The Badge

Short Paper v2.0.0

Nicolás Domínguez, Agustín Pane, Federico Madorey

October 2022

Abstract

The Badge is a decentralized certification platform built on Ethereum. It allows tokenizing any piece of verifiable information under the concept of badges. These badges will be issued as non-transferable NFTs, making accessible the information they represent for any person or platform in the scope of the Ethereum ecosystem.

1 Introduction

Web3 technology has evolved incredibly fast regarding protocols, decentralized finance, art, and autonomous organizations, but there is an important missing key: validate that an event or specific information coming from the off-chain world is authentic. In the world of blockchain, wallet owners are completely anonymous. This has some advantages in terms of privacy. However, there are benefits that would come with the possibility to prove the wallet owner's skills from previously achieved things. For instance, the ability to apply for an open position or for a lower interest on loans, among others. So, if there is a way to validate this information, it will be possible to create an on-chain reputation, unlocking many new use cases.

The Badge is a platform that certifies information in a decentralized way. It will provide an address with badges representing particular events. The most interesting feature of a badge is that it is non-transferable and inalienable from the address, and it can only be obtained through skills or milestones achieved and cannot be simply purchased.

If the blockchain keeps evolving as it has been doing during the last years, the use of non-transferable identities will be crucial for different decentralized platforms, just to mention some of the ones offering employment, learning platforms, and companies seeking funding and many others.

2 Existing problems

We are building a *decentralized platform* to certify information from the real world to the blockchain. Our platform is going to be a public good, any person around the world will be able to use it. We believe that our project will become a very important piece of the ecosystem. We will unlock many usage cases that today are not easy to deal with, let's describe some examples:

Crowdfunding: there are many NGOs (non-governmental organizations) around the world that need funds to keep helping people. We have witnessed many times how willing to help people on web3 they are. Currently, NGOs do not have a way to prove their identity on-chain, they are just addresses on Ethereum asking for funds, people that are willing to help cannot be sure if they are just scammers or fraudulent addresses, in our platform NGOs are going to be able to certify their activities and prove who they are, giving to people willing to donate the trust they need. That's not all, they even could certify how the funds were used by sharing audit reports, bringing transparency to the entity.

Our platform will also help web2 startups to raise funds on web3 crowdfunding protocols like https://mirror.xyz/. There are many startups that have great potential but for them it becomes difficult to get the funds required to kick off. Also, in many countries the access to lines of credit is difficult, using web3 for crowdfunding might be one of the best ways for certain startups to raise the funds they need. With The Badge they will be able to certify documents that will bring confidence for both the startup and the investors. Some examples are documents accrediting who they are, proof of initial funds and documents certifying that the individuals running the startup do not have debts or other financial problems.

Helping to be hired by a DAO: providing addresses with badges could be extremely valuable for different protocols, especially for Decentralized Authority Organizations (Reiff, 2021) (DAOs). DAOs could use this information to objectively select a committee based on different skills or experience and ponderate voting power for addresses that have proved to be better qualified, in order to accept or decline a proposal. Currently, there are many good professionals with outstanding capacities, like developers, community managers, lawyers, and many others. Our platform will allow them to certify their degrees, courses, seminaries, etc on-chain and use these certifications to apply for jobs required in a DAO.

3 The Badge as a platform

The Badge will use Kleros as a base (Kleros, 2017) to fulfill the task of allowing the emission of badges to be addressed in a transparent and verifiable way.

Each badge emitted by The Badge will be an NFT (Sharma, 2021) with some special features. Once a badge is minted, it won't be transferable or waivable. This represents the concept of *soul-bounded NFTs* (Buterin 2022) from Vitalik Buterin. Its metadata will be uploaded to IPFS (Wikipedia contributors, 2019) to prevent data loss or manipulation. The metadata will contain sufficient information about the parameters used to create the badge as well as a description of what it represents, so anyone on the Ethereum network would be able to validate the authenticity of any badge.

3.1 Overview

The platform supports two types of badges, depending on whether the badge is being created directly for individuals or from a third-party entity.

There are two types of badges: **off-chain** and **third-party**.

