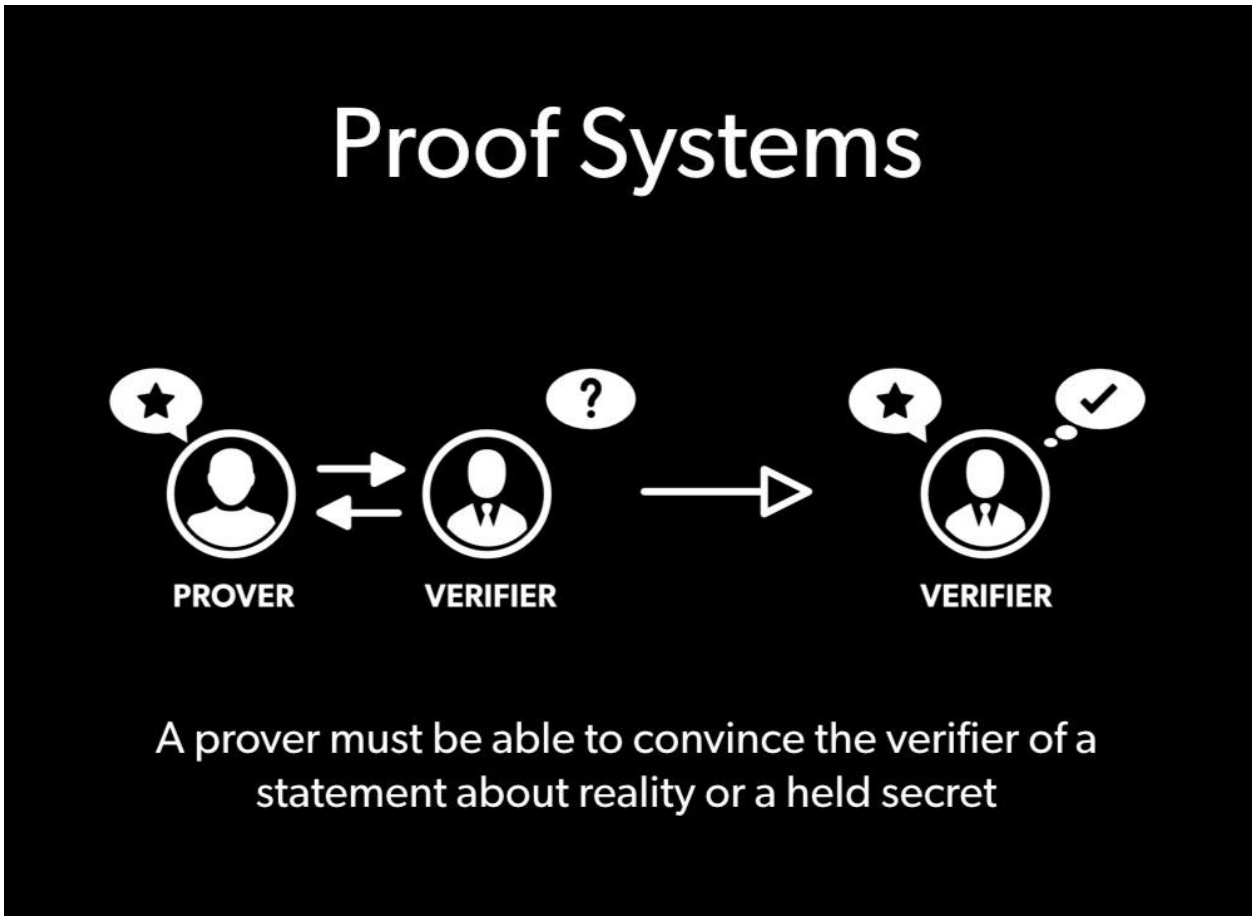
User privacy in DAOs



Ignas Apšega

12/09/2022

3620557

byont

Fontys
University of Applied Sciences

Version Control

Version	Purpose change	Date
0.1	Initial draft	5th August 2022
0.2	Improvements based on feedback: 1. Project description 2. Project goals 3. End products 4. Phasing	6th August 2022
0.3	Improvements based on feedback: 1. Project description 2. Project goals 3. End products 4. Phasing	7th August 2022
0.4	Broaden the scope to be not only about ZK-Proofs	7th August 2022
0.5	Added sub-questions, Byont branding for the document	12th August 2022
0.6	1. White background 2. Problem description 3. Main research question 4. Sub-questions 5. Project Management Approach 6. Deliverables for Byont	19th August 2022
0.7	Changed main research question and sub-questions	26th September 2022

Table of contents

Vocabulary

[1] Blockchain - A blockchain is a distributed database or ledger that is shared among the nodes of a computer network. As a database, a blockchain stores information electronically in digital format.

[2] Decentralized Finance (DeFi) - Decentralised Finance, aka DeFi, is a financial technology based on secure distributed ledgers similar to those used by cryptocurrencies. The system removes banks' and institutions' control over money, financial products, and financial services.

[3] Decentralized Autonomous Organisation (DAO) - DAO, or Decentralised Autonomous Organisation, is an organization without any hierarchy among its members. A DAO also has a set of “rules” of how to manage its treasury (DAO’s money) and how to handle votings, which are essential for making decisions, and a DAO usually has its own Token (Cryptocurrency, in this case). All these aspects are described inside a DAO smart contract.

[4] Chain Bridge - A bridge that makes it possible for a smart contract to act on numerous blockchains rather than on one.

[5] Non-Fungible Token (NFT) - NFTs, or Non-Fungible Tokens, are also Tokens, as well as cryptocurrency, but unlike the last, NFTs are “non-fungible”, which means that they are unique, and there can be only one NFT of a kind.

[6] Tokenomics - Tokenomics is the elements that make a particular cryptocurrency valuable and interesting to investors: the token's supply and how it's issued to things like the utility it has.

