Economic Security for Cross-chain Protocols

Draft/Rough Notes

Luke ”Kayaba” Parker

March 24, 2024

1 Definition: Economic Security

Economic security is the ability to create an economic game where rational actors will participate as desired.

2 The Economic Game for an Oracle Responsible for Value Transfer

We start by defining an actor-controlled oracle σ.

We then define a positive-valuation oracle for the actor, ψ, capable of returning the economic value gained by oraclizing an event.

With $\perp$ representing inactivity and $\psi(\perp) = 0$, the protocol wins the game if for any to-oraclize event E, $\psi(E) > \psi(\perp)$ and $\psi(E') < 0$ where E' is an actor-decided oraclization inequal to E. The protocol loses the game if either condition fails to hold.

Since ψ is a positive-valuation oracle with range $[0, \inf)$, the second condition cannot be satisfied. Accordingly, we modify the game to include the negative-valuation oracle δ (with range $(-\inf, 0]$) and sum oracle Ω where $\Omega(E) = \psi(E) + \delta(E)$.

We now redefine the economic game as follows:

The protocol wins the game if for any to-oraclize event E, $\Omega(E) > \Omega(\perp)$ and $\Omega(E') < 0$.

This requires $\psi(E) > |\delta(E)|$ and $|\delta(E')| > \psi(E')$, with either $\psi(E)! = 0$ or $\delta(\perp)! = 0$ forming the goals of all economically secure protocols.

3 The Decisional δ

For $\psi(E) > |\delta(E)|$ and $|\delta(E')| > \psi(E')$ to be satisfied, ψ and δ must be able to differentiate between E and E'.

Given solely the actor-controlled oracle σ, there is no ability to distinguish. A new oracle, ρ, must be introduced. Unfortunately, the dual-oracle game with σ, ρ can be collapsed to the single-oracle game where the actor is defined as the joint actors behind each oracle, and both oracles become σ in the new game. This problem extends ad infinitum.

Protocols frequently try to define ρ as a cryptographic proof an event actually occurred on a blockchain, yet this fails given blockchains are forking data structures and knowledge of the 'best' blockchain requires a perfect view not realizable. At best, the argument is the cost of corrupting ρ must cause $\delta(E')$ to be so significant, it must exceed $\psi(E')$, frequently without provision of either the ψ oracle or calculation of $\delta(E')$ (preventing explicit evaluation of economic security).

This effectively creates an impossibility result for economically secure value transfer protocols.

4 Message Passing Protocols

Many modern cross-chain protocols do not focus on cross-chain value transfer yet cross-chain message passing. This is argued as a generalization of cross-chain value transfer and is frequently used as a building block for cross-chain value transfer.

This removes the provision of the oracle ψ from the defined game, removing the ability for the game to define its win conditions and be evaluated. While ψ could be dynamically re-instantiated, that converts a message passing protocol back into a value transfer protocol.

The argument in favor of these protocols is similar to the argument for when ρ is a cryptographic proof. $\delta(E')$ is so significant, it must exceed any possible $\psi(E')$.

Given the observed impossibility result for economically secure value transfer protocols, it can be argued message passing protocols are not only more functional, yet also more honest (given the lack of pretense of offering the impossible) protocols.

In practice, economically secure value transfer protocols offer explicit evaluation, and with it enable the possibility to attempt self-limiting the realizable range the output of ψ lies in.

5 ρ as Social Consensus

We look at THORChain as a case study for a protocol aiming to be economically secure.

THORChain has all validators on their network stake a native cryptocurrency, RUNE. They then section their validators into six actors, forming six oracles σ_i for $i \in [1, 6]$. Each oracle σ_i is able to publish E' onto a distinct network. They then form an oracle for their own network, ρ, composed of every validator. Upon oraclization onto a distinct network, ρ publishes onto THORChain the decision E or E'. If E', δ is set to the value captured with an additional penalty, ensuring $|\delta(E')| > \psi(E')$. This causes THORChain to win the economically secure game so long as ρ remains honest.

Upon ρ becoming corrupted, the THORChain blockchain does not inherently win the economically secure game due to the decisional δ problem. In practice, it likely still does due to social consensus.

If THORChain's ρ oracle fails, a supermajority of validators have been corrupted and the network has lost all value. The validators are presumed to have extracted the maximum $\psi(E')$ possible, at notable cost to users, and destroyed its value as an oracle. With this, a reasonable expectation is for the RUNE cryptocurrency to be considered worthless.

Since it is the RUNE cryptocurrency which is staked, the validators' stake is now also worthless. Under the collapsed game (where σ, ρ is modeled solely as σ), if $\delta(E')$ (the cost of the now worthless stake) is worth more than $\psi(E')$, the economically secure game is won by the protocol.

This does assume market behavior upon network collapse, and does require cost to compromise ρ (the δ function, since the cost to compromise is lost under our market assumption) exceeds the maximum $\psi(E')$. THORChain attempts to achieve the latter by enshrining the oracle ψ into their protocol, making δ a derivative, and requiring the maximum possible absolute value of δ exceed the maximum possible value of ψ by a margin. As the margin is endangered, validators are pressured to decide to either $\sigma(E')$ while $|\delta(E')| > \psi(E'))$ or $\sigma(E)$, where E is expected to preserve the margin (such as via rejecting further additions of value to the protocol). Either decision causes THORChain to win the economic security game.

THORChain only loses the economic security game if $|\delta(E')|$ drops so rapidly compared to $\psi(E')$, $|\delta(E')| <= \psi(E'))$ does occur before sufficient adjustments are made.

This effectively causes THORChain to be economically secure given an incorruptible oracle μ, the market, in a tri-oracle game σ, ρ, μ for the decisional δ so long as a margin (not necessarily the target margin) is maintained.