

PARTICIPANTS: Solène Daviaud, Maximilien Dreier, Maxime Dienger, Pierre Guéveneux & Mathias Bougon.



Project

Safe Alert is a decentralized pseudonymous mediation application that enables any user to report a bug and to communicate directly with web 3.0 protocols. Its purpose is to protect the White Hats' interests by providing them with a secure way to alert protocols of detected bugs and providing them with “Proof of Hat” badges to assess publicly their skills and contributions.

LIST OF BOUNTIES

PRIVY	Privy is an API for securely storing encrypted user data off-chain. You can e.g. create allow lists for data access, store user profiles attached to on-chain addresses, or send emails directly using wallet addresses! We award three prizes for projects that integrate the Privy API
SISMO	Best use of Sismo
IPFS/FILECOIN	Best use of Filecoin for decentralized, persistent storage and/or IPFS for content addressing. Projects that use either technology indirectly via NFT.storage, web 3.0.storage, Estuary, Textile, or similar tools may also qualify
KLEROS	Best application relying (directly or indirectly) on Kleros.
POLYGON	Best Tooling/ Infra on Polygon
ALCHEMY	Best use of Alchemy
TRUFFLE	Show us how you build with Infura and Truffle

SUMMARY

INTRODUCTION & CURRENT STATE	2
SAFE ALERT DAPP : OUR SOLUTION	3
First Use Case: Sending a secured Bug alert through Privy and IPFS	3
Second Use Case: Using Kleros as a Bug certifier	5
Third Use Case: Assessing White Hat's skills and contribution through Sismo Badges "Proof of Hat"	7
SOFTWARE ARCHITECTURE	9
ROADMAP	9
OUR TEAM	9
CONCLUSION	10

INTRODUCTION & CURRENT STATE

Blockchain technology has been gaining increased traction over the last few years, with innovative applications that pushes adoption. Unfortunately, at the same time, crypto-currency related crime has reached an all-time high with illicit addresses receiving \$14 billion over the course of the year, up from \$7.8 billion in 2020.

Cybersecurity is one of the many challenges that we as an increasingly digitized society face, especially in the blockchain industry, where users have full ownership of their digital assets but are exposed to many conditions.

One of these many conditions are hacks, executed by money-driven malicious actors that operate in a way that harms not only the platforms they target, but also the users directly and the market indirectly. Additionally, it casts a negative light on the entire environment in the public's view.

Fortunately, there are well-intentioned actors who look for bugs before these malicious actors do and submit them to the relevant platforms in exchange for a reward correlated to the severity of the bug. They are called "White Hats" as opposed to the malicious hackers nicknamed "black hats".

With the sole purpose of making the web 3.0 a safer environment for users, we wanted to provide a secure tool that makes it easier for "White Hats" to submit bugs to decentralized protocols.

SAFE ALERT DAPP : OUR SOLUTION

First Use Case: Sending a secured Bug alert through Privy and IPFS

Safe Alert is a dApp to establish a secured communication for bug alerts between White Hats and protocols. The dApp protects the critical information corresponding to the bug as it is encrypted and only accessible by the White Hat and the protocol's blockchain address. At the same time, it respects and protects the White Hat's primary interest which is to be an alert giver to prevent people and alert them of a risk/danger.

Figure n°1 shows the Bug Submission Process on Safe Alert.

Step 1: The White Hat connects with a blockchain wallet to Safe Alert and fills a form related to the bug information and sends it to the protocol's blockchain address.

Step 2: The information is encrypted and hosted onto IPFS, and readable only by the protocol's blockchain address, i.e the concerned protocol.

Step 2 bis: At the same time of Step 2, a NFT is minted and will be used to prove the White Hat's contribution. Its metadata contains:

- The link toward the encrypted bug data
- The blockchain address used by the White Hat to send the alert.

- A Certification State, set to “uncertified” at the minting time. That value can be changed by the concerned protocol.

Step 3: The protocol has an allotted time to validate the bug detection. If the bug is validated by the protocol, the NFT’s Certification state changes and it becomes “Certified”. If it is not validated, or if the protocol has not been answered in the allotted time, or the protocol has not sent the bug bounty if a bug bounty was promised, the White Hat has the option to open a Kleros Dispute.

