Evidence of Attack on the Technical Court

and Rebuttal of Heliast's Arguments

Honourable members of the jury,

First if you have not done so already, please take the time to review the following evidence which I believe addresses all issues so far brought up in this case:

- Summary of events and argumentation. In particular, sections 1 and 2 where I summarise the events leading to the claim and explain why the claim must be accepted, as well as the conclusion, which I consider essential reading for jurors on this case.
- Rebuttal of juror 0x5e7B's arguments.

In this document, I will clarify my belief that the Blockchain/Technical court is undergoing an attack by a Kleros developer, as I alluded to at the end of my previous document, and will explain what consequences this has and does not have for this court.

I will only address the argumentation submitted by Heliast in this round in Appendix B since it is for the most part just a rehash of arguments I have already refuted in depth in my previous evidence and therefore not worth a fully fledged response.

1 51% Attack

I will keep the main content short and document in Appendix A the many reasons why I believe the following juror addresses, which have recently taken over the Blockchain/Technical court, are controlled by the same Kleros developer, to which I will assign the codename **Cerberus**:

1. `0x5e7b645d5bf86750cb1913122ba8a8545e2a9fd1`: 3M staked in Technical
2. `0x334f12afb7d8740868be04719639616533075234`: 5M staked in Technical + 4.6M in General
3. `0x930c54fd12bc507de14ce3967e715e6d9cd70ec4`: 5M staked in Technical + 16.6M in General

These addresses' Technical Court stakes currently add up to 13M PNK out of a total of 21.2M PNK staked in said court, giving them a 61.3% control of the Technical court. Combined with the fact that these addresses staked in the Technical Court specifically for this case, this justifies the accusations of a 51% attack on this court.

Of interest, the vote distribution in the previous rounds has been the following:

0x546e1f8a771e1b6e867dd0524dcbc1ab368f12aa	Yes	Yes	Yes	Yes
0x60da07cfb273051aa9827dabffcd298c305cd00d	No	Yes	Yes	Yes
0xb2a85da2ecc3ffb4d3a730e119d8cab5743096fc	No	-	-	-
0xc5060b33b82528abf7aa8d7778e267f0feb71792	-	Yes	Yes	-
0xe599435b865cef666f304031f54dfa3fb2e1badf	-	No	-	No
0xc764d75fe1c892ba39caaf02efd44ae606b52a0c	-	-	Yes	Yes
0xc8030b11ff7052436d9670188d00890b9f48a06a	-	-	Yes	Yes
0x5e7b645d5bf86750cb1913122ba8a8545e2a9fd1 (Cerberus 1)	-	-	No	No
0x334f12afb7d8740868be04719639616533075234 (Cerberus 2)	-	-	-	No
0x930c54fd12bc507de14ce3967e715e6d9cd70ec4 (Cerberus 3)	-	-	-	No
No% with Cerberus	-	-	40%	52%
No% without Cerberus	67%	20%	0%	6%

Aggregating the Cerberus accounts into one, we can expect 5 Yes vs 3 No votes if all of these jurors are to be polled again (once each) and they do not change their minds since their last votes. More tellingly still, the last two rows of the above table, show that almost all of the drawn Technical Court stake excluding Cerberus has converged towards accepting the claim. In other words, **Cerberus' position has become increasingly fringe as the case has progressed and they have only been able to win the previous round through a 51% attack**.

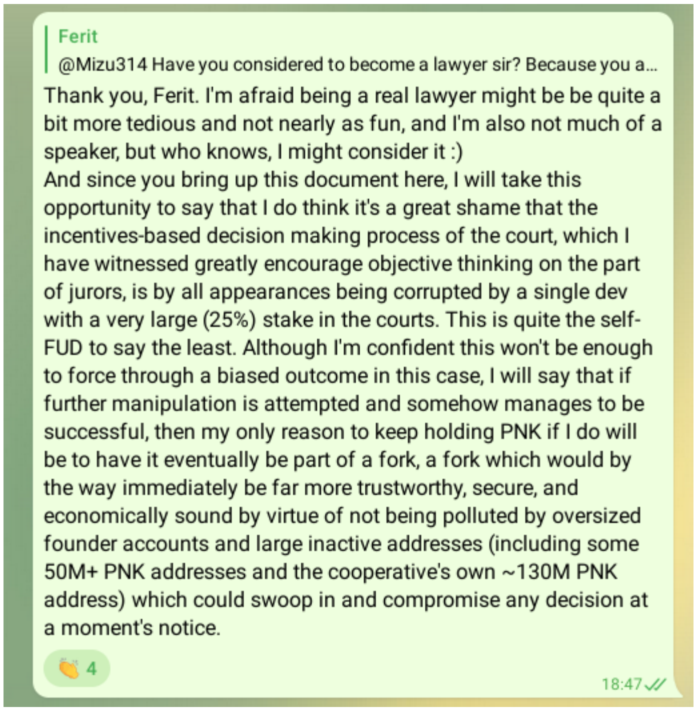
My purpose in exposing this attack is to show that the outcome of the rounds exposed to this attack are not representative of a broader consensus and to encourage jurors to vote based on the case's merits. I will now further explain why, even though Cerberus has a large stake in the general court, I do not think they will be able to win by brute force.

