Cryptoeconomics of the Loki network

The problem of incentivising service nodes in the Loki Blockchain network

Brendan Markey-Towler[1]

11 July 2018

Abstract

Loki is a Blockchain network oriented toward the provision of privacy-preserving services over a network of service nodes. The salient cryptoeconomic problem is how to incentivise actors in the Loki network to operate service nodes in a manner compatible with the objectives of the Loki network, in particular decentralisation and privacy. We use cryptoeconomic game theory to characterise this problem. We derive an equation for the incentives to create service nodes faced by actors in the Loki network, and use this equation to characterise a pure strategy Nash equilibrium in the provision of service nodes. With reasonable assumptions we can discover a condition for the design of the Loki network which supports such a pure strategy Nash equilibrium consistent with the objectives of the Loki network, which is useful in particular for deciding the staking requirement for actors who wish to operate service nodes. We also derive an equation for the value a rogue actor would have to place on undermining this equilibrium and Loki's privacy. We analyse this solution to study how it responds to changes in the parameters of the Loki network.

1 The cryptoeconomic problem in the Loki network

Loki is a Blockchain network which uses a hybrid proof-of-work/proof-of-service system in which cryptoeconomics is employed to incentivise the provision of privacy-preserving services over a network of service nodes. Service nodes will offer routing and data transfer services over a network in a manner not dissimilar to nodes in TOR to run service node apps (SNApps), the first of which will be a privacy-maintaining messenger system (Loki Messenger). In order for actors in the Loki network to operate service nodes they must stake a certain amount of Loki for each service node they operate. The salient cryptoeconomic problem in the Loki network is how to incentivise actors to stake sufficient Loki to operate service nodes and provide services in a manner which is compatible with the objectives of the Loki network. In particular, as service nodes will offer routing and data transfer services such as Loki Messenger in a manner not dissimilar to nodes in TOR, there must be sufficiently many distinct service nodes to maintain decentralisation and thus maximise privacy.

To analyse this problem we first must derive an equation which describes the incentives faced by actors in the Loki network and use it to determine the behaviour of a rational actor in the Loki network. Specifically, we derive a condition which defines the number of service nodes a rational actor in the Loki network will provide. We then use this condition to characterise equilibrium in the provision of service nodes over the Loki network, which is a pure strategy Nash equilibrium. We then

[1] RMIT Blockchain Innovation Hub and School of Economics, University of Queensland

analyse this condition and equilibrium by introducing reasonable assumptions which reduce the dimensionality of the problem, and discover a solution to the design problem faced by Loki in the form of a condition for the design of rewards and staking requirements for operating service nodes. We use this solution to define the staking requirement which supports equilibrium in the provision of service nodes on the Loki network, and a definition of those staking requirements which are consistent with the objectives of the Loki network. We then analyse the response of the staking requirement which supports equilibrium to various parameters in the Loki network. After taking a fairly high-level analysis of the problem thusly, we introduce some specific forms for various parameters of the Loki network and calculate figures for the staking requirement which supports various equilibria under various parameterisations. We then, before concluding, establish the response of the staking requirement to various parameters in this expanded numerical analysis.

2 Characterising incentives and equilibrium strategies

The incentive for any actor in the Loki network to become a service node hosting SNApps is provided for by the allocation of 50% of the Loki cryptocurrency reward for Block processing to be distributed among these nodes. Let us assume, as is reasonable in a game theoretic setting, that the incentive for an actor to run n service nodes is given by profits π. Profits for actors operating service nodes in the Loki network depend, in particular, on the number of nodes they operate, n, and the total number of nodes N in the network. The revenues $r(n \;\; N)$ which accrue to service nodes depends on both variables, while the costs $c(n)$ of running servers which host service nodes depend only on the number of nodes run thereon, so we have

$$\pi(n \;\; N) = r(n \;\; N) - c(n)$$

We will suppose that, since the costs $c(n)$ of running a service node at present are denominated in national currencies, that profits $\pi(n \;\; N)$ are also denominated in national currencies. Let us therefore say that the exchange rate of national currencies for Loki (for instance, USD/Loki) is ϵ, and that the rewards accruing to an actor operating n service nodes out of a total N is, in Loki, $\lambda(n \;\; N)$. Therefore the profits accruing to a service node become

$$\pi(n \;\; N) = \epsilon\lambda(n \;\; N) - c(n)$$

Now in order to operate a service node, an actor in the Loki network must stake s Loki. Suppose that the opportunity cost of staking this Loki is foregoing a rate of return r (for instance, government bond yields or stock market returns), such that the opportunity cost of staking Loki to operate a service nodes is $r(\epsilon s)$. In this case, an actor in the Loki network will stake sufficient Loki to operate n service nodes if

$$\pi(n \;\; N) \geq r(\epsilon n s)$$

and *only if* this is the case *and* they have ns Loki ($n\epsilon s$ in national currencies) available to stake.

We can safely suppose this sufficiently characterises the problem of whether an actor is incentivised to operate service nodes within the Loki network. The "dummy routes" algorithm embedded in the Loki network software can reasonably be said to ensure that the expected profit to be gained by operating dishonestly in the network (i.e. staking but not offering services) is zero, for any such actor will quickly be flagged and removed from the network. So an actor will only ever be incentivised either to operate service nodes, or invest in the outside option.

The *economic profit* obtained from staking sufficient Loki to operate n service nodes when the total network of service nodes is N is therefore given by

$$\pi(n \;\; N) - r(\epsilon ns) = \epsilon\lambda(n \;\; N) - [c(n) + r(\epsilon ns)]$$

A rational agent who maximises economic profits in responding to the incentives embodied in this equation will stake Loki to operate n service nodes up to the point at which marginal revenues are equal to marginal costs. Since $\pi(n \;\; N)$ is concave by construction, so too will $\pi(n \;\; N) - r(\epsilon ns)$ be. Thus a rational agent in the Loki network will operate n^* nodes defined as follows

$$n^* = n{:}\frac{\partial}{\partial n}[\pi(n \;\; N) - r(\epsilon ns)] = 0$$

That is to say, if we solve the problem embedded in the equation, a rational agent in the Loki network will operate n^* service nodes defined as follows

$$n^* = n{:}\,\epsilon\frac{\partial}{\partial n}\lambda(n \;\; N) = r(\epsilon s) + \frac{\partial}{\partial n}c(n)$$

or, equivalently, a rational agent in the Loki network will operate n^* service nodes defined as follows

$$n^* = n{:}\frac{1}{s}\frac{\partial}{\partial n}\lambda(n \;\; N) = r + \frac{1}{\epsilon s}\frac{\partial}{\partial n}c(n)$$

