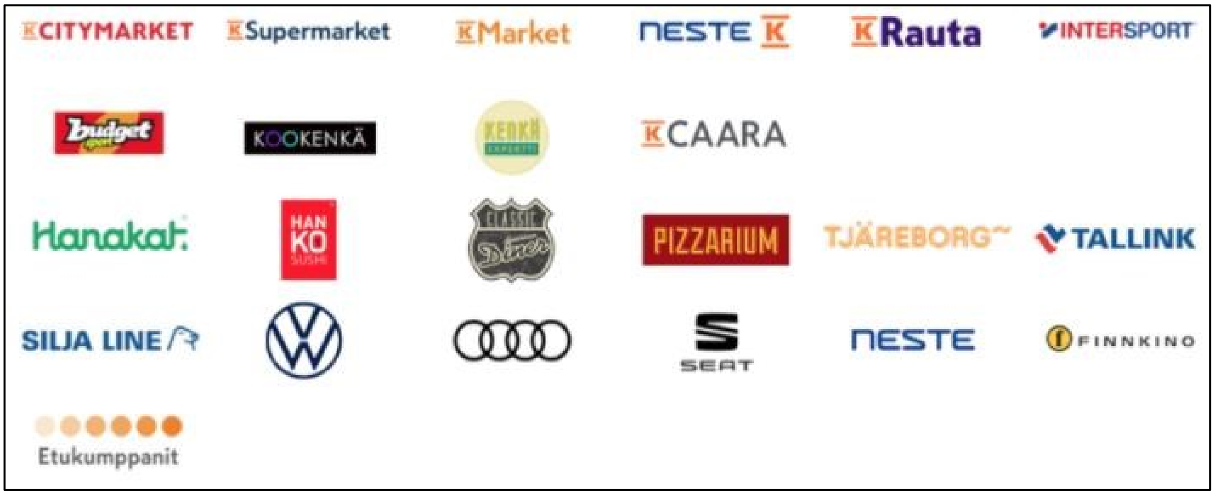


Figure 9 The K Group stores and associated business partners

The K Group also introduce K-Plussa MasterCard for the customers which help to gain more Plussa points when making purchase from the K Group stores and the Plussa points is converted in to Plussa money as 1000 Plussa points gives 5 euros worth of Plussa money which can be used to make the payment in K Group stores. The K-Plussa also stores the warranty information of the products and can be easily accessed by logging in. Below Figure 10 shows the table which illustrates the K Group Plussa points collection based on the purchase.

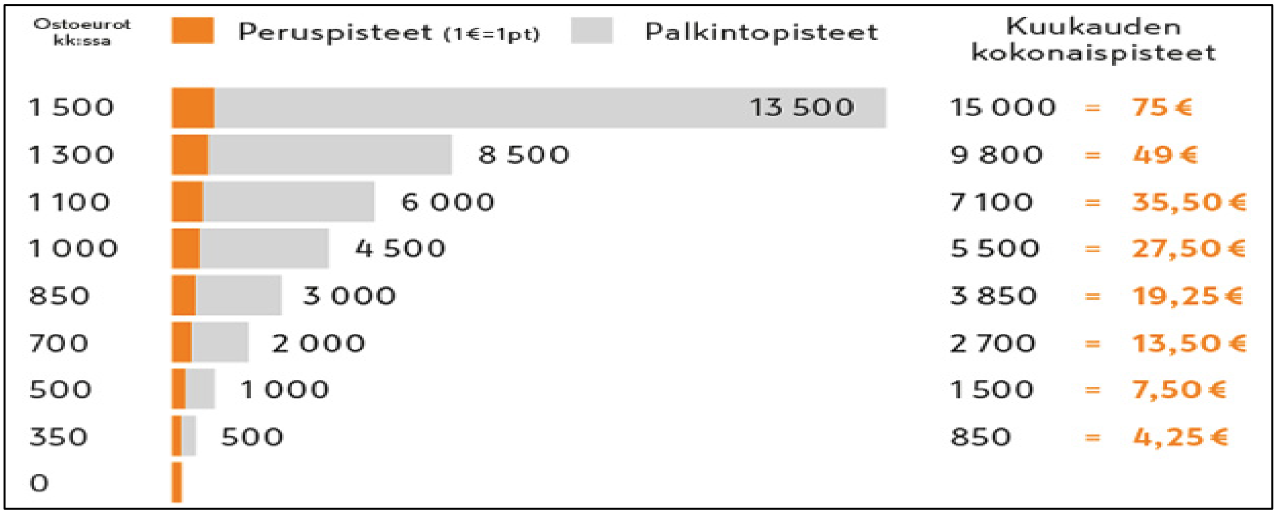


Figure 10 The K Group bonus returns to customers based on their purchase

Use Case 2: SMEs, Gold Gym Membership

The gym membership card can be used to access and log in and out of the gym. With the gym membership card, the customers can get access to the gym and use the service. The gym member can get some benefits such as free use of service for one month by referring their family members and friends to join the gym membership. The membership cards also help to monitor the people who are inside the gym. The membership card also helps to get access to different kinds of group exercises organized by the gym and make their appointment with their trainers. The gym membership cards also work to get access to the gym that are in different cities. Some gym membership also helps to get access to associated sports centers or get discounts on using the services. Thus, a gym membership card helps to get access to all kinds of services that are available.

Moreover, all these membership cards information are stored in the service provider database and have control over the customers information. The company can even sell this information to third parties without the customer's knowledge and even monitor the customer’s purchase behaviors. These membership platforms are usually developed by the organizations using huge amounts of time and resources

Potential Opportunities for SimplyMember

These three membership cards (K-Plussa, S-Etukortti, golden gym) are the main competitor for the SimplyMember and have huge numbers of members associated with them individually. The SimplyMember, which is an SSI based solution helps these companies to get rid of their own application and save some money which they can invest in other departments and can reach out to different groups of customers through the SimplyMember platform. The companies can also keep track of their members and can check the customers who do not have their membership form the SimplyMember. Then, the companies can target those non-members customers from the platform to motivate them to get their company's membership. By using SimplyMember the companies can also get access to their customers purchase behaviors and promote their different products information based on those behaviors through SimplyMember platforms. The transparency and cryptographic measure in SSI based SimplyMember platform helps to create trust and confidence of the companies towards the platform.

The SSI-based SimplyMember platform is more secure because of the end-to-end encryption for all interactions. SimplyMember solution helps customers to gain full control of their information and customers can update or hide their information. SimplyMember also provides customers a unique opportunity to earn money by selling their data. The SimplyMember cannot allow the platform provider to share the data to third parties without consent of the customers and customers can track who has access to their information and how they are being used. SimplyMember platform also disclose the minimum information of the members to protect the privacy of the members. The SimplyMember also provides easy access to their membership bonus or rewards those customers receive and can easily access the information through the platforms. Even members can store their information related to their purchase such as shopping list, compare prices from different stores, check the stores' locations, etc. and use services like information related to their daily workout at the gym. SimplyMember platform makes the customers owners of their data which encourage customers to use SimplyMember and store more securely than organizations own membership applications.

By integrating the different companies' membership into one platform which helps to implement a standard bonus or rewards system for all the customers and can have easy access to their information regarding the use of service or purchase of the products. SimplyMember is an easy, cheap, and more secure platform for the companies and customers to store their bonus or rewards and customer data. Thus, SimplyMember could integrate different other stores, clubs, libraries, restaurants, cafes and so on from their target market (Finland) to keep track of their members activities and add rewards or bonus based on those activities to their members.

4.2 Risk Analysis and Risk Management

The purpose of this section is to identify and plan the mitigation of the key risks for the SimplyMember use case. First, this document presents a comprehensive view of the key risk areas and different risks related to them. Second, this document provides a more detailed explanation of some of the key risks for the SimplyMember use case. Thirdly, we have a short conclusion of trust assurance based on the risk analysis.

4.2.1 Risk Definition and Identification Measures Used

A risk in this document is defined as any potential adverse outcome for the SimplyMember use case that could somehow hurt, for example, the value of or trust towards the SimplyMember use case (Raggad, 2010) (Stoneburner et al., 2002).

"Identity and Verifiable Credential risks matrix"[14] by Trust Over IP was used as a baseline for the risk identification process. The matrix is designed for the identification of risks related to digital identity and verifiable credentials which fits well with the SimplyMember use case. Only the relevant risks were taken from the matrix and relevant risks were added outside of the matrix. Risks that are taken right from the Trust Over IP's matrix are marked with a 'Trust Over IP' in the risk tables below. Most of the risks were identified by processing what we had learned and read about the subject and then reflected on the SimplyMember use case to see how relevant the possible risk is. Some of the risks were also identified according to feedback and ideas we got from mentors or other students. After the identification process, mitigation measures were identified that would help SimplyMember to mitigate the identified risks(Trustoverip, 2020). Mitigation procedures were chosen by discussing between the team members. We agreed on some keyway on every risk to mitigate them. Additional material was also used as a general guide in the risk identification and evaluation processes when needed. All the material can be found below at the end of this report. It is important to note that the content of this document should be regularly updated in the future.

[14] https://wiki.trustoverip.org/display/HOME/Identity+and+Verifiable+Credential+Risks

Risks were categorized into governance, business, technical, security, human and social, legal, and regulatory, and interoperability related risks. A more detailed description of the risk groups can be found below with the risk table including the risks connected to that category. Each risk was evaluated on a scale of 1-5 considering the impact, likelihood, and severity of the risk. Evaluation of the Impact, likelihood and severity were based on the discourse we had on the risks. In that sense numbers used in the risk matrix are not the absolute truth rather than a consensus of five people invested in the matter. Below is an explanation of what impact, likelihood and severity mean in this context.

- Impact: the degree of negative consequences that the risk might cause.
- Likelihood: the possibility/probability that the risk might occur
- Severity: the overall criticality of the risk. How important it is to mitigate and what is the severity of the problem if the risk mitigation is neglected.

Explanation of the numbers used in the risk categorization in Table 4 below. The wording of these were gathered from an article written by (LaConte, 2018)and from a few scientific articles(Markowski, A. S & Mannan, M. S, 2008)

	IMPACT	LIKELIHOOD	SEVERITY
1	Negligible	Unlikely	Controlled
2	Marginal	Remote	Serious
3	Serious	Occasional	Disruptive
4	Major	Certain	Severe
5	Catastrophic	Frequent	Critical

Table 4 Explanation of the Numbers Used in the Risk Matrix

4.2.2 Risk Categorization

Governance

Governance risks in Table 5 are often tied to its decentralized nature in the SSI ecosystem. Policies and practices are an important way to mitigate these risks.

RISK	ACTOR(S) AFFECTED	DESCRIPTION	MITIGATION	IMPACT	LIKELIHOOD	SEVERITY
Issuer Practices not accepted by ecosystem (Trust Over IP)	Provider	Issuer's practices are in conflict with the ecosystem. Issuers must change ways.	Practice conformance procedures	3	3	3
Lack of sufficient policy and practices (Trust Over IP)	Ecosystem	If there are no sufficient policies and practices in place it can create a risk for unregulated use of the ecosystem.	Lack of sufficient policy and practices can be handled inside the ecosystem by having a complete governance framework and feedback look.	4	3	4
Ineffective bias in authority (Trust Over IP)	Ecosystem	Bias in authority can cause wrong use of the ecosystem and end up lowering the trust between parties.	Ineffective bias in authority requires even representation, voting standards and non-discrimination practices.	2	2	3

Table 5 Trust Over IPGovernance Risks

Business

Business risk in Table 6 is the exposure SimplyMember has to factors that will lower its profits or lead it to fail. Anything that threatens SimplyMember's ability to achieve its financial goals is considered a business risk.

RISK	ACTOR(S) AFFECTED	DESCRIPTION	MITIGATION	IMPACT	LIKELIHOOD	SEVERITY
No interest in adoption of the technology	Holder, Issuer, Verifier	If the user base is minimal, SimplyMember cannot provide value/ be tempting to use	Creating interesting service and do good marketing so users will get interested of service	4	3	4
Adoption of SimplyMember is low	Holder, Issuer, Verifier	If the SimplyMember idea does not gather support, the user base might be minimal	Raising user base by marketing and having a good value proposition	4	3	4
Businesses do not see value in adaptation of SimplyMember	Issuer, Verifier	Businesses do not see adaptation of SimplyMember profitable and will not cooperate with the developers	Clear illustration of value created by SimplyMember solution	4	3	4
Holders Give Up Using SimplyMember	Holder, Ecosystem	Holders find SimplyMember solution too complicated or Impractical and do not find using it desirable	User interface and other aspects relating user comfort should be tested and designed so, that people find using SimplyMember solution easy	2	4	2

Table 6Trust Over IP Business Risks

Technical

Technical risks in Table 7 are problems and risks related to technical aspects and solutions of SimplyMember service.

RISK	ACTOR(S) AFFECTED	DESCRIPTION	MITIGATION	IMPACT	LIKELIHOOD	SEVERITY
Missing verification (Trust Over IP)	Verifier	Proof is provided by the issuer to verify VCs, but this verification is lost, and the verification cannot be completed. A major concern as it stops the customer from using the service	There should be regular checks to add missing verifications.	4	3	2
Untimely verification (Trust Over IP)	Verifier	Verification of VCs cannot be done at the right time which creates lag in the verification process. Prohibits the customer from using the service but not for a long period of time.	Mitigation by ensuring that the verification process works correctly, and no delays take place.	2	3	1
Suspended/ Revoked Credential Being Accepted	Verifier, Issuer	VC that is suspended or revoked is accepted as a legitimate VC. Can hurt the credibility of the system and the trust of customers towards the solution. Monetary losses can also occur.	Mitigation by ensuring that the adequate processes are in place to ensure the suspensions and status of the memberships.	2	2	2

Verifier Network Unavailable (Trust Over IP)	Verifier, Holder	The verifier network is unavailable, and no VCs can be legitimately verified. A major risk as it would prohibit the usage of the service. Monetary losses and credibility damage	Mitigation by network redundancy procedures.	4	3	5
Issuer Operations Unavailable (Trust Over IP)	Issuer, Holder	The operations(systems) from the issuers side are unavailable. Transactions are not collected correctly	Network redundancy procedures	4	2	5
Counterfeit Credentials Being Created (Trust Over IP)	Issuer, Verifier	Counterfeit gym memberships or other credentials are made and used	Mitigation by planning software in a way that counterfeit credentials are impossible to create	2	2	3
Lack of Portability of Credential (Trust Over IP)	Holder	Holder can not transfer credentials to new device	Requires adequate technical solutions so portability of credentials is easy and possible	2	2	2
Permission to save data is unanswered	Verifier, Holder	The holder cannot receive their store bonus credits if permission for saving data cannot be granted.	Mitigation by ensuring that the adequate processes are in place to verify the permission for data saving.	2	3	3

Provider Software Does not Operate as Intended (Trust Over IP)	Provider	Bonus card or gym memberships are not recognized by the software	Mitigation by planning and creating software that operates as intended.	4	2	3
Provider Software Does Not Operate on User Devices (Trust Over IP)	Provider	Users' devices are not capable of running the bonus card or membership software.	Mitigation by creating platforms that software works on different kinds of devices.	4	2	2
Provider Code Updates Cause Operational Issues (Trust Over IP)	Provider	When updating code and after the code is updated the bonus cards and gym memberships are not working at all.	Mitigation by carefully testing new code before launching it.	2	2	1
Provider System Unavailable (Trust Over IP)	Provider	Bonus cards and gym memberships are out of reach and the system is unavailable.	Mitigation by customer service and investing proper servers to run the software and system.	4	1	4

Table 7 Trust Over IP Technical Risks

Security

Security related risks in Table 8 are defined as any situation or threat that could somehow compromise the security of the SimplyMember use case.

RISK	ACTOR(S) AFFECTED	DESCRIPTION	MITIGATION	IMPACT	LIKELIHOOD	SEVERITY
Man-In-The-Middle Attack During Legitimate Verification (Trust Over IP)	Verifier, Issuer, Holder	An unauthorized third-party interrupt or alters the verification process of a VC between the verifier and the holder or the issuer.	Mitigation by creating adequate security and verification practices.	4	2	3
Credential issued to impostors	Verifier, Issuer, Holder,	Data is shared with individuals that appear to be correct ones but are not	Trust assurance practices	4	1	4
Lack of accountability of roles in network (Trust Over IP)	Ecosystem	Lack of trust can create a risk of an ecosystem not working because of a lack of trust between different parties.	Lack of accountability of roles in the network requires proper oversight and trust assurance mechanisms embedded into the ecosystem.	4	2	4
Ecosystem Allowing Inappropriate Actors to Participate in Network (Trust Over IP)	Ecosystem	Inappropriate actors can use the ecosystem in an abusive way.	If the ecosystem is allowing inappropriate actors to participate in the network, it needs a provider evaluation and acceptance processes.	4	2	5
Credential Holder's Private Data is Compromised	Holder	There is some way that Holder’s private data is leaked and accessible for non-authorized parties	Requires Adequate Technical solutions that data is kept private	4	2	4

(Trust Over IP)						
Identity Proofing Practices Inadequate for Level of Assurance (Trust Over IP)	Ecosystem, holder	Data security is not correctly stored, and data is false	Governance conformance procedures	4	2	4

Table 8 Trust Over IP Security Risks

Human and Social

Human and social related risks Table 9 are risks that involve human interaction and might be compromised due to human actions.

RISK	ACTOR(S) AFFECTED	DESCRIPTION	MITIGATION	IMPACT	LIKELIHOOD	SEVERITY
Evidence of verification incomplete or in incorrect format(Trust Over IP)	Verifier	VCs cannot be verified before they are corrected to the right format, or the missing information is gathered from the VC holders. Prohibits the customer from using the service but not for a long period of time	Creation of controls and standards for the verification process and ensuring that the verifiers know and understand these controls.	3	2	3
Device lending	Holder, Verifier	A holder lends their device to another person to receive benefits	Two step authentication, biometric authentication	2	4	2
Credential Issued in the wrong format or structure (Trust Over IP)	Holder	The holder gives false information leading to format error in the issuer's operations	Requires standard formats and controls	3	2	3

Lack of competence to perform role (Trust Over IP)	Ecosystem Verifier	Lack of proper knowledge and skills can create risk on an ecosystem. Risk is that the ecosystem is used in an incorrect way.	Lack of competence to perform roles can be mitigated by having experienced personnel, proper training and governance framework.	2	2	3
Lack of communication about governance practices (Trust Over IP)	Ecosystem	Lack of communication can cause risk of misinformation between parties.	Lack of communication about governance practices requires appropriate communication channels opened up inside the network and the participants.	2	3	2
Credential holder given inappropriate access rights (Trust Over IP)	Holder, Issuer	Wrong credentials given to wrong people. For example, are given credentials for services they have not paid for	Clear instructions and processes in giving credentials so mistakes do not happen and adequate Non-Repudiation Practices	2	3	2
Credential Wallet Private Key is Lost or Compromised (Trust Over IP)	Holder	Holder cannot use credentials because they have in some way lost access to them	Mitigation by Using Adequate User Wallet Protection Measures and Way to Restore Credentials	3	2	2

Table 9 Trust Over IP Human and Social Risks

Legal and regulatory

Legal and regulatory risks Table 10 that will affect the business or any of its assets if there are changes made into the current legislation.

RISK	ACTOR(S) AFFECTED	DESCRIPTION	MITIGATION	IMPACT	LIKELIHOOD	SEVERITY
Data given to outsiders without permission	Ecosystem, issuer, holder, provider, verifier	User data is given to outsiders or stolen	Data security training, sufficient security methods	2	1	5
Ecosystem Lacks Jurisdictional Acceptance	Ecosystem	If there is no jurisdictional acceptance it can prevent ecosystem from being used.	If the ecosystem Lacks Jurisdictional Acceptance, it requires Mapping of Jurisdictional Regulation.	4	2	4
Holder Threat of Litigation over Issuer (Trust Over IP)	Holder, Issuer	Holder may feel that their rights have been violated, so there is threat of a lawsuit	Agreements should be made in a way that violations of holders rights are unlikely/impossible to happen	3	1	4

Table 10 Trust Over IP Legal and regulatory Risks

Interoperability

Interoperability risks Table 11 are risks for not working cooperation between different parties.