- Off-chain badges are those which will be minted based on verification by a Kleros curated list.
- Third-party badges are those minted by a third-party entity and are verified by its reputation.

Off chain badges will be **directly minted** to the user who requested it. Entities minting third-party badges, will have the possibility to mint them directly to a specific address or to create a **whitelist of addresses**. The reason for this is that some entities would like to assign the same badge to many addresses at the same time, this could be beneficial to ease the adoption of users who are learning about the blockchain. Some other entities would like to give the user the possibility to mint the badges by themselves.

3.2 Types of badges

3.2.1 Off-chain badges

Off-chain badges will be only granted per request of the user. When a user applies to request a badge and the information submitted is valid, it will be minted directly to the user's address.

Emitting off-chain badges is the most challenging part of our architecture as we pursue transparency and verifiability. Validating something that had happened in the off-chain world is not possible without the help of real people who can analyze evidence and give a verdict about what they consider to be the truth.

We will delegate the verification layer to Kleros through the Kleros curation lists and the community will decide if the evidence provided by the user is authentic or not. If the Kleros community agrees that the information provided is genuine, the badge will be minted. If not, the user will have the possibility to appeal the ruling and provide new evidence. This incentive mechanism will also be used for existing badges, the community will receive bounties for creating challenges against suspicious badges and malicious users not only will lose their badges but they will also be penalized.

3.2.1.1 Creating an off-chain badge step by step

The first step to create an off-chain badge is to create the *badge strategy (step A)*. Each strategy will be created as a list in a "Kleros curation list" (KCL) (Kleros curation, 2020) and each badge requested will be an entry of that list. Once the strategy has been created any user will be able to mint a badge of it for his/her address by submitting the evidence required (step B).

At the beginning the strategies will be created by The Badge team but in the future every member of the community will be able to propose and create new strategies and our platform will grant incentives for them.

Step A): Off-chain badge strategy creation

Strategies are rules that standardize the conditions needed for a badge to be minted. They are customized for each kind of certification that has to be done (Twitter, Github, Udemy, etc.). Each strategy has to be meticulously designed for the following reasons:

- The information a user has to submit will be standardized to reduce the possibility of misunderstandings at the verification moment.
- The rules that the jury has to follow to analyze the information will be predefined.

A strategy encompasses:

1. Name: the name of the strategy. (Example: Twitter)
2. Evidence: how the information is going to be analyzed and validated. (Example: user must provide a twitter account and a link to a tweet with his wallet address)
3. Challenge period duration: this is the time the Kleros community has to analyze the evidence and initiate a challenge if they consider the information fraudulent.
4. Deposit: the number of tokens the user will have to deposit in order to incentivize the community to validate the submission. If nobody challenges the submission, the deposit is returned to the user after the challenge period duration elapses. (Example: 1 DAI)