[7] Metaverse - A graphically rich virtual space with some degree of verisimilitude, where people can work, play, shop, and socialize.

[8] Ethereum - Ethereum is a decentralized, open-source blockchain with smart contract functionality.

[9] ZK-Proof (ZKP) - Zero-Knowledge Proofs (ZKPs) — a method for one party to cryptographically prove to another that they possess knowledge about a piece of information without revealing the actual underlying information. In the context of blockchain networks, the only information revealed on-chain by a ZKP is that some piece of hidden information is valid and known by the prover with a high degree of certainty.

[10] Herd Behaviour - Herd behavior is a phenomenon in which individuals act collectively as part of a group, often making decisions as a group that they would not make as an individual.

[11] Scrum - Within project management, Scrum is a framework for developing, delivering, and sustaining products in a complex environment, with an initial emphasis on software development. However, it also can be applied to research, sales, marketing, and advanced technologies fields.

Introduction

Byont Labs specializes in blockchain[1] development and consultancy. Byont is a public blockchain development agency that is an official partner of Blockchain Netherlands Foundation. Their services are mostly focused on writing highly secure smart contracts for DeFi[2] apps, DAOs[3], chain bridges[4], and NFTs[5]. On top of that, they also help implement tokenomics[6], utilizing smart contracts, publishing NFTs, and helping to expand to the metaverse[7].

1. Project Statement

1.1 Formal Client

The formal client would be the company - Byont Labs themselves - Jasper Verbeet and Rick van Melis the co-founders. Any questions regarding the project can be addressed to them.

1.2 Contact Information

Email: info@byont.nl Phone: 06 40568912

1.3 Project Leader

The project leader is responsible for ensuring that the deadlines are met and the final result is delivered in good quality.

Contact Information Jasper Verbeet Email: jasperverbeet@byont.nl

1.4 Current Situation

• Blockchain data is publicly available and transparent, which also means limited privacy for the users;

• 38% of enterprise blockchain projects are being discontinued due to privacy concerns.