RISK	ACTOR(S) AFFECTED	DESCRIPTION	MITIGATION	IMPACT	LIKELIHOOD	SEVERITY
Credential Issued without sufficient basis (Trust Over IP)	Issuer	The issuer does not get enough information	Requires staff training for the issuer.	2	2	2
Ecosystem Lacks Industry Acceptance (Trust Over IP)	Ecosystem	If an ecosystem lacks industry acceptance it creates the risk of the ecosystem becoming irrelevant and unusable.	In a case where the ecosystem is lacking Industry Acceptance, ecosystem requires Mapping of Industry Regulations.	4	2	5
Credentials are not working in every establishment (Trust Over IP)	Ecosystem	Holder's credentials are not working in every S-market for example	Mitigated by Adequate Credential Interoperability Practices and With Well-Coordinated Pre-Launch Testing Throughout Establishments involved	3	3	3

Table 11 Trust Over IP Interoperability Risks

4.2.3 Key Risks for the SimplyMember Use Cases

This section describes more in depth some of the most critical risks related to the SimplyMember use case. The risks are described in the context of the SimplyMember use case and an example is given on how the risk will impact the SimplyMember solution if the risk is not treated properly. Mitigation measures are also offered to counter these risks. Ecosystem allowing inappropriate actors to participate in network.

First of the observed key risks is the ecosystem allowing inappropriate actors to participate in the network. Inappropriate actors could use the SimplyMember ecosystem in an abusive way. This risk is directly related to the security of the SimplyMember ecosystem. Security related risks are defined as any situation or threat that could somehow compromise the security of the SimplyMember. This risk has been evaluated to be the most critical security related risk. Although having a major impact and critical severity for the whole SimplyMember ecosystem its likelihood has been evaluated as a remote. This means that this scenario is somewhat unlikely to happen. To mitigate the risk of inappropriate actors becoming a part of the SimplyMember ecosystem there needs to be a proper process of provider evaluation and acceptance processes. Every actor that wants to be part of the SimplyMember ecosystem must be thoroughly vetted and processed before acceptance to the network.

Ecosystem lacks industry acceptance

This key risk is a situation where the ecosystem lacks industry acceptance. If the ecosystem lacks industry acceptance it creates the risk of the ecosystem becoming irrelevant and unusable. This risk is affecting the whole SimplyMember ecosystem thus being critical in severity and having a major impact on the usability and acceptance. This risk has been evaluated to be remote to happen. Even though being somewhat unlikely to happen to the SimplyMember ecosystem it has to be observed and mitigated because of its severity and impact. To mitigate the risk of SimplyMember becoming unacceptable in the industry there needs to be a mapping of industry regulations and accepted practices. SimplyMember should be in direct dialogue with industry members to mitigate the possibility of this risk.

Device lending

Device lending is a critical risk for the SimplyMember use case mainly because it is easy to perform and highly likely to occur. An example of device lending in the SimplyMember use case would be a situation in which someone who does not have a gym membership lends a holder's device to enter the gym without a membership. If device lending would occur on a large scale, it could end up damaging the entire SimplyMember ecosystem. User count might not grow as high, and the ecosystem partners would suffer monetary losses. Device lending can be a tricky problem to tackle but some possible mitigation measures are, for example, two step verification and biometric authentication. These measures would make device lending more difficult to commit.

Man-In-The middle attack during legitimate verification

Man-In-The middle attacks refer to attacks in which a malicious third party interrupts the communication between two legitimate parties. If the attack is successful, the malicious actor could steal or tamper with the credentials during the verification process(Ekparinya et al., 2018). By doing this, the attacker could gain access to the SimplyMember ecosystem without a legitimate credential verification or possibly steal bonuses from a legitimate user. This would be a serious issue for the SimplyMember use case as these kinds of attacks could hurt the credibility of the system and the trust of customers, both issuers and holders. This threat can be mitigated by ensuring that adequate security and verification practices are in place to prevent these kinds of attacks. An example of this kind of practice is zero-knowledge verification in which verifications can be made without exchanging keys or private information.

Issuer operations unavailable

One of the key risks from the issuer's side is that the operations are unavailable. This in simple terms means that the necessary operations for the blockchain to work, do not function properly. Usually the problem showcases like this: The holder cannot use the service as the read operations work improperly meaning that the user cannot get any discount or cannot access the gym. The second scenario is that the end-user's actions are not collected correctly. Let us say that the end-user has a one-time-coupon and uses it at the counter, but the write operation does not work properly, and it does not collect the discount meaning that the end-user can use it again. This risk is problematic in both scenarios as it could be inconvenient for the consumer meaning that they could drop the use of service, or the store/gym could lose revenue due to malfunctioning write operations. This risk can be mitigated by using top soft- and hardware that would reduce the risk that the operations are unavailable.

Ecosystem Lacks Jurisdictional Acceptance

As the field of blockchain is still rather fresh from the eyes of legislative representatives it is not yet thoroughly regulated in Finland. As there is now assurance that the current legislation holds, there could be decisions that harm the ecosystem in its current state. The risk could be that the legislation would change its point of view regarding decentralized ecosystems as it could be an issue towards customers rights to control what data the company has of them. Once the data is stored it cannot be altered, however, there could be possible altered ways such as functionality-preserving local erasure. If the legislation would change, this could lead to possible financial risks from investors and the ecosystem's point of view. This risk can be mitigated with proper lobbying and working inside the current legislation of Finland and EU.

Provider Software Does Not Operate as Intended

As SimplyMember is the provider of this project, the errors in software could have a negative effect on the value of the service. If the software does not operate as intended, it could probably affect users' privacy and bonus records. There is a risk that user's bonus or gym membership cards do not work, and they do not get to use them as planned. Mitigation for this risk needs planning and executing working software. When plans are made correctly, and developers do a good job then the software should be ready for users to use and operate as intended.

Provider System Unavailable

An example of a situation like this would be that a user is trying to get into a gym, or show their bonus cards at markets, and the SimplyMember's system is unavailable. This creates a great risk for the usability of the service. It is important that service is available and responding to the users. If bonus and membership cards are out of reach that creates negative value for users. This kind of problem could easily make users unhappy and even drop out of using SimplyMember's service. Mitigation of this risk needs to be started by having proper servers with that service can be reached and available. SimplyMember needs to have working customer service where users can report that software is not working and where users can get help for situations like this. This is a very critical risk for SimplyMember's software and there should be effort put into mitigating this risk.

Adoption of SimplyMember is low

Our discussion of business risks regarding the SimplyMember focused on the risks that there would be a lack of adoption of the technology, or the service. Lack of adoption or low adoption means that businesses like S Group, Kesko or gyms would not see adoption of SimplyMember profitable or valuable enough to start cooperation with the developers. Even though businesses would adopt the SimplyMember solution, there is a risk that users would have low interest and adoption of the service. If the user base would not be sufficient, SimplyMember could not provide real value to any stakeholder. These risks apply to all actors, developers, issuers, verifiers, holders, and the ecosystem. Also, we found that this risk would have a major impact and the overall criticality of the risk is severe. That is the reason why low adoption of SimplyMember is one of the key risks that we identified. We have found a way to mitigate this risk by developing good value propositions and marketing for businesses. To guarantee high adoption by the end users as well, we have concluded that service has to be interesting and easy to use. In addition, that the software and the interface, e.g., are made to be tempting and easy to use, the marketing is a vital part in the mitigation of this risk.

Lack of sufficient policy and practices

One of the key risks is lack of the sufficient policies and practices in the ecosystem. Risk is related to the governance of the SimplyMember. In this risk governance fails to establish sufficient policies and practices for the SimplyMember which could lead to unregulated use of the ecosystem. In the worst-case scenario actors could go “rampant” and do what they want. This would greatly lessen the value of the SimplyMember solution and make usage of the SimplyMember harder for every actor. Because of this we have identified that the risk’s impact would be major, and the overall criticality of the risk is severe. Likelihood of the risk would be occasional so the policies and practices should be inspected from time to time to make sure that they are sufficient. Risk can be mitigated by having a complete governance framework developed to have sufficient policies and practices. Feedback and continuous monitoring should be introduced to ensure that policies and practices are up to date to keep the ecosystem regulated.

4.3 Trust assurance–A summary

Trust assurance can be defined as an insurance to an event that will certainly happen and define how to those involved trust in it. Risk analysis is an important way to build trust on SimplyMember. Presenting risks and ways to mitigate them shows that there is genuine will and knowledge from the providers side to deal with these various risks.

In SimplyMember context the trust assurance could be defined as various ways to create trust and belief towards the ecosystem and its providers.

There are various ways that create trust towards an ecosystem. The most important assurances differ depending on the stakeholder that demands a certain level of assurance on different aspects. For example, investors value the assurance on value creation -estimate. How much would an investment of x Euros create in Y amount of time (Gunderson, 2014).

To connect our risk analysis work to trust assurance we went through Self-sovereign identity: The future of identity document (Moisés Menéndez Andrés et al., 2020) For example, according to OIX (Makaay. E et al., 2017)trustworthiness is an important factor for enabling trust among stakeholders. They present that trustworthiness can be established. “-- *by addressing and managing risks, legal rights, responsibilities, and liabilities; eliminating uncertainties; and facilitating the accessibility and understanding of the trust frameworks to all participants*”.

Although we do not have a full trust framework developed for SimplyMember, we have managed risks and eliminated uncertainties with our risk analysis document. We find that our work has been a vital part of trust assurance for SimplyMember.

5 SimplyMember Pricing Models

Next, we will describe how the value offered by the ecosystem participants to customers is translated into incoming money streams. We will introduce the initial pricing models that were chosen suitable for SimplyMember in the selected use cases retail membership and gym membership. We will also look into the feasibility of selling user data in the SimplyMember ecosystem.

5.1 Introducing the Pricing Model

First, we will analyze and discuss the pricing models to justify the selected options. The chose pricing models are subscription-based and reward-based.

In all pricing models payment for the actual service (e.g., gym monthly fee, grocery shopping, hotel vacation) is an agreement between the Holder and the Issuer/Verifier and has nothing to do with SimplyMember. We believe that SimplyMember should not be involved in transactions where money is transferred. However, for instance in gym use case SimplyMember could provide free verification (identification/access) for first time users, or during campaigns including possible referral rewards which Holders may have acquired from Verifiers. In order to make potential membership as inviting as possible there are no fees for holders.

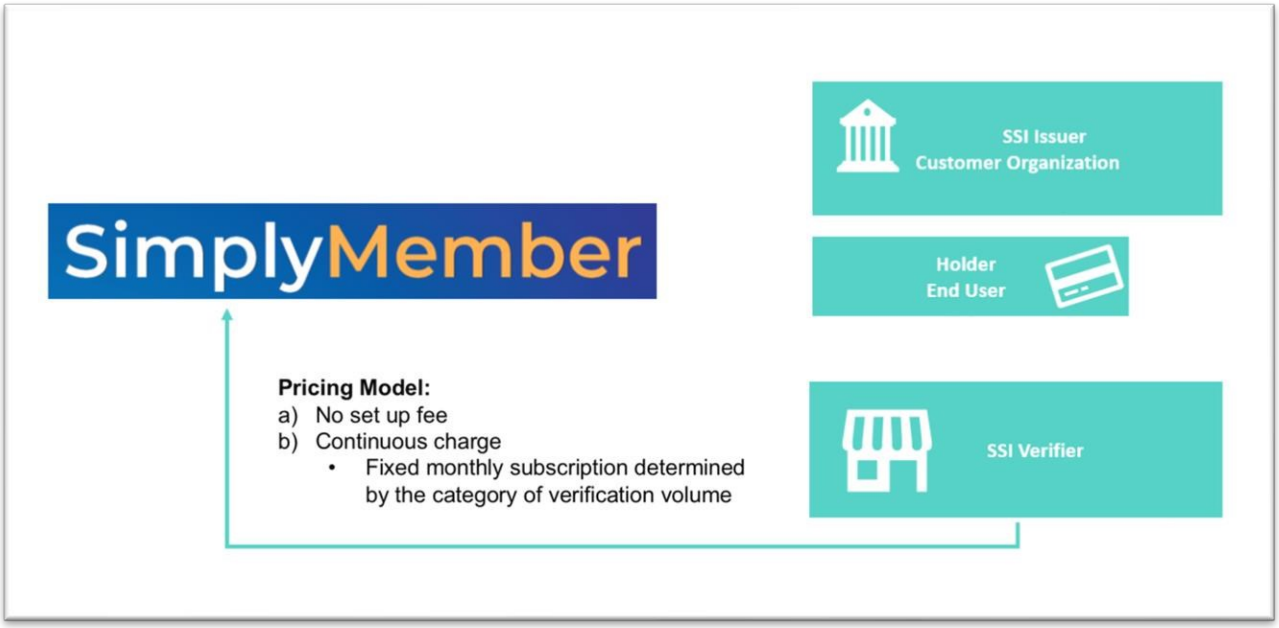
5.1.1 Justification for the chosen models

The two use cases differ greatly in terms of feasible pricing models. Thus, we have come up with a solution most suitable for the bigger partners as shown in Figure 11, the two largest retail chains in Finland, Kesko Corporation and S Group cooperative, and an alternative pricing model for the Gym and SME use case as shown in Figure 12 and a combined pricing model in Figure 13.

Benefits of volume-based pricing model can be considered

- Pay per use
- Fair pricing
- No sign-up fees

Pricing Model for S Group and Kesko Use Case



Pricing Model:

a) No set up fee
b) Continuous charge
   - Fixed monthly subscription determined by the category of verification volume

Figure 11 SimplyMember Pricing model for big partners

Cooperation with bigger retail partners such as S Group and Kesko, is not considered as feasible outside of the use case. Multiple alternative options for membership identification/authentication exist already, and we cannot see the added value that SimplyMember can bring. In terms of pricing models bigger players will see transparency. The most successful entry to market for SimplyMember would probably be collaboration with the public sector.

Pricing Models for the Gym Membership (SMEs) Use case

We see that the Gold Gym and other SMEs use case is a more realistic option for SimplyMember, that can bring actual value to all stakeholder groups. Pricing models for Gyms and other SMEs consist of two cash flows to SimplyMember, a fixed subscription fee and new customer acquisition reward.

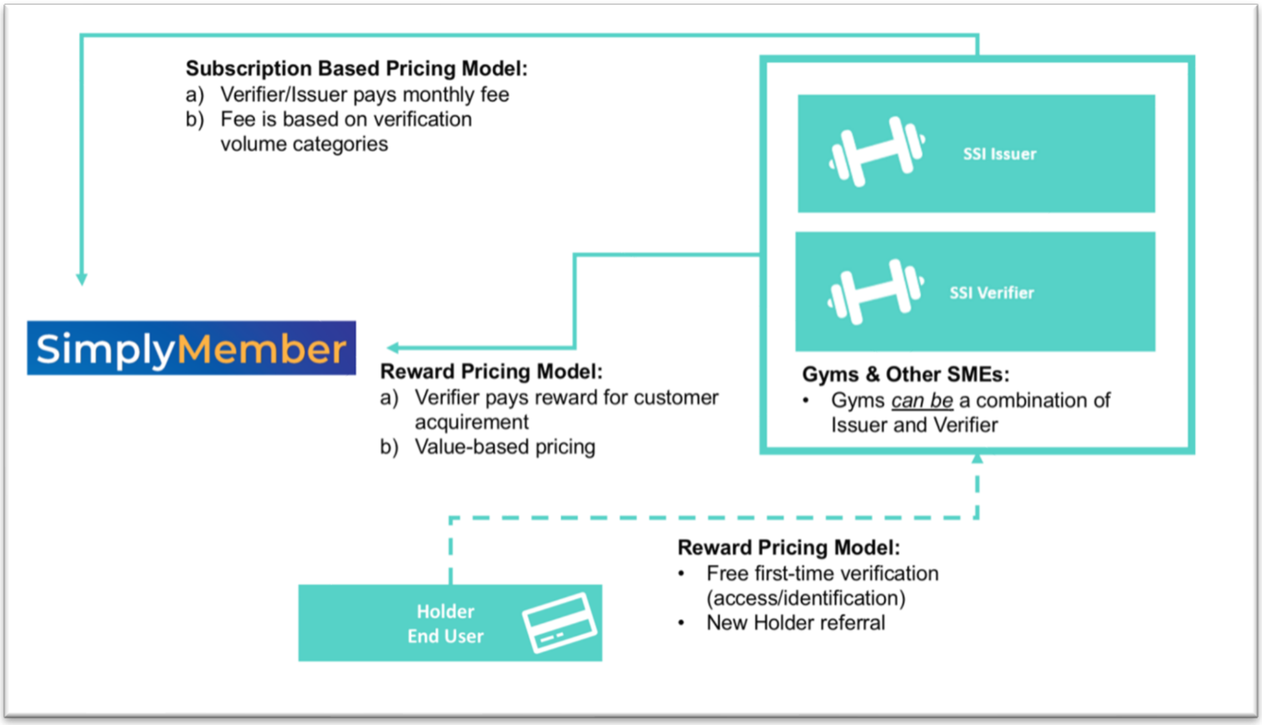

Subscription Based Pricing Model:
a) Verifier/Issuer pays monthly fee
b) Fee is based on verification volume categories
SSI Issuer
SSI Verifier
SimplyMember
Reward Pricing Model:
a) Verifier pays reward for customer acquirement
b) Value-based pricing
Gyms & Other SMEs:
• Gyms can be a combination of Issuer and Verifier
Reward Pricing Model:
• Free first-time verification (access/identification)
• New Holder referral
Holder
End User

Figure 12 SimplyMember Pricing Models for Gyms & other SMEs

Combined Pricing Models

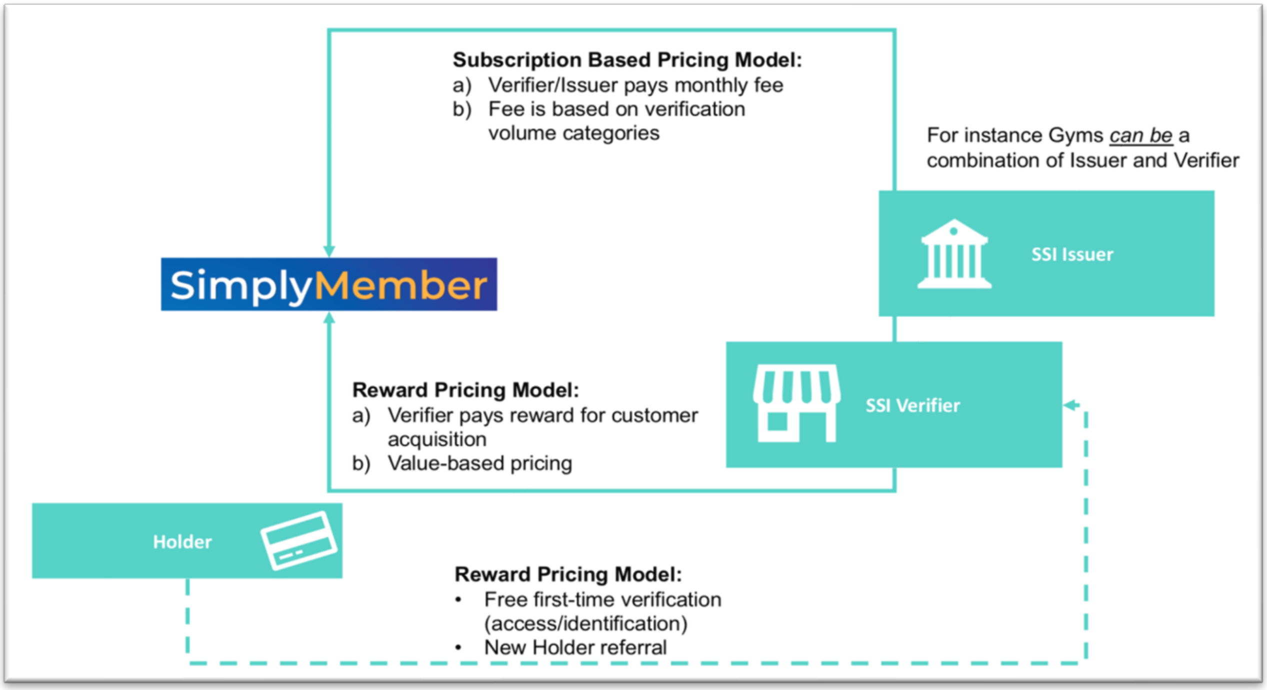

Subscription Based Pricing Model:
a) Verifier/Issuer pays monthly fee
b) Fee is based on verification volume categories
For instance Gyms can be a combination of Issuer and Verifier
SimplyMember
SSI Issuer
Reward Pricing Model:
a) Verifier pays reward for customer acquisition
b) Value-based pricing
SSI Verifier
Holder
Reward Pricing Model:
• Free first-time verification (access/identification)
• New Holder referral

Figure 13 SimplyMember Combined Pricing Model

Firstly, we presume that for instance gyms usually are a combination of Issuer and Holder. Small, private gyms form a combined role of Issuer and Verifier, and in case of large gym-chains the positioning is more similar to S Group's and Kesko's use case, in which the parent company (gym chain) acts as Issuer, and individual gym as Verifier. Nevertheless, our pricing models are suitable for both cases.

