Reward Sharing for Mixnets

Claudia Diaz [†], Harry Halpin [‡], and Aggelos Kiayias [§]

Nym Technologies SA

Abstract. We present a reward sharing scheme for incentivized network privacy infrastructures such as the Nym mixnet. Given a bootstrapping reserve and a bandwidth pricing mechanism, our model enables a decentralized, economically sustainable mixnet that can scale, as increased usage translates into fees that allow the mixnet to grow to meet demand. Our scheme periodically selects mix nodes to mix packets proportionally to their *reputation*, which signals the confidence of stakeholders in the node's reliability and performance. Selected mix nodes are then rewarded proportionally to their reputation and performance, and share their rewards with the stakeholders supporting them. We prove the properties of our scheme with a game-theoretic analysis, showing that the equilibria promote decentralization and mixnet performance. We further evaluate the scheme empirically via simulations that consider non-ideal conditions and show that the mixnet can be viable under realistic assumptions.

1 Introduction

The Nym network[1] is currently deploying an incentivized mixnet to provide a generic message-based communication privacy infrastructure for applications [11]. This paper describes the economic model of the Nym network and the reward scheme used to incentivize mix nodes to reliably mix packets and effectively protect the metadata of users' communications, including financial and other blockchain-enabled services but also applications such as instant messaging or email. To our knowledge, this is the first incentive system that fairly shares rewards the nodes in an anonymous overlay system like a mixnet for provisioning privacy for users.

The two key ingredients of privacy protection for communications' metadata are: a large user base, because *anonymity loves company* [15]; and a technical design and implementation that leverages the user base and translates it into large *anonymity sets* [38] for all communications routed through the network. In terms of technical design the Nym mixnet is, like Tor [17], an *overlay* network where data packets from end users are routed via multiple intermediaries, each performing cryptographic transformations on the data before forwarding to the next hop, until the packet is sent to its final destination. The aggregation of packets from many users at each intermediary is crucial to assemble the large anonymity sets that provide effective privacy protection for all users [12, 41]. Recent results add to the evidence that a key advantage of architectures that distinguish between 'end user' and 'intermediary' roles, compared to solutions where all participants are *both* simultaneously end users and intermediaries for others (e.g., like Dandelion [22] or Lightning Network [40]), is that in the latter, thin traffic per intermediary results in poor anonymity sets that do not leverage the scale of the network [6, 42]. In contrast, in architectures where routing is the same for all traffic [1, 8, 11, 17, 39], users are aggregated in one anonymity set that scales with the user base. In addition, the Nym mixnet is designed to protect communication anonymity against global network adversaries with visibility over all internet communications, which is achieved by routing messages independently, introducing a randomized per-hop 'mixing latency', and adding cover traffic.

Adequately servicing a large user base requires computing resources to scale up operations and meet demand while reliably providing a high quality of service; as well as software usability, maintenance and ease of integration with a broad set of applications, which itself involves significant

[†] Associate Professor at KU Leuven and Chief Scientist of Nym Technologies SA.

[‡] CEO of Nym Technologies SA.

[§] Chair in Cyber Security and Privacy at the University of Edinburgh and Chief Scientist at IOHK. Advisor to Nym Technologies SA.

[1] `https://nymtech.net`

development effort. Furthermore, anonymity networks are decentralized solutions that need to be operated by non-colluding entities, meaning that a large number of independent node operators need to be signed up to run the network.

Tor[2] has had a remarkable degree of success in engaging volunteers who contribute their own resources to operate the network as well as in obtaining public financing and donations to fund software development and community outreach. There are however limitations to volunteer-driven non-profit models. For example, the Tor network steadily grew to six thousand nodes between its launch in 2004 and 2015, but its growth has stalled since and in the last seven years the number of nodes has remained between six and seven thousand,[3] indicating that there is a limited pool of individuals and organizations willing and able to fund out of their own pocket such network operations [27]. A limited supply of well-meaning volunteer operators poses a problem not only for scalability, but also for security: Adversaries can populate the network by simply volunteering to run enough nodes, and thus compromise anonymity for many users (who need that some intermediaries are honest to achieve privacy). Dependency on public funding programs has also made the project resources for development vulnerable to changes in funding priorities.[4]