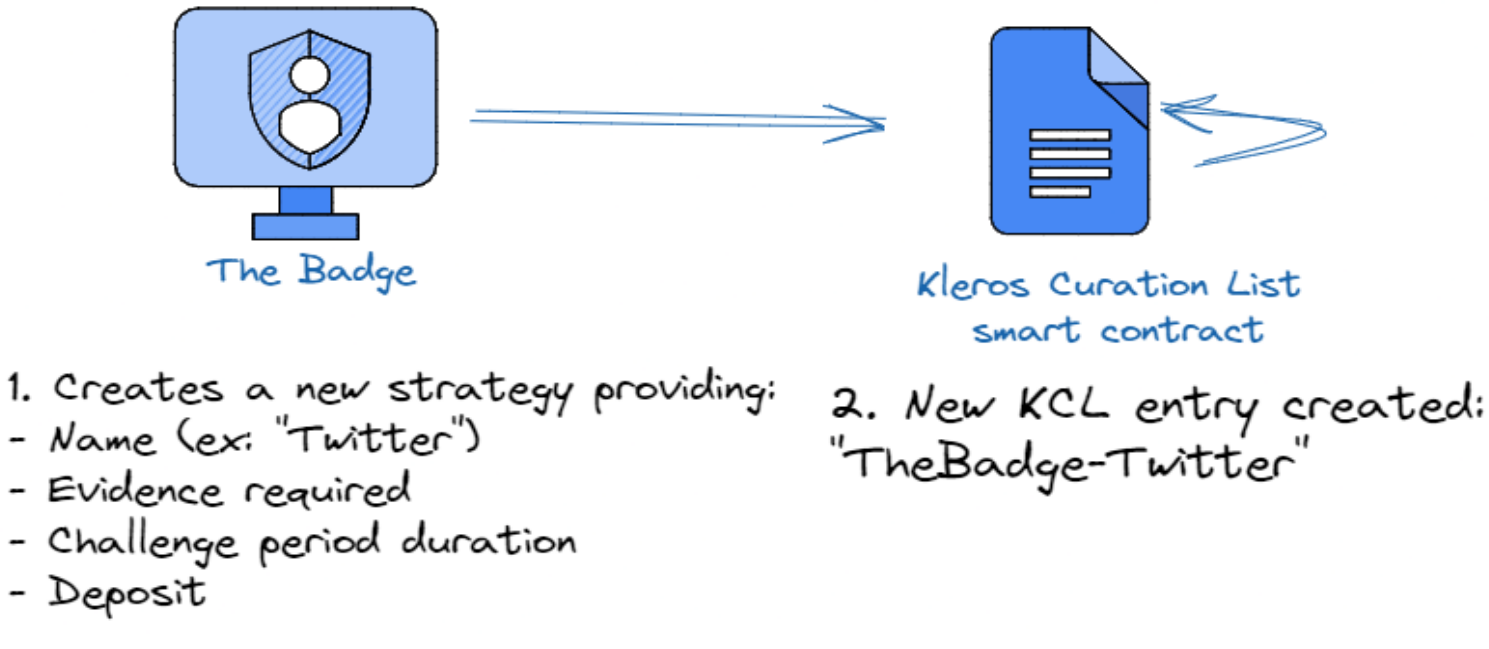

Fig. 1. Off-chain badge strategy creation.

Step B): Off-chain badge minting

Once the strategy has been created, any user will be able to request a badge in case he is able to fulfill the requirements defined on it (Figure 2).