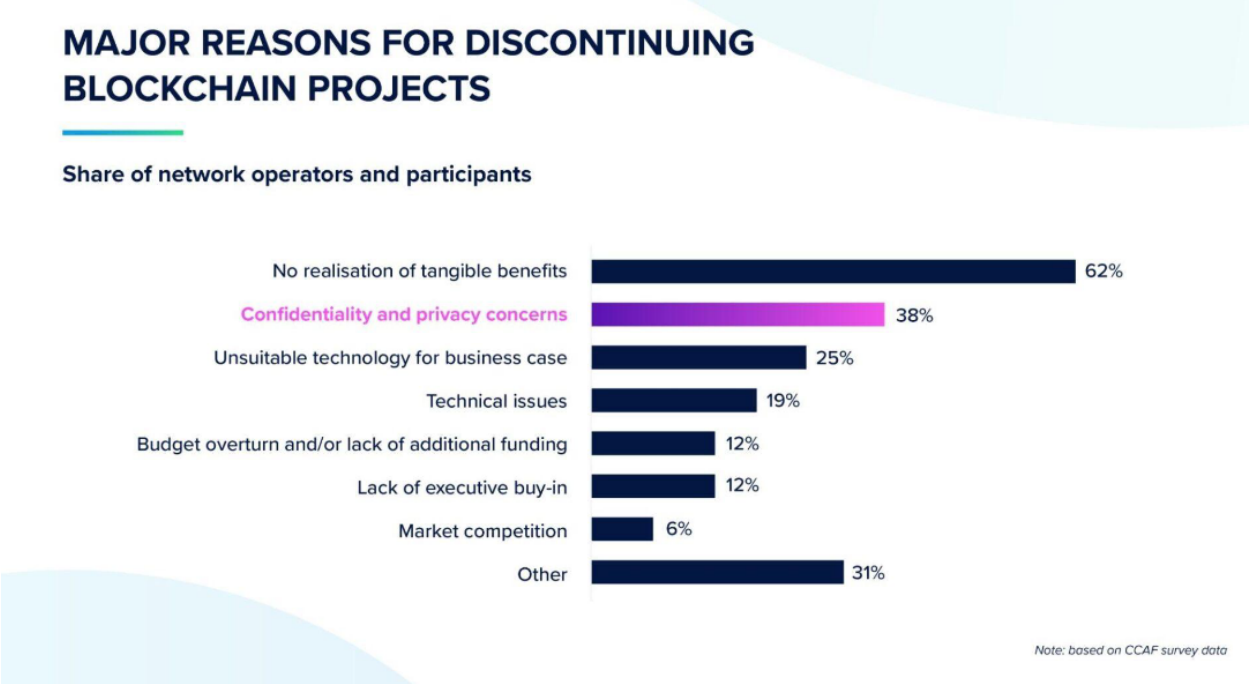
• Currently, it is quite common for DAOs to have herd behavior in participation and voting processes;

• Some DAO members would like to stay anonymous, which is impossible for now;

• DAOs are currently failing to follow the model of a perfect DAO, according to this article;

• ZK-Proofs is an active area of research and development because of its potential to solve on-chain privacy and Layer 2 scaling challenges;

• Byont has an insufficient amount of expertise in ZK-Proofs technology for blockchain development. Thus, the research and development of possible use cases must be done.



1.5 Problem Description

Tooling for DAOs is in active development, as CoinYuppie states, and new improvements and solutions are introduced regularly. One of the main DAO features is that they want to be completely transparent, but DAO members may want to stay anonymous and still be a part of this organization. DAOs use smart contracts to work in a blockchain. These smart contracts are made of chunks of code that help execute operations automatically when a set of criteria are met. While Ethereum[8] was the first blockchain to use smart contracts, it is deployed on various other blockchains. Many blockchain networks operate as public databases, meaning anyone with an Internet connection can view a list of the network's transaction history. This leads to the issue of low privacy because users of DAOs may not want their activities such as voting or proposing to be displayed to everyone on the network.

