The Badge

Short Paper v1.0.1

Nicolás Domínguez, Agustín Pane, Federico Madorey

July 2022

Abstract

The Badge aims to be a decentralized certification platform built on Ethereum. It allows tokenizing any piece of information coming either on-chain or off-chain under the concept of badges. These badges will be issued as non-transferable NFTs[1], making accessible the information they represent and also verifiable 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: verify on-chain or off-chain. In the current world of blockchain, wallet owners are completely anonymous. This has the advantage of privacy. However, there are many additional benefits that can come with the ability to prove the wallet owner's skills from previously achieved things. For instance, the ability to apply for an open position or for lower interest on loans, among others. On-chain identity and reputation combined can unlock many new usage cases.

The Badge aims to become a decentralized certification platform that provides and address together with a badge, representing particular events from the off-chain and on-chain world. The most interesting feature of these badges is that are non-transferable and inalienable from the address, and it can only be obtained through skills or milestones achieved and not with money. Examples of off-chain world events are the ownership of a particular Twitter, Github, or Medium account, proving that the owner of the account has a diploma from a platform like Udemy, or even better, from an University. Examples of events from the on-chain world are addresses that have created Collateralized Debt Positions[2] (CDPs) on Maker[3] by an amount largerthan 50k and have never been liquidated; or addresses that have provided more than 100k liquidity to the top 5 protocols for more than three years.

[1] Non-Fungible-Token (Sharma,2021)
[2] Collateralized Debt Positions (CoinMarketCap, 2020)
[3] Maker (MakerDAO, 2020)

Providing addresses with badges could be extremely valuable for different protocols, especially for Decentralized Authority Organizations[4] (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.

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 like the ones offering employment, lending platforms, and others. For employment or hiring purposes, using badges can guarantee the skills and knowledge of the person that owns that address, while for the lending platforms, a badge canrepresent that a person (address owner) has never been liquidated, and it could be used to apply for getting a loan at a lower interest rate.

2 Existing problems

A big limitation that prevents the web3 ecosystem to keep growing is the lack of mechanisms to verify a wallet identity. Projects like Circles[5], or Proof of Humanity[6], are doing a great job at providing identity to an address, but they do not solve the problem of adding skills to a profile. Let's see two typical examples of unsolved usage cases:

A. Alice is a web3 developer and wants to apply for a Grant on a decentralized platform. She could create a proposal and say she is the owner of a Github account with excellent skills, and has already collaborated on many projects. Unfortunately for the DAO, it is not possible to validate that Alice's address is the true owner of that Github account.
B. DAO_X is looking for qualified candidates to compose a Committee and help to define the future of the DAO. Currently, there are no simple and fully decentralized tools to be used by a DAO in the selection of a set of addresses based on on-chain events or information such as good performance on DeFi[7] protocols, participation in previous DAO, etc.

[4] DAO (Reiff, 2021)
[5] Circle (Circle, 2018)
[6] PoH (Proof of Humanity, 2021)
[7] Decentralized Finance (Sharma, 2021)

3 The Badge as a platform

The Badge will be founded on two main protocols, The Graph[8] and Kleros[9] to accomplish the task of allowing the emission of NFTs (a.k.a badges) to addresses in a transparent and verifiable way. These badges can be used to compose a public profile of skills or tasks that have been accomplished by the address.

Each badge emitted by The Badge will be an NFT with some special features. Once a badge is minted, it won't be transferred or waivable. This represents the concept of *soul-bounded NFTs*[10] from Vitalik Buterin. Its metadata will be uploaded to IPFS[11] 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 will use two types of strategies to emit badges, depending on whether the badge is being created from on-chain or off-chain data. As it is shown in Figure 1, a strategy encompasses:

1. The information required to initiate a badge request emission.
2. How the information submitted is going to be analyzed and validated.