5.1.2 Subscription-Based Pricing Model

The Subscription Based pricing model for Gyms & SMEs is based on a fixed subscription cost that verifier (or Issuer-Verifier combination) pays to SimplyMember. The verification unit price is determined by annual fic (rolling year-to-date) verification volume-based categories. One example of this kind of categorization is illustrated below in Table 12 Table 1SimplyMember could customize the category prices and volume limits according to the customer.

Key takeaways from Subscription Based pricing model

- SimplyMember is free for Holders
- Gym (Issuer/Verifier) pays Subscription fee to SimplyMember based on verification volume
    - Verification = identification/access to Gym
    - Divided into tiers by verification volume
    - Verification volume increase -> unit price for single verification decreases

ANNUAL VERIFICATION VOLUME (UPPER LIMIT)	**VERIFICATION FEE (€)**
50 000	0,121
100 000	0,090
500 000	0,055
1 000 000	0,048
2 000 000	0,042
3 000 000	0,039
9 999 999	0,029
Over 10M	0,019

Table 12 Example of verification fee categories

Another option for Subscription Based pricing categories for this use case was fee based on monthly active holders. This was our initial proposal, and firstly we reasoned that verification (per identification) based pricing model is not the best option for the gym use case. However, lack of market volume information in terms of monthly gym membership holders forced us to use verification-based pricing also in the gym use case. Since total gym user volume ("verification") information was somewhat available, we were able to create a preliminary price tag for the Gym/SME pricing model.

5.1.3 Reward-Based Pricing Model

Besides the Subscription Based pricing model, SimplyMember could adopt a model where Holder can have a free first-time verification, for instance access to the gym in non-working hours when the gym staff is not available. Then, SimplyMember charges a reward from the Verifier for customer acquisition. This model is also capable of referral reward pricing, where SimplyMember charges for customer acquisition from new referred customers.

Price-tag for the Reward pricing model is highly situational, depending on the value of the new customer for the Verifier. Thus, we suggest that SimplyMember adopts the Reward pricing model case sensitively, pricing accordingly to the respective customer (Issuer/Verifier), meaning value-based pricing.

Key takeaways from Reward pricing model

- Offers free first-time verification (access/identification) for new customers (Holders)
- Holders can invite new users (Holders) to the service
- SimplyMember charges from realized customer acquisitions
- Value-based pricing, depending on the contract between SimplyMember and Issuer/Verifier
- Allows Gyms and SMEs 24/7 customer acquisition, lowers the threshold for Holder to try out new services and products.

5.2 Pros and Cons of the Different Pricing Model Options

Table 13 shows the pos and the cons of different pricing models.

PRICING MODEL	PROS	CONS
Subscription Based Pricing Model	Easy invoicing Low threshold (no set up fees) Fair pricing	Could seem unattractive for new customers Argueability of pricing Costs could seem unjust
Reward Based Pricing Model	Pay per reward Low risk Commitment Easy customer acquisition	Administrative load Privacy related issues Rewards need to be negotiated

Table 13 Pros and Cons of the Pricing Models

5.3 Feasibility of Selling Data

We also had some conversation about the possibilities of SimplyMember users selling their data. We concluded that this would not be an option for SimplyMember. Data provided by the user might be of interest to verifiers and issuers but facilitating this verification might be infeasible and prove to be problematic with current day privacy standards especially in European Union (GDPR). This would also require SimplyMember to facilitate verification of funds which we thought would not be part of the SimplyMember scope. Possibilities for data-selling can infringe our user trust factor which is important for long term customer retention. Furthermore, while Holder would be willing to sell the data, the content of data SimplyMember can provide is quite bare as SimplyMember is purely identification/access SSI ecosystem.

6 A Simple, Easy-to-Use Membership Solution

In this section we will report the requirements for a frictionless user experience based on the findings of a user research conducted in the beginning of the SimplyMember's service design. The second part of the section will concentrate on the digital identity wallet, its requirements and design from the holder's perspective.

6.1 Frictionless User Experience

This section reports the user research conducted by team 10 who was responsible for the user experience. The goal of this section is to describe the research process, interviews, data analysis process, and the findings of the user research project.

The main task of the group 10 was to plan and conduct interviews to survey perceptions of possible users of the SimplyMember solution and recognize requirements and concerns of the possible users to deliver a frictionless user experience. We ended up recognizing categories containing perceived benefits, worries, and contemporary pains from the conducted 10 interviews. The categories consist of several features each. Finally, we propose 8 requirements for the SimplyMember system according to the collected interview data.

6.1.1 Research Process

Planning Phase and Forming the Questions

We began planning our work by familiarizing ourselves both with the SimplyMember idea, the SSI concepts related to this course, and our work. As directed, we based our process on Nadine Ostern's and Johana Cabinakova's (2019) research paper: "Pre-Prototype Testing: Empirical Insights on the Expected Usefulness of Decentralized Identity Management Systems".

We adapted Ostern's and Cabinakova's methods for our work and conducted a qualitative study to help determine the viability of the SimplyMember idea. For this study we mostly followed their interview protocol and formed a set of questions designed to gather data on the interviewees' backgrounds, and on their interests, worries, and opinions related to the SimplyMember idea.

After the questions were completed, we conducted one test interview to try out the questions, and to better familiarize ourselves with the interview process. Based on the test interview, and the feedback from our mentors we adjusted the questions and rest of the interview process.

Conducting interviews

Interviewees were recruited initially during one week with a special interest towards elderly people and their perceptions of the application. The interviewees consisted of previous contacts of the project group. We conducted a total of 10 interviews of which six were males and four females. The interviewees ended up being at average 55,4 years old from the range between 23 to 82 years old. Furthermore, 43,8 years was the average age of the male respondents and 72,75 years the average age of female respondents. Eight out of ten did use smartphones and at least half used multiple membership cards instead of just a few(Turner, 2018).

The interviews were conducted some remotely and some face-to-face, taking between ten to thirty minutes each to complete the designed questions. Due to the respondents being previous contacts of the interviewer, we expect the situation having been fairly comfortable for the respondents and resulted in a more open conversation. The interviews were recorded with permission of the respondents while the anonymity of the respondent was guaranteed. This also meant that the recordings were only used for creating accurate transcripts of the interviews.

Analysis method

We did content analysis for the transcriptions (Weber, R. 1990). The data for the final analysis was coded from the interviews in a more rigorous manner as instead of each interviewer coding their own transcriptions, another member of the project group did code them into keywords and corresponding quotes from the interview transcriptions. Next, the coders did come together and discussed the coding keywords to combine and form more coherent keywords without losing important information. The interview quotes were finally translated from Finnish into English for the final table.

6.1.2 Findings

The findings of the study are presented in (Table 14,Table 15 and Table 16) arranged based on three themes which are perceived benefits, perceived worries, and contemporary pains. The tables contain the keywords for the recognized key findings, quotes from the interview transcripts, and the percentage of interviews where the keywords were present.

Perceived benefits

FEATURE	QUOTE	% OF RESPONDERS
No need to carry physical cards	"...Do not have to keep all kinds of tickets and cards and all if all those are in the phone. Would be much easier. [Would be an improvement to] ...Carrying cards and much simpler with a mobile phone." [i4] "Wouldn't have to carry cards around if it went with the application." [i5] "Makes my own life easier so that I do not need to carry different cards with different benefits." [i6] "In my opinion K, S, Moto net and other membership cards like S-Etukortti and Scandic that exist, and others would be really good if they were in one. Now there are still many useless cards I carry which I could get rid of." [i8] ---- "...Sometimes some cards are at home when I'd need them. Then I would have the cards always with me." [i4] "Those [Membership cards] would then always all be with me." [i3] "...Sure, it would be handy if the situation was such that; do I have a membership card, I'd get benefits like so and so right now, and if I'm interested in the benefit, I could just pull that membership card up from the phone." [i10] "Could be really beneficial for the membership cards that are rarely used, so they'd always be with me." [i6]	60
Ease of use	"It would be good when I wouldn't need to search for the cards." [i1] --- "If you could combine everything into one, for example an application or so, it would be really smart, at least in principle." [i7] "This [application] is something I have been hoping for, it would be good if the cards would be bundled. It needs to be easy to work, so it would get used. It's really good that K-plus is integrated into the bankcard which I pay with. And it would be good as well if they all would be in one app or card that I use." [i8] ”Well it sounds good that all cards are in one." [i2] "Much easier to use one application than carry 20 cards." [i6] "[Would be an improvement to] exactly carrying those cards and much simpler to use the phone straight up." [i4]	60

Convenience of the application, overall		90
Transparency	“It’s of course good that the customer is clearly told when opening the connection or contact that what information is requested of [the customer] and can choose to accept or not… Mostly it’s important that it's transparent how it operates.” [i7] “I’m scared that personal information is relayed that I wouldn’t need to give.” [i9]	20
User Control	“And probably in that sense it’s more secure, that no one else can’t use your membership cards, which is kind of positive, that you control your membership cards and so...” [i10]	10
Transparency & User control, overall		30

Table 14 User experience research findings, Perceived benefits

Perceived benefits consist of two main features related to the convenience of the application and improved transparency and control for the users. The first feature of convenience is no need to carry physical cards which furthermore refers to no need to have physical cards as well as having all the cards with the user. The second feature of convenience is the ease of use where it highlights easier access to cards, all memberships in one application, and simpler to use them via smartphone. The improved transparency and control boils down to users' ability to see what information they are sharing as well as the user controlling the data instead of outside entities.

Perceived worries

FEATURE	QUOTE	% OF RESPONDERS
External misuse (Security)	“Well, you do not know if they hacked everyone.” [i1] “Only fear I have is whether they will remain there and, in this world, of course, information from all over the world gets stolen.” [i3] “They would make it so safe that it is not .. no bystanders can get into it.” [i5] “Now that you follow that current situation, there really are a lot of those all sorts of scams so it always comes up whether this is now for sure.” [i9] “One thing that attracts attention and thoughts is just that, security.” [i10] “Well I do not know, security always comes first.” [i4]	70

Internal misuse (Security)	“It is always a question mark that it can be implemented so that the data cannot leak or anything else.” [i7] “I do not want to be tracked in any way based on personal information.” [i2] “..but basically I'm not so enthusiastic about this application, just because data collection and data protection and stuff like that I am against.” [i10] “What I consider important is that privacy remains.” [i6] “..there would be a hack, so all your membership cards and everything else, it would be an insane amount of data about you that would then leak.” [i10]	50
Security, overall		100
Dependency of the phone	“But that worries me the most, if that cell phone disappears then everything else gets lost.” [i1] “Should of course get such memberships (digital) to not having to carry cards.” [i5] “There is always that you have to dig up that phone if you mean to use that card.” [i7] “Yeah, it's the cell phone .. I do not always carry it.” [i2]	40
Using the application	“Well if it was installed and put in then of course I would use it.” [i9] “But it occurred to me that if they started putting them on smartphones, then older people like me would no longer be able to use them.” [i1] “If you learned to use it then it could be just fine.” [i2] “Is the identification difficult?” [i3]	40
The fact that it is a phone app, overall		70

Table 15 User experience research findings, Perceived worries

Perceived worries that came up from the conducted interviews consisted of two major categories that were security and the fact that the solution is a mobile application. All of the interviewees were concerned about security, at least to some extent, some more than the others. Security concerns were related to topics such as hacking, single point of failure, misuse of cards, information privacy, data collection and general information security with the importance of information privacy being mentioned most often. Some worries also surfaced from using the mobile application such as losing the device, the need to get digital membership cards, the need of carrying a phone, and installing and using the application. Especially the elderly were lacking the confidence in their abilities to use the application.

Contemporary pains

FEATURE	QUOTE	% OF RESPONDERS
Inconvenience of physical cards	"(Membership cards) feel cumbersome because I have to carry them always with me. And when I try to find the right card from 20 it takes time. I think membership cards are stupid."[i1] "...Sometimes some cards are at home when you need them. (With the app) they'd be always with me." [i4] "In my opinion (membership cards) are in some ways good, but a little cumbersome when having many. I think it is important to find a solution to this".[i8]	40
Data collection	"Well I do not use membership cards myself, but I think it's bothering me, that always need to have phone when doing shopping and it gives me a dystopian feeling when everything is digitalized" [i10]	10
Pains, overall		50

Table 16 User experience research findings, Contemporary pains

Missing functionalities

We asked the interviewees whether they can think of any other functionalities that they would like the application to have. Functionalities they mentioned included issuing payments: "*It's awkward if you have to open things separately, you should be able to access the benefits and payment options at the same time*" [i8], cross usage/backup for the physical cards: "*those cards may be lost and if you have that app enabled then they will not be lost. So, then I think it would be handy if that application would be sort of a backup*" [i10] and a way to find new memberships: through it one could find some services where one is not yet a member but could be interested or gain benefits" [i6].

6.1.3 User Research Conclusions

In this part we propose requirements for the system and discuss the results. Based on the research we propose following requirements for the membership application. Requirements can be either functional or non-functional. Functional requirements define what the system should do. Non-functional requirements do not define what the system should do, but rather how it should work.

1.

User story: As a card holder, I want to know how damages to myself are limited in case of someone stealing my cards information or my password so that I can feel confident about applications security.
Acceptance criteria: Processes to revoke the memberships in case of robbery or data leak needs to be in place. The process must be communicated to users transparently and clearly before the accidents and after the accidents. User tests should be run to test and verify the clarity of the communication. The whole process of revoking memberships must be tested.

2.

User story: As a card holder, I want to know what I have to do if I am a victim of theft, or I lose my password so that I can gain back control of my memberships.
Acceptance criteria: Processes for users to gain back the control of the memberships need to be in place. Users must be clearly informed about the processes and what responsibilities they have. User tests should be run to test and verify the clarity of the communication.

3.

User story: As a card holder, I want to know how my information is used by the parties I share my information with so that I can trust them with my information.
Acceptance criteria: Data usage is communicated clearly with card holders. User tests should be run to test and verify the clarity of the communication.

4.

User story:

As a card holder, I want to be able to see an overview of all the information I have shared so that I can easily have a clear understanding of what I have shared.

Acceptance criteria:

In the application an overview or a summary of the information shared can be found.

5.

User story:

As a customer, I want to be able to have all my membership and subscription cards easily available and ready to be used so that I can take advantage of discounts and so on that companies offer to me without extra hassle.

Acceptance criteria:

Users can easily and without frustration use the digital cards even if they have a large number of memberships (+100). User tests should be run to test and verify the usability.

6.

User story:

As a customer unconfident in my skills using a smartphone, I want to be able to use the app so that I do not get left out because of technology advancement.

Acceptance criteria:

In the end-user tests, users that are unconfident with technology can use all the features of the app without difficulties, including installing the app and adding new memberships.

7.

User story:

As a customer who doesn’t always carry a phone with me, I want to be able to get the benefits of my membership even if my phone is not with me so that I get the benefits of my membership even if I left my phone at home.

Acceptance criteria:

Discounts, bonuses and benefits of such can be claimed afterwards.

6.1.4 Research Discussion

Our sample for this research was quite biased towards age groups that are not very skilled with digital technologies. According to Norman & Nielsen Group, many digital products still discriminate against elderly people (Norman & Nielsen Group, 2019). Also, it is expected that digital products that are easy to use for people who are not technically skilled will also be easy to use for people who are technologically skilled. Therefore, it is important to gather perceptions of the elders in research like this.

Our interviewees saw benefits with the SimplyMember-idea, but they also had worries about it. Of the interviewees 90% mentioned the applications convenience as a benefit, with benefits focusing on not needing to carry any physical cards, to ease of use. In comparison, only 30% mentioned transparency and user control as potential benefits.

Every interviewee worried about the applications security, citing potential hacks and privacy issues as their main worries. 70% worried about it being a phone application and the problems this might cause if, for example, they lost their phone.

Half of the interviewees identified contemporary pains, that is, they had struggled in some way with membership cards. These issues were either the inconvenience of physical cards, or they had issues with the way data is collected and digital devices needed for simple tasks such as shopping. It should be noted that only one of the participants indicated that the way data is collected currently is problematic, therefore in general in our sample people didn’t find the data collection currently problematic.

From these we can recognize that in order to entice people to use the SimplyMember-application, the people should be shown the benefits of using such an app, while also allaying their fears about issues such as security. Many interviewees showed frustration with the current membership card system and would be willing to use an application instead.

However, as one interviewee suggested, not all companies would be using this application, and the numbers might be especially small at launch. Further research could be done in this area, to see if there exists a tipping point on the number of companies using the app before an individual might be willing to start using it.

6.2 Wallet Requirements and Design

In this section, we describe the lists of functional and nonfunctional requirements for the SimplyMember wallet application from a holder's perspective. The SimplyMember proof-of-concept demo application was set up using CREDEBL platform and an identity wallet called Adeya. The platform and the wallet are developed by a startup called Blockster Labs[15] who offered the course participants a change to demo their solution as well as expertise in the field of developing SSI-based solutions.

For the best understanding for the digital wallets the user needs to distinguish between different types of digital wallets, and what are different purposes they are used for and what is the level of security for each type. We downloaded and tried different wallets, like Electrum, in order to understand which digital wallets are going to support the SSI. Electrum, for example, was easy to use but not suitable for the use cases as it is mainly used for holding bitcoins not VCs. We also downloaded and used the Trinsic Wallet16, and Connepct.me[17], and both the digital wallets were good for saving VCs.

Next, we will introduce the functional and non-functional requirements for the wallet application. At least the following functional and non-functional requirements must be considered when the developing team starts to work on the actual application.