Currently, Byont has not enough resources to look into possible solutions. However, they still want to conduct research and do some possible development of this technology for their projects.

2. Project Objectives

2.1 Project Goals

This internship aims to research possible ways of improving users' privacy in the DAO. Because currently, almost every step of a user in the DAO is seen by other members, including voting, making proposals, etc.

2.2 Research Question

What are the best solutions to hide the data of DAO users for their most common actions?

2.3 Sub-Questions Breakdown

1. What is a DAO?
2. How do DAOs operate?
3. What are the main activities in DAO people participate in?
4. Is privacy really a problem within DAOs?
5. What kind of data can be hidden to improve user experience in DAOs?
6. What tools are there for improving privacy for DAOs?
7. Could the solutions found be implemented in the current projects of Byont?

2.4 End product

The final products of this internship will be research documents, blogs, and advice on the possible solutions for improving user privacy in the DAOs. In addition, proof of concept and prototypes will be submitted to Byont. Finally, if possible, prototype implementation for current projects of Byont should be carried out.

2.5 Project Deliverables and Non-Deliverables

Deliverables for Fontys

- Phased project plan
- Internship portfolio, which consists of
    - Research documents on the privacy of the DAOs
    - Advice document on the privacy of the DAOs
    - Blogs based on findings of the research
    - Prototypes
- Reading guide for external expert

Deliverables for Byont

- Phased project plan
- Research documents on the privacy of the DAOs
- Advice document on the privacy of the DAOs
- Blogs based on findings of the research

- Prototypes of possible solutions for DAOs privacy:
    - Proof of concept: to show if the privacy solution can be implemented
    - Product: A more complex version of Proof of concept
    - Byont Integration: integrated the learned concepts in one of the Byont projects

Non-Deliverables

- Dutch version of the project and documents

2.5 Project Constraints

- Time constraints: The duration of this project will last about a semester and will be divided into sprints.
- Way of documentation: The documentation should be written and saved in Notion.
- Language constraint: Due to an international work environment, all documentation, communication, and programming must be done in English.
- Scope: The focus is on improved privacy of DAOs.

2.6 Project Risks

The risks of the project are assessed below.

Risk factor	Probability	Impact	Mitigation
Late delivery of the sprint deliverable	**Low**	**Medium**	Plan time more correctly and precisely. Always update the stakeholder and other team members
Lack of communication	**Low**	**High**	Have direct communication channels like: 1. Discord 2. WhatsApp. In

			addition, have weekly meetings with the project leader. Also, regularly update the university mentor
Having troubles with new technologies and platforms	**Medium**	**Medium**	Read documentation well, do a lot of research and practice to get good at implementing solutions with different programming languages and platforms. Also, ask colleagues or company mentor for help
Inability to work because of sickness	**Low**	**Medium**	Communicate with the mentors if such a situation happens

3. Project Management Approach

The project management will follow a mix of Agile methodologies. I will follow a Scrum[11] methodology, where I will have weekly stand-ups and sprint deliveries to update my mentor on my progress so far. Each week on Monday, Sprint planning and Sprint review will happen. In addition, each sprint will be one week long.

4. Phasing

4.1 PHASE 1: INITIATION - WEEKS 1 - 2

The first phase is the initiation of the internship and what the project/assignment is all about – defining the scope of the project together with its stakeholders and the need of the project. Alongside the assignment initiation, the employees, the internship mentor, the company mentor, and the workplace are also introduced. The role of the employees is stated. As well as the internal tools, software, and documentation are all introduced as well.

Activity: Adapt to the environment

Tasks for the activity are

- Introduction to the project, software, documentation, team, work environment, and mentor.
    - Get familiar with DAOs privacy by watching videos and reading blogs and documentation.
- Read the documentation of possible tooling of DAOs privacy.
- Document the gathered knowledge and write a short blog/article.
- Work on the project plan document.