Nym has opted instead for an incentivized model where the operators of mix nodes are compensated for their resources and effort, and users can pay a fee for the obtained private bandwidth. The fee is determined via a dynamic posted-price mechanism that accounts for node costs and a rate of profit for the network. This enables a market for private bandwidth that allows the mixnet to arbitrarily scale to meet demand while covering operational costs. Participating as a mix node in an anonymous communication infrastructure involves costs in the form of computation (to perform cryptographic transformations on the traffic) and bandwidth (to relay the traffic). Without compensation for costs and labour, it is difficult to attract sufficiently many independent mix node operators who are appropriately resourced to deliver a high performing network that can arbitrarily scale up to meet demand.

The distribution of rewards to mix nodes further rewards good node performance and cost-effectiveness and motivates stakeholders to support nodes (culminating in a reputation score per node) — while penalizing under-performing nodes and nodes that for some reason fail to attract stakeholder support. By sampling mix nodes to be active in the mixnet based on their reputation, Nym makes it difficult for adversaries to populate the mixnet with malicious nodes. Adversaries not only need to run a set of mix node servers (just as they would for running Tor relays and populating the Tor network), but they also need to attract enough support from stakeholders (or acquire themselves vast amounts of NYM) for those nodes to have high reputation, and thus high chances of selection for routing packets in the mixnet – all that while being in direct competition with other nodes for a finite amount of stakeholder support. A mix node that has poor performance or engages in malicious behaviour is accountable to stakeholders, who may withdraw their support if they are not satisfied with the node operations, thereby diminishing the node's opportunities for participation in providing the service and earning rewards for it. The system incentives are designed in such a way that stakeholders maximize their rewards when they support well-performing mix nodes that have high reputation, which in turn has the effect of populating the mixnet with nodes that are cost-effective and trusted by stakeholders to provide a reliable service to users.

Incentivized anonymity networks typically face a bootstrapping problem: both the privacy offered by the network and the capacity to fund its operations increase with the user base; while at the same time a usable and functional network needs to be already in place for the user base to be willing to pay for the privacy service. Nym addresses the problem of bootstrapping the mixnet with a reserve of funds called the 'mixmining pool' that is initialized with a quarter of the total NYM token supply. The reserve slowly releases rewards over time, providing funds to sustain the network in the first years, until the mixnet has gained enough popularity for user fees to become the primary source of income.

Taking these two sources of income into account (user fees and rewards from the mixmining pool), we adopt reward-sharing concepts from cryptocurrencies [7] and apply them to the setting of provisioning privacy in order to distribute the available rewards among nodes participating in the

[2] `https://www.torproject.org`

[3] `https://metrics.torproject.org/`

[4] One example is the 2020 cut of funding of the Open Technology Fund: `https://www.politico.com/news/2020/07/30/internet-freedom-projects-funding-388983`

Nym mixnet and the stakeholders supporting them. Our reward-sharing scheme is shown to possess equilibria that fairly and efficiently distribute the rewards in a manner that is Sybil resistant, thus creating the conditions for the community of stakeholders to recruit the nodes needed to provision privacy with high quality of service and at the scale of demand.

We complement the theoretical analysis with an empirical evaluation of the reward scheme in non-ideal conditions, which we conduct via simulations. We examine two hypothetical scenarios, one with low traffic and another with fast growing traffic that triggers network scaling, and study the rewards given to participants in both scenarios. We specify the assumptions and parameter values used in the evaluation and discuss the impact of different parameters on the results. The simulation results indicate that, under reasonable assumptions, our scheme can support an economically viable network, which can either serve rapidly scaling demand or initially grow slower. We note that the presented theoretical results cannot be interpreted as determining the amount of rewards that participants can expect in the real world, which may be higher or lower depending on the specific combination parameters of the scenario in question (e.g., rate of staking by stakeholders and overall distribution of node reputation). Rather, these empirical results serve to illustrate the functioning and dynamics of our scheme when the system is not in equilibrium as well as the effects of reputation on the viability of running mix nodes.