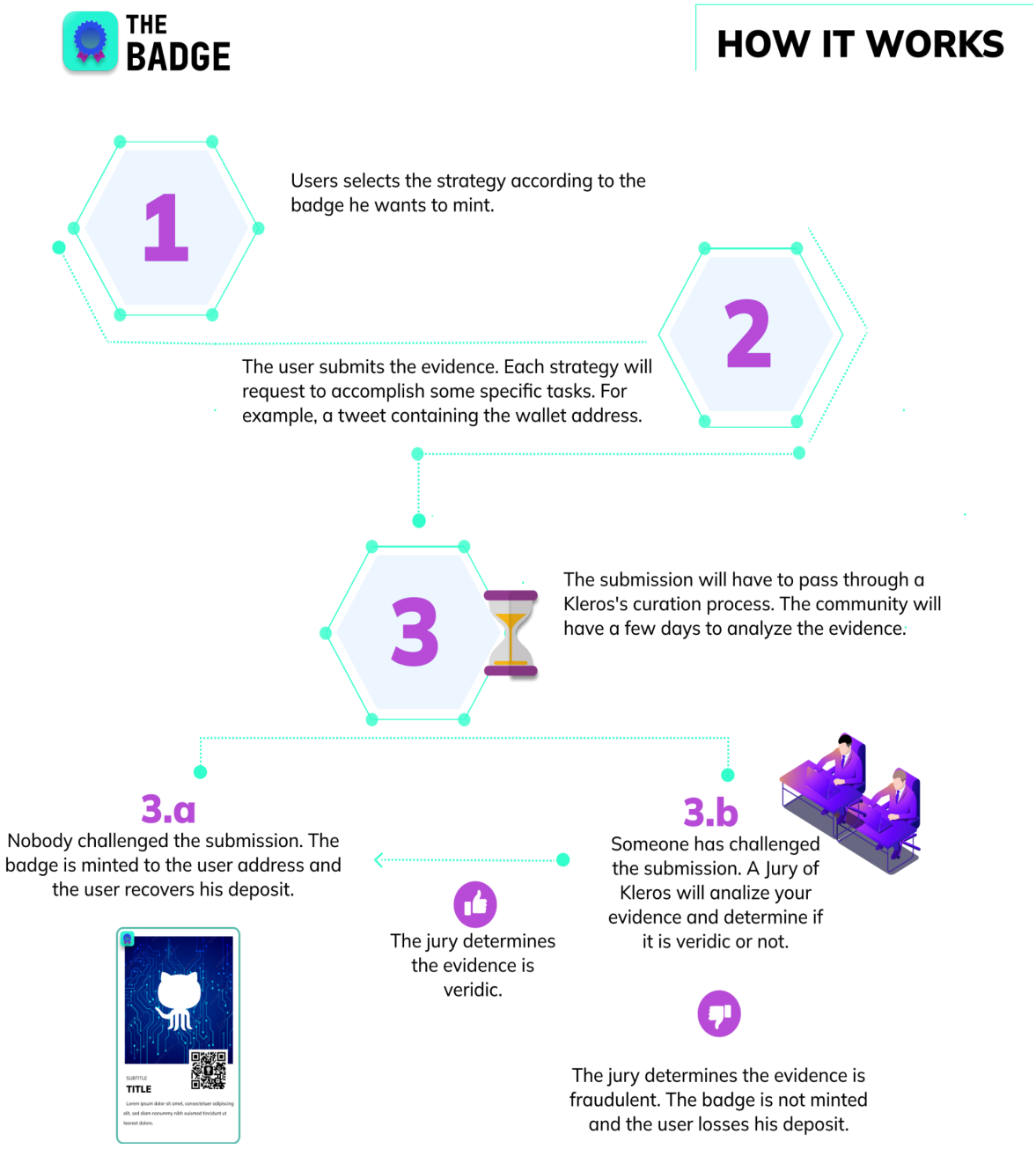

Fig. 2. Off-chain badge minting.

Following the example, he needs to demonstrate he owns a particular Twitter account following the next steps:

1. The user selects the Twitter strategy.
2. The user prepares and submits the evidence. This step will create a new entry in the KCL TheBadge-Twitter. To do so, the user will have to deposit and pay a small fee indicated by the strategy and pay the gas of the transaction.
3. The community will have a few days to review the submission, if they find the evidence veridic, no action is required as this process is optimistic, after the revision days have elapsed the deposit is returned back to the user and the badge is emitted. If a user finds the evidence is fraudulent he might initiate a challenge.

3.2.1.2 Challenging an off-chain badge

Any badge can be challenged at any time and will be treated in the Kleros court. To initiate a challenge a user needs to deposit a predefined amount of ETH. The Badge will analyze each challenge and, if it considers that the badge is legitime, it will pay for the challenge. If The Badge considers that the badge approved by the jury might be fraudulent, the user who has received the badge will have two weeks to accept the challenge by depositing the same amount of ETH. If he/she does not, the badge already emitted will be burned. If he does, after depositing the ETH, a dispute resolution in Kleros will start.

Kleros resolution

- If Kleros' rule in favor of the challenger, the badge is burned, and the challenger earns the deposited ETH from the badge holder, minus the costs of using the services of kleros. The badge holder is penalized.

- If Kleros' rule is in favor of the badge holder, the challenger loses the deposit, and the holder keeps his badge.

3.2.2 Third-party badges

There are entities (companies, universities, institutions, etc) that might want to emit their own custom badges using their own strategies. Our platform will work as a “blockchain-certifications as a service” allowing them to register and start emitting badges on their name.