6.2.1 Functional Requirements

- Setting up the wallet for the user (holder). All these requirements were for security purposes users wanted to guarantee that their data and credentials are safe.
    - PIN code
    - Biometrics sign in
    - Ask user for consent to utilize phone's memory card (privately) to store the VCs and camera for scanning QR codes
    - Ask for user to agree on terms and conditions
- Wallet customization to grantee that they will be able to have an easy access for the wallet.
    - Profile picture, nickname, language preference
    - Ability to change the PIN code
- Ability to set a backup and recovery to cloud to grantee that they will not lose their information and their VCs

[15] https://blockster.global/
[16] https://studio.trinsic.id/
[17] https://www.connect.me/

  - Addressing the risk of phone getting lost or stolen
  - Ability to connect with organizations (e.g., S Group, Kesko, Gold Gym) with QR codes. users wanted to grantee fast use and easy access
  - Alternative methods possible, e.g., manually putting a code
- Ability to accept or decline the offered VCs in the app to grantee to grantee that they would have free choices concerning their VCs.
- Present the wallet's contents (VCs) to the user to grantee transparency and clarity and easy access
  - Search functionality, categorizing user's VC cards into lists to facilitate finding them
- Ability to accept(answer) or decline the requested VC presentations to prioritize their VCs and have quick and easy access
  - Selective disclosure

Verifiable credentials that are presented to the holder should include information about:

- Identifying the subject
  - Full name, type of membership, etc.
- Issuing authority
  - S Group, Kesko or the gym company
- Constraints of the credential
  - Expiration date, terms of use
- Activity related to the credential
  - When issued, when presented

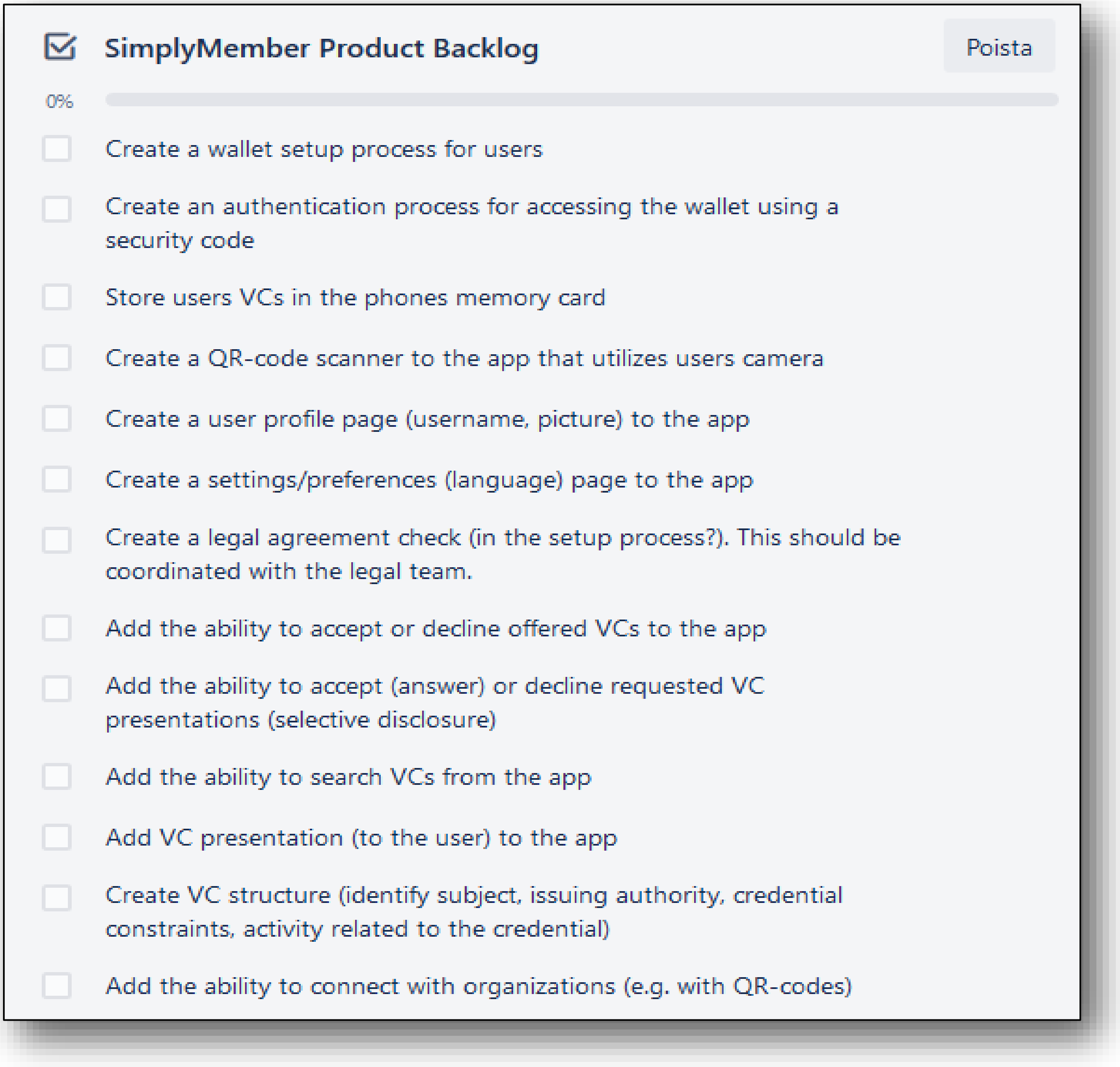
6.2.2 Non-Functional Requirements

- Good performance: To execute the verification efficiently within a short period of time
  - Response times: application loading, refresh times etc.
  - Processing times: Minimum amount of time needed to connect to the blockchain to verify the credentials and reflect them to the verifiers.
- Privacy: Users should be able to control the amount of information shared with verifies and the ability to customize it when needed.
  - Users should be able to choose who to disclose their data with and who to ignore.
  - Anonymous representation: When verifying the credentials, the user should be presented as an identity, not as an actual person.
- Security: Users need a guarantee for confidentiality, availability, and integrity of their data.
- Usability: Users need a wallet application that is easy and comfortable to use.

    - Learnability: Enable the user to learn how to use the wallet effectively.
    - Aesthetics: Attractive and constant interface that understandably guides the user to use the wallet.
- Reliability, availability, and operability: Ability to keep the application in a safe and reliable functioning condition.
    - Being able to successfully identify events that are critical to the application’s success.
- Transparency: The amount and type of data that is requested from the user to get the wallet application working needs to be disclosed clearly to the user.
- Following the data flow: Users should be able to have the option to track the incoming and outgoing data flow in the wallet application
- Scalability: The wallet should be developed in a way that it can work fluently even with a high number of users and organizations.
- Portability: The wallet application should be able to work in different environments, at least Android and iOS.
- Interoperability: The wallet solution should allow identification to cross organizational borders without users losing control of what information is shared. Individuals should be able to maintain their identities across platforms and geographical locations.

6.2.3 Wallet Development Product Backlog

Product backlog for the functional requirements shown in Figure 14 Product backlog for the wallet functional requirements:



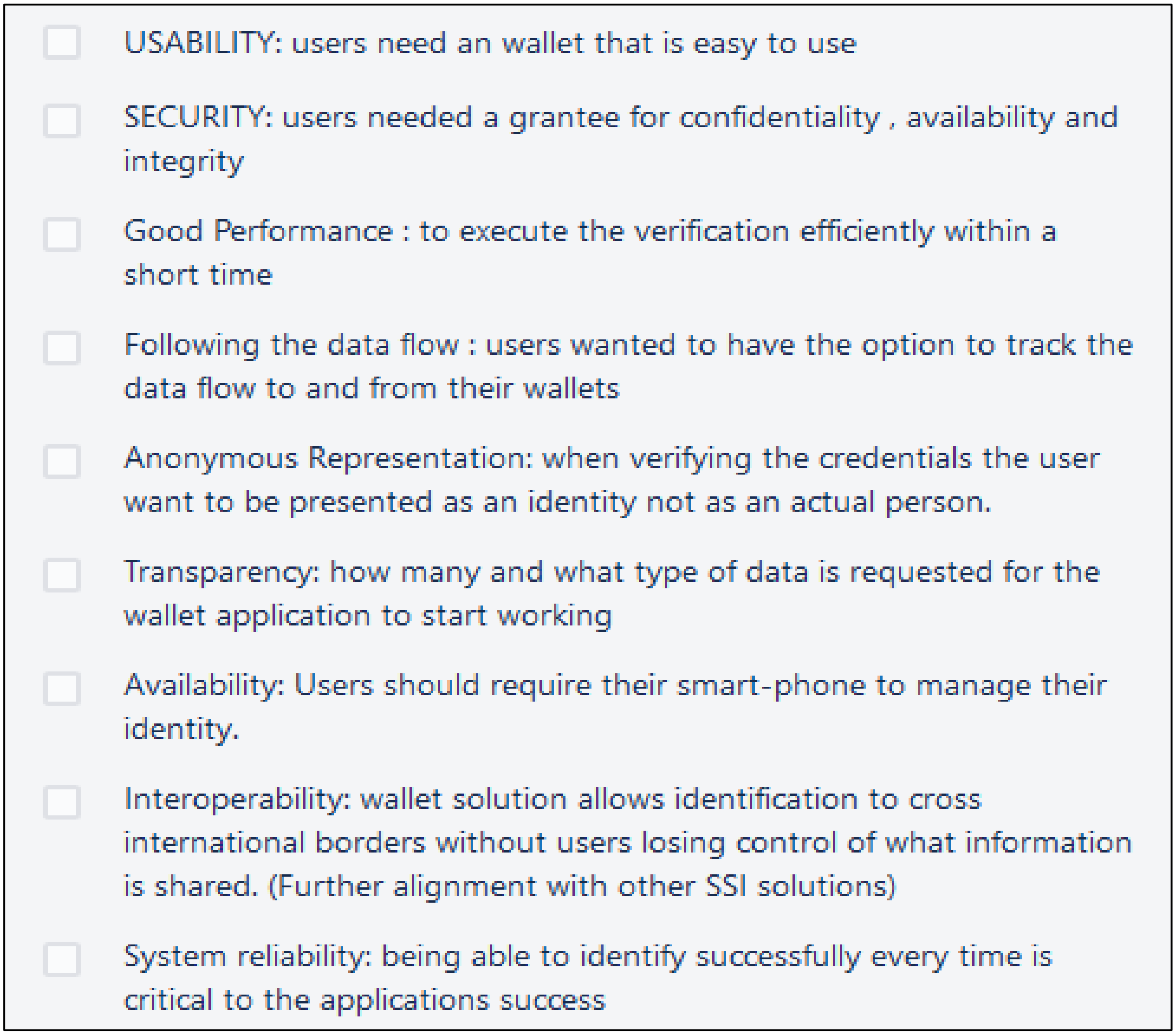
☑ SimplyMember Product Backlog

0%

- □ Create a wallet setup process for users
- □ Create an authentication process for accessing the wallet using a security code
- □ Store users VCs in the phones memory card
- □ Create a QR-code scanner to the app that utilizes users camera
- □ Create a user profile page (username, picture) to the app
- □ Create a settings/preferences (language) page to the app
- □ Create a legal agreement check (in the setup process?). This should be coordinated with the legal team.
- □ Add the ability to accept or decline offered VCs to the app
- □ Add the ability to accept (answer) or decline requested VC presentations (selective disclosure)
- □ Add the ability to search VCs from the app
- □ Add VC presentation (to the user) to the app
- □ Create VC structure (identify subject, issuing authority, credential constraints, activity related to the credential)
- □ Add the ability to connect with organizations (e.g. with QR-codes)

Figure 14 Product backlog for the wallet functional requirements

Product backlog for the nonfunctional requirements shown in Figure 15 Product backlog for the wallet nonfunctional requirements:



□ USABILITY: users need an wallet that is easy to use

□ SECURITY: users needed a grantee for confidentiality , availability and integrity

□ Good Performance : to execute the verification efficiently within a short time

□ Following the data flow : users wanted to have the option to track the data flow to and from their wallets

□ Anonymous Representation: when verifying the credentials the user want to be presented as an identity not as an actual person.

□ Transparency: how many and what type of data is requested for the wallet application to start working

□ Availability: Users should require their smart-phone to manage their identity.

□ Interoperability: wallet solution allows identification to cross international borders without users losing control of what information is shared. (Further alignment with other SSI solutions)

□ System reliability: being able to identify successfully every time is critical to the applications success

Figure 15 Product backlog for the wallet nonfunctional requirements

6.2.4 A Simple User Workflow for the SimplyMember Wallet

Below we will introduce how the SimplyMember identity wallet works from the holder's perspective. The ADEYA [18]wallet is offered by our company partner in the course, Blockster Labs.

[18] https://apps.apple.com/us/app/adeya-wallet/id1561779080 https://play.google.com/store/apps/details?id=com.credebl

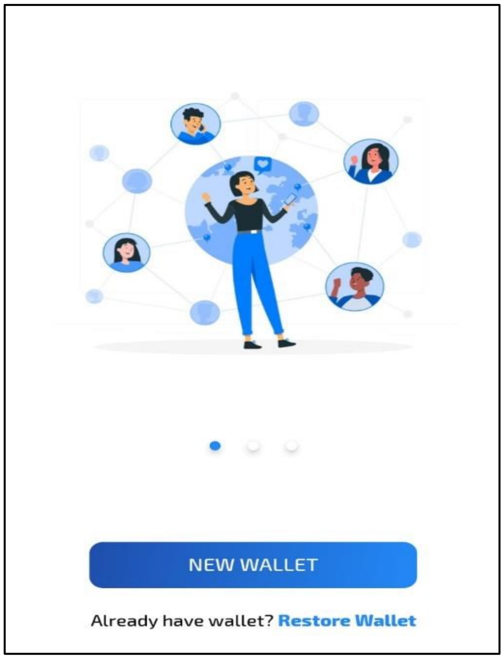


Figure 16 New wallet creation

Step 1–Downloading and starting the wallet

In this step the user should download the wallet on their mobile device and start it.

User can choose between two options as shown in Figure 16

- Start new wallet
- Restore an old wallet

This will be the users first wallet so the user should choose a new wallet.

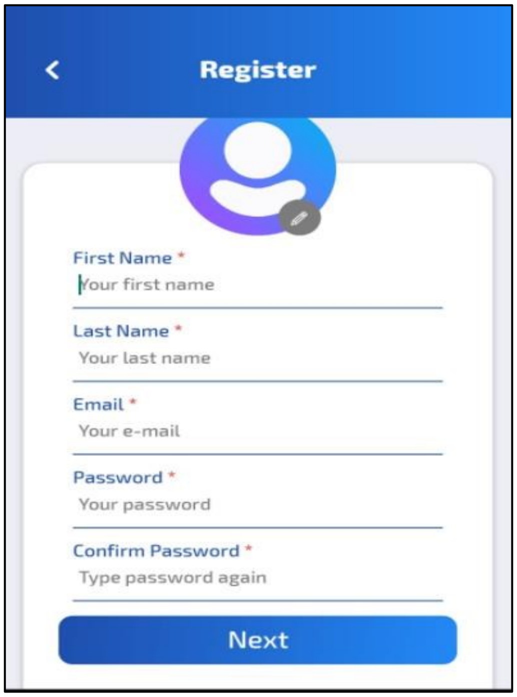
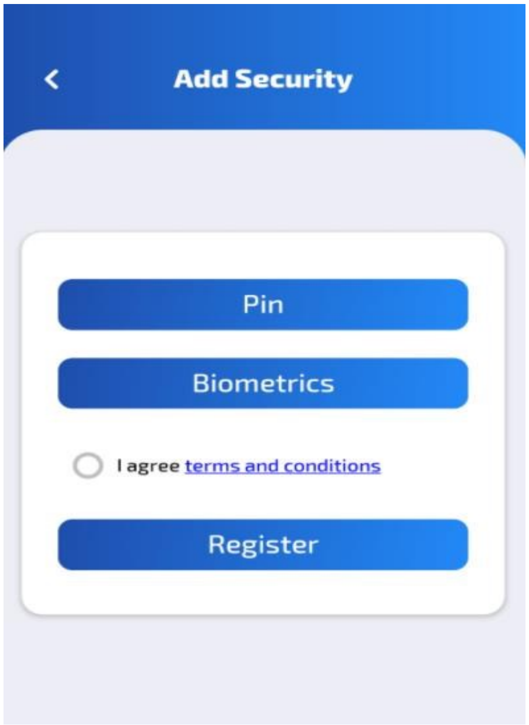


Figure 17 New wallet registration

Step 2–Registration In this step, the user should fill in their persona as shown in Figure 17 I in order to register They need to fill in their:

- First name
- Last name
- Email address that will be connected to the wallet
- The password



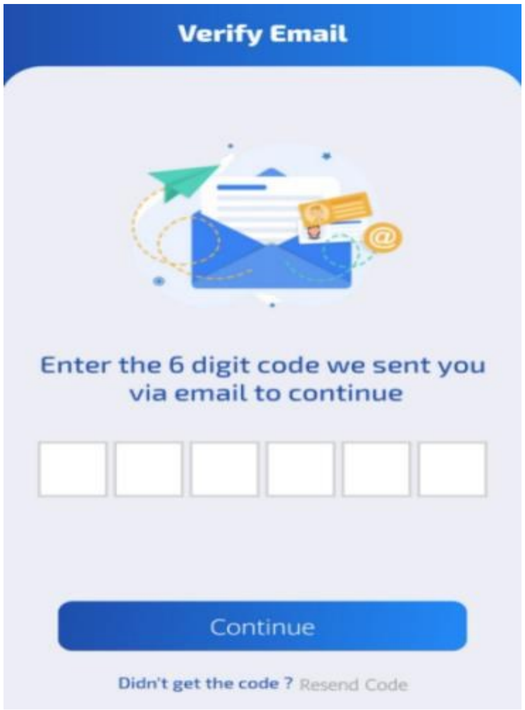
○ I agree terms and conditions

Figure 18 New wallet security types

Step 3–Add the security

In this step the user can decide how they would like to secure their account. The user can choose pin code, biometrics, or both.

User should read and agree to the terms and conditions and then register as shown in Figure 18



Enter the 6 digit code we sent you via email to continue

Figure 19 Wallet verification code

Step 4–Verifying Email

The user will get an email with a verification code to their registered email with a six-digit code.

The user must enter this code to the wallet in order to verify the email and start the wallet as shown in Figure 19

Step 5–Starting the wallet

Now the wallet is ready to be used as shown in Figure 20. The user can now customize the wallet options, add credentials, add proof requests and add new connections.

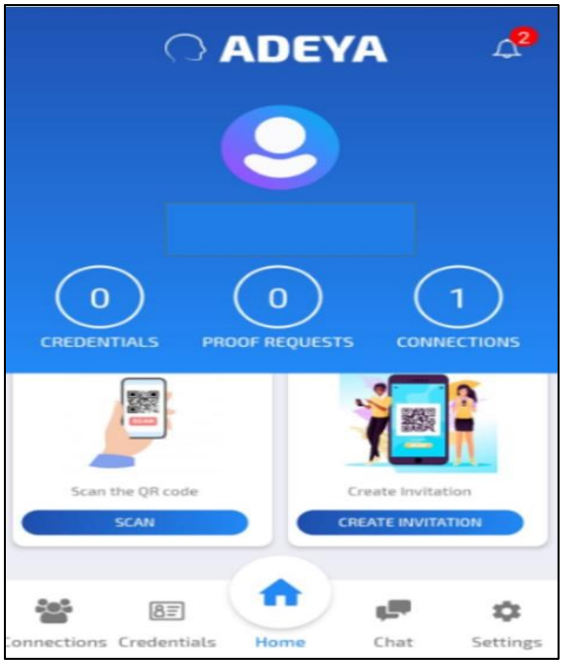
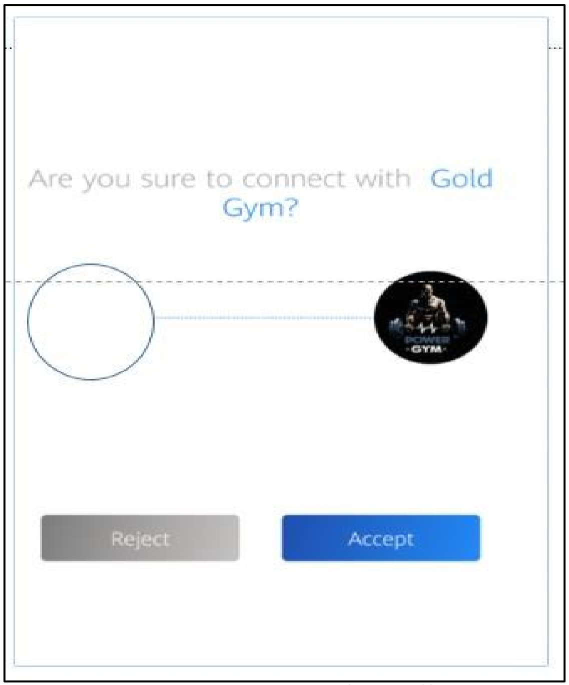


Figure 20 User's wallet main view

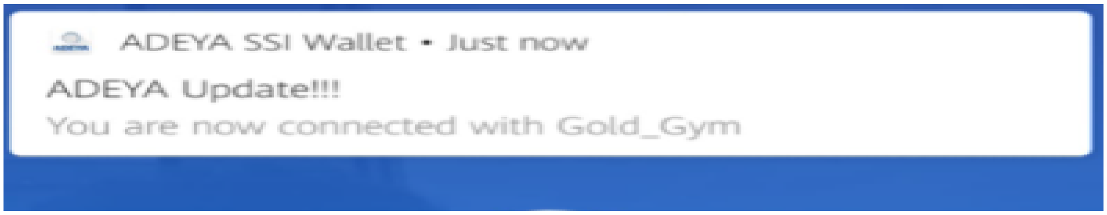
Step 6 – Using the wallet

To use the wallet, click on scan the QR code > scan the QR code > or choose your connection. The user should accept the connection as shown in Figure 21. Then the connection is now approved, and the user will receive a notification as shown in Figure 22.



