tellorX

a community, an oracle, unstoppable

The Tellor oracle system has been operational on Ethereum for almost two years and is establishing itself as the preeminent secure, fully decentralized oracle. This paper outlines a major upgrade in the system to a faster and more flexible oracle. Tellor X continues to work with simple crypto-economic incentives to secure data through staking and dispute mechanisms, but builds a more secure Tellor through novel uses of the system's monetary policy and the introduction of a more equitable governance system.

The Oracle

At a high level, Tellor is an oracle system where a bonded set of "reporters" compete to add data points to an on-chain data bank. To create a properly incentivized system, Tellor mints a native token, "Tributes" (TRB). Reporters are incentivized to submit data using both payments and inflationary rewards. Using TRB, parties can "tip" a specific piece of data they want updated, then reporters can choose whether the reward for fetching the data is worth the cost of placing the value on-chain. The security of Tellor comes through a deposit of TRB that acts as a bond or stake requirement in order for reporters to participate in providing data. The reporters risk losing this stake if they submit data that is successfully disputed.

Data Submission

The new architecture is very similar to the current version of Tellor as miners(data reporters) will still need to submit data on-chain, but there are some implementation differences in the way data is reported in Tellor X:

> 1) There will no longer be a 'current challenge' and therefore no PoW component to the architecture. Hence, **miners will now be referred to as "reporters"**.
> 2) There will be an increased flexibility for data submission. Reporters can submit data for any request id instead of the designated top five and instead of needing five miners to reach an official value (median of 5) only 1 reporter is needed now.

To become a reporter, an address will deposit 100 TRB. Those TRB are locked (they act as a bond) until the reporter requests to withdraw them. The reporter then must wait one week (the time open for disputes) before they can withdraw.

Once the reporter has submitted their deposit (is bonded), a reporter can submit values for given ID's (e.g. 1-ETH/USD, 2 - BTC/USD). After a reporter submits a value however, they must wait a certain time period (a configurable variable, starting at 12 hours), before submitting again. This is both to allow time for disputes as well as to increase the number of reporters in the system. Reporters can choose to submit values

for any ID they want, but in practice will likely pick the ID with the highest tip. ID's can be updated as frequently as they want. Reporters are rewarded in two ways:

- The tip (half of the tip is burned, the other half goes to the reporter)
- Time-based inflationary rewards

Time-based inflationary rewards are a growing amount of tokens that resets after each mining event. These rewards start at zero and grow at a constant rate of .5 TRB per 5 minutes (this is configurable). When an ID is reported, the time-based rewards go to that reporter and then the amount for the next report restarts at zero. These rewards help ensure liveness by keeping the Tellor system going in times of low demand and in times of higher gas prices, allowing reporters to better predict returns.

For parties needing data more frequently than when the time-based rewards are greater than the gas costs, they can simply add tips. The Tellor oracle can therefore be as fast as needed, parties will just need to pay for tips to cover expenses of the reporters.