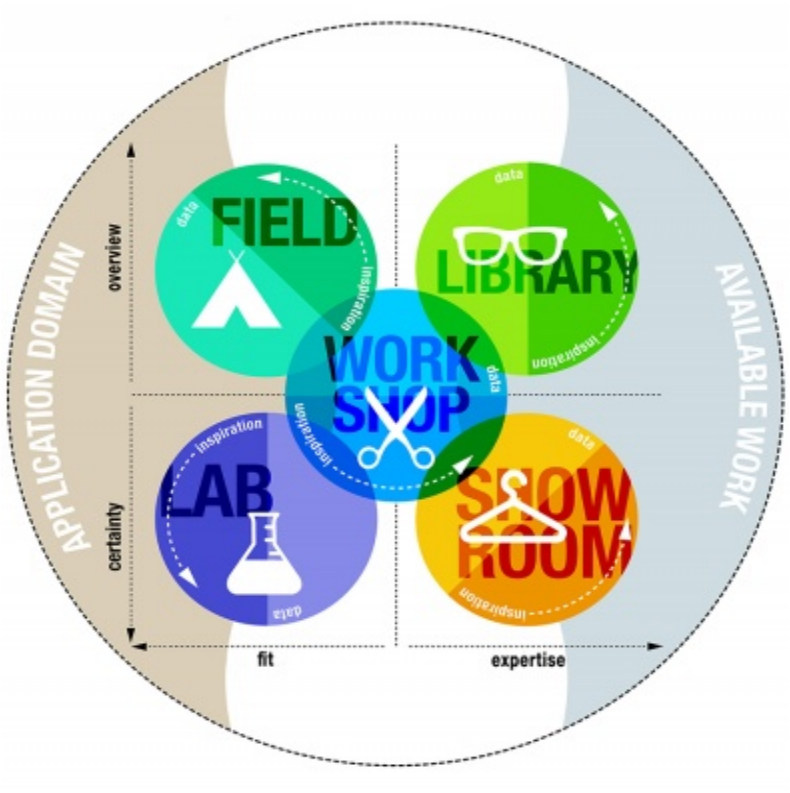
Deliverables:

- Project plan (version one)

Estimated working time: two weeks

4.2 PHASE 2: RESEARCH AND METHODOLOGY - WEEKS 3 - 5

This phase focuses on the research of the assignment of this internship; since this field is new, there will be extensive research and learning for the different platforms there are to learn. With the help of the DOT framework, which helps to figure out the research strategies, I will be using it to conduct research and learn for the internship.



The research methods used in this project are as follows:

- **Library**: With this research strategy, I will learn the possible privacy solutions for DAOs. In addition, I will learn more in-depth knowledge about it and its technologies, libraries, tooling, and programming languages. To do this, I will carefully research google and its given articles and documentation. After

gathering a sufficient amount of information, I will write a blog about it for Byont.

- **Field**: I will analyze the stakeholders and problems more deeply with this research strategy. Thus, several meetings will be held to gather the information. In addition, the current documents of Byont will be analyzed. This will let me know the right approach for the expected documentation.

- **Workshop**: After understanding the concepts of DAO privacy. I can acquire practical knowledge through hands-on tooling, libraries, and programming languages. This will allow small-scale prototypes or IT-architecture sketches for future implementations.

- **Lab**: With this research methodology, I will improve and/or scale the prototypes with A/B or Usability testing. If needed, solutions will be implemented in the current projects of Byont.

- **Showroom**: With this research strategy. I will be showing my contribution, input of ideas, and solutions to the team constantly during the meetings. At the end of the project, the final internship portfolio and the research with prototypes and how it has helped the company will be presented to the stakeholders and university mentor.