Step 4: Thanks to the NFT “Certified” state, the White Hat can claim a Sismo Badge related to that achievement. That part is described in detail below in the part “C) Third Use Case: Assessing White Hats skills and contribution through Sismo Badges”.

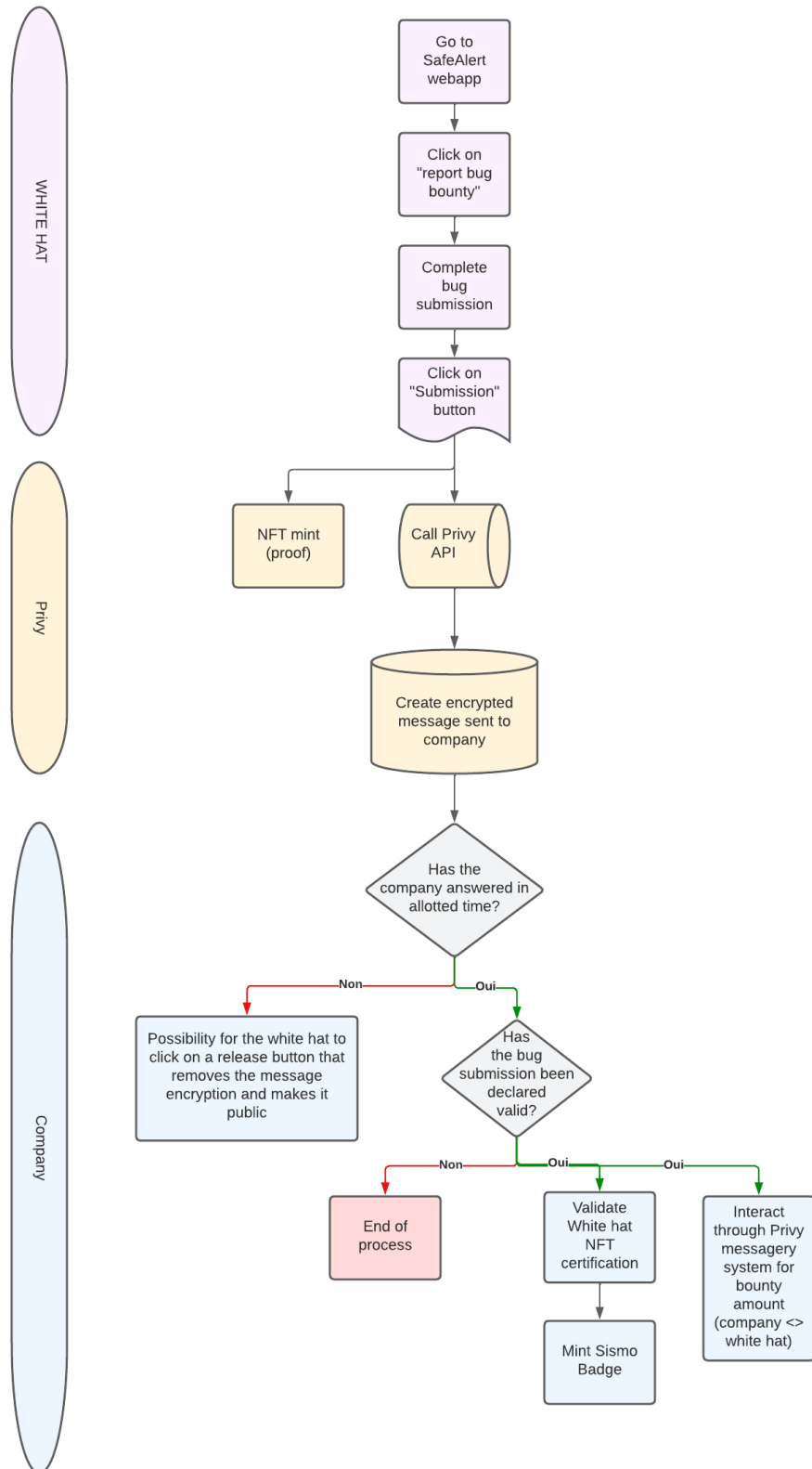


Figure 1: Bug Submission Process

Protection of the White Hat's interests: The goal of the White Hat is to be an alert creator. If the protocol does not fulfill the White Hat's expectation such as paying the bug bounty, correcting the bug, or not validating the bug information, the White Hat will be able to release the bug information publicly. It is done by clicking on a button on the Safe Alert dApp that changes the encryption settings so that anyone will be able to see the bug data.