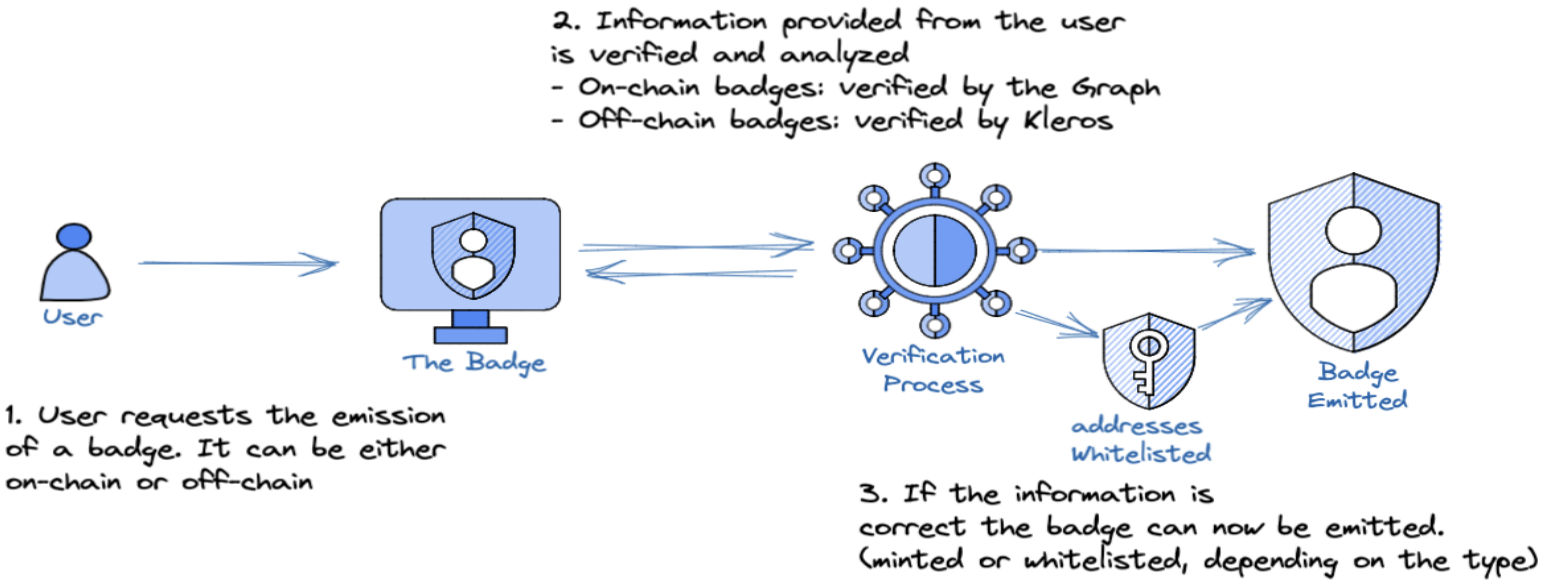

Fig. 1. Strategy for badge emission.

Note: In Fig. 1, the user represents an address interested in getting a badge for itself or anyone else.

[8] The Graph (The Graph, 2020)
[9] Kleros (Kleros, 2017)
[10] Soul Bound NFTs (Buterin, 2022)
[11] IPFS (Wikipedia contributors, 2019)

There are two types of badges: **on-chain** and **off-chain**. On-chain badges are those that can be emitted based on information that already exists on the Ethereum blockchain, while off-chain badges are those which can be emitted based on events or information from the real world. Once the verification process ends (Step 2 in Fig. 1), the badge can be **emitted**.
If the badge is an on-chain badge, it will be **whitelisted to be minted**. If the badge is an off-chain badge it will be **directly minted**. The reason for this is that mostly (but not exclusively) on-chain badges will be requested by third-party platforms to assign badges to users of their community. As the number of badges might be big, some users won't be interested in adding them to their profiles, therefore they will be able to mint them to their profiles only if they want to.
On the contrary, off-chain badges will be only requested by the user that wants the badge on his profile. When a user applies to request a badge and the information submitted is valid, the badge requested will be minted directly to the user's address.

