

Challenge types matter and their definitions are very clear. Incorrect Submission challenges do not include cases of submitters attempting an attack to the registry, no matter whether they are willful or guilty. "A challenge can be rejected if the challenge type specified is incorrect".

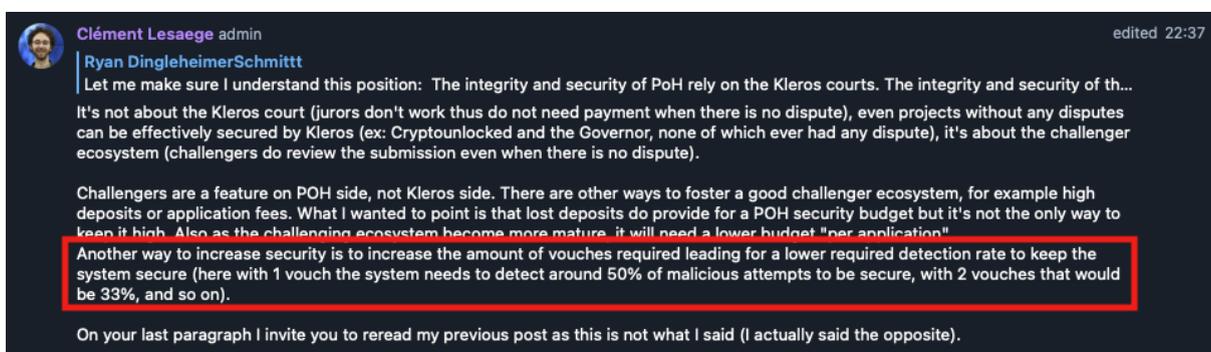
As explained in cases 829, 830, 831 and 834 and then admitted in the Manifesto of the Cryptoevangelist by the wrongdoer, many profiles including this one are managed by one (or two) person. This person failed to provide a proof of life for most challenged profiles. The first-round verdicts of the Humanity Court at the time of writing are aligned with this accusation. For example, in case 834 a proof of life was submitted, where Hermin is clearly visible showing a blockhash. Nevertheless, this is not enough evidence to counter-argue the duplicate challenge.

Regarding the 2 previous pieces of evidence:

- "It could not do it because it is dead or does not have access to the Ethereum address. As the registration policy says: "Submitters not able to give recent proof of life are to be considered deceased". Therefore the request to register should not be accepted". If this argument was valid, then the current challenge should be rejected in favor of the "Deceased" type challenge.
- "At first, this submission is being manipulated by a third person for their own benefit to collect UBI. For this reason, in the entire challenge process, "ElGato" could not demonstrate that it is alive as required by the registration policy. Either because he doesn't have access to his Ethereum address or because he's just dead". Precisely this is an argument in favor of the "Duplicate" challenge type, maybe in favor of the "Deceased" type, but by no means supports the "Incorrect Submission" type.

Not only is the current challenge type wrong according to the written policy, but it also decreases the security of the registry by not removing the malicious voucher. If this challenge is accepted, it could create a precedent that allows attackers to front-run "Duplicate" challenges with "Incorrect Submission" challenges in order to dodge the major punishment.

I leave you with a quote by Mr Clément Lesaëge, CTO of Kleros, where the importance of the Duplicate/Fake challenge type is explained.



The screenshot shows a forum post by Clément Lesaëge, CTO of Kleros. The post is titled "Let me make sure I understand this position: The integrity and security of PoH rely on the Kleros courts. The integrity and security of th...". The post contains several paragraphs of text. A red box highlights a specific paragraph: "Another way to increase security is to increase the amount of vouchers required leading for a lower required detection rate to keep the system secure (here with 1 vouch the system needs to detect around 50% of malicious attempts to be secure, with 2 vouchers that would be 33%, and so on).". The post also includes a reply from Ryan DingleheimerSchmittt and a note from Clément Lesaëge at the bottom: "On your last paragraph I invite you to reread my previous post as this is not what I said (I actually said the opposite).".

Clément Lesaëge admin edited 22:37

Ryan DingleheimerSchmittt

Let me make sure I understand this position: The integrity and security of PoH rely on the Kleros courts. The integrity and security of th...

It's not about the Kleros court (jurors don't work thus do not need payment when there is no dispute), even projects without any disputes can be effectively secured by Kleros (ex: Cryptounlocked and the Governor, none of which ever had any dispute), it's about the challenger ecosystem (challengers do review the submission even when there is no dispute).

Challengers are a feature on POH side, not Kleros side. There are other ways to foster a good challenger ecosystem, for example high deposits or application fees. What I wanted to point is that lost deposits do provide for a POH security budget but it's not the only way to keep it high. Also as the challenging ecosystem become more mature, it will need a lower budget "per application".

Another way to increase security is to increase the amount of vouchers required leading for a lower required detection rate to keep the system secure (here with 1 vouch the system needs to detect around 50% of malicious attempts to be secure, with 2 vouchers that would be 33%, and so on).

On your last paragraph I invite you to reread my previous post as this is not what I said (I actually said the opposite).