Equilibrium will be reached on the Loki network when all actors in the Loki network are operating n^* service nodes so defined. Such equilibria are strategic (game theoretic equilibria), because the decision of each actor in the Loki network about how many service nodes to operate depends on the decision of every other actor in the Loki network. The exact form of such equilibria can be derived if we make explicit the fact that the total number of nodes N in the network on which the rewards $\lambda(n \;\; N)$ for operating a service node are defined, though it does create some notational complexity. If the set of actors in the Loki network who might operate service nodes is I, then the total number of nodes in the network of N service nodes is

$$N = \sum_{i \in I} n_i$$

where n_i is the number of service nodes provided by actor i in the Loki network. In equilibrium therefore, each actor i in the Loki network operates n_i^* service nodes defined as follows

$$n_i^* = n_i{:}\frac{1}{s}\frac{\partial}{\partial n_i}\lambda\left(n_i \;\; \left[n_i + \sum_{j \neq i \in I} n_j^*\right]\right) = r + \frac{1}{\epsilon s}\frac{\partial}{\partial n_i}c(n_i)$$

Such equilibria as defined by this condition are pure strategy Nash equilibria. In such pure strategy Nash equilibria, actors in the Loki network will obtain profits of

$$\pi_i\left(n_i^* \;\; \sum_{j \in I} n_j^*\right) = \epsilon\lambda\left(n_i^* \;\; \sum_{j \in I} n_j^*\right) - c(n_i^*)$$

and thus rates of return on their service node stakes s of

$$\frac{1}{sn_i^*}\pi_i\left(n_i^* \quad \sum_{j\in I} n_j^*\right) = \frac{1}{sn_i^*}\left[\epsilon\lambda\left(n_i^* \quad \sum_{j\in I} n_j^*\right) - c(n_i^*)\right]$$

where n_i^* is defined as above.

3 Analysis

We can make use of the incentive structure thus established in the Loki network, and the behaviour of rational agents in response to it in equilibrium to characterise a design problem for Loki, which is the setting of the staking requirement for operating a service node in the Loki network. Obviously the equilibrium established above has a high degree of dimensionality as a mathematical problem, so this will have to be reduced by exogenising certain variables. After we do this, we can recover a solution to the design problem which specifies a staking requirement which will support a given desired equilibrium distribution of service nodes operated by actors in the Loki network.

3.1 Simplifying assumptions and exogenisations

If we consider again the problem of responding to incentives to provide service nodes on the part of any given actor in the Loki network, we can introduce further reasonable simplifications which allow for better analysis. For convenience we restate that, a rational agent in the Loki network will operate n^* service nodes defined as follows

$$n^* = n{:}\frac{1}{s}\frac{\partial}{\partial n}\lambda(n \quad N) = r + \frac{1}{\epsilon s}\frac{\partial}{\partial n}c(n)$$

A reasonable assumption we may introduce is that the marginal cost of operating a service node is constant. This is reasonable because of the state of server technology at the present time means that the cost of providing greater routing and data transfer services on that server will increase at a fairly constant rate. Since the marginal cost of operating a service node is constant, we might say that it can be defined as a constant c. That is,

$$\frac{\partial^2}{(\partial n)^2}c(n) = 0 \Rightarrow \frac{\partial}{\partial n}c(n) = c$$

And so we have that a rational agent in the Loki network will operate n^* service nodes defined as follows

$$n^* = n{:}\frac{1}{s}\frac{\partial}{\partial n}\lambda(n \quad N) = r + \frac{c}{\epsilon s}$$

Still, we can see that apart from the fact that the form of $\lambda(n \quad N)$ has not yet been explicitly defined, that this is an equation in more than one variable, so for analytical purposes we wish to further fix certain variables and define them as exogenous for analytical purposes. Doing this means that we may simply base their values on such data as exist rather than endogenous modelling. We will denote these exogenous variables in the standard manner by "barring" their variables.

Obviously, first, we might allow the cost of operating a service node to be simply defined as the cost of operating a server over the relevant time period of analysis, i.e. $c = \bar{c}$. We might also set the exchange rate to be exogenously determined rather than endogenously by a market, so that we set it based on projections from data on the exchange rate of national currency for Loki prior to the relevant

time period of analysis, i.e. $\epsilon = \bar{\epsilon}$. Further, we may also set the rate of return r foregone by staking Loki to operate a service node by reference to government bond yields or stock market returns prior to the relevant time period of analysis, i.e. $r = \bar{r}$. Introducing these exogenisations, we see that a rational agent in the Loki network will operate n^* service nodes defined as follows

$$n^* = n: \frac{1}{s}\frac{\partial}{\partial n}\lambda(n \;\; N) = \bar{r} + \frac{\bar{c}}{\bar{\epsilon} s}$$

If we collect all remaining endogenous variables to the left hand side of this condition, we find that a rational agent in the Loki network will operate n^* service nodes defined as follows

$$n^* = n: \frac{1}{s}\left[\frac{\partial}{\partial n}\lambda(n \;\; N) - \frac{\bar{c}}{\bar{\epsilon}}\right] = \bar{r}$$

We still have more variables than equations, but we have reduced the dimensionality of the problem significantly by exogenising the variables we have and allowing them to be set relative to relevant data for the time period of analysis. Specifically, outside of the specific functional form of the reward $\lambda(\cdot)$ for operating a service node, we have two variables yet to be determined before we can determine how many service nodes n^* a rational agent will operate in the Loki network. Before we can determine n^*, we need to define the staking requirement s and the total number of service nodes on the network N.

3.2 The design problem

For design purposes we may of course recast this problem now a little differently. In equilibrium, each actor i in the Loki network operates n_i^* service nodes defined now as follows

$$n_i^* = n_i: \frac{1}{s}\left[\frac{\partial}{\partial n_i}\lambda\left(n_i \;\; \left[n_i + \sum_{j \neq i \in I} n_j^*\right]\right) - \frac{\bar{c}_i}{\bar{\epsilon}}\right] = \bar{r}_i$$

where we have selected $\bar{c}$, $\bar{\epsilon}$, and $\bar{r}$ exogenously based on such relevant data as exist. If we wish to implement a mechanism $\lambda(n \;\; N)$ which incentivises rational agents $i \in I$ in the Loki network to operate n_i^* nodes on the network such that there are $N = \sum_{i \in I} n_i^*$ nodes overall, we need to pick a form for the reward $\lambda(n \;\; N)$ for operating a service node and a staking requirement s. The specific form of $\lambda(n \;\; N)$ is not especially important however and may be designed relatively arbitrarily. Alternatively, of course, it might be designed relative to the *monetary policy* objectives of the network. What is far more important for the cryptoeconomic problem in the Loki network is the value of the staking requirement s.

To formulate a solution to this problem of discovering the staking requirements that would support an equilibrium of our choice, let us introduce some further reasonable assumptions. Firstly, if we suppose that $\bar{c}_i$ and $\bar{r}_i$ are homogenous across the set of actors in the Loki network (as is not unreasonable) we have that each actor in the Loki network faces a homogenous incentive structure. In this case, the equilibrium we would wish to support could be a symmetric one in which all actors in the Loki network operate a homogenous number of service nodes $n_i^* = n^* \; \forall \; i \in I$. In this case, therefore, we can characterise equilibrium between homogenous agents, and focus on that staking requirement which would support the desired operation of service nodes by the representative agent in the Loki network.