3.2 Types of strategies

3.2.1 On-chain strategy

This strategy is the one used when a user requests the emission of a badge based on Ethereum data. The only way to emit an on-chain badge is by creating a query that can be executed in The Graph and also providing extra information such as badge name, description, etc. The addresses resulting from running the query will be whitelisted to claim the badge.

3.2.2 Off-chain strategies

Off-chain strategies are customized for each third-party service (Github, Udemy, etc.). Each strategy has to be meticulously designed for the following reasons:

1. The information that a user has to submit will be standardized to reduce the possibility of misunderstandings at theverification moment.
2. The rules that the jury has to follow to analyze the information, will be predefined.
3. If the jury approves the emission, a badge will be minted programmatically without any human intervention, directly to the address which requested the badge.

This whole process makes it hard to automatize off-chain strategies. For this reason, each strategy will be made ad-hoc. In the beginning, there will be just a few strategies defined by The Badge. Soon after, the integration of new strategies will be defined by the community.

These are some examples of different strategies:

- On-chain "Whale" badge: Emitting a badge for addresses that have deposited more than 1 Million dollars on Aave protocol in the last two years.
- Off-chain "Github" badge: The Badge creates the strategy to allow Github users to emit a badge proving they are the owners of a particular Github profile.

3.3 On-chain and off-chain models architectures

3.3.1 On-chain badges

For on-chain badges, we are relying on The Graph, a decentralized platform that allows querying passed events of the blockchain in the form of an API. Anyone can create a subgraph, each subgraph represents the history of a particular smart contract.

As shown in Fig. 2, any user or entity requesting to emit a badge will have to create a transaction to a smart contract created by The Badge (badge-request smart-contract). This transaction will be sent with the following data:

a. Well-formed Graphql query, this query must return an array of addresses.
b. Information about the badge to be emitted (name, description, image, etc).

The Badge will run a relayer that will be listening to transactions created on badge-request smart-contract. Each time a new transaction comes, the relayer will extract the Graphql query and execute it on The Graph. If the query compiles correctly and returns a list of addresses, the relayer will execute a transaction against The Badge NFT collection smart contract, whitelisting the addresses returned by the query. Whitelisted addresses will be able to claim the badge.