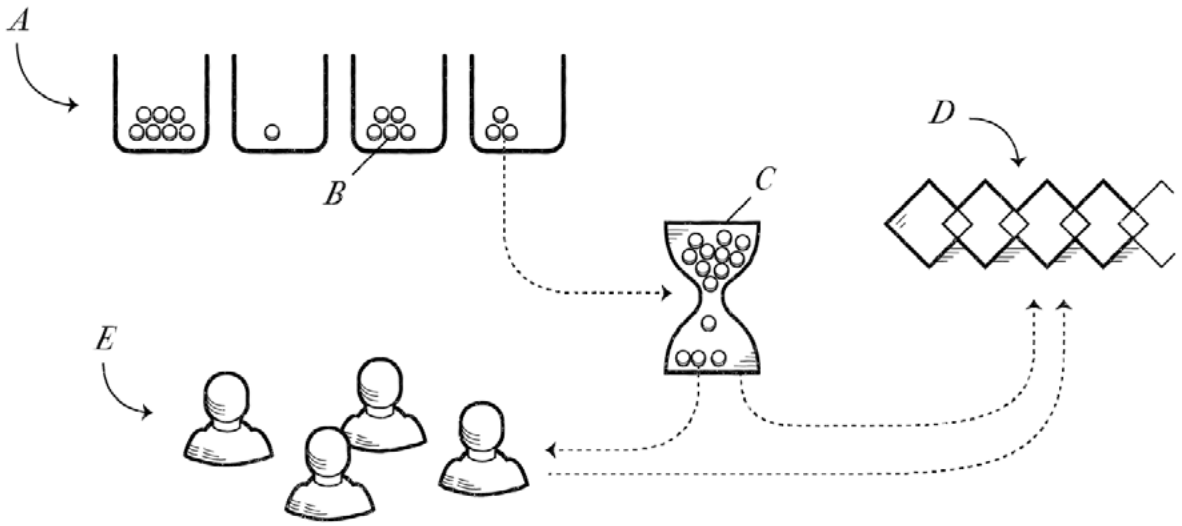

Fig. 1

A. Data IDs | *B.* Tips | *C.* Time-based Rewards | *D.* Onchain Data Feed | *E.* Reporters

The Data

Each request for data is given an ID on-chain, but specifications for the data are off-chain. An example would be ID 50 correlating to the TRB/USD price.

Unlike the previous versions of Tellor, data in Tellor X is submitted as bytes, meaning any data type or number of variables can be pulled in a single query. An example of this type of data could be that a new request ID could be a BTC blockheader, a simple price (e.g. ETH/USD), or even an array of prices (e.g. [ETH price, BTC price, SPX price, VIX, EUR/USD]). The more data batching the system can provide in request ID's, the more efficient the system becomes (more values per transaction).Reporters get to select which values they submit for. Some data requests may be very vague (e.g. the price of BTC/USD), but some may be

more specific or manual (the rainfall in inches in Nairobi as measured by one website). All new data types (request IDs) will need to be approved by a vote from the governance contract. This is to minimize the confusion of new ids and to force Tellor Improvement Proposals (TIP's), which will provide clarity as to data definition for those needing to verify the validity of the data. If reporters do not feel comfortable submitting or supporting a certain ID (e.g. if you need a paid api feed), the reporter does not have to submit for it. Parties who wish to build reporter support for their ID should follow best practices when selecting data to query, but will also need to tip a higher amount to incentivize activity[1].

Disputes

Tellor data values can always be disputed and taken off-chain, however the longer a user waits once the data is submitted on chain, the more probable it is to remain, and therefore be secure; assuming any value that remains on-chain is valid due to economic incentives to dispute invalid ones.