The staking requirement $\hat{s}$ which would support a symmetric equilibrium under these conditions in which rational agents in the Loki network provide n^* service nodes, given a particular form for the reward $\lambda(n \;\; N)$ for operating a service node, is given by

$$\hat{s} = \frac{1}{\bar{r}}\left[\frac{\partial}{\partial n}\lambda\left(n^* \;\; \overline{|I|}\right) - \frac{\bar{c}}{\bar{\epsilon}}\right]$$

where we can alter the function $\lambda(n \;\; N)$ since $N = n^*|I|$ is endogenised by the number $\overline{|I|}$ of actors $i \in I$ in the Loki network (which is itself an exogenous, given number) and the desired provision n^* of service nodes by the representative agent within them.

That the solution to the staking requirement problem takes this form is vital given the objectives of the Loki network. Service nodes offer routing and data transfer services over a network in a manner not dissimilar to nodes in TOR to preserve privacy, and so it is vital that no one actor have an incentive in equilibrium to come to provide service nodes beyond a certain proportion of service nodes in the Loki network. With the solution to the staking requirement problem we have discovered, we can formally characterise the staking requirements which are compatible with this objective of the network.

If ϕ (for "FBI") is the proportion of service nodes any given actor must operate in order to undermine the privacy in SNApps provided on the Loki network, then it is vital that in equilibrium, a rational actor in the Loki network has no incentive to provide service nodes in excess of this proportion. That is, for equilibrium compatible with the privacy of SNApps provided by $N = n^*|I|$ service nodes in the Loki network (where $\overline{|I|}$ is the number of actors in the Loki network) we must have that

$$n_i^* \leq \phi N$$

for any given actor $i \in I$ in the Loki network. This allows us to immediately eliminate a range of staking requirements from consideration. If $\overline{|I|}$ is the number of actors in the Loki network, and n^* the desired provision of service nodes by the representative agent within them, then the set of acceptable staking requirements (those which will support an equilibrium compatible with Loki's objectives) is

$$\Omega = \left\{s = \hat{s}\left(n_i^* \;\; \overline{|I|}\right) : n_i^* \leq \phi\left(n^*\overline{|I|}\right)\right\}$$

for an arbitrary actor i, where $\hat{s}\left(n_i^* \;\; \overline{|I|}\right) = \frac{1}{\bar{r}}\left[\frac{\partial}{\partial n}\lambda\left(n_i^* \;\; \overline{|I|}\right) - \frac{\bar{c}}{\bar{\epsilon}}\right]$. We could, alternatively and more intuitively, approximate this by picking an arbitrary number of service nodes N to be provided homogenously across the network and so define Ω, the set of acceptable staking requirements, as follows

$$\Omega = \{s = \hat{s}(n^* \;\; N) : n^* \leq \phi N\}$$

where $\hat{s}(n^* \;\; N) = \frac{1}{\bar{r}}\left[\frac{\partial}{\partial n}\lambda(n^* \;\; N) - \frac{\bar{c}}{\bar{\epsilon}}\right]$.

Throwing down the gauntlet: the approximate monetary cost of undermining privacy in Loki

With this analysis in hand we can actually determine how much an actor intent on undermining the privacy of the Loki network must value that undermining in monetary terms. Suppose we have selected the staking requirement $\hat{s}$ to support a symmetric equilibrium in which the $\overline{|I|}$ actors in the Loki network provide $n^* \leq \phi N$ service nodes. Suppose we now have an actor ρ (for "rogue") in the Loki network. If this actor seeks to provide $n_\rho \geq \phi N$ service nodes, then their profit will be, approximately

$$\pi\big(n_\rho \;\; \big[\big(n_\rho - n^*\big) + n^*\overline{|I|}\big]\big) - \bar{r}\big(\bar{\epsilon} n_\rho \hat{s}\big) = \bar{\epsilon}\lambda\big(n_\rho \;\; \big[\big(n_\rho - n^*\big) + n^*\overline{|I|}\big]\big) - \big[\bar{c} + \bar{r}\big(\bar{\epsilon} n_\rho \hat{s}\big)\big]$$

Now notice that, $\pi(n \;\; N) - r(\epsilon n s)$ is concave by construction, and $\hat{s}$ was selected to support a symmetric equilibrium in which the $\overline{|I|}$ actors in the Loki network provide $n^* \leq \phi N$ service nodes, and equilibrium is characterised by rational agents maximising their economic profits. At this point we would have therefore, were $n_\rho = n^*$ and ρ acting rationally that

$$\bar{\epsilon}\frac{\partial}{\partial n}\lambda\big(n_\rho \;\; \big[\big(n_\rho - n^*\big) + n^*\overline{|I|}\big]\big) = \bar{c} + \bar{r}(\bar{\epsilon}\hat{s})$$

Now as n_ρ increases to some $n_\rho \geq \phi N$, we see that, because $\lambda(\cdot)$ is concave by construction, that the left hand side of this equation decreases while the left hand side remains constant, and thus does economic profit at the margin. The value of the profit foregone relative the equilibrium $\hat{s}$ was selected to support therefore will be approximately

$$\begin{aligned}\pi\big(n^* \;\; n^*\overline{|I|}\big) - \bar{r}(\bar{\epsilon} n^* \hat{s}) - \pi\big(n_\rho \;\; \big[\big(n_\rho - n^*\big) + n^*\overline{|I|}\big]\big) + \bar{r}\big(\bar{\epsilon} n_\rho \hat{s}\big) \\ = \bar{\epsilon}\lambda\big(n^* \;\; n^*\overline{|I|}\big) - [\bar{c} n^* + \bar{r}(\bar{\epsilon} n^* \hat{s})] - \bar{\epsilon}\lambda\big(n_\rho \;\; \big[\big(n_\rho - n^*\big) + n^*\overline{|I|}\big]\big) \\ + \big[\bar{c} n_\rho + \bar{r}\big(\bar{\epsilon} n_\rho \hat{s}\big)\big]\end{aligned}$$

Gathering like terms, the value of the profit foregone by the rogue actor ρ (let us call it v_ρ) relative the equilibrium $\hat{s}$ was selected to support therefore will be approximately given by

$$\frac{v_\rho}{\bar{\epsilon}} = \lambda\big(n^* \;\; n^*\overline{|I|}\big) - \lambda\big(n_\rho \;\; \big[\big(n_\rho - n^*\big) + n^*\overline{|I|}\big]\big) + (\bar{r}\hat{s} + \bar{c})\big(n_\rho - n^*\big)$$

In order for it to be rational for a rogue actor ρ to seek to undermine the privacy of the Loki network, they must value that undermining by *at least* v_ρ in terms of national currency, and at least v_ρ/ϵ in terms of Loki. Now what we can see here, quite readily in fact, is that the value of the profit foregone relative to that the equilibrium $\hat{s}$ was selected to support by the rogue actor ρ increasing the service nodes they are providing to some to some $n_\rho \geq \phi N$ will grow quite rapidly. Notice that this expression *linear* in the staking requirement $\hat{s}$ and marginal cost $\bar{c}$ of operating a server (while the concavity of $\lambda(\cdot)$ means it will offset this only in decreasing increments) and so a rogue actor must value the undermining of the Loki network by (likely) *substantial* multiples of the opportunity cost of staking Loki to operate service nodes *as well as* the server cost. It is therefore increasingly expensive in terms of profits forgone, and likely becomes prohibitively so even for government authorities, to operate sufficient nodes in the Loki network as to undermine its privacy when the staking requirement has been designed to solve the cryptoeconomic problem faced by the Loki network.