The paper is organized as follows: First, an overview of the relevant components of the Nym network is in Section 2. The incentives and reward-sharing scheme are described in Section 3, along with the equilibrium analysis. Section 4 introduces our simulation framework and Section 5 describes in detail the experimental setup we used to conduct experiments. Section 6 offers a number of simulations showing that the reward-sharing scheme leads to sustainable rates of return under various realistic conditions. We summarize relevant related work in Section 7 and conclude with a summary and directions for future work in Section 8.

2 System model

The Nym network [11] implements an anonymous communication service that relies on the NYM[5] token to take usage fees and reward the operators provisioning privacy. The system model from the perspective of service functionality is shown in Figure 1. The core component of Nym is a **mixnet** (mix network) that provides multi-hop anonymous packet routing functionalities to **end users**. In addition, **gateways** act as interface between end users and the mixnet, while a set of **validators** maintain the Nyx blockchain,[6] which broadcasts public Nym network parameters, executes the Nym smart contracts, and keeps the ledger of NYM transactions. Thus in addition to recording NYM transactions and ownership, validators of the Nyx blockchain serves a similar purpose as directory authorities in Tor. We describe in the rest of this section these different components from a service functionality perspective, as well as introduce the underlying economic model and the flows of NYM token between components.

2.1 The Nym mixnet

The Nym mixnet encodes data in a cryptographic packet format similar to Sphinx [10]. Packets are then routed through multiple mix nodes, each performing a decryption on the packets and reordering the flow of packets they route. The mixnet is composed of continuous-time mix nodes organized in a layered topology, such that messages traverse one mix per layer [11,39]. The number of nodes per layer, called the *mixnet width* (denoted by W), is proportional to the throughput of the mixnet. Nym assigns an equal number W of nodes to each of the L mixnet layers, for a total of $A = LW$ *active nodes* in the mixnet. When choosing a packet route, in each layer all W mix nodes are selected with the same probability $\frac{1}{W}$, i.e., there are W^L possible mixnet routes, each selected with probability W^{-L}. As result, the A nodes that are simultaneously active in the mixnet perform an equal share of work routing packets. Note that this imposes minimum throughput requirements on mix nodes. Nodes with insufficient network or processing capacity may not be able to route their share of packets during peaks of traffic, resulting in poor node performance and diminished rewards.

[5] Denoted "NYM" to distinguish it from the Nym network itself.