Research Methods

Research Methods	DOT-Research Framework
1. What is a DAO? 2. How do DAOs operate? 3. What are the main activities in DAO people participate in? These questions will be researched by following the Library research methodology.	**Library,**
4. Is privacy really a problem within DAOs? It is important to conduct field	**Library,** **Field,**

research and ask users if privacy is a problem.	
5. What kind of data can be hidden to improve user experience in DAOs?	**Library,** **Field,**
6. What tools are there for improving privacy for DAOs? The possible solutions will be tested and showcased to Byont.	**Library,** **Workshop,** **Showroom,**
7. Could the solutions found be implemented in the current projects of Byont? After research and prototyping. Advise Byont on how they could improve their current projects.	**Library,** **Workshop,** **Lab,** **Showroom,**

Activity: Research into project problem

Tasks for the activity are:

- Research into sub-questions of the main research question
- Document the findings

Activity and Deliverables:

- Week 3
  - Project Plan (final version)
- Week 4
  - Research document(s)/blog(s) on:
    - What is a DAO?
    - How do DAOs operate?
    - What are the main activities in DAO people participate in?
    - Is privacy really a problem in DAOs?
- Week 5
  - Research document(s)/blog(s) on:
    - What tools are there for improving privacy for DAOs?

Estimated working time: three weeks

4.3 PHASE 3: EXECUTION - WEEKS 6 - 16

In this phase, all implementation and development during the project occur. Here is where the project requirements will be implemented, and the research done in the previous phase will be applied.

Activity: Prototypes based on acquired use cases and tooling

Tasks for the activity are:

- Test the possible tooling for solving the privacy of DAOs
- Build Proof of Concept which uses the tooling
- Build Product which is a more complex system of Proof of Concept
- Gather feedback and improve on it

Activity and Deliverables:

- Week 6
    - Test the tooling for the privacy of DAOs

- Week 7
    - Documentation(s)/blog(s) for the tooling

- Week 8 - 9: Proof of concept

  Description: shows the code implementation of the privacy solution in an imitation of a familiar DAO environment and explains how it works.
  Purpose: to show if the privacy solution can be implemented for our use case

- Week 10 -13: Product Building

  Description: a product which is a more complex system of proof of concept that is designed to keep the privacy of the users of DAOs using found privacy tooling/solutions

  Purpose: the purpose of this product is to show how found solutions could work in a more complex product that has DAO-related issues.

- Week 13 - 16: Byont Integration

  When the final product is thoroughly tested and works perfectly, then it is time to integrate this system into the Byont environment.

Estimated working time: ten weeks

4.4 PHASE 4: CLOSURE - WEEKS 16 - 20

During this phase, the project is reviewed and reflected on what went well and what could have been done better.

Activity: Polishing the product

Tasks for the activity are:

- Polished prototypes and documentation
- Final internship portfolio
- Advice on current Byont projects

Deliverables for Milestone 3:

- Final advice for the privacy of DAOs, current projects

Estimated working time: three weeks

Activity: Present final result to the team and university

Tasks for the activity are:

- Create a presentation
- Discuss the final result with the team
- Ask for any feedback

Deliverables for Milestone 4:

- Final presentation

Estimated working time: two weeks

5.1 Communication plan

This section demonstrates the communication plan between the student and the university. Regular meetings with the university or company tutor can be scheduled if necessary. In addition, weekly meetings with the company tutor will be held.

The main deliverables for the university are as follows:

- Project plan – It will create a plan for approaching the project.
- Mid-term presentation – It will present the project's current progress to the university.
- Internship portfolio – It will describe and showcase the process of realizing the project.
- Final presentation – It will present what has been achieved during the internship.

Activity	Estimated Date
First company visit	Monday 12th - Friday 30th September 2022
Project plan (version one)	Monday 5th September 2022
Project plan (final version)	Monday 12th September 2022
Internship portfolio (version one)	Monday 17th - Friday 21st October 2022
Mid-term presentation	Monday 31st October - Friday 4th November 2022
Internship portfolio (version two)	Monday, December 19th, 2022
Internship portfolio (final version)	Tuesday, January 10th, 2023