3.3 Simple analytics of solutions to the staking requirement design problem

Even without introducing a specific functional form for $\lambda\big(n^* \;\; \overline{|I|}\big)$, we can establish a variety of effects on the staking requirement which will support an equilibrium in which $\overline{|I|}$ symmetric rational agents in the Loki network provide n^* service nodes. The staking requirement which would support such equilibrium is, as we have above

$$\hat{s} = \frac{1}{\bar{r}}\left[\frac{\partial}{\partial n}\lambda\big(n^* \;\; \overline{|I|}\big) - \frac{\bar{c}}{\bar{\epsilon}}\right]$$

Now if we take partial derivatives of this function, we can establish various effects on the staking requirement which will support an equilibrium in which $\overline{|I|}$ symmetric rational agents in the Loki network provide n^* service nodes.

The effect of an decrease in desired nodes provided by each actor in the Loki network
Firstly, and most importantly, let us examine the effect on the staking requirement which solves the design problem of a change in the number of service nodes we wish for each actor in the Loki network to operate. We have that

$$\frac{\partial}{\partial n^*}\hat{s} = \frac{1}{\bar{r}}\frac{\partial^2}{(\partial n^*)^2}\lambda\left(n^* \quad \overline{|I|}\right)$$

and so, since $\lambda\left(n^* \quad \overline{|I|}\right)$ is concave by construction

$$\bar{r} \geq 0 \;\&\; \frac{\partial}{\partial n^*}\lambda\left(n^* \quad \overline{|I|}\right) \leq 0 \Rightarrow \frac{\partial}{\partial n^*}\hat{s} \leq 0$$

Therefore, given $\overline{|I|}$ symmetric rational agents in the Loki network and a desired provision of n^* service nodes by those agents, the fewer service nodes we wish for a rational agent in the Loki network to have an incentive to operate in equilibrium, the higher we must set the staking requirement. This effect is particularly salient given the objectives of the Loki network. As we have discussed above, service nodes offer routing and data transfer services over a network in a manner not dissimilar to nodes in TOR to preserve privacy, and so it is vital that no one actor have an incentive in equilibrium to come to provide a certain proportion of nodes in the network. The fewer – relative to the equilibrium number of service nodes – any one actor provides the more secure privacy of SNApps on the Loki network. The more secure we wish the privacy of the Loki network to be the higher we must set the staking requirement for actors in the Loki network to provide service nodes.

The effect of changes in operating costs, the exchange rate and opportunity costs
Now let us examine the effect on the staking requirement which solves the design problem of a change in, in turn, operating costs $\bar{c}$, the exchange rate $\bar{\epsilon}$, and opportunity costs $\bar{r}$.

Firstly, we have for a change in operating costs that

$$\frac{\partial}{\partial \bar{c}}\hat{s} = -\frac{1}{\bar{r}\bar{\epsilon}}$$

Opportunity costs and the exchange rate are both positive, so we have that

$$\bar{r} \geq 0 \;\&\; \bar{\epsilon} \geq 0 \Rightarrow \frac{\partial}{\partial \bar{c}}\hat{s} \leq 0$$

Therefore, given $\overline{|I|}$ symmetric rational agents in the Loki network and a desired provision of n^* service nodes by those agents, the greater are the costs of operating a service node, the lower the staking requirement which supports equilibrium among rational agents providing service nodes in the Loki network. This effect, however, is most salient as the cost of operating a service node decreases for server costs are subject to Moore's law. Therefore, given $\overline{|I|}$ symmetric rational agents in the Loki network and a desired provision of n^* service nodes by those agents, a decrease in the cost of operating service nodes causes the staking requirement which supports equilibrium among rational agents providing service nodes in the Loki network to *increase*.

Now take the exchange rate $\bar{\epsilon}$ of national currency for Loki. We have for a change in this exchange rate that

$$\frac{\partial}{\partial \bar{\epsilon}} \hat{s} = \frac{\bar{c}}{\bar{r}(\bar{\epsilon})^2}$$

Opportunity and operating costs are both positive, so we have that

$$\bar{r} \geq 0 \;\&\; \bar{c} \geq 0 \Rightarrow \frac{\partial}{\partial \bar{\epsilon}} \hat{s} = \frac{\bar{c}}{\bar{r}(\bar{\epsilon})^2} \geq 0$$

Therefore, given $\overline{|I|}$ symmetric rational agents in the Loki network and a desired provision of n^* service nodes by those agents, the greater the exchange rate (the more valuable is Loki), the greater the staking requirement ought to be. That is to say, as Loki appreciates, the greater the staking requirement ought to be to implement a given equilibrium. The reason for this is fairly straightforward – an appreciation in Loki increases the value of the reward for operating service nodes and thus the incentive to operate them, and this must be countered to support equilibrium. Over time, we can expect Loki to appreciate in value as it is adopted at greater rates and demand for the currency increases, so over time the staking requirement which would support a given equilibrium increases with it.

Now, finally, take the rate $\bar{r}$ at which opportunity costs are accrued for operating service nodes in the Loki network. We have for a change in this rate that

$$\frac{\partial}{\partial \bar{r}} \hat{s} = \frac{1}{\bar{r}^2}\left[\frac{\partial}{\partial n}\lambda\left(n^* \;\; \overline{|I|}\right) - \frac{\bar{c}}{\bar{\epsilon}}\right]$$

Now this is an ambiguous effect, for we have that

$$\frac{\partial}{\partial \bar{r}} \hat{s} \begin{cases} \leq 0 \;\forall\; \bar{\epsilon} \leq \dfrac{\bar{c}}{\dfrac{\partial}{\partial n}\lambda\left(n^* \;\; \overline{|I|}\right)} \\ \geq 0 \;\forall\; \bar{\epsilon} \geq \dfrac{\bar{c}}{\dfrac{\partial}{\partial n}\lambda\left(n^* \;\; \overline{|I|}\right)} \end{cases}$$

So, for a sufficiently low exchange rate of national currency for Loki (a sufficiently depreciated exchange rate) relative to the marginal cost-benefit ratio of operating a service node, an increase in the opportunity cost of staking Loki and operating a service node causes the staking requirement that would support equilibrium to *decrease*. On the other hand, for a sufficiently high exchange rate of national currency for Loki (a sufficiently appreciated exchange rate) relative to the marginal cost-benefit ratio of operating a service node, an increase in the opportunity cost of staking Loki and operating a service node causes the staking requirement that would support equilibrium to *increase*. A more intuitive way to express this is as follows:

$$\frac{\partial}{\partial \bar{r}} \hat{s} \begin{cases} \leq 0 \;\forall\; 1 \leq \dfrac{\bar{c}}{\bar{\epsilon}\dfrac{\partial}{\partial n}\lambda\left(n^* \;\; \overline{|I|}\right)} \\ \geq 0 \;\forall\; 1 \geq \dfrac{\bar{c}}{\bar{\epsilon}\dfrac{\partial}{\partial n}\lambda\left(n^* \;\; \overline{|I|}\right)} \end{cases}$$

We can see quite clearly that the cost-benefit ratio in national currency of operating a service node in the Loki network determines whether the staking requirement ought to increase or decrease in response to a change to the opportunity cost of operating a service node. As the cost of operating a service node decreases relative to the reward for operating a service node in terms of national currency, we tend away from having to *increase* the staking requirement to support equilibrium as the opportunity cost of operating a service node increases, and have to *decrease* the staking requirement to support equilibrium once costs fall below rewards. This is important, for we can expect over time for the exchange rate of Loki to increase and the cost of operating a service node to decrease, and thus for the latter case to become the more dominant.

