# Using bug bounty programs to tackle cryptocurrency security challenges

BY ANNA HAMMOND · SEPTEMBER 17, 2021 · LAST UPDATED ON MARCH 6, 2025

With cryptocurrency becoming a more regular investment, holders must take steps to protect their investments. One organisation that helps crypto holders do this is Safe Haven through its digital inheritance solution, Inheriti.

In this blog post, Intigriti sits down with Safe Haven's Chief Technology Officer (CTO) and CEO, Jürgen Schouppe, to discuss cryptocurrency security challenges, as well as how the organisation ensures their product is secure in a world where cybercrime is forever on the rise.


Safe Haven: Intigriti bug bounty program

## Intigriti: Hi Jürgen! Nice to meet you. Can you tell us about the challenges that crypto holders have when it comes to keeping their crypto wealth safe?

**Jürgen:** Nice to meet you too! Cryptocurrency holders access their crypto wealth within a "wallet", which is initially created using a private key or seed phrases. However, in the event the holder loses access to their wallet and is not able to re-enter their private key or seed phrases, there is no support line you can call to reclaim your funds. Your money is forever out there, in limbo.

There is also the challenge of what happens to the crypto wealth in the event of the holders' passing. Let's take the case of Matthew Mellon, for example. Mellon was a banking heir who invested heavily in Ripple (XRP), turning an initial $2m investment into well over $1Billion. He was a family man with a wife and a young family. But at the age of 54, he died suddenly of a heart attack — taking his cryptocurrency fortune with him.

While Mellon had had the foresight to take steps to secure his Ripple, he failed to make secure copies of his private keys with clear instructions on how his family could access his crypto wealth after his death.

Sadly, this is the case for many people.

A 2019 report found that 89% of crypto holders don't have a documented plan for passing their crypto assets onto loved ones in the case of their death. However, for the 23% of people that do have a backup plan, any copy they make of their private keys becomes open to being stolen, lost, and/or misplaced. Security, therefore, is a major concern for crypto holders – which brings us to the third challenge of how people can keep their crypto assets safe.

> "*Enthusiasts love cryptocurrency because of its ease of access, storage and transfer — but that's also its biggest flaw. If a malicious actor were to get access to your private keys, they also have access to your crypto.*
>
> JÜRGEN SCHOUPPE, CHIEF TECHNOLOGY OFFICER AND CEO, SAFE HAVEN "

## Intigriti: How does Safe Haven help crypto holders tackle these challenges?

**Jürgen:** Crypto holders need to be able to make copies of their private keys or seed phrases so that they can gain access to their crypto again in the event of unforeseen accidents — without fear of their keys falling into the wrong hands.

Inheriti is Safe Haven's flagship product and we're incredibly proud to say that it is the only truly decentralised (and totally secure) digital inheritance solution available in the world.

Not only does Inheriti ensure that private keys can be safely and securely passed to relatives of crypto holders in the event of their death, but there are various fail-safe mechanisms in place to ensure that no one else can gain access to your keys while you are still alive.

## Intigriti: You describe Inheriti as "totally secure". Can you tell us more about how you tackle security?

**Jürgen:** The very nature of Inheriti signifies that safeguarding the security of a user's data is our top priority, and the steps we have taken to ensure this means we're confident in saying our solution is totally secure.

Our solution does not store any private key, secret data or any other critical information on our back-end systems and repositories. Independent audits by Red4Sec Cybersecurity Services have verified this for us.

We use blockchain and Hardware Security Module (HSM) device technology (utilising Safe Haven's own 'SafeKeys') to safely distribute heavily encrypted pieces – or 'shares' – of inheritance information to separate cold-storage devices.

Through the various security audits that we undertake on an ongoing basis – with Red4Sec as well as other cyber security specialist organisations – our understanding of security best practices and approach to security testing has improved significantly over time through dialogue.  We listen closely to the recommendations that are provided as part of any initial audit.  And, as well as any addressing

vulnerabilities that might arise, we will also look wider to see what aspects of our overall development and testing practices we can improve for the next time.

In addition to ensuring our practices around unit, systems and integration testing are solid, we do also like to get independent views regularly through the development lifecycle so we will typically undertake several independent audits over a year – and these will include code audits, smart contract audits and data integrity and data privacy audits.

## Intigriti: How does working with ethical hackers through a bug bounty program provide your clients with more assurance that their assets are safe?

**Jürgen:** At Safe Haven, we recognise the importance of ethical hackers in helping to keep our technology safe. These people actively seek out vulnerabilities in our digital systems and then inform us of all potential security risks they find. By continuously testing our systems, we can keep a constant eye on our cyber defences. This assures our customers that we never stop working to protect their digital assets.

Intigriti was integral in helping us launch our bug bounty program successfully — and offers continuous support now that the program is live. For example, vulnerability reports that are submitted to our internal team go through a layer of quality assurance before they reach us. This means we don't waste time dealing with poor quality, out of scope or duplicate vulnerabilities because we can count on Intigriti's triage team to screen these reports out for us.

We can also incentivise security researchers through bounty pay-outs, which helps drive quality. A vulnerability disclosure policy, for example, is much more of a passive approach. It asks people who stumble across a problem to report it to us, but it doesn't incentivise someone to go out looking for a vulnerability with the potential to be exploited. Just like malicious hackers, security researchers are proactive in finding hacking opportunities – but they operate on the right side of the law.

To outsmart a hacker, we must think like one. Intigriti enables us to do this.

### About Jürgen Schouppe

Jürgen Schouppe is Safe Haven's Founding Director, Chief Technology Officer (CTO) and CEO.  He has a background in security systems engineering including more than 13 years of experience working as a consultant with the European Parliament.  Jürgen is also a Certified Blockchain Professional and inventor of the technology behind Inheriti and the Inheritance as a Service (InaaS), protected by 3 worldwide pending patents in the US, Europe and China.

**REQUEST A DEMO**

intigriti.com/demo

**VISIT THE WEBSITE**

intigriti.com

**GET IN TOUCH**

hello@intigriti.com