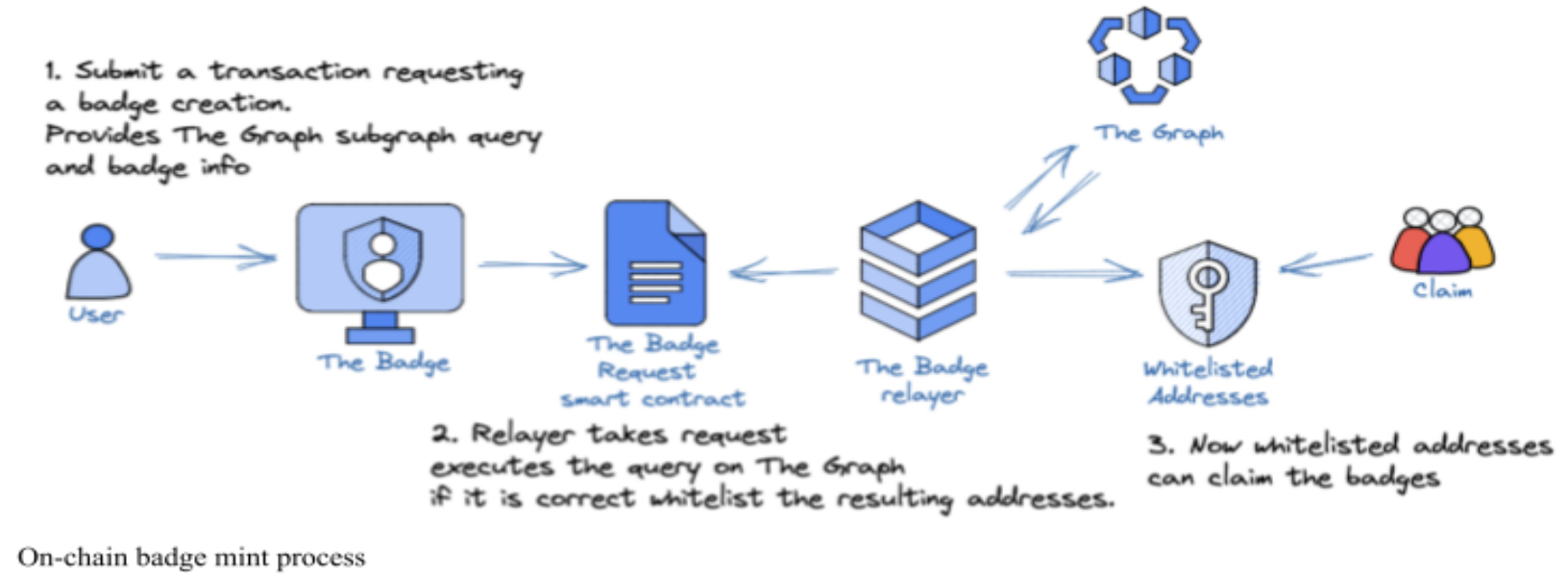

Fig. 2. On-chain badge mint process.

Note: We are analyzing the possibility of allowing badge emission without needing a user to claim it explicitly. To make it possible The Badge DAO will need to approve this emission explicitly as the badges emitted might contain undesired content. This use case will be evaluated in a future version of the platform.

An example of how a DAO can use it:

DAO_X is a DAO owning a big capital fund to administrate and needs to invest its funds to get the best profit from different DeFi protocols and wants to select a committee of 10 addresses who have participated actively in different DeFi platforms with earnings above 20% during the last year.

DAO_X will be looking at:

- **UniswapV3** addresses who have provided liquidity for more than 200k to different Pools in the last year with an APY above 30%.
- **Aave** for addresses taking loans by a value greater than 300k for at least 6 months and haven't been liquidated.

According to Fig. 2, these are the steps to follow to whitelist the badges:

1. DAO_X has to create two different queries, one pointing to the subgraph for UniswapV3 and the other for Aave. Query arguments and specific blockchain blocks are defined by DAO_X. It is required that both queries return an array of addresses.
2. DAO_X will send a transaction to The Badge smart contract requesting to emit a badge and providing the queries, and information related to the badge like image, name, description, etc.
3. The Badge relayer will create the whitelist for the addresses provided if the query executes successfully.
4. DAO_X can now notify its community about the possibility to claim the badge so they can apply to be part of the committee.

3.3.2 Off-chain badges

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, people who can analyze evidence and give a verdict about what they consider to be the truth.

Kleros will be responsible for analyzing all the off-chain requests and the information provided by the user interested in emitting a badge. If Kleros court agrees that the information provided is genuine, the badge will be automatically minted. If not, the user will have the possibility to appeal the ruling and provide new evidence.

3.3.2.1 Creating an off-chain badge step by step

To emit an off-chain badge the user will need to select the strategy he/she is interested in. Each strategy will integrate a specific third-party service, like Github, and will contain instructions for the user and the committee about the required information that needs to be submitted when a request is created. Once the request has been created, a verification process has to be agreed upon or not whereas the information submitted is legitime or not to mint the badge requested (Fig. 3).