Second Use Case: Using Kleros as a Bug certifier

Safe Alert protects the White Hat's interests by providing them with an efficient and irrefutable process to assess their contribution.

Figure N°2 shows the Dispute process between a White Hat and a protocol concerning a bug submission.

Step 1: The White Hat opens a Kleros dispute because they disagree with the protocol's actions or because the protocol has not been answered in the allotted time.

Step 2: The encryption settings concerning the bug information are changed and the Kleros's jurist(s) are now able to read the data corresponding to the filled form by the White Hat at the submission time. Also, the NFT settings are changed and the Kleros' jurist(s) are now able to change the certification state and the protocol is not able to do it anymore.

Step 3: The Kleros' jurist(s) use that data to produce their verdict, according to the Safe Alert policy rules of dispute. That policy is detailed below in the "Kleros & Safe Alert Dispute policy rules" and mainly rely on the information provided by the White Hat called "Proof of Bug" which contains a set of actions to exploit and assess the existence of the bug. And it also relies on the NFT minting time to assess that the White Hat was the first to detect the bug. Thus, that information provides an easy and secure way for a Kleros Jurist to assess the veracity and existence of the bug.

Step 4: If the Kleros' verdict agrees with the protocol, nothing happens. But if the Kleros's verdict agrees with the White Hat, they enforce the "Certified" state of the NFT, so that the White Hat can prove they have rightfully detected a bug.