Summary, analytics of the staking requirement which supports equilibrium

We have identified the effect of a change of four variables on the staking requirement which implements an equilibrium in which $\overline{|I|}$ symmetric rational agents in the Loki network provide n^* service nodes: the number of service nodes we wish for each actor to operate, operating costs, the exchange rate of national currency for Loki and opportunity costs. We can expect in the future for operating costs to decrease and the exchange rate to increase (appreciate). As the number of service nodes we wish for each actor to operate decreases, the staking requirement which supports equilibrium increases. As operating costs decrease, the staking requirement which supports equilibrium increases. As the exchange rate of national currency for Loki increases (Loki appreciates), the staking requirement which supports equilibrium increases. So we can expect in the future for the staking requirement which supports equilibrium to increase *ceteris paribus*.

The confounding factor in this analysis is the effect of opportunity costs. We can expect over time for costs to decrease and the exchange rate to appreciate, so we can expect to find that the staking requirement which supports equilibrium will have an inverse proportional relationship with the rate at which opportunity costs of operating a Loki service node accrue. Over time therefore, as economies operating on national currencies increasingly enter either secular stagnation or suffer recessions, we can expect for the staking requirement which supports equilibrium to increase. For those periods where economies operating on national currencies experience strong activity however, we can expect the staking requirement which supports equilibrium to decrease *ceteris paribus*.

4 Calculations

It will be valuable now to calculate some specific solutions to the staking requirement design problem using the cryptoeconomic solution developed above and establish some responses to parameters around that equilibrium point. First, however, we will need to specify a specific form for the revenue function $\lambda(n \;\; N)$. Loki's revenue function depends on its emissions curve, which in turn depends on the reward for processing a Block in its Blockchain.

4.1 Specifying and modelling a revenue function

The form of the Block reward B_r is an inverse exponential function in Block height variable B_h so that the Block reward is decreasing over time, and thus the growth rate of Loki's total supply stabilising. We have that

$$B_r = \alpha + \exp\{-\beta(B_h)\}$$

where $\beta(B_h)$ is increasing in B_h. As B_r is emitted over time by the processing of Blocks, some 45% of it is made available for miners, 5% is made available for the Loki governance pool and 50% is made available for service nodes. Service nodes are not paid out on a pro-rata basis, but rather are

tabulated in an ordered list of which the top service node is paid the entire reward available for service nodes. That node is then replaced to the bottom of the list, and each node moves up the list by one entry. Roughly speaking therefore, a service node will be paid out once every N processing periods. An appropriate way to model the revenue function over the Block processing period for any given actor running n service nodes on the Loki network nonetheless is as follows

$$\lambda(n \quad N) = n\left(\frac{1}{N}\widetilde{B_r}\right)$$

where $\widetilde{B_r} = .5B_h$. The marginal revenue for an actor on the Loki network operating n service nodes is therefore (since, of course, $N = \sum_{i \in I} n_i$)

$$\frac{\partial \lambda(n \quad N)}{\partial n} = \frac{N - n}{N^2}\widetilde{B_r}$$

As a check that the assumptions of our analysis hold above and playing a little fast and loose with notation we can see that marginal revenue is indeed concave in the operation of service nodes. We have that

$$\frac{\partial^2}{(\partial n_i)^2}\lambda(n_i \quad N) = \widetilde{B_r}\frac{\partial^2}{(\partial n_i)^2}\frac{\sum_{j \neq i} n_j}{\left(\sum_{j \in I} n_j\right)^2} = -\frac{2\sum_{j \neq i} n_j}{\left(\sum_{j \in I} n_j\right)^3}\widetilde{B_r}$$

As it is rather difficult to conceptualise what a *negative* operation of service nodes would be, we can safely assume that $n_j \geq 0 \; \forall \; j \in I$, and so we have that

$$\frac{\partial^2}{(\partial n_i)^2}\lambda(n_i \quad N) \leq 0$$

Now within this revenue function we have one final problem before we can pick parameters relatively freely. That is that we wish for a given desired equilibrium in the provision of service nodes to be *feasible* in the sense that actors are in fact incentivised to operate service nodes. We would observe this being the case so long as the staking requirement which would support an equilibrium is positive (were it to be negative, the Loki network would have to reverse the staking requirement so that stakes were *provided* to actors). So, for our revenue function we must have that $\hat{s} \geq 0$. Now since $\bar{r} \geq 0$ in all but extreme situations, we have

$$\hat{s} \geq 0 \Leftrightarrow \frac{\partial}{\partial n}\lambda\left(n^* \quad \overline{|I|}\right) \geq \frac{\bar{c}}{\bar{\epsilon}}$$

Inputting the form of $\lambda\left(n^* \quad \overline{|I|}\right)$ and picking a symmetric equilibrium provision of service nodes n^* by $|I|$ actors, we see that for $\hat{s} \geq 0$ we require that

$$\frac{n^*(|I| - 1)}{(n^*|I|)^2}\widetilde{B_r} \geq \frac{\bar{c}}{\bar{\epsilon}}$$

The relevant variable which may ensure this requirement is met is the asymptote α of the Block reward function. As the Loki Blockchain grows, we find that the Block reward converges to this asymptote, for

$$\frac{\partial \beta}{\partial B_h}B_h \geq 0 \Rightarrow \lim_{B_h \to \infty} B_r = \alpha$$

So, inputting this limit into the requirement immediately above, we have that for $\hat{s} \geq 0$ we require

$$\frac{n^*(|I|-1)}{(n^*|I|)^2}.5\alpha \geq \frac{\bar{c}}{\bar{\epsilon}}$$

Any particular form for the parameters of the Block reward must maintain this condition for the Loki network to be feasible in the sense of requiring non-negative stakes. This is difficult to guarantee universally, so we will suppose the following form for our calculations which appears reasonable at the present time:

$$B_r = 28 + 2^8 \exp\{(-10 \times (10^{-6})) \times B_h\}$$

The design problem now being fully specified for a given symmetric equilibrium provision of service nodes n^* by $|I|$ actors, we may now calculate various staking requirements for specific parameterisations of operating cost $\bar{c}$, exchange rate $\bar{\epsilon}$, opportunity cost $\bar{r}$ and Block height B_h.

4.2 Staking requirement under specific parameterisations

Let us suppose, to begin with, that the equilibrium Loki wishes to achieve is a symmetric operation of 1 service node by 8,000 actors in the network. This would make Loki not dissimilar to TOR in terms of the distribution of routing and data transfer services and therefore would offer (in equilibrium) privacy-preserving Service Node Apps of a similar security. These objectives established, let us suppose the following parameterisation based on extant data at the present time for the Loki network.