Are you sure to connect with Gold Gym?

Figure 21: Using the wallet



ADEYA SSI Wallet • Just now

ADEYA Update!!!

You are now connected with Gold_Gym

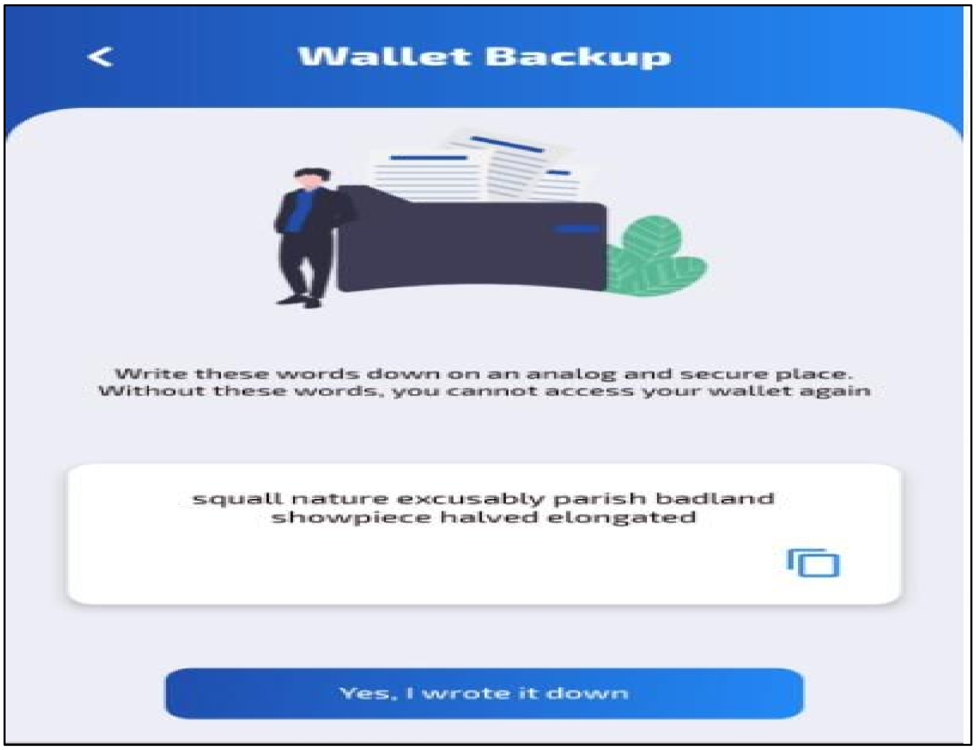
Figure 22 Wallet user notification approving connection

There are few points that need to be considered while installing the wallet that would make the user experience more efficient and easier.

Taking a wallet backup

It is advised to make a wallet backup. If the user's phone is lost or they want to install the wallet on another device, they will need to back up their wallet.

First select Setting > wallet backup. The wallet will show a recovery phrase that can be used to recover the wallet again. Then the user needs to verify the recovery phrase. The wallet backup is shown in Figure 23.



Wallet Backup

Write these words down on an analog and secure place.
Without these words, you cannot access your wallet again

squall nature excusably parish badland
showpiece halved elongated

Figure 23 Wallet backup

The user should keep the recovery phrase in a safe place. Users can send it to their email as shown in Figure 24.

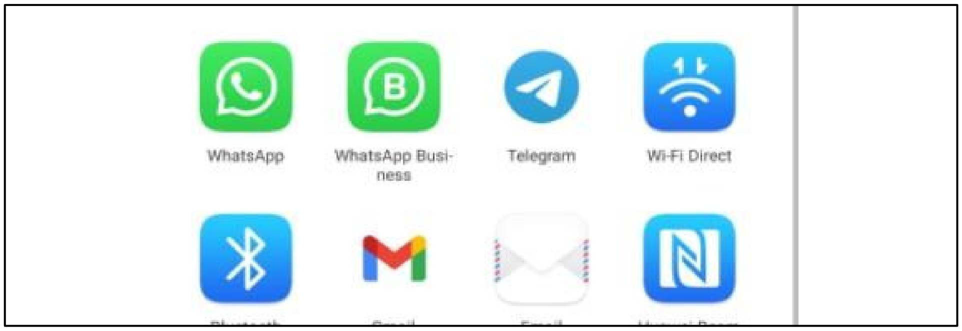


Figure 24 User icons to send the seeds

Categorizing the credentials

The user can create categories for their cards in order to make finding and using them easier as shown in Figure 25. Use the Credential tab > Add (+)> Create the category > Save.

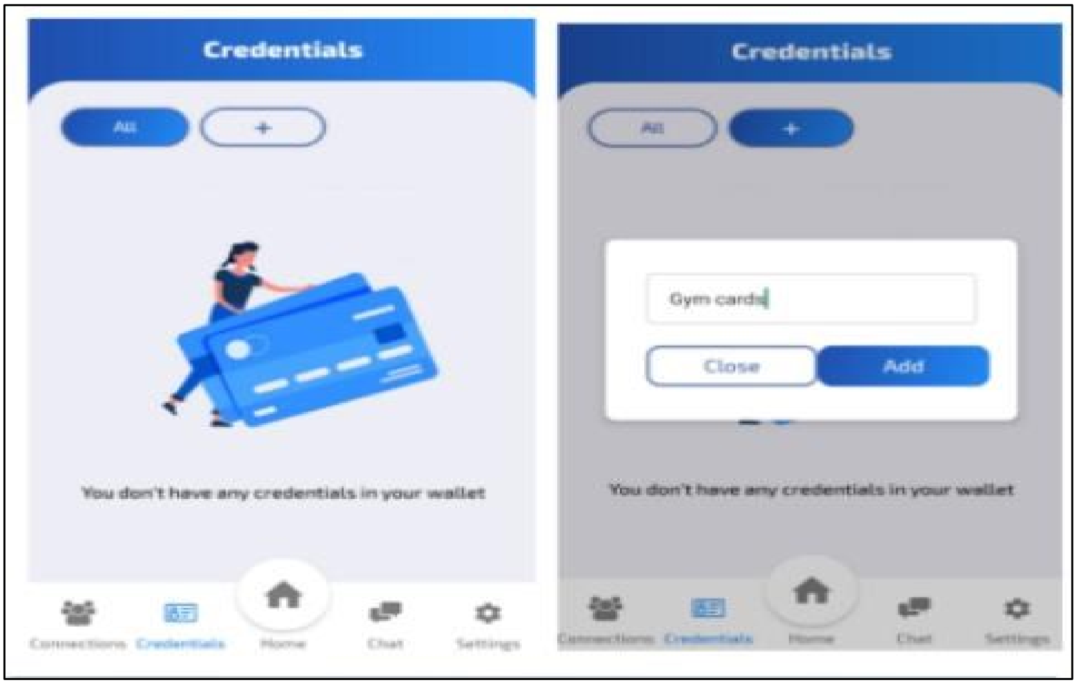


Figure 25 Wallet credential tab

6.3 Proof Of Concept, Demo of SimplyMember

Next, we introduce SimplyMember's demo in its early stage. The demo was built using a credential platform called CREDEBL[19], and an identity wallet ADEYA[20] by Blockster Labs.

The solution was first developed for two chosen digital membership use cases: retail membership and gym membership representing SMEs (workflow shown in Figure 26). The retail use case (workflow shown in Figure 27) includes two largest retail chains in Finland, Kesko Corporation and S Group cooperative. The two videos serve as a proof-of-concept demo for the SimplyMember solution.

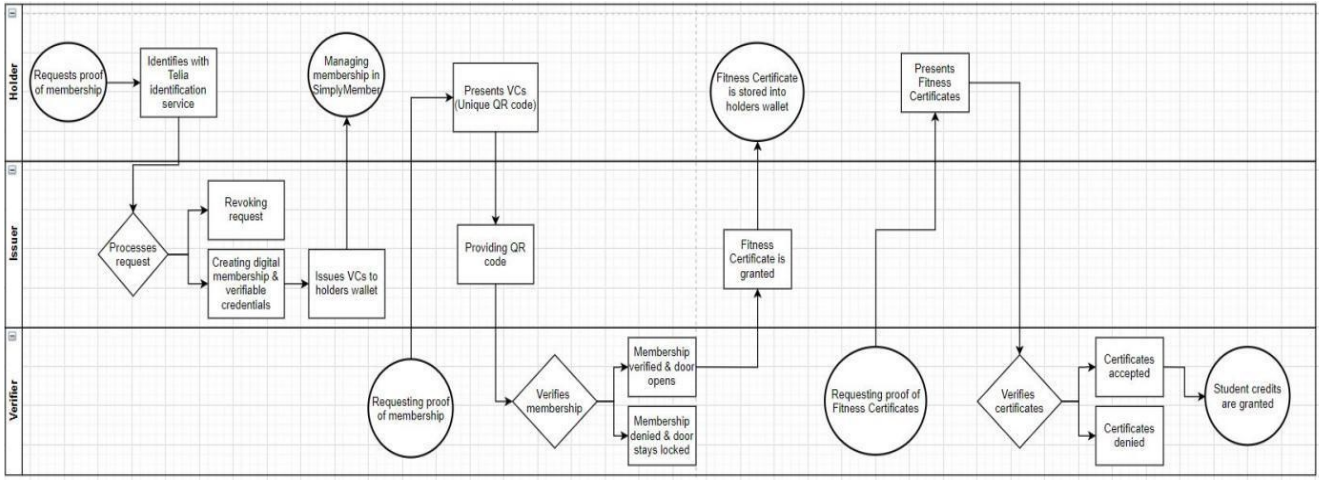

Holder
Issuer
Verifier
Requests proof of membership
Identifies with Telia identification service
Managing membership in SimplyMember
Presents VCs (Unique QR code)
Fitness Certificate is stored into holders wallet
Presents Fitness Certificates
Revoking request
Processes request
Creating digital membership & verifiable credentials
Issues VCs to holders wallet
Providing QR code
Fitness Certificate is granted
Requesting proof of membership
Verifies membership
Membership verified & door opens
Membership denied & door stays locked
Requesting proof of Fitness Certificates
Verifies certificates
Certificates accepted
Certificates denied
Student credits are granted

Figure 26 SimplyMember Gold Gym use case visualized as a workflow chart

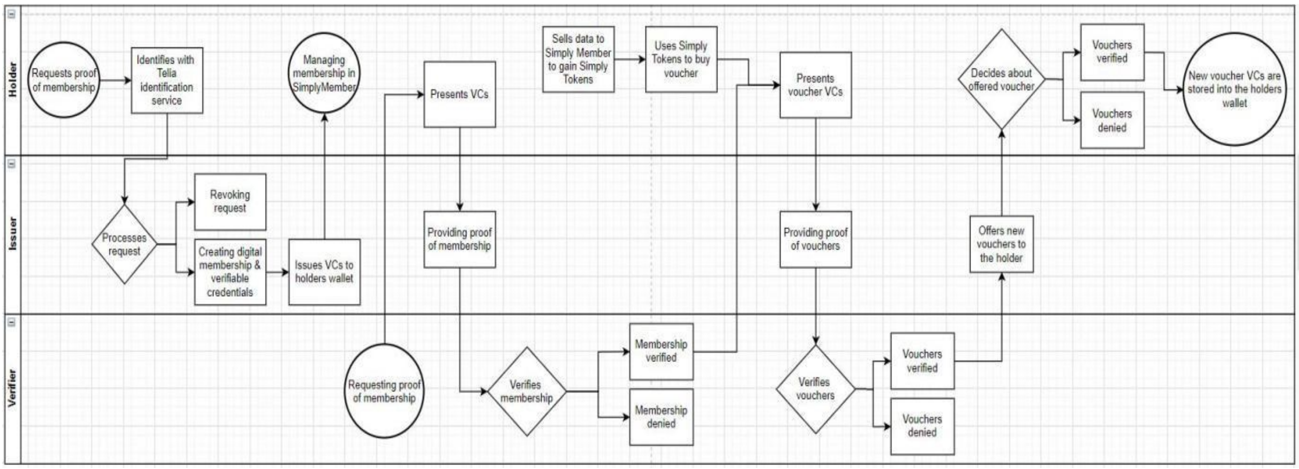

Holder
Issuer
Verifier
Requests proof of membership
Identifies with Telia identification service
Managing membership in SimplyMember
Presents VCs
Sells data to Simply Member to gain Simply Tokens
Uses Simply Tokens to buy voucher
Presents voucher VCs
Decides about offered voucher
Vouchers verified
Vouchers denied
New voucher VCs are stored into the holders wallet
Revoking request
Processes request
Creating digital membership & verifiable credentials
Issues VCs to holders wallet
Providing proof of membership
Providing proof of vouchers
Offers new vouchers to the holder
Requesting proof of membership
Verifies membership
Membership verified
Membership denied
Verifies vouchers
Vouchers verified
Vouchers denied

Figure 27 SimplyMember retail use case visualized as a workflow chart

[19] https://blockster.global/products/credebl/

[20] https://blockster.global/products/adeya/

Team 3 responsible for creating the SimplyMember proof-of-concept collaborated with the consultants from Blockster Labs in order to configure the Simplymember solution on CREDEBL platform. Both the platform and the digital wallet application ADEYA were used in the demoing the solution. The ADEYA wallet application is available to download to holders' phones from Google Play[21] for Android and App Store[22] for iOS. In the end of the 6-week development period, it was possible for the course participants to issuer and receive verifiable credentials, VCs, for the Gold Gym use case.

Next, we will introduce the two SimplyMember use cases and demo how to use the CREDEBL platform and the ADEYA wallet in a video format.

6.3.1 Gold Gym Membership, the SME Use Case

The Gold Gym was created as an example for the SME use case. In this video we will also demo how to configure SimplyMember on the CREDEBL platform, how to create new issuers and wallets on the platform and present what information the issuers can see and what can they do in the application.

The Gold Gym demo video includes the following action points:

- Gym offers a membership credential.
- Holder stores the credential in the wallet.
- User goes to the gym and presents a QR-code to proof membership.
    - If the membership is accepted, the gym door opens, and the user receives Fitness Certificate.
- Fitness Certificate is issued by the gym to user's wallet.
- The holder presents the certificate to the verifier.
- The certificate is verified.

[21] https://play.google.com/store/apps/details?id=com.credebl

[22] https://apps.apple.com/us/app/adeya-wallet/id1561779080

6.3.2 The Retail Membership Use Case for Kesko and S Group

For the demoing purposes, the retail use case demo video presents the process of receiving tokens and using them to buy vouchers. Also, the holder has now ability to decide if they want to collect the offered voucher or not.

Ideally, the identification and authorizing in the SimplyMember solution would be offered by a common identification service, such as Suomi.fi. However, currently the Suomi.fi service can only be used in public corporations. Thus, in our demo we use Telia's identification services.

Use case for the retail membership (Kesko and S Group) includes the following action points:

- User downloads the ADEYA wallet application and gives any needed permission.
- User registers and applies membership.
- User identifies with an identification service.
- User is accepted as a member.
- Verifiable credentials are issued to user's wallet (with the relevant information only).
- User has tokens which are exchanged to discount vouchers.
- User goes to a store and purchases items with the vouchers
- User searches vouchers from the wallet application.
- User presents the vouchers to the verifier.
- Verifier accepts the vouchers.

- Store offers new vouchers for the user.
  - User can accept or decline voucher.
  - If accepted, new verifiable credentials are issued to user’s wallet application.

7 Legal and Regulatory Contexts for SSI

In the following section, our main goal is to understand and identify the applicable legislation and legal framework which can be built to launch SimplyMember service based on Self-Sovereign Identity. According to our current understanding of the SimplyMember use cases and the current legislation, the solution facilitates a digital wallet platform. First, as SimplyMember exploits personal data, it is compatible with GDPR regulation. The user has to agree legally, that their information is being used and stored. Any service based on EU-based customer data must comply with GDPR "by design by default" and consider data protection.

We used the Sovrin Foundation (2018) as a base for our regulatory requirement analysis as Sovrin network is a stable identity metasystem for SSI with a highly developed governance framework. The foundation states in their white paper that this kind of a new marketplace can support GDPR-compliant privacy preservation. This could be possible to match and ensure with the Sovrin privacy by design implementation. The privacy as the default setting covers three different levels, like Pseudonymity by default, private agents by default, and selective disclosure by default. Sovrin also strongly follows GDPR to adjust their user rights.

Further, Sovrin ensures that no private data is stored in its ledger, even in encrypted form; this would be a great advantage towards the GDPR regulation practices.

7.1 The Key Legal Challenges to Be Considered

- The regulation of utility tokens and questions around the tech neutrality
- The regulation of Decentralized Finance and decentralized token issuance
- Configure the GDPR and/or applicable regulation according to the nature of blockchain tech
- Right to be forgotten
- Issues with Private key loss

7.2 General Data Protection Regulation (GDPR)

When observing the area of blockchain, there is no such thing as a GDPR-compliant blockchain technology, only GDPR-compliant use cases and applications. As we mentioned above, any service based on EU-based customer data must comply with GDPR "by design by default" and consider data protection. The content of GDPR aims to protect consumer's rights to their data by rights to: To access, erasure, to be informed, restrict processing, portability, rectification, object, and rights to related automated decision making.

The blockchain of SimplyMember does exploit personal data and is therefore compatible with GDPR regulation. In this case the user must agree legally, that their information is being used and stored. SimplyMember collects data regarding user behavior, and this is on their responsibility to store with cyber security standards. Kesko and S Group are responsible for user's information, such as memberships as shown in Figure 28 The blockchain is responsible for following up to GDPR, and in this case, we have concluded that service utilities (Sovrin/Ethereum) need to be chosen to adapt GDPR and SimplyMember has to carry their responsibility for a good GDPR-governance.

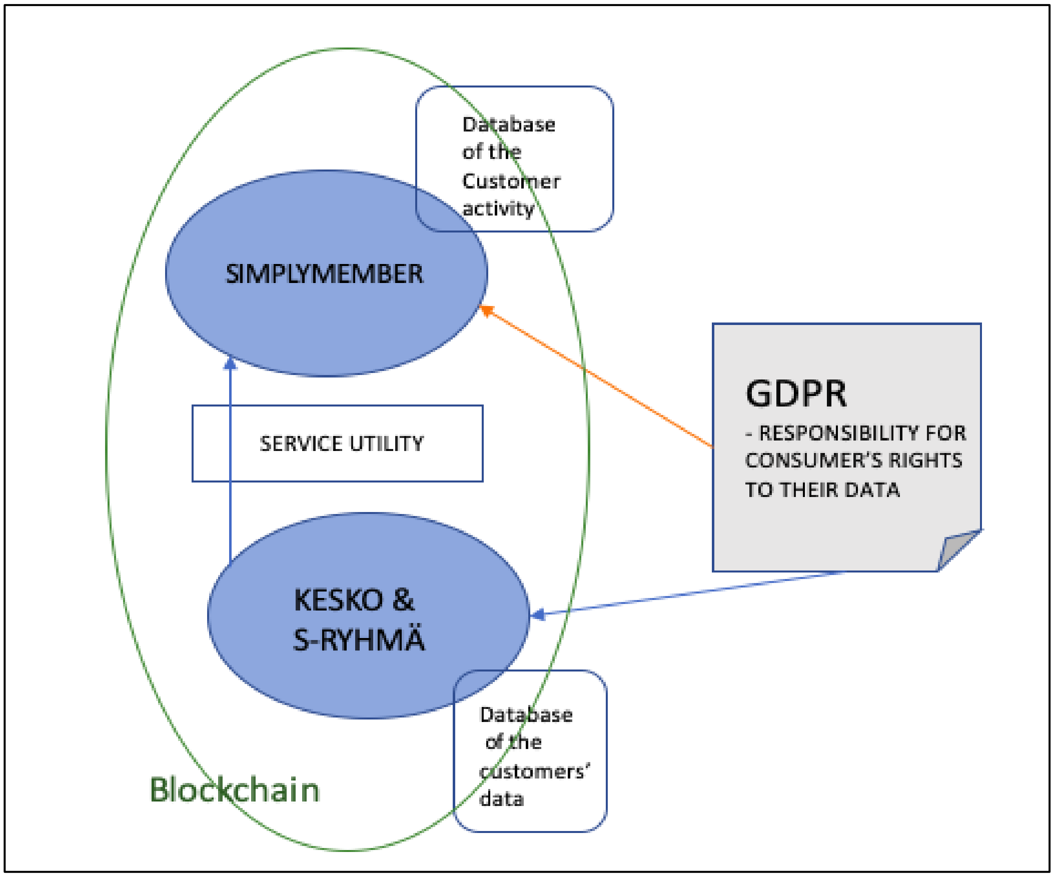

Database of the Customer activity
SIMPLYMEMBER
SERVICE UTILITY
GDPR
- RESPONSIBILITY FOR CONSUMER'S RIGHTS TO THEIR DATA
KESKO & S-RYHMÄ
Database of the customers' data
Blockchain

Figure 28 GDPR effects for SimplyMember in the retail use case

If SimplyMember's network was developed on Sovrin, it would be possibly exploiting Sovrin as a service provider to exchange the data. Sovrin has acknowledged GDPR in their conditions. If SimplyMember chooses to exploit another blockchain technology, such as Ethereum-based token, the compliance with GDPR must be taken notice. Also, the governance will change in this case.