3.2.2.1 Third-party badge minting

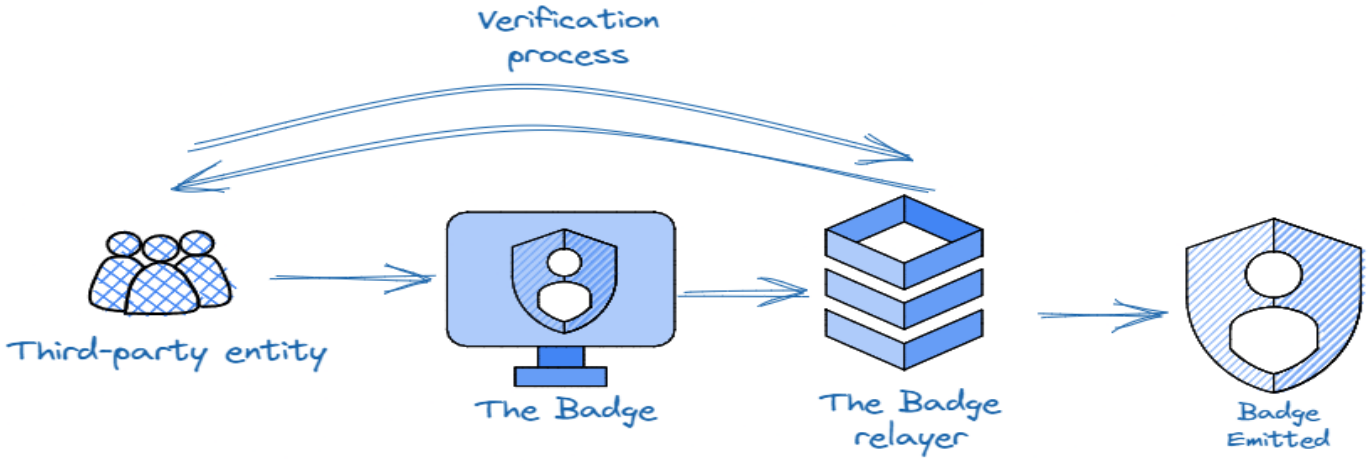

Fig. 3. Third-party badge minting.

1) First the entity has to register within the platform. They should be approved in order to participate.
2) After the approval process is done and they are registered as third-party entities they are allowed to mint their own custom badges. They will be able to create different badges according to their needs.
3) They now are able to directly mint badges to their users or to whitelist addresses that would then mint the badge to themselves.

Each badge minted will be backed by the reputation of the entity. Entities will also have the possibility to revoke a badge already minted.

3.2.2.2 Challenging a third-party badge

Third-party badges won’t participate in the Kleros as the reputation of those badges is being backed by the entity itself. Nevertheless, the third-party entities that are willing to emit badges within our platform must be approved and recognized as a real entity in order to be able to mint directly to address, entities not recognized will only be able to whitelist address to mint badges, this will avoid that malicious users use our platform to spam badges to users.At early stages of the project, The Badge team will be in charge of approving new entities but in the future these decisions will be taken by The Badge DAO.

3.2 Architecture

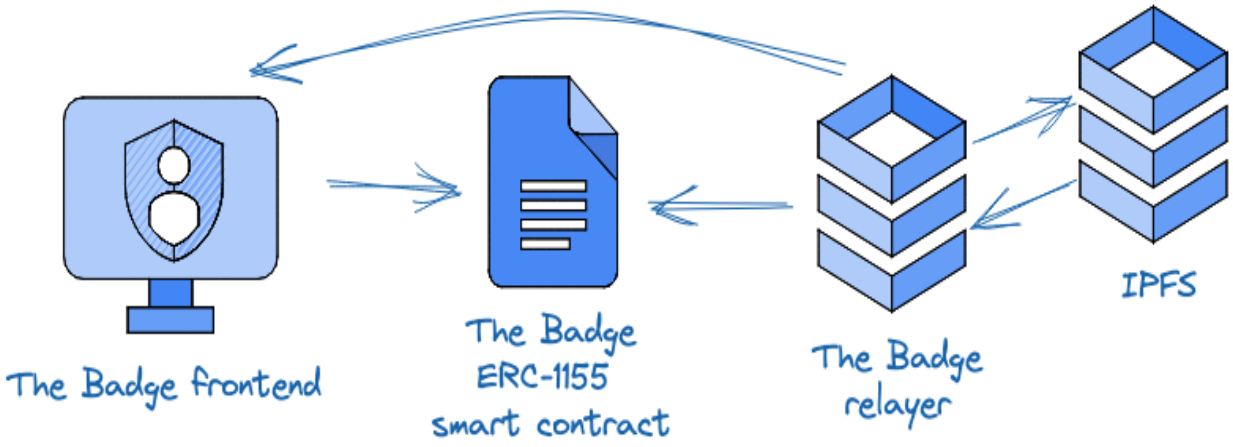

Fig. 4. Architecture.

