tellor security 301 – the multi-chain world

if voting mechanism not broken ->

leads to challenge of disputers

attacker will want to dispute all good values

honest participants will want to dispute all bad values

Once again, assuming that the voting is not broken,

CTB vote – team share, not happening. token weighted (50% of voting share), reporter share (50% of voting share), user share (50% of voting share)

for users and reporters, it safe to assume that if the voting system is actually under attack, they’ll all vote. Most votes in the tellor system (or any system) don’t get nearly full participation. And usually its for good reason; why waste your money on gas when the answer looks correct?

So cost to break reporter share – stakeAmounts + gas\*numberOfSubmits on chain. Remember they can be honest for this part (accumulating voting share). This is why its important for tellor reporters to be distributed. Too much power in one person’s hands can lead to centralization. As for the stakeAmounts, they’ll likely lose it unless they withdraw, so in general this is a long attack if the chain has been running for a while. It’s also a number that can be gamed by good guys too. If the system is under too much of an attack here, the honest reporters can submit more to gain more share as well. In the end it becomes a competition of who is willing to blow more gas trying to submit values, but with the protection of historical honest values.

Cost to break user share is similar. historical usage is in the bank and the users should vote if their app is still alive. If the system becomes under an attack, someone tips maliciously just to gain share, it would be painfully obvious what’s going on. The honest participants then could either let it go or do the same thing. It would take a while to break this one as well since tip amounts are basically capped at the stake amount plus gas (good values would be disputed over stake amounts larger than this). Again, it becomes a competition of who is willing to blow more ETH on gas to buy TRB and submit it as a tip, but this method has additional caveats of 2% being taken for the stakers in the system, something that would incentivize more honest reporters, something an attacker wouldn’t want.

tellor governance – why do we do it this way?

tellor is a governance minimized system. We’ve definitely evolved over the years, but the fact remains that anything you can vote on is a potential attack vector. This is why tellor’s removed upgradeablility and voting on everything in our system except the one thing we can’t get rid of…voting on disputes.

Original design – we could have used schelling schemes like other protocols. This is where tellor users stake tokens on what they believe to be the right answer and then you lose the tokens if you didn’t vote with the majority. This is the design for a lot of oracle like systems (kleros, augur, witnet, and more) and it works really well. We went back on forth for a while internally on whether or not to use this kind of design but ultimately felt that the subjectivity of the data makes slashing people voting incorrectly a tough sell (a great example would be if someone asked the oracle whether or not roe v wade was constitutional. 6 of 3 supreme court justices said no…does that mean the other 3 should get slashed?). Obviously, as with most things in life, nuance makes hard codified decisions about right and wrong difficult and we want to create a system that can handle a little subjectivity (vs simple proofs which other systems work better for).

Knowing we started off with just a token weighted vote, the next thing we wanted to do was add some balance. In the same way you have three branches of government in the US, we figured we needed that kind separation of powers. This is why we split up the vote between reporters (likely to not want super strict slashing), users (likely to want strict slashing), token holders (want the system as a whole to promote the value of TRB), and the team (same as token holders, but with a longer time horizon). This balance in the system ensures that no honest section is actually going to ruin the system. A lot of times you see token holders voting always for “no wrongdoing” on behalf of the system solely because they don’t want their protocol to look bad. By giving users and the team shares in the vote, this self interest can hopefully be bridled.

Why do we do governance per chain?

Now for the multichain world. There are quite a few ways to do multichain. For tellor we wanted to keep our system as similar on every chain as possible, but this leads to some questions: whats the staking token, what’s the governance contract?

For the staking token, you have three options: bridgedTRB, a new token, some other token (e.g. the native token or a stable coin). BridgedTRB is great, being it leads to higher demand for TRB and the community isn’t confused by other tokens. There are downsides however. The first being that bridges generally suck and you have to rely on them. The second is that the total balance on any chain of TRB is lower than the overall market cap. This means the cost to buy 51% of the tokens on a chain to break that portion of the vote is much lower. Luckily for tellor users though, the multiple vote rounds ensures that other supporters can bridge trb over to the chain in case of a dispute to support, so it’s not a complete non-starter. For a new token, there are benefits; namely that you have a chain native token and no bridging is required. The obvious downside is just huge though…how much value does each chain’s token hold? Especially on early chains and less utilized systems, it is likely that the token on each chain would not have the exchange support or liquidity even necessary to foster a proper ecosystem. As for the last option, this one can work, but it has the downside of the token holding value even if the system is broken. One great thing about having your own token is that if the token holders trash the system, they’re generally left with a valueless token. If you use a token that holds value outside of the ecosystem, there can be additional attack vectors due to the token holding value even when the tellor system is compromised.

For these reasons, tellor picked to use bridged TRB, but to be honest, it depends on the chain. Chains without bridges (like Algorand) use their native token, and the tellor system can be deployed by anyone, so we expect to even see other tokens used as collateral in the future.

The other decision to made about cross-chain tellor is what the governance system looks like. Going with out main governance system (and not a third party), you have two options, either each chain has it’s own governance, or you have one chain that handles all the disputes and then you bridge the result back. We had thought about going this route, but the issue of bridges comes up again. While token bridges tend to be relatively mature, data bridges are very new and even more so than token bridges are simply controlled by multi-sigs. We may explore this route in the future, but another benefit of the one governance per chain approach is that attacks on one chain don’t affect attacks on another chain. If a user wants to compromise a voting mechanism on one chain, the users of other chains sort of don’t care. In fact, an attacker on a given chain would be well served if they could even signal that their attack doesn’t affect any other data points! For the censoring of tellor (disputing or submitting bad values to flood the system), it only affects individual data points. Users of other data don’t even care. With the voting (since any attack would likely go through weeks or months of disputes), a successful attacker would want to signify that the attack only affects one piece of data so as to minimize voting or other projects using their funds to save the system since their feeds are and will continue to be fine.

This approach by tellor to make attacks as siloed as possible is very intentional. We’ve known from the beginning, that any project can use tellor. This even means projects that shouldn’t use tellor or use tellor in a way that is unsafe. Tellor has a cost to break. It’s roughly equal to our market cap for the voting piece and then a few hundred thousand per day to censor. If you’re protocol can’t live with these numbers, you either need to add more data feeds (e.g. two or three data feeds for tellor would double or triple the cost to censor) or add additional security to your oracle (staking on your end, limits to the exposure side, another oracle or two to the calculation).

We know that there are ways to break tellor, but we’ve designed a system that is very, very expensive to break completely and when attacks happen, they are siloed and affect only one data point/ chain at a time. We know it’s a tradeoff, and we’ll continue to research and explore the best governance methods. The cool thing about tellor is we can always deploy a new tellor contract (even a competing one!) with a different governance structure and then let the market decide. Overall these are tough choices and we’re constantly engaged in thinking about them. If you have any comments or thoughts, definitely let us know!