2 Cerberus Cannot Win By Sheer Force or Influence

To jurors, if you are worried that Cerberus will win this case by simply throwing limitless PNK at it or that they may influence founders with large stakes to help them in this travesty of justice, **there is very good reason to believe they do not actually have the funds or influence for this, and I therefore encourage you to vote on legal merit alone**:

- In this week's Kleros cooperative team meeting, someone who I presume to be Cerberus spent considerable time arguing in favour of forking Kleros if this case were to be ruled in favour of the claimant. This is a good indication that they are not confident in their ability to win, be it through brute force or argument. What is more, team members were (unsurprisingly) very taken aback by this stance. It is also clear to me that one would have to be delusional to believe such a fork would be anything but worthless, having neither team nor community support. I do not have a recording of this meeting but skeptical jurors are free to ask team members for confirmation of this in private.

- Ferit, who is also a founder of Kleros, has publicly expressed disapproval towards Cerberus's behaviour in this case on Kleros' main telegram channel:

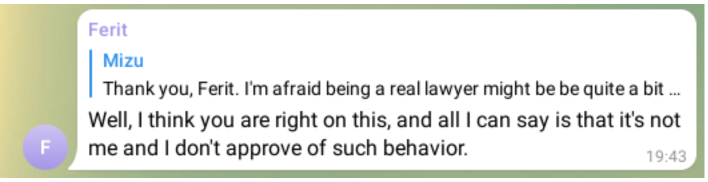


Ferit
@Mizu314 Have you considered to become a lawyer sir? Because you a...

Thank you, Ferit. I'm afraid being a real lawyer might be be quite a bit more tedious and not nearly as fun, and I'm also not much of a speaker, but who knows, I might consider it :)
And since you bring up this document here, I will take this opportunity to say that I do think it's a great shame that the incentives-based decision making process of the court, which I have witnessed greatly encourage objective thinking on the part of jurors, is by all appearances being corrupted by a single dev with a very large (25%) stake in the courts. This is quite the self-FUD to say the least. Although I'm confident this won't be enough to force through a biased outcome in this case, I will say that if further manipulation is attempted and somehow manages to be successful, then my only reason to keep holding PNK if I do will be to have it eventually be part of a fork, a fork which would by the way immediately be far more trustworthy, secure, and economically sound by virtue of not being polluted by oversized founder accounts and large inactive addresses (including some 50M+ PNK addresses and the cooperative's own ~130M PNK address) which could swoop in and compromise any decision at a moment's notice.

👏 4

18:47



Ferit

Mizu
Thank you, Ferit. I'm afraid being a real lawyer might be be quite a bit ...

Well, I think you are right on this, and all I can say is that it's not me and I don't approve of such behavior.

19:43

A Evidence that the Cerberus Addresses are Controlled by the Same Person

The evidence presented here is of course circumstantial, however my purpose is not to prove guilt beyond a reasonable doubt, but to show by preponderance of the evidence that there is a very high probability that these addresses belong to a same individual attempting to covertly (although very clumsily so) assert control over the Technical court and that their opinion is therefore not representative of any broader consensus.