The heart of The Badge is its smart contract. A collection based on the standard ERC-1155 with some modifications that will allow us to develop non-transferable assets, assets that are valid for a period of time, collect fees, challenge badges, etc.

Another important part of our architecture is the frontend, which will allow users to interact easily with our protocol. Users will be able to create new strategies, request the emission of a badge, submit evidence, and all the features our platform will support. The frontend will also work as a wallet profile, where users will be able to share a link to others to show the badges they already have.

There is going to be a backend, which will help users to interact with services like IPFS so they can submit their evidence without worrying about the technical difficulties. Also It will serve the frontend with information from the blockchain in a performant way.

4 The Badge as a product for profile management and discovery

We aim to build a platform that everyone can use to get their own badges, but this is just our first milestone. Our second milestone will be to create a wallet to facilitate profile administration (Fig. 5), this wallet will have features like badge listing, search and filtering for addresses containing a certain type of badge, in order to help to discover profiles, and also to help users to manage their badged acquired in other platforms.

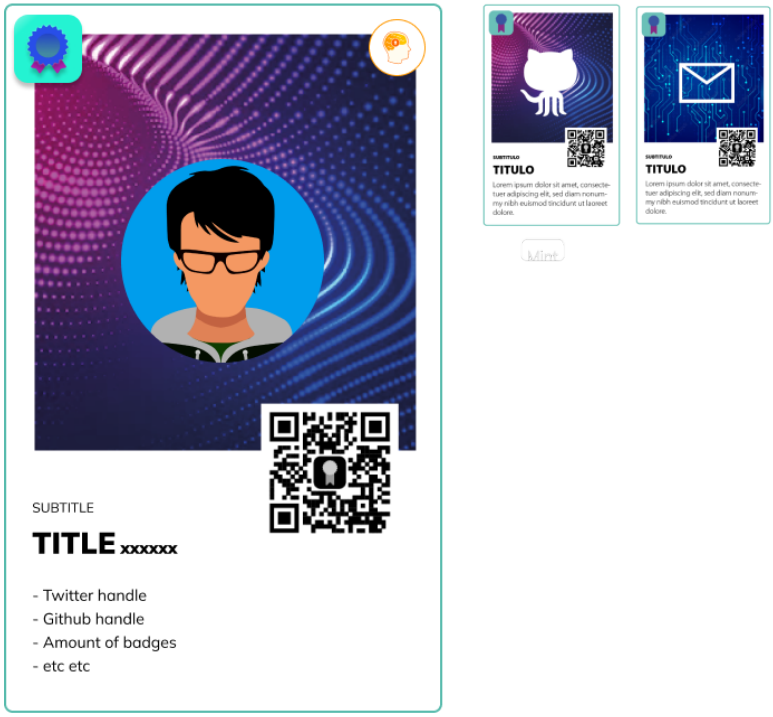

Fig. 5. Different types of profiles.

5 Privacy

A right for all humans is the ability to maintain a certain level of privacy. Currently, it is not possible to prevent others from seeing all the NFTs that an address possesses. The Badge understands the value of privacy, that's why we would like to support privacy in a way that a user could prove he/she possesses certain badges without exposing them publicly. Our first implementation for off-chain badges will not support this feature as the zkSnarks(Jo, 2019; Zcash, 2017) technology is still not very mature but we are going to work on it as soon as the technology evolves.

However, third-party badges are not required to be validated through Kleros, so they will have multi-recipient encryption enabled by default (but can be configured according to the entity needs). This means that both the user recipient of the badge and the emitter (the third-party entity) will be able to read the information about the badge while the rest of the users won't.