[6] `https://blog.nymtech.net/nym-now-supports-smart-contracts-2186da46bc7f`

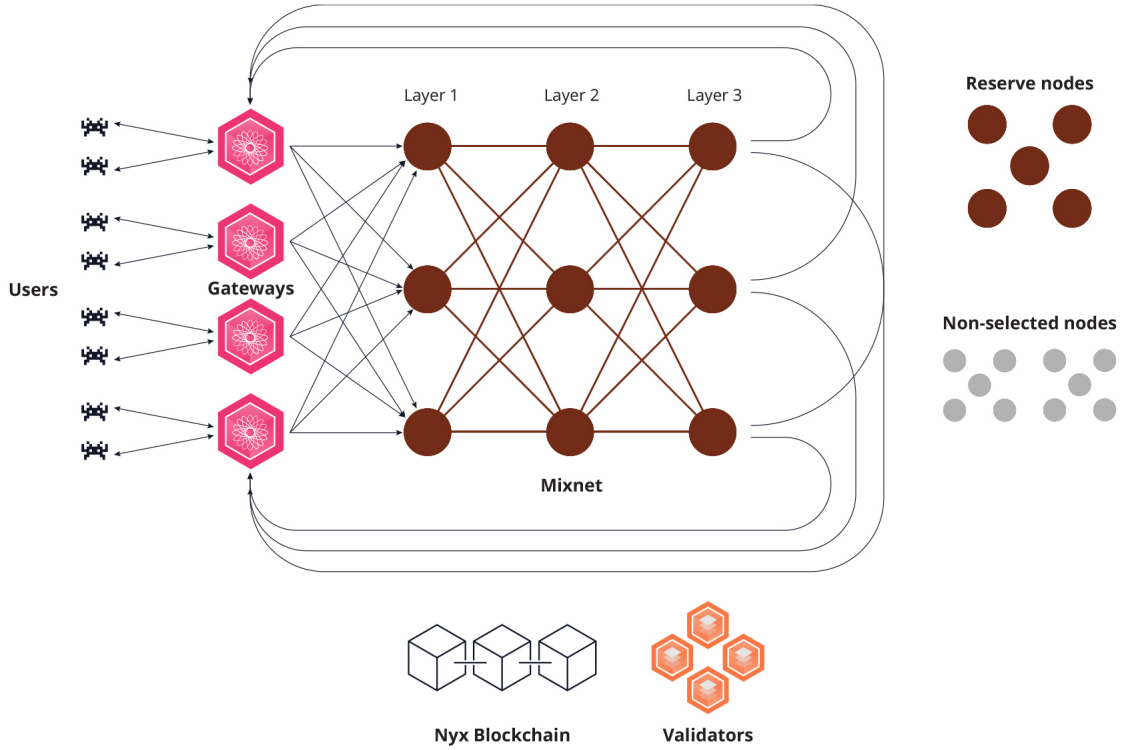


Fig. 1: Nym system model

The growth in demand for mixnet bandwidth can be met by increasing the mixnet width W, with the extra nodes linearly increasing overall mixnet throughput. In addition, the Nym network may increase (via software updates accepted by the majority of participants) the expected throughput of mix nodes, e.g., requiring additional bandwidth and processor cores per mix to handle more traffic.

The selection of $A = LW$ nodes and their assignment to L mixnet layers is refreshed periodically, at hourly *epochs* (hourly reconfiguration allows adjusting mixnet size to demand). Given a number N of registered *mix node candidates* such that $N > A$, and a periodic publicly verifiable random beacon [44], a smart contract can sample the set of $A = LW$ nodes selected to be *active* in the mixnet for the next epoch. Nodes are selected proportionally to their *reputation*, defined as the aggregate amount of token pledged and delegated to the node (see Section 2.4 for the distinction between these operations), relative to the *stake saturation point*, which is a system-wide parameter; i.e., a node's reputation takes values between zero and one, and the maximum reputation of one is reached when the token pledged and delegated to the node is equal (or superior) to the saturation point. High-reputation nodes have higher chances of selection for the mixnet than low-reputation nodes, as described in Section 3.2, and thus better opportunities for contributing to the service and earning rewards for their work.

Mixnet bandwidth demand may grow suddenly, requiring W to be increased significantly from one epoch to the next. To incentivize the existence of additional mix nodes that can provide extra capacity on short notice, our scheme selects an additional set of B nodes to be kept in *reserve* or *standby* for the epoch. These B nodes are also rewarded, albeit at a lower rate, for a total of $K = A + B$ nodes being rewarded, while the $N - K$ nodes that are not selected do not receive any rewards for that epoch. As shown in the next section, the reward scheme reaches equilibrium when there are $N = K$ mix node candidates with maximum reputation. In practice, we expect $N > K$, meaning that there is an excess of mix node candidates, of which K are sampled and rewarded per epoch.

2.2 Gateways

Gateways act as entry points to the mixnet, as first-layer mix nodes only accept traffic from gateways. To register with the Nym network, prospective gateway operators have to lock up a NYM token deposit and make their public keys available in a declaration added to the Nyx blockchain. A gateway declaration binds the deposit to its public key and allows all network participants to verify they are interacting with a legitimate gateway, preventing gateway impersonation.

Users acquire NYM in the open market and can deposit an amount of NYM to a smart contract in exchange for private bandwidth to be routed via the Nym mixnet. The amount of bandwidth (data) the users can buy for a certain amount of NYM (fee) is determined by a pricing mechanism as described in Section 3.3. When obtaining the bandwidth, users can tie it to a gateway of their choice (among all the registered gateways). Funding for gateways is allocated at this step as a fraction of the NYM fees deposited by the users for the bandwidth. The remaining fraction of NYM fees are held in the contract, to be distributed to mix nodes following our reward sharing scheme, introduced in Section 3.4. The user proves the payment to the chosen gateway and registers with it for the amount of purchased bandwidth. The bandwidth credential itself is a privacy-preserving anonymous credential [43] so the user does not reveal unnecessary information when using a gateway to access the mixnet [26].