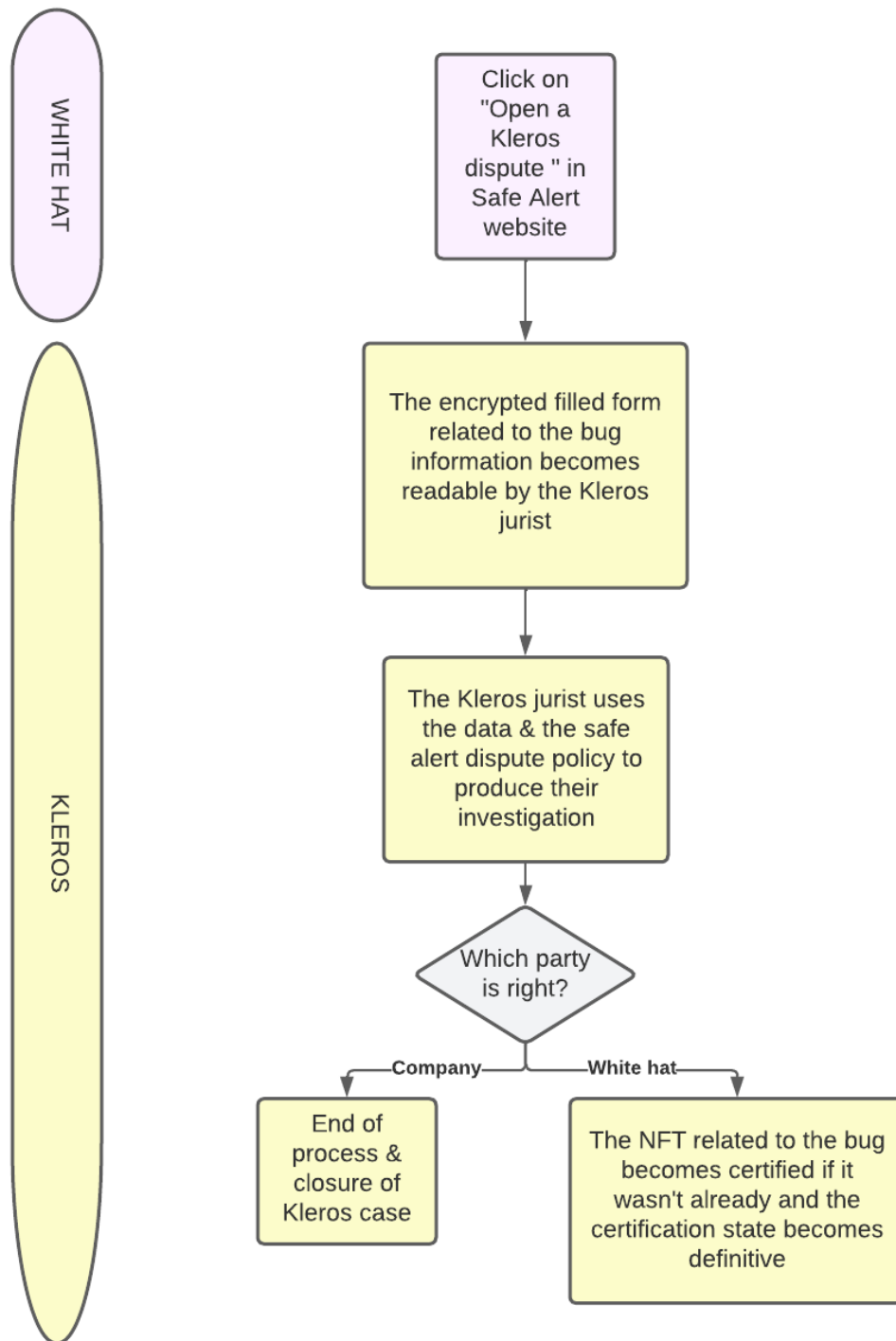



Figure 2: Process of Bug Dispute Resolution through Kleros

Kleros & Safe Alert Dispute policy rules:

In order to make an informed decision, Kleros's jurist will base his investigation on our

 **Safe Alert x Kleros - Dispute policy**

Third Use Case: Assessing White Hat's skills and contribution through Sismo Badges "Proof of Hat"

We use Sismo to provide a way for White Hats to differentiate the address on which they are paid if there is a bug bounty involved, with which they target a specific protocol, and the address they use to showcase their Sismo badges that certify their skills and contributions to the ecosystem.

The Figure 3 shows the process of minting a Sismo "Proof of Hat" badge by the White Hat.

Step 1: The White Hat connects themselves on the Sismo dApp with the same blockchain address they used on Safe Alert that is linked to a certified NFT.

Step 2: The White Hat provides a blockchain address on which they want to receive their Sismo badge.

Step 3: The White Hat follows the Sismo process flow that verify the validity of their request and if validated, they can mint a Sismo badge on their filled address and the badge represents their contribution quality and importance (Bronze, Silver, Gold badges exist)

Feature: on the roadmap, we plan to actively contribute to the personal and professional reputation of White Hat thanks to a plug-in integration on different careers websites of web 3.0 companies. That allows the White Hats to apply with their Metamask account in order to permit the companies to view the different proof of hat certification.