Operating Cost	Opportunity Cost	Exchange Rate	Block Height	Processing Time
400USD p.a.	3% p.a.	.325USD	129,600	2 minutes

Table 1: Parameterisation for equilibrium where 8,000 actors operate 1 service node each

Under this baseline parameterisation, the staking requirement which supports such an equilibrium as is consistent with the objective of having 8,000 actors provide 1 service node each is **12648.80Loki, or 4110.86USD**. While these actors earn less than .01USD per Block processed in equilibrium, this translates to a yearly accounting profit of some 123.39USD for operating a service node in the Loki network which hosts routing and data transfer services for Service Node Apps. In equilibrium, of course, this means that actors in the Loki network obtain an accounting return on investment of 3% p.a for operating service nodes.

Now this parameterisation assumes a rate of return commensurate with the long-term average rate of return on Australian government debt at the time of writing. Of course, the true opportunity cost of staking sufficient Loki to operate service nodes is likely to be substantially higher as Australian government debt does provide something of a baseline return. So, an alternative parameterisation substitutes a rate of return more commensurate with good commercial rates of return.

Operating Cost	Opportunity Cost	Exchange Rate	Block Height	Processing Time
400USD p.a.	7% p.a.	.325USD	129,600	2 minutes

Table 2: Alternative parameterisation for equilibrium where 8,000 actors operate 1 service node each

Under this parameterisation, the staking requirement which supports such an equilibrium as is consistent with the objective of having 8,000 actors provide 1 service node each is **30,030.53Loki, or 9,759.92USD**. While these actors again earn less than .01USD profit per Block processed in equilibrium, this still translates to a yearly profit of some 123.39USD. In equilibrium however, of course, actors now earn an accounting return on investment of 7% p.a.

Now in the early stages of developing the network of service nodes over which SNApps will be provided by the Loki system, it might be aspirational to suppose that a network with the security of TOR might be achieved in equilibrium. Instead, it might be better to set more realistic objectives for equilibrium which might be revised over time. We might suppose then, that initially we might wish to set that staking requirement which supports an equilibrium in which 1,000 actors operate 1 service node each with the following parameterisation.

Operating Cost	Opportunity Cost	Exchange Rate	Block Height	Processing Time
400USD p.a.	7% p.a.	.325USD	129,600	2 minutes

Table 3: Parameterisation for equilibrium where 1,000 actors operate 1 service node each

Under this parameterisation, the staking requirement which supports such an equilibrium as is consistent with the objective of having 1,000 actors operate 1 service node each is **166,283.20 Loki, or 54042.04USD**. Actors earn an accounting profit of 3787.13USD and an accounting rate of return of 7% in equilibrium in this scenario. Clearly this is a difficult equilibrium to obtain given that the staking requirement it demands is on the order of a deposit for a house, so we might try to relax the strict requirement that each actor provide but 1 service node in equilibrium. We might wish to set that staking requirement which supports and equilibrium in which 1,000 actors operate 2 service nodes each with the following parameterisation.

Operating Cost	Opportunity Cost	Exchange Rate	Block Height	Processing Time
400USD p.a.	7% p.a.	.325USD	129,600	2 minutes

Table 4: Parameterisation for equilibrium where 1,000 actors operate 2 service nodes each

Under this parameterisation, the staking requirement which supports an alternative equilibrium which is consistent with the objective of having 1,000 actors operate 2 service nodes each is **74350.39Loki, or 24,163.88USD**. Actors earn an accounting profit of 7574.26USD in this equilibrium and an accounting rate of return of 7% p.a. Now this is still a difficult staking requirement to obtain, so in the early phases of developing the network of service nodes over which SNApps will be provided by the Loki system it may be worthwhile to seek to allow actors to pool funds in order to stake sufficient Loki to operate service nodes. But we might also wish to consider more generally how the staking requirements in response to the change of variables around this desired equilibrium.

4.3 Equilibrium responses to changing parameters

Now let us suppose that we wish to implement an equilibrium in which 8000 actors provide 1 service node each and take our alternative parameterisation above (specified in Table 2) whereby we allow for an opportunity cost of 7% p.a. in equilibrium. It will be interesting to investigate the response of the staking requirement to changes of the objectives of the Loki network and opportunity cost allowed for under this parameterisation. We will run projections for changes to the number of desired service nodes operated by a given actor in equilibrium, the number of actors overall, and the opportunity cost allowed for. We will not run projections for the effect of an increasing Block height. The reason for this is that it can be readily verified that, with the Block reward rate being such as it is, Block height has little effect on marginal revenue and thus staking requirement until it becomes very large indeed, and so can be fairly easily set aside.

Take first the effect of number of desired service nodes operated by a given actor in equilibrium. This is shown in figure 1. What we can see is that as the number of desired service nodes we wish to be operated by any given actor in equilibrium decreases, the staking requirement must increase, and at an increasing rate. The reason for this is quite obvious – it must become more difficult to stake sufficient

Loki to become a service node, and for this to disincentivise doing so by eroding return on investment.

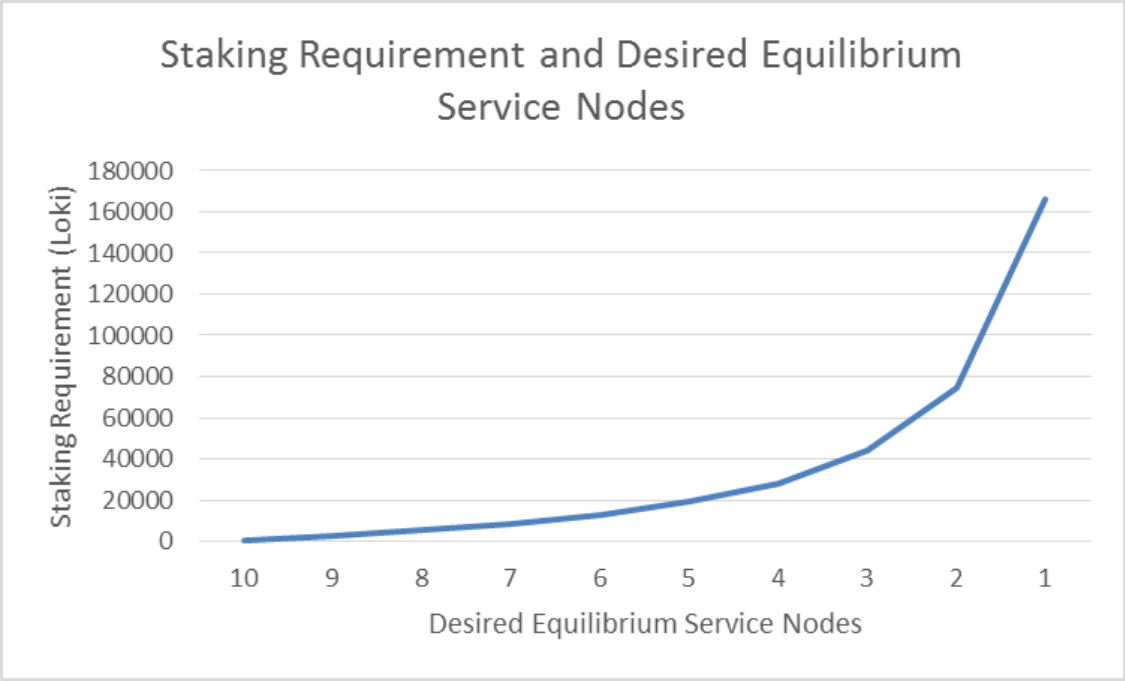

Figure 1: Effect on staking requirement of changing the number of desired service nodes operated by a given actor in equilibrium with 8,000 actors and the parameterisation in Table 2

Over time therefore, should the Loki network begin with a fairly relaxed attitude toward the number of desired service nodes operated by a given actor in equilibrium, and then, with a view to the security of the network, tighten this attitude, the staking requirement which will support these objectives will increase. Relative to a particular size of the Loki network in other words, the greater the desire for its security in terms of providing privacy, the greater the staking requirement will have to be which implements those desires in the equilibrium provision of service nodes.