In addition to forwarding packets from the user to the mixnet, the gateway keeps packets received for the user if needed, e.g., when the user device is offline, and it may bundle additional services (which may or may not be charged additionally), such as data storage or censorship circumvention functionalities. Gateways have incentives to attract and retain as many users as possible in order to receive more rewards, since they are purely rewarded based on work: a gateway that fails to attract users receives no rewards; while a popular gateway that attracts many users will receive substantial rewards. Users who run their own gateway get in practice a discount on their Nym network use (they are refunded the gateway share of the fee), at the cost of maintaining their own gateway server. In this paper we account for gateways when considering the income from fees, from which gateways take a cut, but otherwise leave out of scope an in-depth analysis of gateway incentives.

To prevent free riding from gateways, mix nodes locally keep count of the aggregate amount of traffic received from each registered gateway, which is compared to the paid bandwidth fees associated to the gateway in the smart contract managing the NYM bandwidth transactions. Mix nodes blacklist gateways that they detect engaging in free riding, i.e., that forward more traffic to the mixnet than the declared total that has been paid for. Once a gateway is blacklisted by a critical mass of mix nodes, its registration may be revoked and its deposit confiscated, to compensate for the costs caused by their free riding. Note that gateway registration deposits are not treated as staking: delegation is not possible and gateways are not rewarded proportionally to the deposited amount, which acts simply as locked collateral to disincentivize misbehaviour and compensate for any costs caused in case of abuse.

2.3 Validators

The validators are the nodes that maintain the Nyx blockchain, which records the ledger of NYM transactions and executes the smart contracts for distributing NYM rewards. The blockchain also acts as broadcast channel for the Nym network. It makes available to all participants the global network parameters, the publicly verifiable random beacon, the list of registered gateways and the public declarations of mix nodes, which include their public keys and contact information, necessary for users to prepare mixnet packets to send through the network.

Validators are funded by transaction fees that are necessary to interact with the Nyx blockchain. These fees are needed both to reward validators for their service and to protect the blockchain from spam. Transaction fees are paid by all Nym participants: end users converting token to bandwidth, mix nodes and gateways registering their node declarations, NYM stakeholders making token transfers, operator pledges or token delegation operations. The transaction fees are payable in NYM and in any other token that is accepted by the Nyx blockchain validators, who may also receive transaction fees from running smart contracts for others besides Nym. For the purposes of our analysis we factor transaction fees as part of the mix node operational costs, while leaving a

detailed analysis of validator economics out of the scope of this paper, as the paper is focused on mixnet incentives.

2.4 NYM token flows

Nym distributes rewards in NYM token that act as financial incentive to operate the service. As already mentioned, gateways receive a percentage of the fees paid by their users in exchange for mixnet bandwidth, while validators are funded by transaction fees paid by anyone writing to the blockchain. Mix nodes are rewarded from user fees as well as from a mixmining reserve, as we explain below. In addition to enabling fees and rewards, the NYM token is instrumental to determining *node reputation*, which is proportional to the aggregate amount of NYM token pledged and delegated to a mix node. The node reputation is expressed as fraction relative to the *stake saturation point*, which defines the maximum desirable amount of token accumulated on a single node. A node's reputation in turn determines its likelihood of selection for participation in the mixnet as well as the amount of rewards it receives for its work.