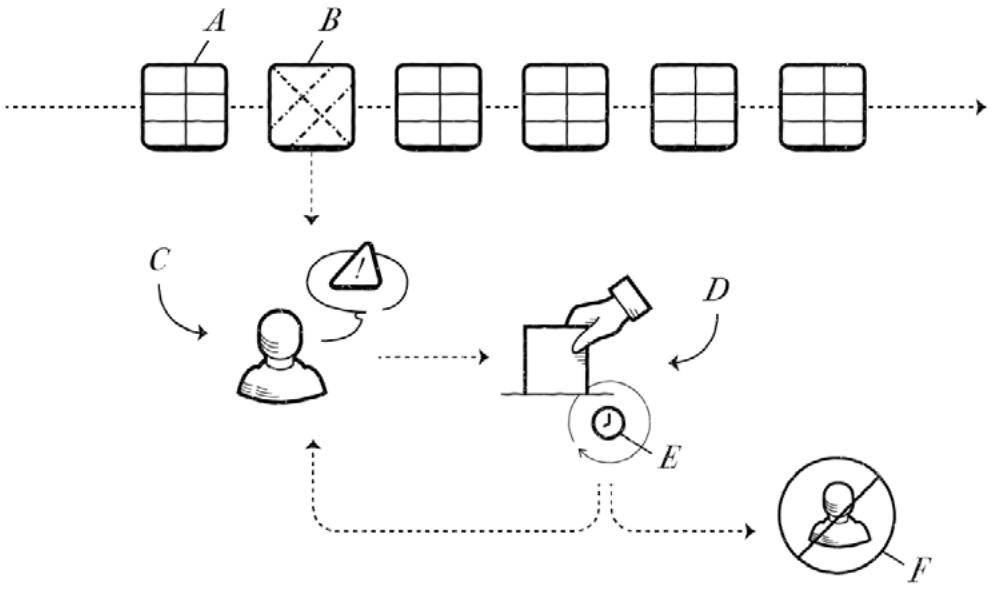

Fig. 2

A. Good Data | *B.* Bad Data | *C.* Disputed Reporter | *D.* Vote | *E.* Voting Period | *F.* Slashing

Any party can challenge data submissions when a value is placed on-chain. A challenger must submit a dispute fee to each challenge. Once a challenge is submitted, the potentially malicious reporter (C in Figure 2) who submitted the value is placed in a locked state for the duration of the vote. For the next two days, the Tellor governance contract votes on the validity of the reported value (D in Figure 2). A proper submission is one that corresponds to a valid query as defined off-chain in the Tellor TIP's. Although a correct answer should be known to the reporters, the ambiguity (lack of an exact correctness in this case) of validity is a feature and corresponds to "correct" being at the discretion or interpretation of the Tellor community.

[1] *https://medium.com/tellor/subjectivity-in-oracles-f7c3c06f69f1*

Dispute Rounds

The Tellor dispute mechanism allows for multiple rounds of disputes. The length of each dispute round and its cost increases each round in steps:

$$Dispute\ voting\ period\ =\ now + 2\ days\ \times\ disputeRounds_{t,id}$$

$$disputeFee_{t}\ =\ disputeFee_{i}\ \times\ disputeRounds_{t,id}$$

Where

$disputeFee_{i}$ is the initial dispute fee
$disputeRounds_{t,id}$ is the number of disputes open for a specific/same ID at that point in time

Dispute Resolution

At the end of the voting period, and if no new round is initiated, the votes are tallied. If found guilty, the malicious reporter's deposit goes to the disputing party; otherwise a portion of the fee paid by the disputer is given to the wrongly accused reporter.

Dispute Fees

The dispute fee is calculated based upon how many reporters are in the system and for which value you are disputing. The cost to dispute values is:

$$disputeFee_{i}\ =\ max\ (\ 10\ TRB,\ bondAmount\ \times\ \left(\ 1\ -\ \frac{reporters}{200}\ \right)$$

Where

bondAmount is the deposit required from each reporter to be able to provide data
reporters are the number of bonded reporters that are not under dispute

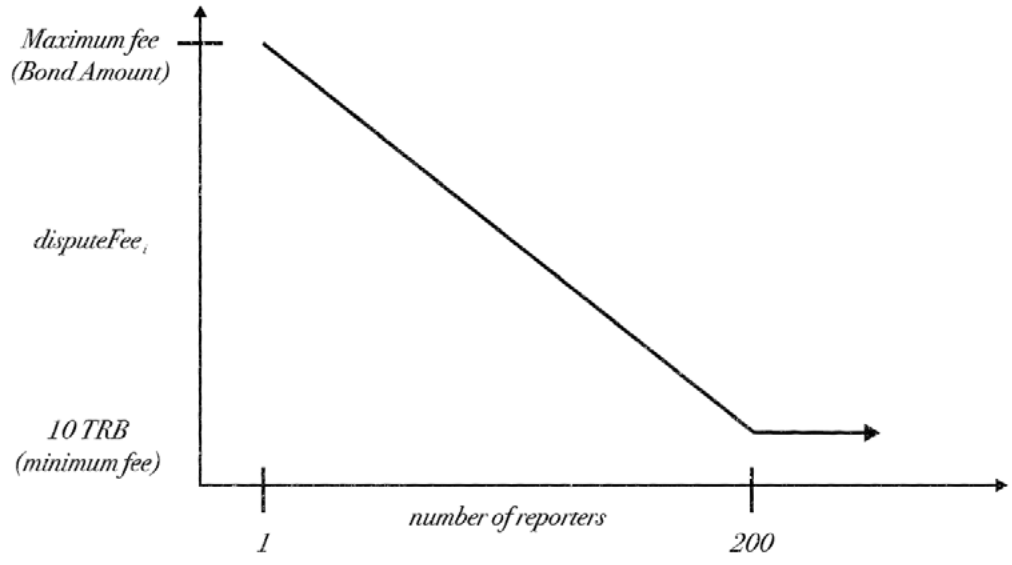

Fig. 3

Then if multiple disputes are performed on the same ID, a party might be trying to censor values by disputing good values. To counteract this, the dispute fee increases with each dispute on the same ID.

$$disputeFee_{t,id} = disputeFee_{i} \times disputeRounds_{t,id}$$

Where

$disputeFee_{i,id}$ is the initial dispute fee

$disputeRounds_{t,id}$ is the number of disputes open for a specific/same ID at that point in time

For this reason, it quickly becomes prohibitively expensive for a malicious party to simply dispute good values to censor a contract from reading them.