Now take the effect of an increase in the number of actors present in the Loki network. In figure 2 we can see that given a desired operation of service nodes in equilibrium, the staking requirement decreases as more actors enter the network. The reason for this is a little subtle.

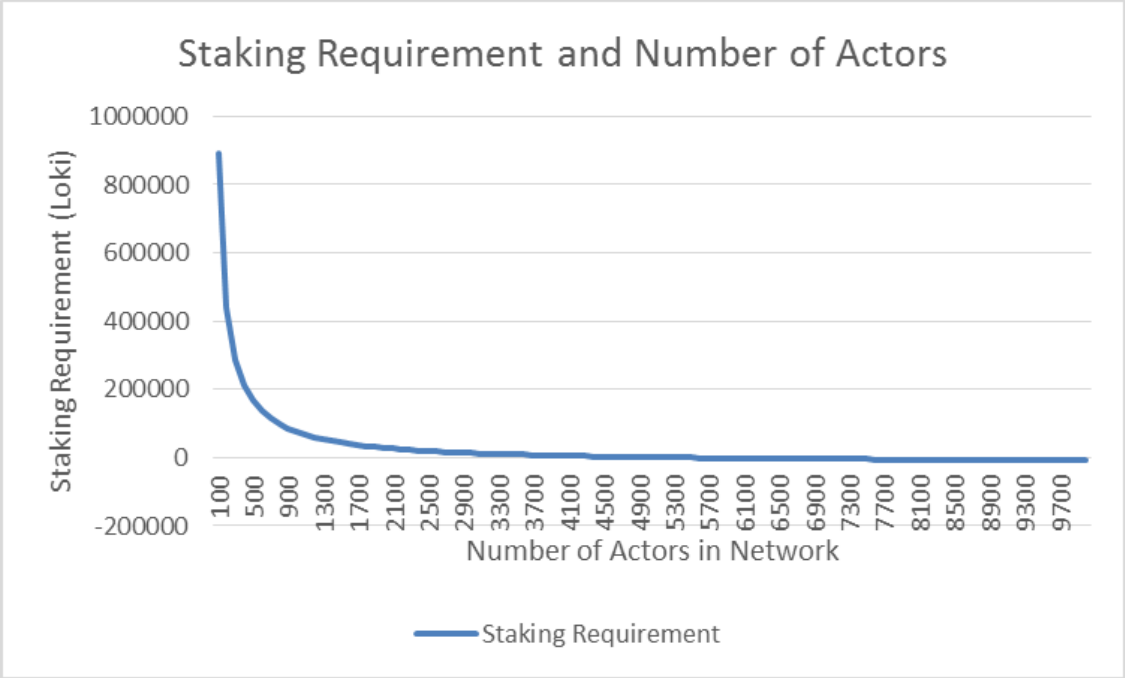

Figure 2: Effect on staking requirement of changing the number of actors in the network when desired operation of service nodes is one per actor given the parameterisation in Table 2

As more actors enter the network, they erode the revenues earned by any given service node across the network spread across Block processing periods. For a given parameterisation of the system then, the staking requirement has to decrease to incentivise the provision of service nodes by restoring the accounting rate of return. Over time then, unless the number of actors in the network remains fairly stable, we can imagine that there may be countervailing pressure against pure security desires on the staking requirement to decrease to restore accounting rates of return which incentivise the provision of service nodes on the Loki network.

Now finally take the opportunity cost which is allowed for. There are good reasons we may wish to allow this to vary over time, for in its early years Loki may be a relatively risky investment until the network develops more fully. To offset this risk, we might wish to set the opportunity cost allowed for to be relatively high (reflecting the opportunities forgone by allocating resources to operating service nodes within the Loki network) and then decrease it over time. The effect of this on the staking requirement given a desired equilibrium in which 8,000 actors provide 1 service node each can be seen in figure 3.

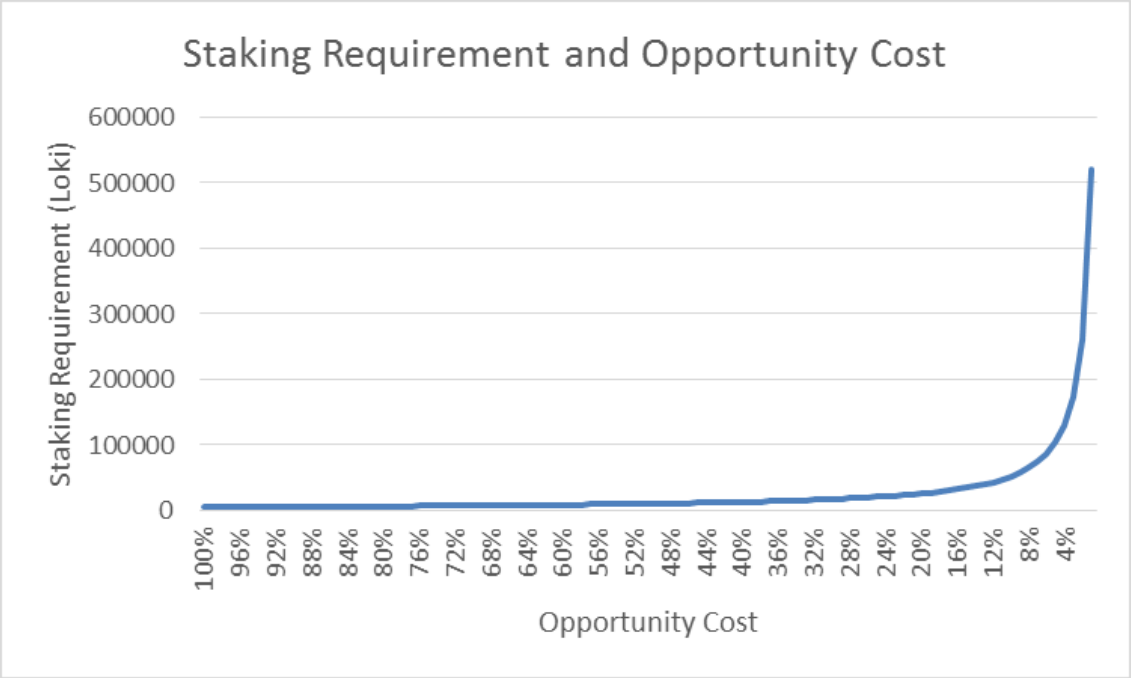

Figure 3: Effect on staking requirement of a change of opportunity cost allowed for given a desired equilibrium in which 8,000 actors provide 1 service node each and the parameterisation in Table 2