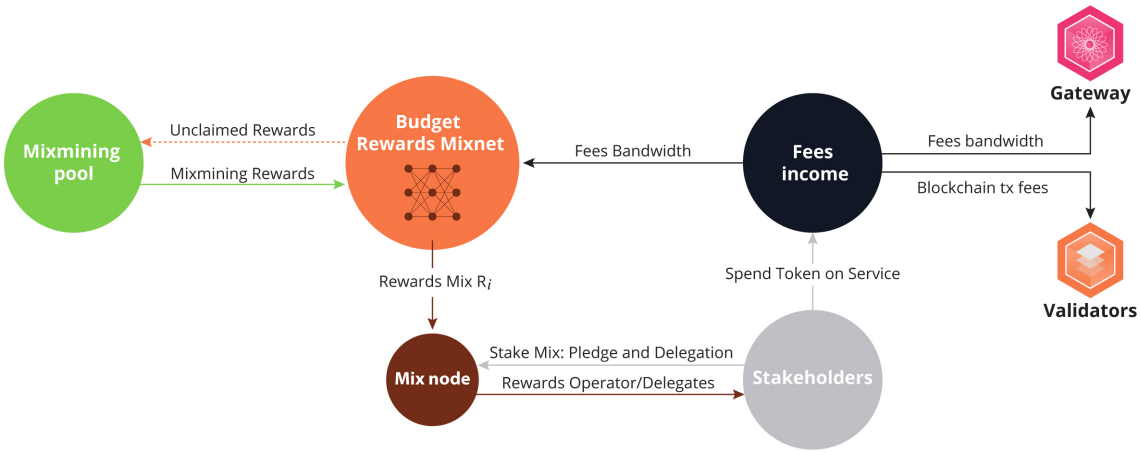


Fig. 2: Token flows.

Figure 2 depicts the main flows of NYM token between components. In a nutshell, the budget of rewards periodically available for distribution to mix nodes is the aggregation of income from two sources: (1) a mixmining pool reserve that periodically emits rewards, and (2) a fraction of the fees collected from network usage. Using our scheme, this budget of rewards is distributed among individual mix nodes, and further divided between each node's operator and its stakeholders, who are rewarded proportionally to the amount of token they have delegated to the node. Per-node rewards are dependent on the node's pledge, reputation and performance, and nodes may not realize their full reward potential if they under-perform or have low reputation, meaning that not all of the available reward budget is allocated. Any unclaimed rewards are returned to the mixmining pool for future distribution.

Stakeholders. Any holder of NYM token is a *stakeholder*. NYM stakeholders can deposit their token in exchange for an allowance of mixnet bandwidth. These deposits constitute fees that fund the mix nodes and gateways routing that bandwidth. All NYM stakeholders also pay transaction fees to validators for publishing information in the blockchain.

Additionally, stakeholders can **pledge** NYM token to become *mix node operators*. Pledging involves locking an amount of NYM in a smart contract, together with the registration of the node's public keys, address and parameters. This registers the node as a valid mix node candidate that can be chosen to route packets in the mixnet. It also enables all other stakeholders to **delegate** token to the node, to increase its reputation, participation in the mixnet and potential earnings.

If the node performs adequately and rewards materialize, *delegates* receive a share of the node's rewards.

The NYM token is thus required both by the end users (to pay for their private traffic as a utility token) and by the mix node operators that provision privacy to those users (as a reputation token needed for eligibility to be part of the network and thus receive rewards in exchange for work). All NYM stakeholders collectively determine node reputation by 'voting' with their token which node to support. This raises the cost of deploying Sybil attacks [19]: In order to get their nodes to be part of the Nym mixnet, adversaries need to either buy large amounts of NYM or somehow persuade enough NYM stakeholders to delegate their token to adversarial nodes.

Mixmining pool. The *mixmining pool* is a token reserve used to bootstrap the network by providing rewards to mix nodes during the initial years of operation. The pool is implemented as a smart contract initialized with an amount of NYM token that is locked and slowly released as rewards. The emitted rewards function in practice as inflation, in the sense that they increase the circulating supply of NYM. Note however that there is a finite supply of NYM, and thus the supply increase is bounded.

Every monthly interval, a fraction of the pool funds are emitted as rewards; i.e., the emission follows an exponential decay function. The emitted rewards become available for distribution to the mix nodes that contributed to the mixnet in any of the epochs over the interval (considering 720 hourly epochs per monthly interval). Note in any actual deployment the interval and epoch lengths may change. Some of the rewards available in an interval may remain unclaimed, e.g., due to poor performance or to low levels of node reputation. In such cases, those funds are returned to the pool and distributed in subsequent intervals. These bootstrapping reserve rewards are necessary as nodes need to cover operational costs even if the user traffic is initially insufficient to bring in enough fees to sustain the network. Once usage increases, fees can replace the pool as main source of income for the network.