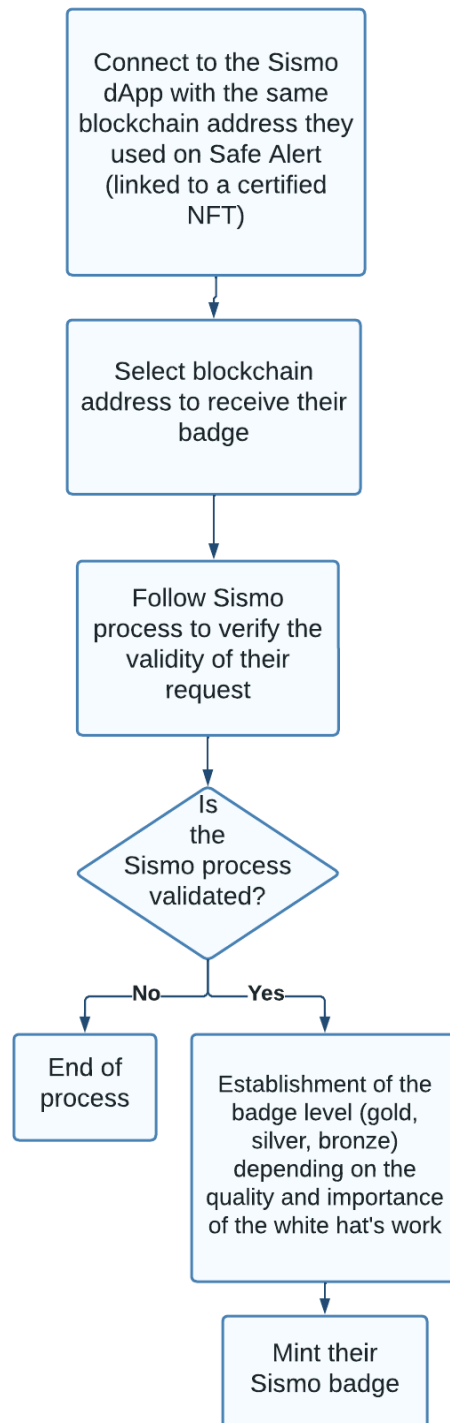


Figure 3: Process of Sismo Certification Badge

SOFTWARE ARCHITECTURE

Our platform is built and is using these different technologies :

- Privy, API enabling user data management off-chain
- IPFS, IPFS is a distributed system for storing and accessing files, websites, applications, and data.
- SISMO, Sismo is a modular Attestations Protocol focused on decentralization, privacy and usability.
- Kleros, a decentralized dispute resolution protocol.
- Polygon, a decentralized Ethereum scaling platform : we deployed our dApp on Polygon.
- Alchemy, a blockchain developer platform providing a suite of developer tools: we used it to deploy our NFT that acts as a public asset to certify the White Hat's contribution.

Our platform is the product of the successful fusion of these technologies, effectively working together and in perfect harmony.

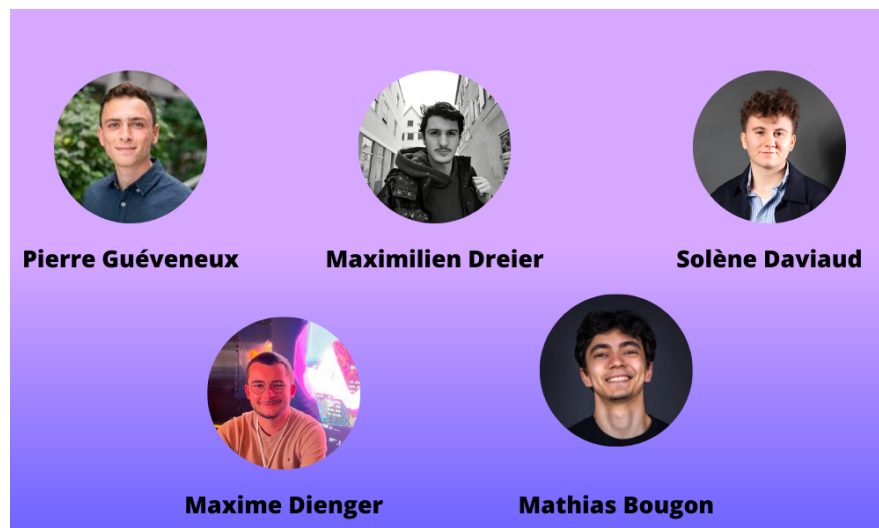
ROADMAP

We plan to simplify the search for White Hats through our Sismo badge. This will promote employment. That's why we want to put more initiatives in place to employ these profiles more quickly and easily in the web 3.0 companies.

- Development of the features on hiring platforms and social networks to showcase Sismo reputation badges of White Hats/developers thanks to a plug-in integration on different careers websites of web 3.0 companies. That allows the White Hats to apply with their Metamask account in order to enable the companies to view the different proof of hat certification.
- Challenge between White Hats in relation to a bug bounty (thanks to the encrypted and safe Privy database that contains the lists of all the White Hats addresses)

OUR TEAM

The team's diversity of backgrounds and perspectives significantly influenced the creation of our project. We were able to challenge one another's viewpoints and think differently from our colleagues, which made it possible for us to develop our project. We are essentially recent graduates or young students who have bonded over our shared interest in blockchain technology.



CONCLUSION

The Ethereum Community Conference Hackathon 2022 was the opportunity for blockchain enthusiasts to gather around their passion and build innovative projects while developing their technical skills. During 3 days, we were collectively making progress on our project, developing, writing, implementing and discovering new cutting-edge technologies. We combined our knowledge and skills to contribute to the development of the web 3.0, and we support initiatives that seek to bring a secure environment for everyone.