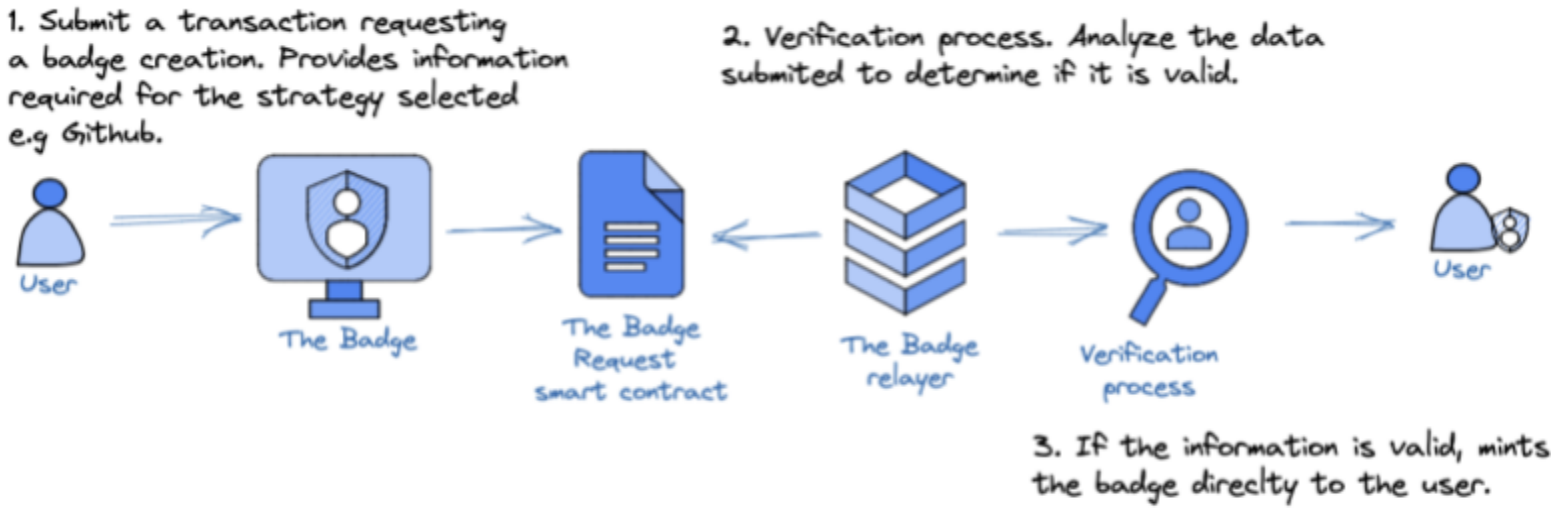

Fig. 3. Off-chain verification process.

3.3.2.2 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, the kleros case 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.

4 The Badge as a product for profile management and discovery

We aim to build a platform that everyone can use to emit badges, but this is just our first milestone. Our second milestone is about creating a decentralized platform to facilitate profiles administration (Fig. 4), badge requesting, badge listing of a particular address, and search and filtering for addresses containing a certain type of badge, in order to help to discover profiles.