3 Reward sharing scheme

This section describes our rewards mechanism and offers a theoretical analysis of its equilibrium properties. The reward sharing scheme aims to incentivize the set of NYM stakeholders to coalesce around a target number of well-performing, cost-effective operational mix nodes, relying on the "wisdom of the market" to assign reputation in terms of pledging and delegating NYM tokens to mix nodes.

We have two main objectives for our mechanism: (i) there exists an equilibrium where rational, utility-maximizing actions by the stakeholders lead them to propose and operate a sufficient number of well-functioning nodes that can be used to populate the mixnet, (ii) a financial impediment should be imposed to any stakeholder who attempts to control multiple nodes at the same time as in a Sybil attack [19].

We design and analyze a mechanism for the above objectives under two fundamental assumptions: (i) there is a diverse distribution of stake across a fairly large set of stakeholders; in particular, the number of stakeholders exceeds the number of nodes required by the mixnet; (ii) the rewards offered by the system in NYM token are sufficient to fund the operational costs of the mixnet; i.e., operators rewarded in NYM can use the token to offset their costs. We return to these assumptions validating them experimentally in Section 6.

The parameters and notations we use to describe the mechanism are the following:

- L, the number of layers in the mixnet.
- W, the width of the mixnet (i.e., number of mix nodes per layer).
- $A = LW$, the number of active nodes in the mixnet.
- B, the total number of idling nodes that are kept 'on reserve'.
- $K = A + B$, the total number of mix nodes that receive rewards for their contributions in a certain epoch.
- N, total number of mix node registrations.
- R, the total amount of rewards in NYM available for the mixnet in an epoch.

- n, the total number of stakeholders.
- s_i, the stake of the i-th stakeholder expressed as a fraction of the total circulating supply.
- M, a random variable expressing the number of packets routed by the mixnet per epoch.
- M_i, a random variable expressing the number of packets processed by the i-th mix node per epoch.
- $C_i(x)$, the cost declared by the i-th node to route x packets.
- μ_i, the profit margin declared by node i.
- ρ_i, the performance factor associated with node i, defined as percentage of correctly routed packets, which we assume to be publicly available.
- β, the saturation level for nodes (set by default to $\frac{1}{K}$).

We note that it is beyond the scope of the current exposition to detail how ρ_i is estimated. One straightforward option is to delegate this task to dedicated entities trusted to correctly report measurements, e.g., a bandwidth scanner[7] such as those used to measure performance in Tor [17]. More decentralized solutions are also possible; e.g., having a larger number of entities send measurement messages and issue verifiable statistical data "on-chain" that can then be averaged publicly to compute an estimated ρ_i per node [11]. We leave the detailed specification of such a decentralized mechanism as the subject of follow-up work, while considering here that accurate ρ_i are available for all nodes.

We divide the description of the mechanism in the following five subsections: Section 3.1 describes how stakeholders propose nodes and become operators; Section 3.2 explains how mix nodes are selected and assigned to the mixnet; the bandwidth pricing mechanism is explained in Section 3.3; the algorithm for distributing rewards among individual mix nodes and stakeholders is described in Section 3.4; and, finally, Section 3.5 provides the equilibrium analysis.

3.1 Registering a mix node

A prospective operator who wishes to run a mix node must **pledge** some of their NYM tokens as initial stake to register the node. These pledges will be specially treated by the reward function to ensure that operators are rewarded for having "skin in the game". Pledges can be arbitrary amounts of token as long as they exceed a minimum threshold, which helps prevent spam consisting of bogus registrations. As we will show later, there is a soft cap (saturation point) for the upper limit on how much to pledge to a node.

In more detail, operators who wish to run a mix node submit a **declaration** to the Nyx blockchain that includes their pledge, their cost function $C(x)$ and a desired profit margin μ to be applied on the node revenue. For mix nodes, $C(x)$ maps the number x of routed packets to the amount of NYM that the node operator spends to cover its costs. For some operators the cost function can be approximated by a constant value that represents monthly costs in a flat-rate setup with unlimited bandwidth allowance. Other operators may have more sophisticated cost functions $C(x)$, e.g., where the price increases linearly per packet or "jumps" after a certain amount of bandwidth is used. Large stakeholders who posses stake exceeding the saturation point have the option of declaring multiple nodes that are operated by the same entity.