Additionally, each of the possible network has their own agreements that SimplyMember needs to consider. For Sovrin the agreements would be for example Sovrin Web of Trust Governance Framework, Sovrin Governance Framework[23] and other contracts associated with Sovrin. The Sovrin Foundation also has mandatory obligations toward SimplyMember and to other users to provide information about changes to its network or policies. Sovrin, its committees, working group and board of trustees, do the different governance of Sovrin policies.

7.3 Conclusion on SSI Legal and Regulatory Context

According to our observation in certain sections, Sovrin handles the issues in an innovative way like the right to be forgotten can be achieved by strongly disallowing or never putting any private data on the ledger, instead of placing the DID and allowing the process safely and securely. This stage clearly categorizing and classifying the data and following the strict rules on the processing could mitigate the risks.

However, encryption has a certain lifetime. In case of a data breach or break the encryption by using advanced technologies like quantum cryptography or computing can lead to the immediate risk is that private keys of the encrypted data would be disclosed from globally replicated data records. This would be a real disaster. Further, there are developments and research progressing to handle these challenges and issues.

Thus, SimplyMember ecosystem should mitigate the risks and can avoid legal issues associated with SSI and blockchain by following a well-structured legal framework based on applicable guidelines widely in the EU and internationally.

Overall, the best way to adapt the regulatory landscape involves giving all the stakeholders adequate and accurate information in a comprehensive and clear manner along with building the smart legislation strategy. Further, once set up the clear legal framework structure, keep the highest priority for the regular documentation audit.

[23] https://sovrin.org/library/sovrin-governance-framework/

8 Marketing Strategy and Impact Measures

In this section we will describe how SimplyMember is going to penetrate the digital identity market and how we will set goals to the ecosystem growth. First, we analyzed the potential customer for the solution and did a situation analysis on the current market. Next, we defined measurement and control tools for the success of the developed marketing strategy.

8.1 Creating a Marketing Strategy

The promotion plan's main objectives are twofold. First if we look at the initial promotion plan from the ICO's point of view we can establish that the most important goal is to make possible investors aware of this new self-sovereign system that makes membership cards more secure, reliable, and easy to use. As the blockchain industry is still quite young and narrow at the moment it is important to gain attention to the benefits of the solution in this expanding industry. Our initial promotion plan is meant to draw attention and interest towards the SimplyMember solution, leading to a successful crowdfunding campaign and launch of SimplyMember.

When we look at the initial promotion plan from the end user's perspective, we can see that the objectives are somewhere similar to the ICO point of view. It is important to add knowledge of the SimplyMember solution, to gain a good amount of end users for the solution in the early phase of the launch. Our initial promotion plan aims to give a tempting Figure of the solution that will draw end user customers to take the solution into active use. Of course, when end users show interest in the solution, more companies offering memberships want to be involved in SimplyMember.

As a conclusion of the initial promotion plan objectives could be said that it is essential to achieve attention and interest of possible investors in the ICO phase, but also to gain the interest of end users who will after all be the ones using SimplyMember solution.

8.2 Situation Analysis

The current market state including the competitors will be analyzed with guidance of the Porter's Five Forces Framework which helps us to determine changes and rivalry in the given market. Customers are in control over the currency they want to make transactions and where to store assets, anyone can trade, and direct payment solutions are offering a substitute to traditional banking solutions.

8.2.1 Competitive Rivalry

The most prominent competitor in the field is Stocard, a company providing a mobile loyalty card application for cards from multiple providers. The company claims to have over 60 million users globally, and it provides the service to end users for free. The application supports collecting reward points for the loyalty cards added, and it is possible to browse through coupons, discounts, and advertising magazines through the app. Any card can be added to the wallet by reading a QR-code.

Stocard does not appear to use blockchain technologies in their solution. Another key competitor not using blockchain, Key Ring with over one million downloads on Google Play claims to have discontinued their service in the EU due to the new requirements set by GDPR.

There are some existing loyalty platforms based on blockchain as well. One of these, LCredits (LYL) acts as a single token system for loyalty rewards, built as an ERC-20 token. They offer their customers the possibility to store loyalty points on a mobile wallet, and to convert them to other cryptocurrencies or fiat currencies.

8.2.2 Threat of New Entrants

The barrier for entering the competition of providing blockchain-based multi-card applications is high due to the young age of the technology and the lack of major existing solutions built using blockchain. Major groundwork must be done in order to develop the systems in an emerging field.

8.2.3 Threat of Substitute Products

The threat of absolute substitute products appearing on the market is low, but not nonexistent. Blockchain as a technology has existed long enough for it to be considered a practical foundation for secure applications to be built on, and it currently allows the unique, secure, and scalable basis that is unlikely to be substituted in a quick period of time.

8.2.4 Bargaining Power of Suppliers

One benefit of developing the SimplyMember solution on blockchain is the lower presence of suppliers such as hosting capacity providers due to the decentralized nature of Sovrin and blockchain in general. Using open-source solutions in the technical development also decreases the number of tech-suppliers in the mix. Key suppliers are found in the mobile application store industry, as distributing the application is practical via the largest stores such as Google Play and Apple iOS App Store.

8.2.5 Bargaining Power of Buyers

The amount of traditional physical membership card users worldwide is massive, and most membership cards are still issued as physical cards. We therefore see the bargaining power of buyers to be mostly affected by the ability to substitute these physical cards instead of opting for e-cards. The promotion must therefore especially support the benefits given by the technological advancements in the SimplyMember solution, such as the security, centralization of memberships and trust.

8.3 Target Market Description

Based on customer analysis and situation analysis we came together with target market description.

8.3.1 Holders

The target market consists of young adults to middle aged adults aged approximately from 18 to 49 and of both males and females. Geographical area of our target market is Finland and especially people living in urban areas with different services within their reach. As a target market location Finland is characterized by a high level of digitalization and the high quality of services. That's why Finland is a favorable location for SimplyMember. The values of the target market audience are for example reliability and practically as well as accessibility. Also, the target market audience is likely to maintain a rather active lifestyle and use multiple different services.

8.3.2 Issuers

In the SimplyMember solution, the customer organizations are seen as the issuers who provide the membership cards into the wallets of the holders in a digital form. This is achieved through an SSI component called Decentralized Identifier (DID), which is written together with a public key to a blockchain. The targeted issuers are organizations providing membership cards and bonus/loyalty cards, such as large Finnish retailer chains S Group and Kesko (K Group stores). Another key target issuer group includes SMEs providing similar cards to their customers, such as gyms and sport centers.

8.3.3 Verifiers

Verifiers are directly co-operating with the issuers in the SimplyMember solution since they request a digital proof of the holder's credentials in form of the presented wallet application. Verifiers, such as the concrete store locations of the participating issuer chains, are provided with the hardware and training required to read the holder's membership cards. This forms the verifiable credential trust triangle, and the functionality is achieved once all the three participants, holders, issuers, and verifiers have adopted the system into use.

8.3.4 Tactics

Blockchain, cryptocurrencies, distributed ledgers and SSI are more popular than ever, but people still do not understand what they are. This raises a challenge for startups like SimplyMember trying to gain large visibility for our actors. Our tactic is to create a comprehensive marketing strategy for a 1-year campaign (minimum). Our strategy is to take advantage of the following marketing channel to communicate our unique selling points:

Unique Branding for SimplyMember

Selective marketing is a strategy used by many ICO's and cryptocurrencies to differentiate themselves from their rivals by branding themselves towards a certain subculture or demographic. Our strategy is to create a brand which appeals to our holders, issuers, verifiers, investors, and other stakeholders.

Immersive Web Design

After unique branding the most important thing to do is to create a stylish, simple and appealing website for SimplyMember and its ICO. Our website will tell our holders, issuers and verifiers everything they need to know about SimplyMember, our ICO and our brand. It is arguably the most important channel we have with our customers. Our website will also attract potential investors by explaining the advantages of investing into our ICO. This is crucial for our brand's future.

Social Media and Crypto Communities

Social media and Crypto Communities are our second most important channels to keep in touch mostly with our holders. Our strategy is to create a solid ground in: Instagram, YouTube, TikTok, Reddit, and Finnish blockchain communities.

Our plan is to create appealing and informative content for Instagram, YouTube and TikTok. This includes advertisements, videos, pictures, giveaways, and Q&A sessions for our holders. Our strategy is to create funny, ironic, and viral content which will spread throughout the platform.

As Reddit being one of the most visited sites in the world it works as an excellent platform to create a community for our brand. Reddit has hundreds of different cryptocurrencies and blockchain related subreddits with a diverse audience. We will create a subreddit for SimplyMember's where our employees can be in touch with the holders.

We will start a collaboration with Blockchain Forum Finland Ry that produces content, hosts events, and creates partnerships that help development of blockchain in Finland. They bring together companies, government agencies, universities, and individuals. Blockchain Forum Finland helps us and our issuers and verifiers bringing us insight, cooperation, and credibility.

Display Campaigns

With display campaigns our goal is to create advertising content which will promote our brand across relevant sites. This will be paid advertising and it will include banderols, Figures, and similar videos that we use in our social media platforms. With these campaigns we will spread information about SimplyMember's benefits, value proposition and pricing model. Part of the strategy is to pump a relatively large amount of our budget for Search Engine Optimization (SEO) to get maximum coverage for our brand and get noticed by potential verifiers, holders, and issuers.

Conferences

Conferences offer us a great platform to meet blockchain developers, enthusiasts, investors and potential customers. Our goal is to take part in conferences by being part of a panel, having solo presentations or even hosting a conference on our own. Our potential conferences to attend would be Internet Identity Workshops, Blockchain Summit Helsinki, and Trust Over IP Webinars coming this year.

8.4 Measuring & Control

With efficient marketing strategy, we can ensure that consumers can be turned into customers. As a measurement and control tool for the success of the marketing strategy we can use KPI (Key Performance Indicators) and OKR (Objective and Key Results). KPI's are quantifiable metrics that can be used for measuring and monitoring the success of digital marketing strategy. KPI measures efficiency of the strategy and they can be updated and changed when needed. There are a variety of KPIs that can be used, and they often depend on the type of the organization, industry, and the business department that is using them.

8.4.1 Key Performance Indicators

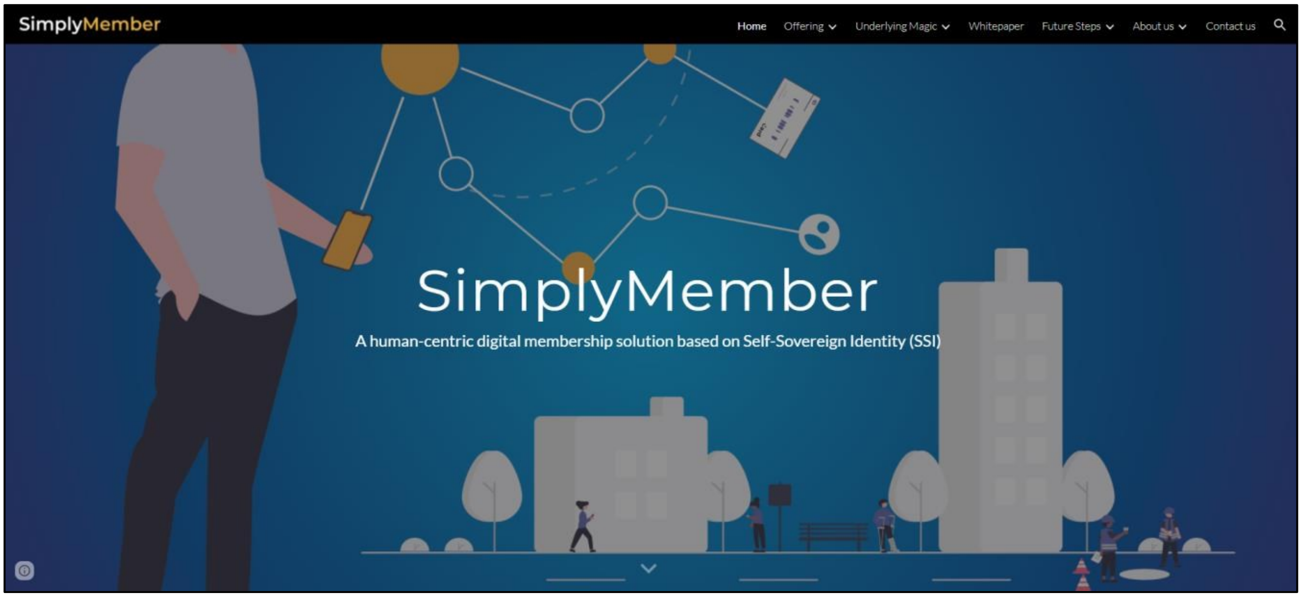
In our case, the platforms and forms of marketing are website, social media and crypto communities, display campaigns and conferences. We can use a variety of KPIs, for example measuring the amount of the users of SimplyMember and the number of social media following in different platforms. We could also analyze the overall media coverage and display campaigns. Other KPIs could be measuring the website traffic which would provide us a lot of information about the performance of the marketing strategy. It enables analyzing the amount and the source of the traffic on the website. For example, we could measure the number of visits on the site, the page views and the duration of the sessions and analyze the amount of new and returning visitors on the site.

8.4.2 Objectives and Key Results

OKR (Objectives and key results) are the objectives, and the goals of the company and key results are the desired outcome of those goals. When the objectives and goals are well defined and the key results established, it is easier to work towards those set goals. Typically, there are 3-5 defined key results for each set goal, and they can be scaled between 0–1 (or by percentage between 0–100) to measure whether the objectives are met or not. In our case, an example of an OKR could be launching a social media campaign. The key results could be that during the campaign, the amount of SimplyMember users increases by 5%, number of social media followers increases by 15% and the number of visitors on the website will be boosted by 10%. After the campaign we would measure whether we have reached our goals.

8.5 Marketing and Promoting in Practice

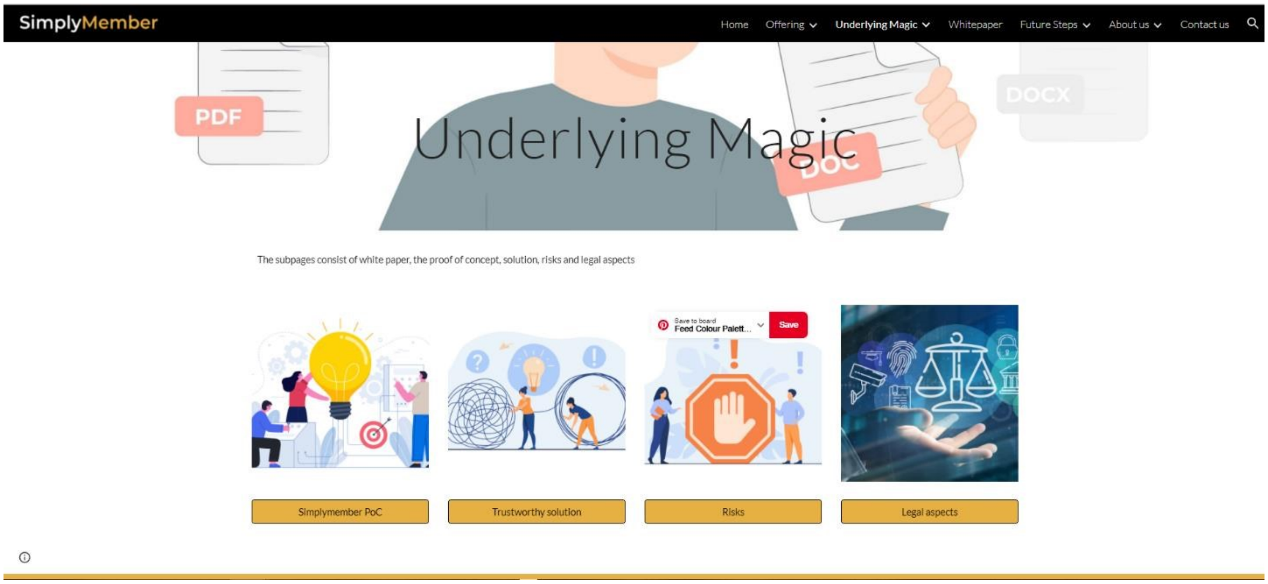
Website is one of the most important channels to promote a new, innovative services. For the website we did eventually end up using Google sites shown in Figure 29 and Figure 30. The first version of the SimplyMember website was done using just plain HTML and CSS and it had some basic bootstrap template in it but then we were informed that cooperation with other teams will be too difficult with that solution, so we decided to change it to google sites as it is more flexible and easier to use.



SimplyMember

A human-centric digital membership solution based on Self-Sovereign Identity (SSI)

Figure 29 SimplyMember website homepage



Underlying Magic

The subpages consist of white paper, the proof of concept, solution, risks and legal aspects

Figure 30 Underlying magic section in SimplyMember webpage

We also created a marketing video for the value proposition of SimplyMember as well as the final event in April. Video script:

“Have you ever counted how many membership cards you have in your wallet or how many different apps you have for memberships? That’s right, many. The world around us is evolving rapidly. Now, it is time to bring membership cards to the 21st century. We present, a Universal membership card, that is enabled with SSI-technology: SimplyMember.

For the end users SimplyMember will provide easier, more reliable, secure, and trusted membership than any membership card before. And for the membership providers SimplyMember will offer an easier, more reliable, secure, and scalable solution than any membership program has ever been. Together, we can make the world of memberships a better one. The Initial Coin Offering of SimplyMember will soon be published.”

9 The Roadmap to the Future Growth

In this section we will illustrate the future market and funding possibilities for the SimplyMember digital membership solution. The next steps after realizing the proof-of-concept in Finnish markets would gaining ground in the international markets and raising funds for business growth and innovation. Following, we will introduce a plan for expanding abroad beyond borders and in the later section introduce SimplyMember ICO as an alternative funding method based on cryptocurrency.

9.1 Internationalization Plan

SimplyMember wants to expand abroad. Below we will introduce the internationalization plan including the rough schedule and a more general project road map visualizing the key development milestones as shown in Figure 31.

We considered Estonia, Germany, India, Sweden, and the United States for our target country and after popular vote by our team and by project's other teams, we decided to choose Estonia for internationalization. Internationalization plan includes a rough schedule and justification and information about Estonia, its attitude on technology, attitude on cooperation and its legislation. The plan is targeted to retail and gym markets in Estonia. If SimplyMember works in Estonia, it can then be expanded to other countries in the EU.