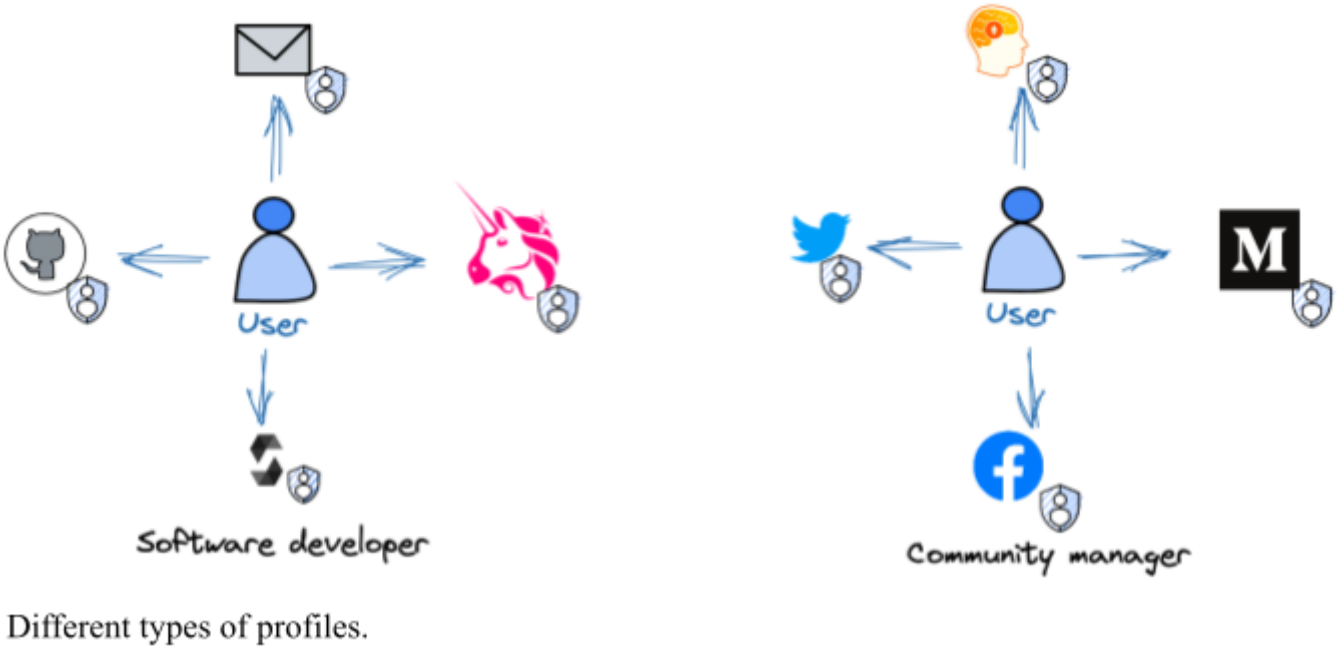

Fig. 4. Different types of profiles.

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 will not support this feature. Once zkSnarks[12] is more mature, we would like to explore this path.

[12] zkSnarks (Zcash, 2017), (Jo, 2019)

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. Snapshot is a well-known tool used by many DAOS that allows taking a picture of the state of the blockchain at any particular block. Based on this picture, it is possible to make decisions. An example could be to whitelist users for an airdrop who has a series of badges.
b. Provide a negative mark. 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. Credit score, if a user has different badges proving that he is a finance expert and has good behavior, it might be possible for some platform to grant the user a discount at the moment of taking a loan.
d. Creating a wallet/funds recovery mechanism as some web2 platforms do. They can validate the identity of the user through a badge.

7 Governance

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 on-chain and off-chain world. Transparency is a fundamental feature we pursue so each badge has to 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. We do not pretend to reinvent the wheel, we step on two main trusted platforms to build our solution, The Graph, and Kleros.

Last but not least, we pretend our platform to become a building block for other projects that will require any type of decentralized data validation.

9 References

Buterin, Vitalik. “Soulbound.” *Vitalik.ca*, 26 Jan. 2022, vitalik.ca/general/2022/01/26/soulbound.html.

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

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

Jo, Terrence. *An Exploration of Zero-Knowledge Proofs and Zk-SNARKs*. 2019.

Kleros. “Introduction to Kleros - Kleros.” *Gitbook.io*, 2017, kleros.gitbook.io/docs/. Accessed 20 July 2022.

MakerDAO. “The Maker Protocol White Paper | Feb 2020.” *Makerdao.com*, makerdao.com/en/whitepaper#abstract.

Proof of Humanity. “Proof of Humanity.” *Www.proofofhumanity.id*, 2021, www.proofofhumanity.id/.

Reiff, Nathan. “What Is a DAO?” *Investopedia*, 24 Sep. 2021, www.investopedia.com/tech/what-dao/.

Sharma, Rakesh. “Non-Fungible Token Definition: Understanding NFTs.” *Investopedia*, 8 Mar. 2021, www.investopedia.com/non-fungible-tokens-nft-5115211.

Sharma, Rakesh. “Decentralized Finance (Defi) Definition and Use Cases.” *Investopedia*, 24 Mar. 2021, www.investopedia.com/decentralized-finance-defi-5113835.

The Graph. “About the Graph.” *The Graph Docs*, 2020, thegraph.com/docs/en/about/. Accessed 20 July 2022.

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

Zcash. “What Are Zk-SNARKs? | Zcash.” *Zcash*, 2017, z.cash/technology/zksnarks/.