Replacement Data Tipping

Once a value is disputed it is taken off chain. For users who do not wish to wait for the result of the two day (or longer) vote, they can simply request the value again. To help support the users in this cost, upon the initiation of the dispute, 10% of the dispute fee is given as a tip to the disputed ID to ensure a quick replacement of the disputed value.

Invalid Data Query

A new addition to Tellor X is that votes can now be settled in one of three ways, true, false, or invalid. An invalid result means that the data is removed from the chain, but the reporter and the disputer do not lose tokens. An example of this would be a prediction market on who is the president the day after an election. If the election is not settled (the winner is unknown), but the oracle places a value on-chain before the result is known, it may end up being right, but at the time of the dispute/value submission, it isn't. This could be a case where the community decides to rule on the dispute as invalid. Leaving this option of ambiguity to the community affords the Tellor system more flexibility and reduces the chances that one of two honest parties (a disputer and a reporter) are punished.

Governance

Tellor governance is used to settle disputes, to vote on Tellor upgrades, adding data types supported (request Ids), as well as new features such as monetary policy. In previous versions of Tellor each vote was weighted by the amount of TRB tokens held at the time a dispute or an update was proposed. As the Tellor community continues to grow, there is a need to balance the voting power among stakeholders: holders, reporters, and users. TRB stakeholders all want Tellor to continue to grow, but the approach and needs of each group can be different. Weighting their votes differently can provide some checks and balances when considering the benefits of various proposals.

For Tellor X, there are three groups of stakeholders identified in the Tellor system:

- Reporters
- TRB holders
- Users

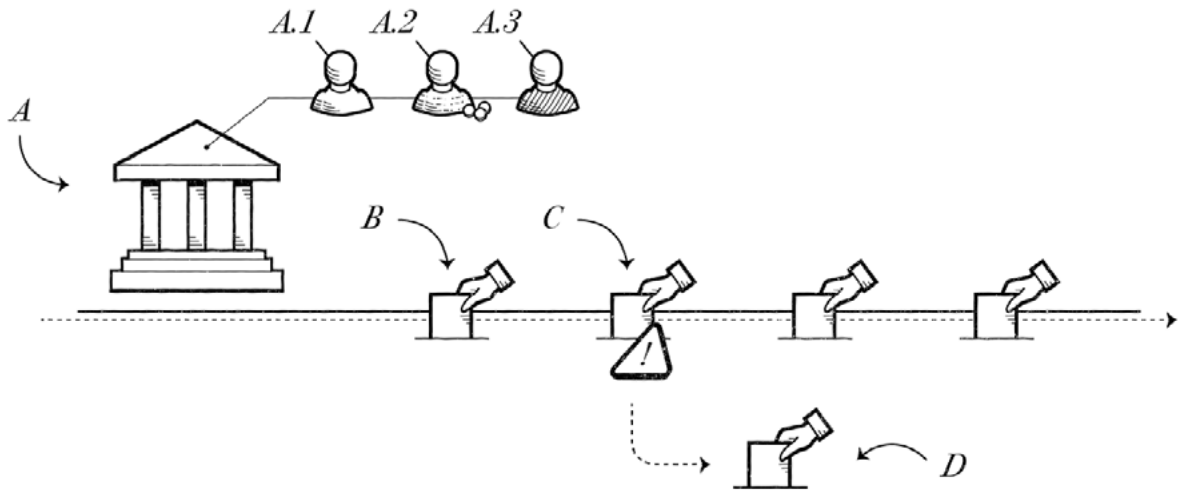

Fig. 4

A. Tellor Governance | *A.1-3* Stakeholders | *B.* Vote for proposal X | *C.* Vote for proposal Y is disputed | *D.* new round of voting

TRB holder weights are measured as the balance of TRB on the chain where the vote is taking place. For reporters, each submitted data point affords them additional non-transferable voting power weighted at 1TRB per successful submission. However, reporters must be actively bonded to be able to vote with their allocated non-transferable voting power. Users are weighted by the number of tips they have paid into the system at a .5 rate. As an example, if a user tips 2 TRB, they are afforded 1 TRB worth of voting power in the system.