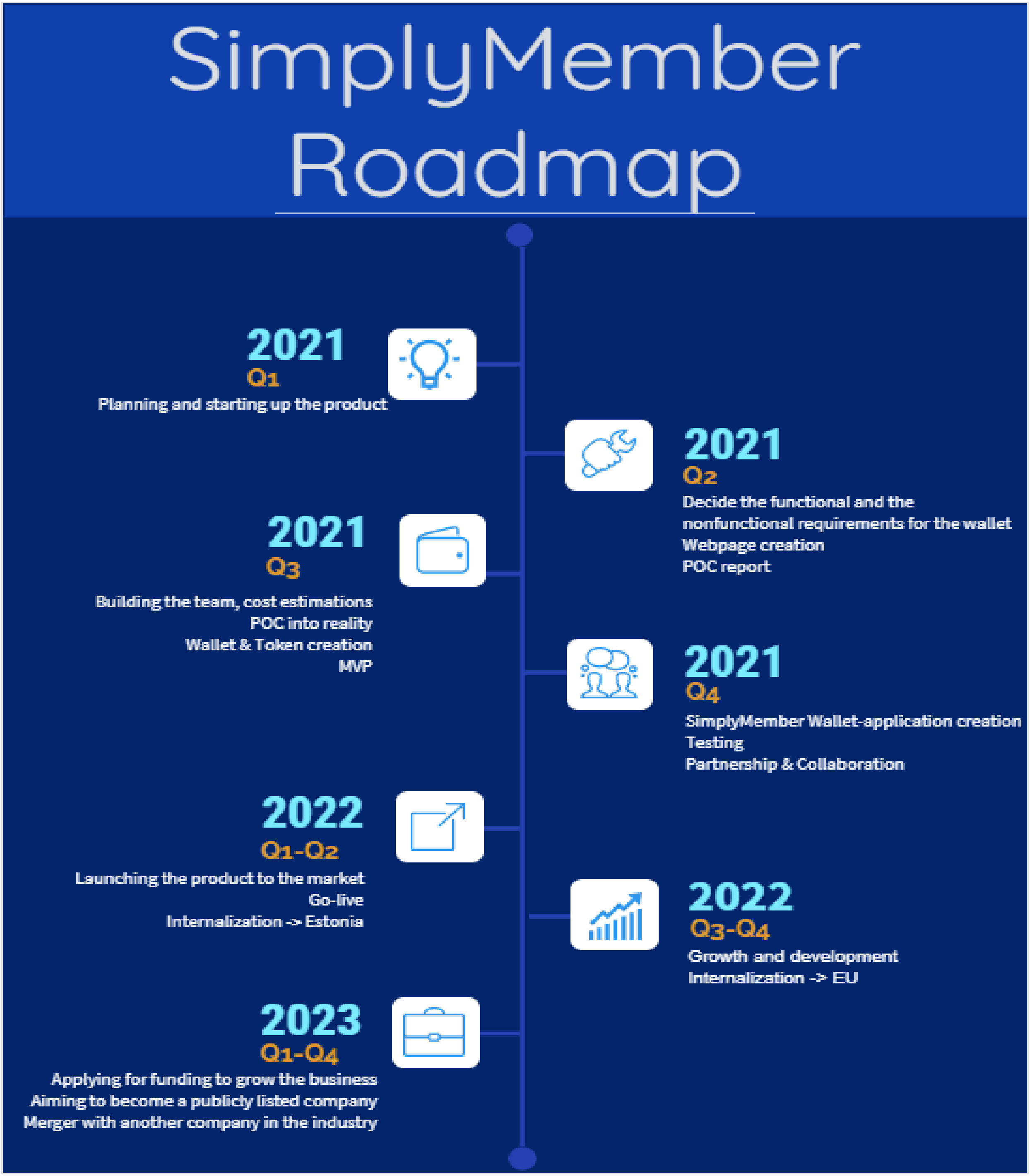
9.1.1 Schedule for Internationalization

Year 2022

- Attend Latitude59 in Estonia to create contacts with Estonian companies, people, and government https://latitude59.ee/
- Contact Finnish and Estonian governments about internationalization to Estonia
- Contact Estonian companies and Finnish companies operating in Estonia
- Hire/contact consultants

Year 2023

- Start making possible chances or creating new app for Estonia
- Look for starting subsidiary in Estonia
- Translation for Estonian language option (maybe Russian)
- Start marketing SimplyMember in Estonia



SimplyMember Roadmap

2021
Q1
Planning and starting up the product

2021
Q2
Decide the functional and the nonfunctional requirements for the wallet
Webpage creation
POC report

2021
Q3
Building the team, cost estimations
POC into reality
Wallet & Token creation
MVP

2021
Q4
SimplyMember Wallet-application creation
Testing
Partnership & Collaboration

2022
Q1-Q2
Launching the product to the market
Go-live
Internalization -> Estonia

2022
Q3-Q4
Growth and development
Internalization -> EU

2023
Q1-Q4
Applying for funding to grow the business
Aiming to become a publicly listed company
Merger with another company in the industry

Figure 31 SimplyMember roadmap

9.1.2 Internationalization Factors

Estonia is one of our candidates for global expansion is the country of Estonia, which has one of the world’s most advanced digital societies as 99% of the nation's public services are available online. It is a digitally aware nation of 1,3 million people which shows by the statistics that 90% of the population use the internet regularly and 98% hold a valid Digi-ID.

Attitude on technology and digital identity

Estonia has strived to be a digitally driven country since the early days of the 21st century. It has been a digital frontrunner as it was the first country to take voting online and legalize cryptocurrency firms' operations. Estonian citizens’ information is secured by Blockchain, so the country and structures are already familiar with the technology. In addition, Estonian's vision to achieve e-governance speaks for its readiness to implement digital identity in the form that SimplyMember solution offers. These factors encourage SimplyMember to move towards Estonia, as the nation is no stranger to blockchain technology and digital ID. However, Estonia has already commissioned a solution for digital ID and there are three candidate companies that are proposing the solution. Of course, the commissioned solution is not fully the same as the SimplyMember solution, but as the solution will be taken into operation someday, it could be challenging to replace. Therefore, SimplyMember should consider possible cooperation with the entity that will be chosen to provide the solution of digital ID, or even using it as a verifier.

Attitude on cooperation

Estonia encourages other nations and global companies to cooperate with it. The country’s objective is to attract tech companies to Estonia by seamless governance. They even have this thing called e-residency, where any global citizen can join a borderless digital society and gain the rights to conduct business and utilize Estonian e-services. Therefore, lots of consultancy services specialized in the Estonian business environment exist to ensure efficient cooperation. Also, Finland and Estonia have a data exchange facility called Nordic Institute for Interoperability Solutions (NIIS). In 2019, the national business registers and tax boards in Estonia and Finland moved towards cooperation that would allow the agencies to exchange data in a more accurate and efficient way by using X-Road trust federation between the countries.

Legislation

Estonia has been a member of the European Union since 2003 and therefore it follows union-wide laws such as GDPR. Even though Estonia is a developed country in the field of crypto and blockchain, the regulation concerning utility tokens is a bit unclear because utility or payment type of token does not fall under legal regulation. However, there are lots of consultancy and expert services available in Estonia considering blockchain and applied laws (e.g., NJORD, maxcorp, e-Estonia). For example, e-Estonia offers service packages for specific groups and companies to ensure efficient legal cooperation. Also, the fact that Estonia utilizes blockchain technology in restoring its citizens' information speaks for successful governance and regulation of blockchain at a certain level. In addition, the cooperation between Finnish and Estonian entities should be easier due to the establishment of the data exchange facility of NIIS.

Our Blockchain legislation team presented the summary of potential target countries in workshop 4 and the most promising one was selected by voting. The result of the voting was that Estonia came up on top as SimplyMember's number one location for international expansion. There were several reasons to justify the selection such as EU membership, digital advancement, legislation, cooperative readiness, and location of the country. Only three downsides were recognized but they were considered as solvable issues. The first challenge was the size of the market as there are only 1,3 million people in Estonia. However, the country could be still seen as a great test country for internationalization due to the EU membership and digitally savvy structures and citizens. The second challenge is that the nation has already commissioned a solution for digital ID and there are candidates to deliver it. However, this challenge could be seen as a possibility as SimplyMember could cooperate with the final solution provider or even use it as a verifier. The third challenge is the lack of legislation on utility tokens, but the issue could be handled by utilizing consultancy services that Estonia has plenty of. Also, one essential factor that encourages SimplyMember to move towards Estonia is the fact that Estonia was the first country to legalize cryptocurrency firms' operation, so there have been many examples and use cases of successful and unsuccessful crypto and blockchain projects to learn from, so that knowledge could be utilized by experts, consultants, and SimplyMember.

As mentioned earlier, the first step of expanding to Estonia would take its place in 2022, as SimplyMember representatives would attend Latitude59–an Estonian tech conference–to create a name and relationships abroad. By 2023 at the latest, the Estonian government and consultancy services would be contacted to ensure necessary licenses and efficient cooperation to lay the foundation for partnership. For starters, possible companies for cooperation could include Stockmann, Prisma Peremarket, R-Kiosk, Coop, SuperALKO, and MyFitness. The first three companies have connections to Finland, which could help to initiate the collaboration. On the other hand, Coop Estonia is Estonia's oldest and biggest group in retail trade with a wide and stable customer base, while SuperALKO has its own membership system and is popular among Finnish tourists. In turn, MyFitness is the biggest gym and wellness company in Estonia, whose membership could be acquired and controlled by using SimplyMember. Naturally, the Estonian language should also be added as one of the application’s official languages.

9.2 Initial Coin Offering as an Alternative Funding Method

An ICO offers interested investors a change to buy into the offering and receiving the SimplyMember cryptocurrency token. The course participants got familiar with reputable ICO projects recommended by e.g., field expert Mikko Ohtamaa. The projects were:

- Uniswap: a decentralized exchange built on Ethereum https://messari.io/asset/uniswap/profile
- Compound: a lending platform built on Ethereum https://messari.io/asset/compound/profile
- USDC: fiat-collateralized stablecoin that offers the advantages of transacting with blockchain-based, assets https://messari.io/asset/usd-coin/profile
- Yearn.Finance: a decentralized asset management platform https://messari.io/asset/yearnfinance/
- profile Streamr: data management and data marketplace https://messari.io/asset/streamr/profile
- Aave: a peer-to-peer lending platform on Ethereum https://messari.io/asset/aave

The tokens used in the SimplyMember ecosystem will be utility tokens named S1MPLY Data (SMPLD). Below we will describe their functionality as well as the key characteristics of the ICO launching.

9.2.1 Launching an ICO

Role of Tokens

Holders (Storeowners) participate in the ICO to buy S1MPLY Data (SMPLD) tokens. These tokens are utility tokens that can then be used to buy customer data. The customer data is gathered by SimplyMember every time the customers use their SimplyMember app. The customer can then choose to sell all or a part of all of the data gathered from their purchase history from the previous month and receives tokens from all of the holders as a payment for this data. These tokens will not be sent to a customer's wallet, instead, back to SimplyMember where they are assigned to the individual customers. This is done to avoid problems with wallets and transaction costs. The more data gathered from the customer and sold to the holders, the more tokens the customer receives.

The price of the token (the amount of data one can buys for one token) is determined by the price the holders want to pay for the data and can change dynamically depending on market conditions. The customer can exchange these tokens to vouchers and other types of benefits that apply to the holder owned stores, for example a token can be used to get a free ice-cream from a store.

SimplyMember’s ICO Characteristics

SimplyMember ICO will start in the ICO enlistment site Dao Maker. In the ICO investors can buy Simply Data tokens, SMPLD (the logo shown in Figure 32) that are used in the SimplyMember ecosystem. There will be a total amount of 1 billion SMPLD with 50 % of them available to purchase for the price of 0,002 euro per token. Purchases will be made with Ethereum tokens, which are used to create the SMPLD tokens on the Ethereum blockchain. ICO will be available for organizations that want to join the SimplyMember ecosystem and operate in Finland, Estonia, or Sweden. Rest of the tokens will be held by SimplyMember and can be purchased later by companies included in the ecosystem that want more tokens to acquire more data or for new companies wanting to join the SimplyMember ecosystem.

Figure 32 S1mply Data token logo

Minimum amount of purchase will be 500euro (0,025% of all tokens) and maximum amount will be 40 000euro (2% of all tokens). There will be a 60-day money to token wait period which means that SimplyMember gathers funding for 60 days after which it starts sending any tokens to the investors.

The ICO will be also listed on the website ICO Drops, where the ICO can be followed by investors and it at the same time provides marketing for the ICO. ICO drops is a popular and growing website for listing any ICOs. They have many useful lists for current, upcoming, and ending ICOs which makes the SimplyMember solution to be more visible in the world of ICOs. The lists look like a Kanban board (Inbox, In Progress, Done). The site is also very user friendly which also goes well in hand with the way SimplyMember sites look like.

To be listed on the website, SimplyMember must submit their ICO details. If the details make the site makers interested, they will list the ICO to the website. Needed information requires a name and other contacts, link to the project website and some miscellaneous information about the project. ICO ranking factors are highly dependent on the site which ICO is being looked at. For example, CoinGecko uses 20 different sources and compiles them together to form their own ICO ranking divided with equal weighing. These include sources like other reviewers or other website ratings. More details can be found at their website[24].

The SMPLD token aims to be a utility token and hence it would be regulated by the common consumer laws in the EU, as well as GDPR for the gathering of data. However, it is not trivial to assess if the current legal requirements for ICO in Finland would consider the token as a security. It would be highly advisable to seek professional legal opinion before launching the token as it is the responsibility of SimplyMember to make sure that their business complies with the regulatory framework.

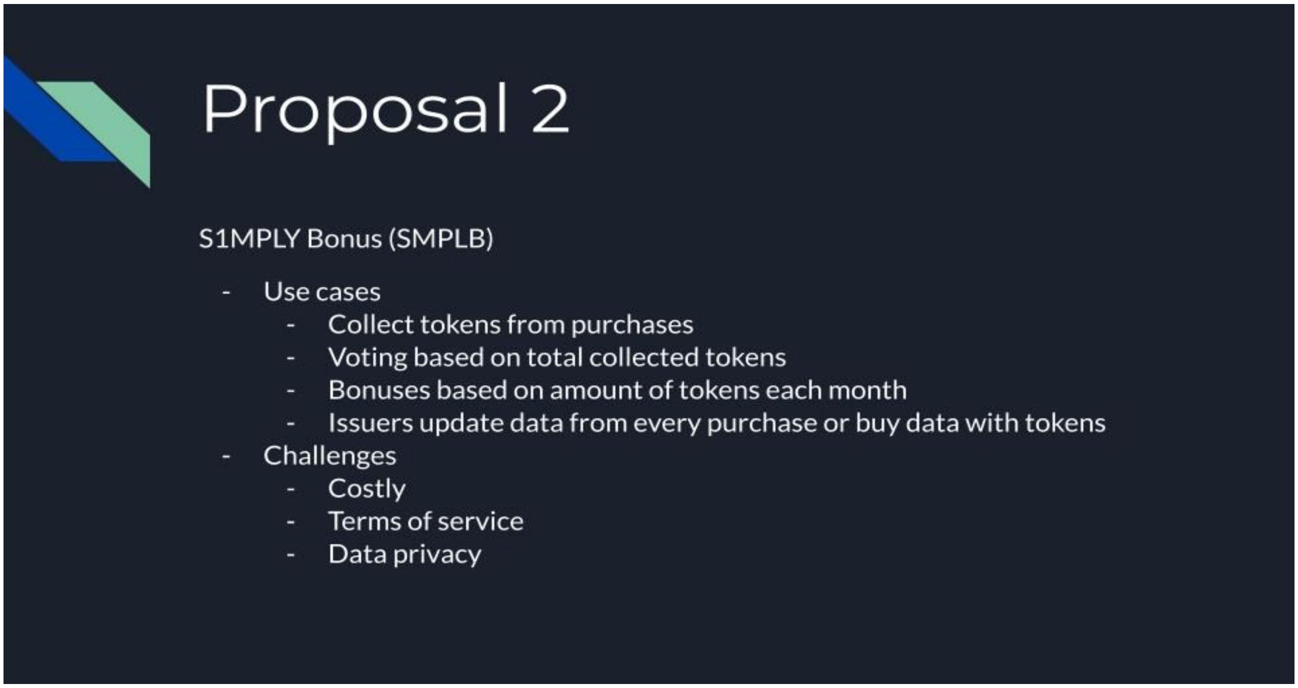
Alternative Roles for the Token

There were two other options for the utility token to be had if we hadn't chosen the previous one. The other one of these was a payment token where the user would buy these tokens with fiat (euros etc.) currency and spend the tokens in local stores whether it was to buy groceries or gym memberships. In this case the utility token would have focused making payments but after some research and discussion we concluded that it would not be feasible to have this kind of system mostly because of high gas prices and because of low incentives taking action into the system from holder and issuer perspective. Some other positives were that it would have allowed data exchange with the system's usage, but this wasn't enough to beat the inherent difficulties of the system.

The other option was to create a bonus-based utility token where users would buy groceries etc. with fiat currency and with purchase, they would sign into SimplyMember solution and users would receive tokens for the amount they purchased. The number of tokens would end up giving holders a discount based on how much they have spent during the previous month, and they would gather voting power based on how much they have spent in total to the system.

[24] https://www.coingecko.com/en/ico_methodology

The issuers would have access to the customers data for exchange of the tokens. The systems would have good incentives for users and issuers, but it would be quite challenging to be built. There were many challenges regarding any voting which could have been done and it felt like the system may have become obsolete and impossible to set up in the end. We present the token proposals in Figure 33, Figure 34 and Figure 35.