6 Applications

The value of a project is given by how many problems it solves. Use cases and possible domains for The Badge are many. Some areas where it can be used are finance, human resources, penalization, rewarding, etc. Here are some examples of applications:

a. Certifications, our main goal is to be the platform where people could bring off-chain certification and link them to an on-chain identity. Some examples are courses, training, legal documents, skills, etc.
b. Negative marks. If The Badge allows to mint a badge to addresses without them having to claim the badge explicitly, it might be possible to mark addresses as dangerous. For example, the addresses that have been involved in a hack.
c. Creating a wallet/funds recovery mechanism as some web2 platforms do. They can validate the identity of the user through a badge.
d. Two factors of authentication (2fa, Authy), it might be possible to emit a badge for a profile ID. This badge integrated with centralized services could work as 2fa. Every time a user wants to login to a web2 application, he could sign a message with his wallet to prove he/she is the owner of the account.
e. Custom certifications, Reputation

7 Governance and BADGE token

The Badge's greatest purpose is to add value to the web3 ecosystem and strives to do so with the highest level of decentralization possible. Therefore, The Badge has the goal to eventually create a decentralized governing system, best known as DAO, that will define the evolution of the project.

8 Conclusion

The Badge aims to become a platform capable of certifying any data from the off-chain world based in decentralization, transparency and reliability, each badge will have the evidence necessary to prove its authenticity and if it does not, it can be challenged and our platform will act in consequence to remedy the problem using the Kleros decentralized arbitration service.

We are very confident about what we are building, we think that The Badge platform will become the most important web3 certification platform and a building block for other projects that will require any type of decentralized data validation. Kleros already gave the community decentralized justice, now we want to build on top of it in order to create a web3 clerkship that the community will be able to also work on top and develop their protocols with a solid document certification layer.

Our platform will unlock a lot of use cases: from universities emitting web3 diplomas, beneficial institutions and startups certifying legal documents in order to get sponsorship within the web3 ecosystem to people minting their skills on-chain or even things like their ownership of real estate for example. But the most interesting part is that most of them are currently unknown or do not even exist, the world is starting to slowly move from web2 to web3 and our project will help to set up the bases for allowing that to become real.

9 References

Buterin V. (Jan. 26, 2022). *Soulbound*. Vitalik.ca. vitalik.ca/general/2022/01/26/soulbound.html.

Circle. 2018. *Circles - a Basic Income on the Blockchain*. Circles. joincircles.net/.

CoinMarketCap. 2020. *Collateralized Debt Position (CDP) | CoinMarketCap*. CoinMarketCap. coinmarketcap.com/alexandria/glossary/collateralized-debt-position-cdp.

Jo, T. 2019. *An Exploration of Zero-Knowledge Proofs and Zk-SNARKs*. Thesis. https://fisher.wharton.upenn.edu/wp-content/uploads/2020/09/Thesis_Terrence-Jo.pdf

Kleros. (July 20, 2022). *Introduction to Kleros*. Gitbook.io. kleros.gitbook.io/docs/..

MakerDAO. 2020. *The Maker Protocol*. White Paper. Makerdao.com. makerdao.com/en/whitepaper#abstract.

Proof of Humanity. 2021. *Proof of Humanity*. www.proofofhumanity.id/.

Reiff, N. (Sep 24, 2021). *What Is a DAO? Investopedia*.www.investopedia.com/tech/what-dao/.

Sharma, R.(a). (March 8, 2021). *Non-Fungible Token Definition: Understanding NFTs*. Investopedia. www.investopedia.com/non-fungible-tokens-nft-5115211.

Sharma, R.(b). (March 24, 2021). *Decentralized Finance (Defi) Definition and Use Cases*. Investopedia. www.investopedia.com/decentralized-finance-defi-5113835.

The Graph. (July 20, 2022). *About the Graph*. The Graph Docs.. thegraph.com/docs/en/about/.

Wikipedia Contributors. “InterPlanetary File System.” *Wikipedia*, Wikimedia Foundation, 2 Dec. 2019, en.wikipedia.org/wiki/InterPlanetary_File_System.

Zcash. 2017. *What Are Zk-SNARKs?*. Zcash. z.cash/technology/zksnarks/.

Kleros curated, (Kleros curated, 2020). Kleros curate the explainer https://blog.kleros.io/kleros-curate-the-explainer/

Authy. 2fa. https://authy.com/what-is-2fa/

Kleros Curation List (KCL). https://kleros.gitbook.io/docs/products/curate