It is important to note that Tellor X can be deployed on multiple chains. Although the main Tellor token is staying on the Ethereum network, users or the Tellor team can launch Tellor on any chain that has a functioning token bridge (e.g. Polygon, rollups, etc.). The exact structure of the governance on each separate chain would need to be on a case-by-case basis (tips and mining start out at zero, so the cost to break is low), but most likely the governance of that specific chain would be controlled by the stakeholders on that chain.

Delegation

TRB holders in the Tellor system are also able to delegate their voting rights. By specifying an address which they want to give their balances voting power to, it allows smaller and more inactive holders to give their vote to a trusted party, which will help increase the overall voting participation in the network. Reporters and users will not be able to delegate (or sell) their voting rights.

Technical Details

A proposal will be submitted for a vote by paying a fee. Parties then vote on the proposal for a week. Like disputes, these votes are also subject to multiple rounds if there is a dispute. Certain functions can also require various quorums or vote lengths, but will not be enforced at the governance level. Once the vote is settled with no disputes, the proposal is executed.

Quorum

Governance proposals for system updates and token minting, at implementation, will require a 5% quorum and have to be won by 5% percent above the losing option. Disputes have no quorum requirement.

Monetary Policy

Tellor X will utilize a new structure for managing circulating supply (the total supply is essentially meaningless) and the overall growth rate in the supply of TRB. There are two ways to manipulate the supply of Tellor, via locking/unlocking (reducing/increasing the circulating supply) and then minting/burning.

Through the current mining process of Tellor, tokens are both minted (for new values) and then burned (half of all tips to the Tellor system are burned). This system works well for initially generating demand for TRB and reducing the supply to create a commodity like demand for the product, however fails to afford flexibility in the cases of multiple chains and large exogenous shocks to demand for TRB (i.e. speculation).

To create a system that allows the governance of Tellor to better achieve its mission of a secure, decentralized oracle, Tellor is introducing a new structure of flexible supply growth rates for mining networks (each chain can have a different inflationary reward system) as well as Tellor Treasuries (staking pools) to reduce the circulating supply and increase governance participation.

Flexible Supply Growth Rates

The Tellor system will allow minting tokens at discrete intervals to be used for various endeavors. A proposal will be voted on (and subject to multiple rounds like other votes) by the governance contract. The proposal will be to initiate a one time minting event to a specific contract. Some examples of proposals can include:

> The Dev Share
>
> The current dev share is about 1000 TRB/month. For Tellor X, the dev share will be issued for a certain period of time via a vote, at which point the contract will mint the dev share in one lump sum to a contract that releases it slowly over time. This will not only save gas costs on transfers (currently every block has a transfer to the dev wallet), but also limits the dev share in terms of time. This means that if the team does not perform, the community does not need to continue the dev share.
>
> Inflationary Mining Rewards
>
> Inflationary mining rewards will no longer be built into the system (minting from the mining contract). Instead, each chain that has a mining operation will need to be funded by a vote. An initial vote will be put forth to fund the Ethereum mining contract for two years at a certain rate. When the vote is complete, a one time minting event will fund the oracle contract with tokens (e.g. 24,000 at a rate of ~1,000/ month). In two years, the community will need to vote again on whether to fund the Ethereum mining contract.

This flexibility allows for other chains to also be funded with inflationary rewards. The overall supply growth rate will need to be managed, but the more flexible nature of the monetary policy should afford an initial lower rate of inflation with the ability to mint more if needed.

Grants Program

The Tellor community can also begin a grants program, with votes to simply mint tokens to new users and promising projects. This inflationary based funding of grants means that the community can continue to grow even if large philanthropic individuals are not present in the ecosystem and can support projects that help Tellor succeed even if they are not profitable themselves.

Tellor Treasuries

Tellor treasuries are staking pools that reward users for locking up their TRB in exchange for future TRB with interest. The purpose of Tellor treasuries is to enable the Tellor community to manipulate the circulating supply of Tellor to provide a more stable Tellor price. The security of the Tellor oracles stems in many ways from the price of TRB, so having a countercyclical way to remove tokens from circulation will be a key component of this stabilization.