1. The claimant has compiled evidence in the form of tweets, showing that all 3 Cerberus addresses are linked in ways which would be unnatural were they controlled by different persons. I will simply reproduce the contents of these tweets here:

   > Some data, can be confirmed on-chain:
   >
   > 3 addresses recently staked large amounts of PNK in the technical court, ID 4.
   >
   > 0x5e7B645d5Bf86750CB1913122ba8A8545e2A9FD1 staked 3M
   >
   > 0x930c54fd12bc507de14ce3967e715e6d9cd70ec4 staked 5M
   >
   > 0x334f12afb7d8740868be04719639616533075234 staked 5M
   >
   > All 3 are tightly linked and appear to be dev/team accounts.
   >
   > 0x930c54fd12bc507de14ce3967e715e6d9cd70ec4 ran the Kleros token sale in 2020. See e.g. 0x1412a992a5aeb286b4891651379672fe1c9a02cc4b350fc0dfc46ceedc9ce9dc minting them 150M PNK that then got distributed to token buyers.
   >
   > That tx was *submitted* by 0x334f12afb7d8740868be04719639616533075234, one of the accounts above.
   >
   > 0x6531c69fd848ca14674459cd027430a9aec762283da42788cbd5bcd15bfffe2d this is the 0x33 address receiving some USF, the unslashed token.
   >
   > 0x388f973d288d28f3271a7f096d73af5c342daa15b8d148764d60c26b58cfee57 the 0x33 address putting eth into the unslashed insurance pool
   >
   > 0x3c6219619cd8e663b57bbf5cc32db11530b307d3de56b801b96feab37609fd5c here's the 0x5e address putting 30 eth into the unslashed insurance pool.
   >
   > 0x83231ee3618fd9d88b10f21c0f015918b35c55a196010456bb6fcb5da01de5a8 0x5e sending 0x33 some USF
   >
   > 0x41083b17c222c3180dea86e71df63d821bd3ce7dad103590d9dac550f23c9a27 0x5e sending 0x33 some yearn/crv LP tokens
   >
   > 0x511be8004f639b01785678d80d6cfb456c46d6f59edce25fcd9b637077c9d7aa another transfer from 0x33 to 0x5e
   >
   > So to summarize: 0x33, 0x5e, and 0x93 are all linked and appear to be dev accounts. 0x33 and 0x53 both have significant financial stakes in @UnslashedF insurance pool. And the three accounts together have launched an attack on their own protocol, the kleros technical court.

2. 0x930c (Cerberus 3) staked 5M PNK in Technical Court only two hours before 0x5e7B (Cerberus 1) funded the appeal in the third round.

3. Addresses 0x930c (Cerberus 3) and 0x5e7B (Cerberus 1) both failed to vote on the same case, case 574, and otherwise voted coherently during the period in which they were both active.

4. All three Cerberus addresses have left similar justifications on the fourth round of this case (i.e. the previous one), albeit in decreasing levels of detail:

   - 0x5e7b (May-07-2022 14:10:34 UTC)

     > There was no loss, only a bridge delay compared to the usual time of the bridge. The claimant sent USDN, he received USDN. He hasn’t lost anything so there is nothing to compensate. This is a loss insurance, not a ”delay” insurance.
     > Moreover, the delay is relatively small (a bit more than a day) and the bridge only indicates an average time. The bridge is handled by an external account which took longer than usual to have the TX confirmed.
     > Moreover, behaviour of external accounts is specifically excluded from both unslahed policy documents.
     > There is therefore a strong case to reject the claim because:
     > - There was no loss, only a delay (not covered by the insurance).
     > - The bridge doesn’t guarantee any time, it has a ideal time, but offers no guarantees it can’t take more (and 1 day is very slow for a withdrawal, rollup bridges will take way longer and even more in case of attackers delaying the bridges).
     > - The delay (compared to the average time) is not due to a contract bug (what the policy is about), but about an external account (specifically excluded from the policy) taking longer to confirm a transaction.

   - 0x334f (May-13-2022 14:45:22 UTC)

     > Despite the beautiful argumentation of Mizu, the facts of the case are simple:
     > - A bridge took longer than expected.
     > - The asset bridged lost some value in between
     > - No assets were lost
     >
     > Should the insurance compensate the loss of value during the bridge time?
     > The answer to this is no. The insurance intent is to insure toward the bridge risk, not the risk of asset price going through it. Since no assets were lost, there is no basis for this claim as this is not a delay insurance.

   - 0x930c (May-13-2022 21:14:19 UTC)

     > No funds were lost. What the claimant could have done if the bridging was faster is irrelevant.

These all boil down to the same leitmotif: “no funds were lost”. But perhaps more revealing is the fact that none of these justifications address the suspicions I expressed in the conclusion of my previous evidence, that the three addresses are controlled by the same person (although admittedly, address 0x5e7B could not have responded to that at the time of voting since I submitted this evidence on the next day, May 8th).