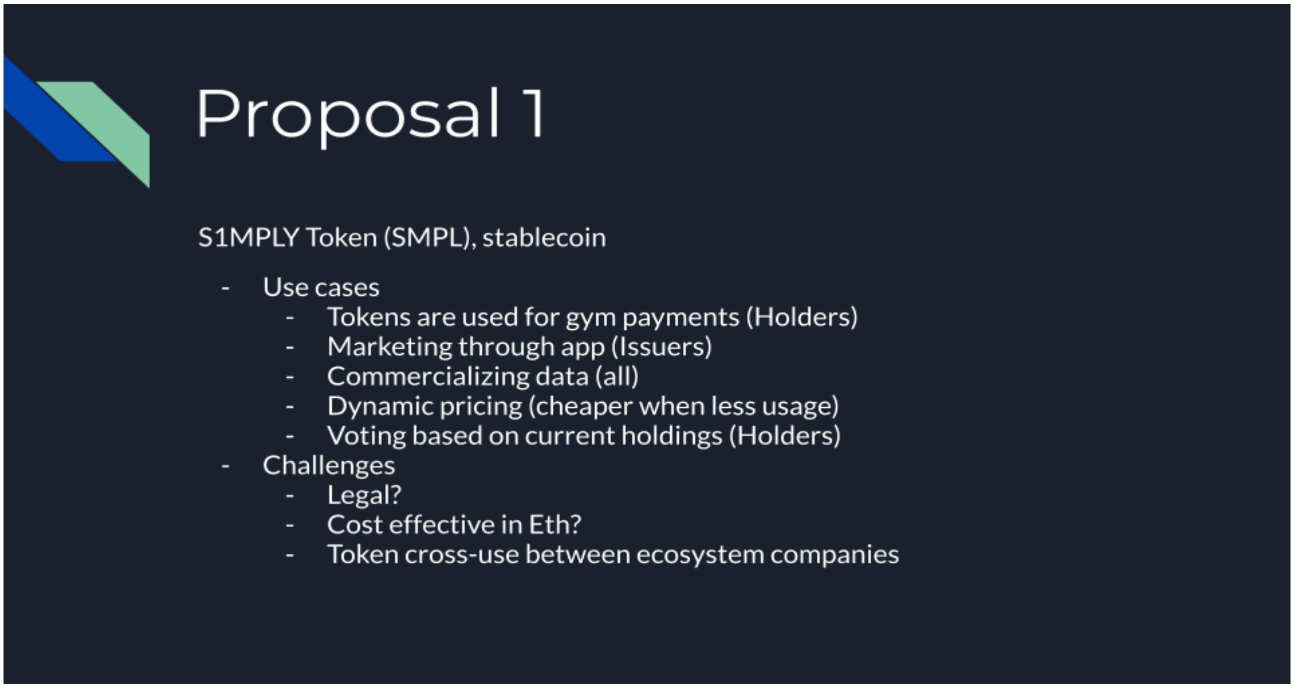


Proposal 2

S1MPLY Bonus (SMPLB)

- Use cases
  - Collect tokens from purchases
  - Voting based on total collected tokens
  - Bonuses based on amount of tokens each month
  - Issuers update data from every purchase or buy data with tokens
- Challenges
  - Costly
  - Terms of service
  - Data privacy

Figure 33 SimplyMember token proposal 1

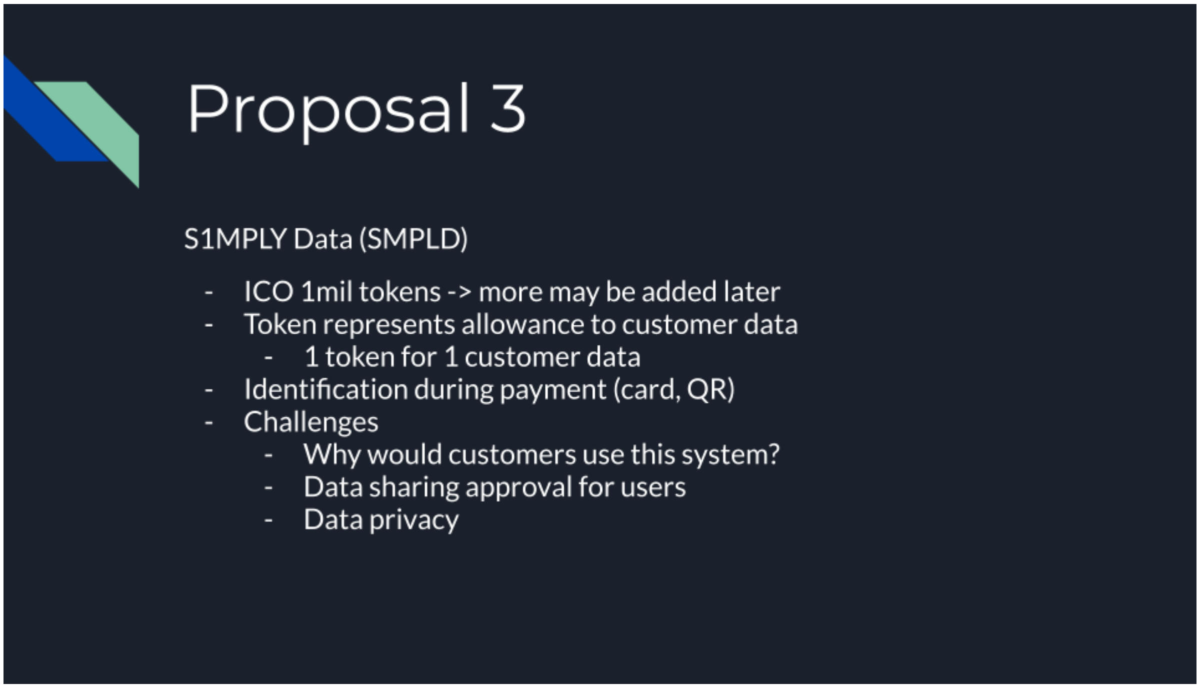


Proposal 1

S1MPLY Token (SMPL), stablecoin

- Use cases
  - Tokens are used for gym payments (Holders)
  - Marketing through app (Issuers)
  - Commercializing data (all)
  - Dynamic pricing (cheaper when less usage)
  - Voting based on current holdings (Holders)
- Challenges
  - Legal?
  - Cost effective in Eth?
  - Token cross-use between ecosystem companies

Figure 34 SimblyMemeber token proposal 2



Proposal 3

S1MPLY Data (SMPLD)

- ICO 1mil tokens -> more may be added later
- Token represents allowance to customer data
  - 1 token for 1 customer data
- Identification during payment (card, QR)
- Challenges
  - Why would customers use this system?
  - Data sharing approval for users
  - Data privacy

Figure 35 SimblyMember token proposal 3

9.2.2 Legal Framework for the ICO

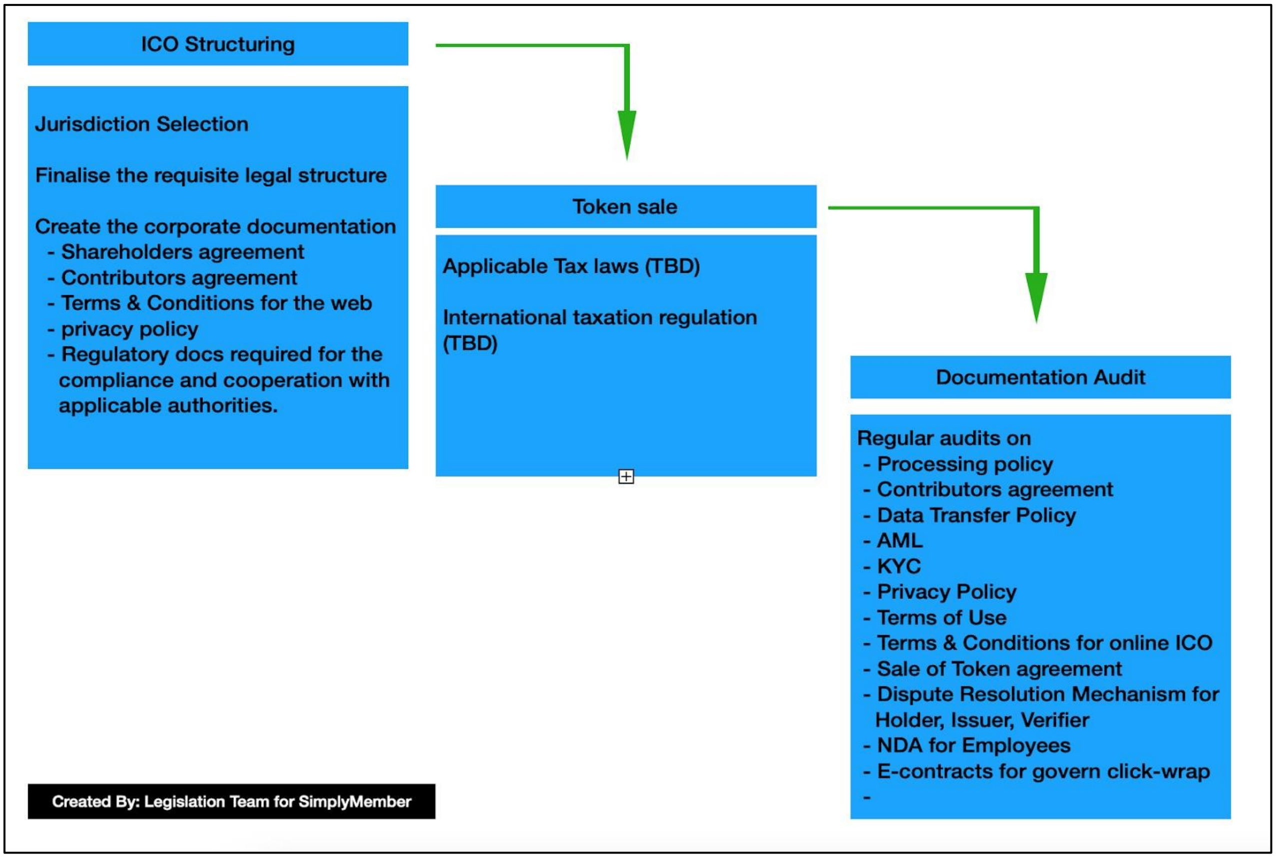
Firstly, ICO set the novel and innovative way to raise the investment. As it hit the huge popularity since 2016, global regulatory authorities have been trying to regulate ICO, otherwise non-compliance brings greater risks to the ecosystem.

Simple Agreement for Future Tokens (SAFT) is a common agreement executed for the ICO purpose, including all the provisions that set the transactions between the company and the token buyers. Further, this specifically describes the nature of token as a utility, not security. Additional information can be found from SAFT Project white paper.

According to our studies observations and Rahul Dev, author of the ICO legal framework, the following list of key points should be taken into consideration before raising the funds using the ICO’s such as,

- Adherence to the GDPR, Anti Money Laundering (AML).
- following KYC regulations.
- Execution of proper registration and disclosure statements.
- Drafting and pointing out the strong legal disclaimers across all the applicable documents.
- Defines if the tokens or coin fall under the scope of security.
- All the taxation implication of the token of its buying/selling timeline or during ICO.
- Duly considering the legality of the coin offered to investors/buyers.
- Take all the necessary steps to prevent Counter Terrorist Financing (CTF).

Further, ensure the processes embrace along with the legislation, this would help to SimplyMember to tackle the legal issues and challenges which its dynamic environmental journey. Road map shown in (Figure 36) gives a clear picture to the various stakeholders.



ICO Structuring

Jurisdiction Selection

Finalise the requisite legal structure

Create the corporate documentation
- Shareholders agreement
- Contributors agreement
- Terms & Conditions for the web
- privacy policy
- Regulatory docs required for the compliance and cooperation with applicable authorities.

Token sale

Applicable Tax laws (TBD)

International taxation regulation (TBD)

Documentation Audit

Regular audits on
- Processing policy
- Contributors agreement
- Data Transfer Policy
- AML
- KYC
- Privacy Policy
- Terms of Use
- Terms & Conditions for online ICO
- Sale of Token agreement
- Dispute Resolution Mechanism for Holder, Issuer, Verifier
- NDA for Employees
- E-contracts for govern click-wrap
-

Created By: Legislation Team for SimplyMember

Figure 36 Legislation roadmap for SimplyMember

Considerations About Legal Requirements for the SimplyMember ICO in Finland

The token called S1MPLY Data (SMPLD) is planned to be a utility token. Holders gather their data to the system maintained by SimplyMember and manage the data themselves. Customers will receive S1MPLY Data tokens for selling their data and customers can exchange these tokens into vouchers of their choice (discounts, cheaper gym). Issuers may buy data in bulk to reduce fees.00 euros and maximum 39 600 euros.

According to our still limited understanding, the S1MPLY Data token would be considered virtual currency as defined by the Act on Virtual Currency Providers25 (Valtiovarainministeriö, 2019). However, SimplyMember falls outside of the scope of the Act if it is considered that SimplyMember provides virtual currency services within a limited network. Otherwise, SimplyMember would have to comply with the requirements laid down by the Act (e.g. obligation to register, obligations regarding the preservation of client funds, obligations regarding marketing) and the Act on Money Laundering (Valtiovarainministeriö, 1.7.2019) would also be applicable (obligation to do risk assessment, obligation to know and identify customers, obligation to notify). The possible obligations under the proposed MiCA (EUROPEAN COMMISSION, 2020)should be further analyzed.

Regarding ICOs, they must always be considered on a case-by-case basis. Regulation is technology neutral and obtaining funding through the ICO does not exclusively resolve the issue of applicable regulation. When assessing applicable regulation, one must always consider what the investor receives from the ICO in return. Depending on how it is implemented, the ICO may be subject to, for example, crowdfunding regulation, securities legislation or the ICO may also be an implementation solution outside the scope of financial regulation.

The virtual currency to be issued via an ICO may fall within the scope of the definition of a security or financial instrument. A security is negotiable and issued or meant to be issued to the public [26]together with several other securities with similar rights. In assessing whether a virtual currency is considered to be a security the FIN-FSA uses a list of 20 questions (Financial Supervisory Authority, *2019).*

If a virtual currency is considered to be a security, regulation applicable to issuing a security must be complied with and the issuer may have an obligation to prepare and publish a prospectus. The general principles of the Securities Market Act (Valtiovarainministeriö, 2013) must be adhered to, even if a prospectus obligation does not arise. Also, the Act on Virtual Currency Providers would be applicable.

Based on S1MPLY Data token features, it might be that S1MPLY Data token would not be considered as a security. In that case the general provisions of the Consumer Protection Act (Oikeusministeriö,1978), such as the provisions relating to distance selling, should nevertheless be taken into consideration.

[25] https://www.finlex.fi/fi/laki/alkup/2019/20190572

[26]https://www.finanssivalvonta.fi/en/fintech--financial-sector-innovations/innovation-help-desk- advises-on-licence-issues/

Finally, as it is up to the companies themselves to consider the regulatory framework, obtain the necessary permits and meet the applicable requirements and any failure to comply with the applicable rules would constitute a breach(ESMA, 2017), we highly recommend SimplyMember to contact the FIN-FSA ice on organizing the ICO.

Conclusion on ICO and Finnish Legislation

- Based on the token features and planned ICO, it might be that SimplyMember's solution falls mostly out of the scope of Finnish legislation.
- In the above scenario investors cannot benefit from the protection laws provide, and potential investors may be skeptical.
- Overall, the uncertainty currently prevailing around the legal framework is a challenge for SimplyMember in Finland and elsewhere in the EU.
- We highlight that SimplyMember should determine the applicable legislation itself and therefore we recommend that SimplyMember contacts the FIN-FSA Innovation Help Desk for advice.
- The regulation is constantly evolving and SimplyMember should monitor regulatory developments at the Finnish and EU level.

Even if the SimplyMember's ICO falls outside of the regulated space, the reliability of the ICO should be ensured because ESMA and the FIN-FSA have issued warnings about participating in ICOs and attitudes may be skeptical. In addition, regulatory developments must be constantly monitored.

References

- Ekparinya, P., Gramoli, V., & Jourjon, G. (2018). Impact of Man-In-The-Middle Attacks on Ethereum. 2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS), 11–20. https://doi.org/10.1109/SRDS.2018.00012

- ESMA. (2017). ESMA alerts firms involved in Initial Coin Offerings (ICOs) to the need to meet relevant regulatory requirements. Esma.Europa.Eu. https://www.esma.europa.eu/sites/default/files/library/esma50-157-828_ico_statement_firms.pdf

- EUROPEAN COMMISSION. (2020). EUR-Lex—52020PC0593—EN - EUR-Lex. Eur-Lex.Europa. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0593

- Keski kirjastot. (2021). Tietosuoja | Keski-Finna. Keski.Finna. https://keski.finna.fi/Content/privacy

- LaConte, G. (2018, December 2). How to Calculate the Impact and Probability of Business Risk. LaConte Consulting. https://laconteconsulting.com/2018/12/02/calculate-impact-and-probability/

- Makaay. E, Smedinghoff, & Thibeau.D. (2017). OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf. Connectis.Com. https://connectis.com/wp-content/uploads/2018/05/OIX-White-Paper_Trust-Frameworks-for-Identity-Systems_Final.pdf

- Markowski, A. S, & Mannan, M. S. (2008). Fuzzy risk matrix—ScienceDirect. https://www.sciencedirect.com/science/article/pii/S0304389408004019

- maximize market research. (2019). Global Membership Management Software Market – Industry Analysis and Forecast (2019-2026) – by Type, End-User, Application and Region. MAXIMIZE MARKET RESEARCH. https://www.maximizemarketresearch.com/market-report/global-membership-management-software-market/16047/

- Moisés Menéndez Andrés, BazoberryOscar, Ismael Arribas, & Ibi Rodríguez Jaramillo. (2020). Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain | Publications. https://publications.iadb.org/publications/english/document/Self-Sovereign-Identity-The-Future-of-Identity-Self-Sovereignity-Digital-Wallets-and-Blockchain.pdf

- Oy, E. P. (2021a). FINLEX ® - Ajantasainen lainsäädäntö: Arvopaperimarkkinalaki 746/2012. Oikeusministeriö, Edita Publishing Oy. https://www.finlex.fi/fi/laki/ajantasa/2012/20120746
- Oy, E. P. (2021b). FINLEX ® - Ajantasainen lainsäädäntö: Kuluttajansuojalaki 38/1978. Oikeusministeriö, Edita Publishing Oy. https://www.finlex.fi/fi/laki/ajantasa/1978/19780038
- Oy, E. P. (2021c). FINLEX ® - Ajantasainen lainsäädäntö: Laki rahanpesun ja terrorismin rahoittamisen… 444/2017. Oikeusministeriö, Edita Publishing Oy. https://www.finlex.fi/fi/laki/ajantasa/2017/20170444
- Raggad, B. G. (2010). Information Security Management: Concepts and Practice. CRC Press.
- S group. (2019). S-ryhmän asiakasomistaja- ja asiakasrekisteri. S-kanava. https://www.s-kanava.fi/asiakasomistaja/artikkeli/s-ryhman-asiakasomistaja-ja-asiakasrekisteri/580dr26haWkdjYWimKQkVM
- S group. (2020). Keskeiset luvut. s-ryhma.fi. https://s-ryhma.fi/talous-ja-hallinto/keskeiset-luvut
- Sporny, M., Noble, G., & Longley, D. (2019). Verifiable Credentials Data Model 1.0. https://www.w3.org/TR/vc-data-model/
- Sporny, S., Longley, D., & Sabadello, M. (2021). Decentralized Identifiers (DIDs) v1.0. https://www.w3.org/TR/did-core/
- Stoneburner, G., Goguen, A., & Feringa, A. (2002). Risk management guide for information technology systems: Recommendations of the National Institute of Standards and Technology (NIST SP 800-30; 0 ed., p. NIST SP 800-30). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-30
- TRUSTOVERIP. (2020). Learn About Trust Over IP. https://idramp.com/learn-about-trust-over-ip/
- Trustoverip. (2020). Identity and Verifiable Credential Risks—Home—Confluence. Wiki.Trustoverip.Org. https://wiki.trustoverip.org/display/HOME/Identity+and+Verifiable+Credential+Risks
- Turner, A. (2018, July 10). How Many People Have Smartphones Worldwide (Sept 2021). https://www.bankmycell.com/blog/how-many-phones-are-in-the-world

- Vakkuri, V., Kemell, K.-K., & Abrahamsson, P. (2020). ECCOLA - a Method for Implementing Ethically Aligned AI Systems. 2020 46th Euromicro Conference on Software Engineering and Advanced Applications (SEAA), 195–204. https://doi.org/10.1109/SEAA51224.2020.00043
- Wang, F., & De Filippi, P. (2020). 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
- www.finanssivalvonta.fi. (2019a). Frequently asked questions on virtual currencies and their issuance (Initial Coin Offering). Www.Finanssivalvonta.Fi. https://www.finanssivalvonta.fi/en/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/frequently-asked-questions-on-virtual-currencies-and-their-issuance-initial-coin-offering/
- www.finanssivalvonta.fi. (2019b). Innovation Help Desk advises on licence issues. Www.Finanssivalvonta.Fi. https://www.finanssivalvonta.fi/en/fintech--financial-sector-innovations/innovation-help-desk-advises-on-licence-issues/
- www.finanssivalvonta.fi. (2019c). Kryptovaluutat ja ICO (Initial Coin Offering) sijoituskohteina, onko kyse kuplasta? www.finanssivalvonta.fi. https://www.finanssivalvonta.fi/tiedotteet-ja-julkaisut/blogit/2017/kryptovaluutat-ja-ico-initial-coin-offering-sijoituskohteina-onko-kyse-kuplasta/
- www.finanssivalvonta.fi. (2019d). Questions about tokens and ICOs. Www.Finanssivalvonta.Fi. https://www.finanssivalvonta.fi/en/fintech--financial-sector-innovations/virtuaalivaluutan-tarjoajat/frequently-asked-questions-on-virtual-currencies-and-their-issuance-initial-coin-offering/questions-about-tokens-and-icos/
- Yli-Korhonen, J. (2020). Tutkimus: Älypuhelimien määrä yhä kasvussa - 96 prosentilla 16-74-vuotiaista on jo älypuhelin. Puhelinvertailu. https://www.puhelinvertailu.com/uutiset/2020/05/22/tutkimus-96-prosentilla-16-74-vuotiaista-on-alypuhelin

SimplyMember: from an idea to a proof of concept as a collaborative effort

In this book, we provided an overview of the state of Self-Sovereign Identity (SSI) in spring 2021, as described by the teams working together on several SSI-related research topics. 13 teams and more than 70 enthusiastic individuals worked together and developed a proof of concept for an SSI-based digital service. We are open for collaboration! Please contact our research and educational team at Startuplab, University of Jyväskylä.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

Startuplab JYU LabStartup

JYU AI ethics Lab