As we allow for a lesser and lesser opportunity cost, the staking requirement which will support an equilibrium in which 8,000 actors provide 1 service node each, given the parameterisation in Table 2, will increase. The reason for this, again, is a little subtle and involves nuanced cryptoeconomic reasoning. As we decrease the opportunity cost allowed for given a desired equilibrium and parameterisation, the opportunities for investing outside of the Loki system decrease in value, and it becomes more attractive to invest in the Loki system by operating service nodes. In order to preserve the security of the network then by ensuring the equilibrium operation of service nodes by actors in the network does not change, the staking requirement must increase to disincentivise the operation of more than that number of service nodes by eroding return on investment.

So over time, provided that the number of actors on the Loki network remains fairly constant, we can expect that for a given parameterisation (here that in Table 2) and a desired equilibrium (here one in which 8,000 provide 1 service node each) the staking requirement for service nodes in the Loki network to increase. This is because of the desire to maintain security on the network by ensuring that no one actor has an incentive in equilibrium to operate more than a certain proportion of the service nodes in the Loki network, and the decreasing allowance for opportunity costs as the Loki network stabilises. The staking requirement will have to increase to disincentivise operating more than the desired number of service nodes in equilibrium, and to offset the increased attractiveness of the Loki network relative to the opportunities forgone by operating service nodes within it.

5 Conclusion: solutions to Loki's cryptoeconomic problem

Loki is a Blockchain network oriented toward the provision of privacy-preserving services over a network of service nodes. The salient cryptoeconomic problem we addressed here was how to incentivise service nodes in a manner compatible with the objectives of the Loki network, in particular decentralisation and privacy. We used cryptoeconomic game theory to characterise this problem and formulate a solution to the design problem.

An actor in the Loki network will stake sufficient Loki to operate n service nodes among N on the network if the profit $\pi(n \;\; N)$ to be gained from doing so is greater than the opportunity cost of investing the stake ns in terms of national currency (the exchange rate thereof for Loki being ϵ) to obtain a return r

$$\pi(n \;\; N) \geq r(\epsilon ns)$$

and *only if* this is the case *and* they have ns Loki ($n\epsilon s$ in national currencies) available to stake. So the *economic profit* obtained from staking sufficient Loki to operate n service nodes when the total network of service nodes is N is given by

$$\pi(n \;\; N) - r(\epsilon ns) = \epsilon\lambda(n \;\; N) - [c(n) + r(\epsilon ns)]$$

where $\lambda(n \;\; N)$ is the reward allocated to n service nodes when there are N in the network and $c(n)$ is the cost of operating those nodes. A rational agent in the Loki network will therefore operate n^* service nodes defined as follows

$$n^* = n{:}\frac{1}{s}\frac{\partial}{\partial n}\lambda(n \;\; N) = r + \frac{1}{\epsilon s}\frac{\partial}{\partial n}c(n)$$

which, after introducing certain reasonable assumptions which exogenise certain variables, reduces to

$$n^* = n{:}\frac{1}{s}\left[\frac{\partial}{\partial n}\lambda(n \;\; N) - \frac{\bar{c}}{\bar{\epsilon}}\right] = \bar{r}$$

In equilibrium, each actor i in the Loki network operates n_i^* service nodes defined as follows

$$n_i^* = n_i{:}\frac{1}{s}\left[\frac{\partial}{\partial n_i}\lambda\left(n_i \;\; \left[n_i + \sum_{j\neq i\in I} n_j^*\right]\right) - \frac{\bar{c}_i}{\bar{\epsilon}}\right] = \bar{r}_i$$

This equilibrium is a pure strategy Nash equilibrium. We found as a result that the staking requirement $\hat{s}$ which would support a symmetric equilibrium in which rational agents in the Loki network provide n^* service nodes is given by

$$\hat{s} = \frac{1}{\bar{r}}\left[\frac{\partial}{\partial n}\lambda\left(n^* \;\; \overline{|I|}\right) - \frac{\bar{c}}{\bar{\epsilon}}\right]$$

where $\overline{|I|}$ is the number of actors $i \in I$ in the Loki network. If ϕ is the proportion of service nodes any given actor must operate in order to undermine the privacy in SNApps provided on the Loki network, we may define the approximate set of acceptable staking requirements (those which will support an equilibrium compatible with Loki's objectives) by picking an arbitrary number of service nodes N to be provided homogenously across the network and so define Ω, the set of acceptable staking requirements, as follows

$$\Omega = \{s = \hat{s}(n^* \;\; N){:}\, n^* \leq \phi N\}$$

where $\hat{s}(n^* \;\; N) = \frac{1}{\bar{r}}\left[\frac{\partial}{\partial n}\lambda(n^* \;\; N) - \frac{\bar{c}}{\bar{\epsilon}}\right]$. To undermine the privacy of the Loki network by providing $n_\rho > \phi N$ service nodes, a rogue actor ρ must value this undermining by *at least* approximately

$$\frac{v_\rho}{\bar{\epsilon}} = \lambda\left(n^* \;\; n^*\overline{|I|}\right) - \lambda\left(n_\rho \;\; \left[\left(n_\rho - n^*\right) + n^*\overline{|I|}\right]\right) + (\bar{r}\hat{s} + \bar{c})\left(n_\rho - n^*\right)$$

which is strongly increasing in *substantial* multiples of the opportunity cost of staking Loki to operate service nodes *as well as* the server cost.

We also established the effects on the staking requirement which will support an equilibrium in which $\overline{|I|}$ symmetric rational agents in the Loki network provide n^* service nodes of the number of service nodes we wish for each actor to operate, operating costs, the exchange rate of national currency for Loki and opportunity costs. These analytical effects notwithstanding, we also investigated various numerical iterations of the design problem to discover the response of the staking requirement to various objectives and parameterisations of the Loki network.

We found that given a particular parameterisation based on extant conditions in the Loki network, a fairly reasonable opportunity cost of 7%, and a desired equilibrium (in which 8,000 actors provide 1 node each) which roughly mirrors the structure of TOR, a staking requirement of 5420.92.53 Loki, or 1761.80USD. This generates an accounting profit of 123.39USD p.a. and, of course, an account return on investment of 7% p.a. in equilibrium. This, however, is a very strict objective for the Loki network to begin with, and so we considered alternative scenarios which might be adopted in the interim. We also considered in this numerical context how the staking requirement which would support a TOR-like equilibrium would change in response to the desired number of nodes, the overall number of actors in the network, and the opportunity cost allowed for. We found, as a result, that we can expect the staking requirement that would support a TOR-like equilibrium to increase over time as a result of seeking to ensure the security of the network and the declining opportunity cost allowed for relative to the attractiveness of operating service nodes in Loki.