B Rebuttal of Heliast’s Arguments

As I have stated in the introduction, Heliast’s argumentation is little more than a rehash of previous arguments which I have already thoroughly refuted in my previous pieces of evidence, linked at the start of the current document. I will therefore just briefly address each point in order:

1. First of all, I would like to state that Heliast is confused about the characters involved in this case. I, mizu.eth, am not the claimant, Avraham Eisenberg, but only a Kleros community member who decided to defend him after having analysed the case in depth, initially looking for evidence and arguments against him, and being unable to find any substantial cause for rejecting the claim.

2. (1.) Re: “The Claimant has attempted by various means, including the less legal ones, to mislead the Kleros jurors despite its application being unsustainable, as already decided.” This point is nonsensical on so many levels:

    - What “less legal” means is Heliast talking about? What does that even mean?
    - How did the claimant (or myself) ever attempt to mislead the jury? No specifics are given. Just baseless accusations.
    - What has been “already decided”? The fact that two out of three jurors voted to deny the claim on the first round when the arguments on both sides had not yet been fleshed out is not indicative of anything much, even less so when one considers that one of the first round jurors flipped their vote on the following round and has consistently voted to accept the claim since.

3. (2.1.) Re: “Kleros is a dispute resolution protocol running on the Ethereum blockchain [...]”. I don’t think the Technical Court jurors, or any of the Kleros jurors, need to be reminded of what Kleros is.

4. (2.1.) Re: “In the absence of contractual provisions, or for their interpretation, it is usually in the arbitration to rely on equity rules (Ex aequo et bono). Equity rules allow jurors to interpret the contractual or legal provision to reach a consensual decision.” Contractual provisions were provided in the form of advertising material and the primary document, and I have actually already proposed a reasonable (and in my opinion, equitable) framework for interpreting the primary document given the circumstances as part of my first evidence document.

5. (2.2.1./1B) Re: “The Claimant also attempts to persuade the jury with false and irrelevant arguments, explaining that Challenger has a shallow opinion of the jury” I, not the claimant, used the word “shallow”, and I used it to describe the arguments and thought process of juror and appelant 0x5e7B, not anyone’s opinion of the jury.

6. (2.2.1./1B) After having argued in favour of equity and *ex aequo et bono* decision making a few paragraphs prior, Heliast proceeds to change their tone entirely and argue that “the insurance cannot cover the damage suffered by the Claimant insofar as it relies on inexistent [sic] contractual grounds”, even though as I have already argued at length, there is plenty enough material to derive a reasonable expectation of what the bridge cover should entail.

7. (2.2.1./1B) The claimant obviously did not “[buy] the insurance knowing it would not cover the bridge’s defects” since Unslashed’s advertising material for the insurance policy at stake unequivocally included cover for bridge defects, as I have already shown in my first evidence.

8. (2.2.2./1A&1D) Re: “the notion of loss does not include speculative losses”. This is in no way defined in the policy, and regardless, as I have already argued at length in my second evidence, the loss in question was not speculative.

9. (2.2.3./2A&2D) Re: “If the Policy were applicable, it would cover the failures causing unavailability or failure to access or process covered smart contracts: consequently, the financial losses must be caused solely by the Challenger’s failure to comply.” This is incomprehensible and makes absolutely no sense.

10. (2.2.3./2A&2D) Re: “the Claimant complains for the loss of chance for not having received assets with a higher value”:

- First of all, the claimant did not merely lose a chance to make a profit, as implied by Heliast's wording here, but incurred an *effective* loss due to the devaluation of the USDN token over the course of the abnormal 28 hour bridge delay.
- Secondly, the policy covers losses "*due to* [...] unavailability or failure to access or process [the] covered smart contracts". There is no doubt here that the claimant's loss was *due to* the (unexpected and abnormal) bridge delay and it is always the insurer's responsibility to outline exclusions if they desire to have them applied.

11. (2.2.3./2A&2D) The claimant then goes on to argue that "European law only considers compensating the victim for the chance that a favorable event might have benefited him or her if the occurrence of this event was not merely hypothetical, but real and serious". However (and disregarding the question of the relevance of European law):

    - Once again, this was an effective loss (the claimant lost money, they did not just miss out on profits), and not a mere loss of chance.
    - The event that would have "benefited" the claimant in this case was being able to sell their USDN within 10 minutes of transferring the tokens to the bridge, at a price close to the price before bridging. The chance of this happening had the bridge not failed was clearly "real and serious" and in no way "merely hypothetical", as attested by the USDN price chart on the day of the event and by the consistent success of this trading strategy for the many other USDN bridgings performed by the claimant. So according to Heliast's *own* explanation of European law, the loss in question would be eligible for compensation as a loss of chance (which I maintain is not even the case).