The treasury events will work as quarterly votes to either increase, decrease, or continue a certain number of TRB locked in treasury contracts. For example, for the first 4 quarters of Tellor X, we allow 100,000 TRB each quarter to be locked (A in Figure 5). Once one year comes around, 105,000 TRB are set to be released into circulation. If the price of TRB (D in Figure 5) has increased substantially, the community should allow these coins to be released, maybe even decreasing the amount locked (e.g. issue only 75,000 in Treasuries next month (B in Figure 5)). If the price however has decreased, the Tellor community can vote to increase the Treasury issuance to 200,000, thus creating external demand for parties to buy TRB to lock in the treasury, increasing the price by reducing the circulating supply (C in Figure 5).

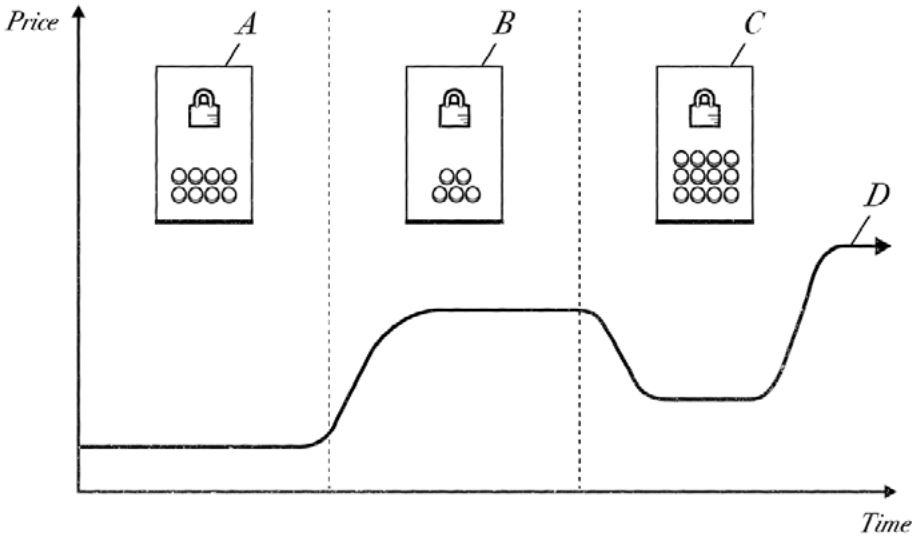

Fig. 5

A. Q1 Treasury | *B.* Q2 Treasury | *C.* Q3 Treasury | *D.* TRB Price Fluctuations

Another benefit of locking participants is to increase voting activity. Upon exit of a Tellor treasury, parties are punished if they did not vote on Tellor governance proposals. Parties are subject to lose any percentage of the interest gained in the treasury contract based upon the percentage of votes they abstained from. As an example, if a holder has 100 TRB locked into a one year treasury contract at 5%, and there were 10 voting events over the year; if the party voted on only 2 of the events, they would only receive 101 TRB upon exiting versus 105 if they had voted on every event.

Although the treasury contracts have fixed interest rates, each new issuance can change the interest rate. If demand for treasuries is very high, the interest rate can be low. If however, there is little interest and some of the treasury offering remains empty, the community can vote to increase the interest rate on subsequent offerings.

Security

Security is achieved through Tellor's architecture, which uses a simple bond/dispute mechanism to source correct values. Ultimate ownership and security in the system is afforded by our governance contract, which we aim to align incentives from holders, reporters, and users.

There are two primary metrics used when determining the security of an oracle:

- How can a bad value get put on-chain? (e.g. BTC/USD is 10M)
- How much does it cost to censor the oracle? (no good values can get through)

For the former, this is the cost to break the governance contract of Tellor. If we assume that a bad value will get caught (not go through unnoticed), then the bad value would go to a dispute. In order for the value to be put back on-chain, the vote would need to settle such that an incorrect value is deemed correct. With multiple rounds of voting, the malicious party would need to get to the point where they have 51% of the voting power in the system.

Since the governance contract is only partially based on the token weight (token weighted holders, reporters, users), there are other factors at play. The cost to break is not straightforward as it could be garnered several ways:

Where VS = voting shares

$$VS = \text{total supply} + \text{reporter votes} + \text{user(tipping) votes}$$

If the system is newly deployed, there will be minimal reporter and tipping votes. The system would therefore continue a straight token weighted vote, with the cost to get 51% simply being 51% of the market cap.