12. (2.2.3./2A&2D) Other bridge execution delays are then brought up again, completely ignoring the counterarguments I laid out in my second piece of evidence.

13. (2.2.3./2A&2D) Re: "the Challenger cannot retroactively be held responsible for the fluctuations in digital asset prices - neither the rise nor the stability of value - which are unforeseeable to an ordinarily competent and informed professional": the asset in question was a stablecoin and its volatility over the course of a normal 10-minute bridge delay was presumably well understood by the claimant. Its devaluation over the course of an abnormal and unexpected bridge delay of over a day is however the financial responsibility of the insurer as per the insurance contract.

14. (2.2.3./2A&2D) Re: "in European law, the courts are careful to point out that the losses incurred can only be borne by the professional if they are the result of his fault and not of the randomness of the markets." This is very unclear to me. Who is the "professional" and who is the "investor" here? Besides, the USDN market was acting far from randomly at that time.

15. (2.2.3./2A&2D) Re: "Mere opportunism should not be allowed to enrich oneself. We recall in this respect that the Claimant subscribed to the insurance and asked to activate it on the same day, being aware of the risk of a significant drop in USDN prices." That the event at stake occurred soon after the activation of the insurance is mere chance and in no way justifies accusations of "opportunism". The insurance is either active or it is not and it is dishonest to use the fact of this coincidence to defame the claimant.

16. (2.2.3./2A&2D) Re: "This is the reason why insurances generally do not cover speculative risks as they are hard to quantify, hazardous and unbounded." Once again, the risk was not speculative. Furthermore, the risk was bounded both by the maximum insurable amount of the claimant's contract (whose purchase cost is purely proportional to said amount) and the value of the USDN being bridged. Regarding this second fact, this is no different than having any other asset insured: an insured house risks being destroyed in a fire, requiring the insurance company to fully cover its reconstruction costs, and a car risks being stolen, requiring the insurance company to fully refund it (assuming the insurance covers the full value of the insured object, of course). Once

again, **if the insurer does not wish to cover certain types of losses, it falls upon them to explicitly exclude them**.

17. (2.2.3./2A&2D) Heliast then brings up the primary document's clause about losses "due to external inputs" which I have already thoroughly addressed in my second piece of evidence (a fact which they completely ignore). They furthermore dishonestly represent this clause as a *should* clause when it in fact worded as a *may* clause in the primary document.

18. (2.2.3./2A&2D) Re: "The Claimant strategy to use Unslashed Finance to prevent USDNs from losing their value is therefore neither relevant nor admissible to this case." Heliast is once again slandering the claimant, implying that their goal in purchasing insurance was to protect themselves from short-term USDN downturns as part of their trading strategy, when there is simply no indication of that. In this case, the bridge malfunctioned and incurred a totally unexpected and undesirable loss to the claimant. It should further be noted that as a result of the abnormal delay, the claimant certainly incurred loss of profits as well as the claimed effective loss, but they did not make a claim for those lost profits.

19. (2.2.4./1C&2C) Heliast goes on to bring up the bridge's terms of service again, but I have already explained why these are irrelevant to this case in my first piece of evidence.

20. (2.2.4./1C&2C) They then go on to make this absurd claim: "The length taken by the bridge to execute the transaction flows from technical issues on the blockchain due to its large amount (1,000,036 USDN). As previously explained, the small value transaction (619,963.8 USDN) executed on the same day in ten minutes." This makes no sense from a technical perspective. On a blockchain, billion dollar transfers are just as fast and reliable as one dollar transfers. This claim is also demonstrably false since the claimant managed to bridge larger amounts of USDN the very same day without undue delay: 1.9M USDN, 1.3M USDN, 1.6M USDN.

21. (2.2.4./1C&2C) Re: "More broadly, the Policy review reveals that this insurance was not intended to cover a risk exceeding the underlying service itself (such as a time delay in the Tokens' transfer through the Bridge)." I have no idea what "exceeding the underlying service" is supposed to mean here. The bridge is definitely covered by the claimant's policy and is also definitely part of the covered Waves+Vires smart contract network.