In a system with reporter and tipper votes, the attack vectors are different. The total number of mining votes in the system is the count of all historical mining events among actively bonded reporters. At a rate of one mining event per minute (a very fast chain), this would indicate 525,000 mining votes given each year. With a current supply of around 2M TRB and about 1/10 that many mining events, this makes even a best-case scenario for the attacker prohibitively expensive to carry out in any manner that is not a multi-year attack. Since other chains are faster and cheaper than Ethereum, this governance parameter would need to be carefully considered when deploying to other chains.

To break the system via tipping, the cost would be higher than if just using the token weighted option(holder).. If you buy the token and tip, you get half a vote. The malicious attacker could recycle the tips so as not to drain liquidity and increase the price (easier to buy in smaller lots and tip versus actually buying 51% of the total supply), additionally, due to the fact that half of the tips are burned, the reduction in total supply would drastically increase the token price, making each additional tip more expensive.

Overall, the cost to get a bad value on-chain is prohibitively high. With Tellor's current market cap over $100 Million dollars, breaking the governance system is no easy feat. Unless a party was breaking Tellor just for the fun of it, the much cheaper option is to simply censor Tellor for a certain period of time, as most use cases require some finality in the oracle (they will not wait for the entire Tellor system to settle a bad value dispute).

Since any value that is disputed will be put to a vote by all token holders, the simple cost to censor is:

Cost of a stake × *block time of underlying system (since Tellor is as fast the underlying system)*

As long as this value is higher than the cost to 51% attack a given chain (e.g. on Ethereum, to censor transactions at the miner level), Tellor should be considered a censorship resistant oracle for use on that network. With current costs at a 100 TRB bond requirement and a $50 price, if you assume even 10 second block times on Ethereum, it would cost:

$$100 \text{ TRB bond} \times \$50/\text{TRB} \times (6 \times 60) = \sim\$1{,}800{,}000 / \text{hr}$$

Currently it costs around $1,500,000/ hr to simply 51% attack Ethereum, so the security is sufficient for almost any application on the network[2].

Another change in Tellor X that makes it more secure than previous Tellor versions is our removal of the "current challenge". Since anyone can submit for any data point, it now becomes impossible to have a monopoly on the mining in the Tellor system. If a user wanted to, they could stake themselves and place values on-chain for themselves. They would still be subject to being disputed, but larger users can even have more than 1 stake to prevent censorship through disputes. The cost to censor via disputes is:

$$\text{Cost to censor} = \text{disputeFee} * 2^{\text{blocks per period}}$$

Therefore the cost to dispute for even 10 minutes on a 30 second block chain (assuming the minimum 10 TRB cost at a $50 price):

$$10 \text{ TRB bond} \times \$50/\text{TRB} \times 2^{(2 \times 10)} = \sim\$524\text{M}$$

Looking at our formula, we can summarize that security increases when:

- The share of those voting increases
- The price of the token increases

---

[2] *https://www.crypto51.app/*

Additionally, a minimum threshold of reporters is also essential to the proper functioning of the Tellor X system. The more parties that are available to submit data, the more decentralized our reporter set will be. An active and watchful community is also one of the big missing pieces in many protocols. Just because you are "theoretically" secure if there is an arbitrage opportunity, defi has seen many protocols exploited because those opportunities are left unfilled. It is the job of the Tellor ecosystem to properly incentivize and monitor the activity to make sure active diligence is being performed.

Use Cases

The new Tellor system, with its expansion to arbitrary data types, works as an oracle for any piece of off-chain information. The specific structure of Tellor X, with its lack of finality and ambiguously defined data points make it a unique oracle and one that is not fit for high speed values needing instant accuracy or trusted endpoints that are not open to any reporter.

That said, there are still a number of use cases that Tellor works well for and we look forward to expanding our user base and our community around these and even more creative use cases:

- Price feeds (e.g. BTC/USD TWAP)
- Prediction Markets (e.g. who is the current president of the United States?)
- Bridging assets (e.g. bring BTC block headers onto Ethereum)
- L2 Security (data availability, sequencer validation)

Contact

If you are interested in using Tellor, please reach out to us at info@tellor.io.