Once a mix node is registered, any stakeholder can **delegate** NYM to that node and support it by increasing its reputation (until the saturation point), which leads to increased selection probability and increased rewards, which are in turn shared with the node's delegates.

3.2 Assignment of nodes to the Nym mixnet

At each epoch, K mix nodes are elected to be rewarded, with K being a parameter of the reward mechanism, and under the assumption that there are at least $N \geq K$ candidate mix nodes registered in the system at any time. The K selected nodes are divided in two groups, the first $A = LW$ nodes to be sampled are assigned to be active mix nodes that route traffic in the mixnet, while the next $B = K - A$ are selected for rewards but kept idling. The selection of active and idling nodes is performed by sampling without replacement [20], with each node weighted according to its reputation (a value between zero and one that represents the amount of NYM pledged and delegated

[7] `https://github.com/AdrienLE/torflow`

to the node, relative to the stake saturation point β). For sampling purposes, we use the following *water-filling principle* when nodes exceed the saturation level: any excess stake over the saturation level does not increase the sampling weight of a node, and is instead 'added' to the sampling weight of the following candidate nodes, allocated in order of decreasing reputation, always capping the sampling weight at saturation. The A nodes active in an epoch are assigned to a position in the LxW mixnet uniformly at random (using a public random seed) with the restriction that nodes operated by the same entity are always placed in the same layer. This prevents adversaries with prior knowledge of the stake and registered nodes to strategically position compromised nodes in the mixnet. We remark that the parameter K, as well as the mixnet parameter W, are periodically adjusted (though in larger intervals consisting of multiple epochs) so that the available mixnet capacity exceeds in a suitable way the running average of demand in the last few epochs. Having an excess in capacity at any given moment is necessary to service peaks in demand that may invariably occur during mixnet operation.

The total amount of token staked (both pledged and delegated) to a node is a measure of the node's reputation. We expect most nodes to be operated by stakeholders with limited resources to pledge, who obtain most of their stake from the support of delegates (who, by virtue of delegating their NYM, implicitly signal trust in the node to deliver rewards). On the other hand, operators with large resources to pledge have the strongest incentives to run well-performing nodes, as they have significant 'skin in the game' dependent on their node's performance. Therefore, weighing by total stake the selection of mix nodes results in a mixnet mostly populated by nodes that have high reputation and strong incentives for offering a high quality of service. If a mix node has a large amount of delegated stake, this suggests that the community stands behind the reputation of the node, as the node regularly provides rewards to its delegates by being reliably online and keeping a good performance factor. As we will see in the next sections, this node selection process also optimizes the cost for users, favoring the selection of nodes that are not only reliable but also economically efficient. A mix node that declares a $C(x)$ function that is too expensive will distribute lower rewards to delegates, since the lower $C(x)$ is, the higher the remaining rewards available for the node's delegates.

To summarize, in order to attract delegation, mix node candidates must offer attractive parameters, such as more competitive (lower) costs $C(x)$ and profit margin μ, which leaves more share of rewards for delegates. It is also possible though to introduce other attractive externalities, such as giving some proceeds to a good cause such as "sponsored access" to Nym for human rights activists, which may resonate with some delegates and appear as free usage of the Nym mixnet to these end users. Some nodes may also capitalize on reputation in other mediums (e.g., nodes run by a well-recognized organization or personality). As we show in the next sections, underperforming and inefficient nodes receive diminished or no rewards, incentivizing delegates to move away from backing them, and creating opportunities for new mix nodes to attract delegates.

3.3 Bandwidth pricing and budget balance

In this section we describe the mechanism that prices the mixnet bandwidth to its prospective users. The problem we want to solve is to price bandwidth in a way that is proportional to the mixing effort required to route user traffic, so that the whole system, at minimum, can deliver anonymous routing as a service, generating enough revenue to cover its expenses and allowing the operators to make some profit. The mechanism follows a "dynamic" posted price approach continuously adjusting the price as users place requests for bandwidth that are serialized by a smart contract. Each request is assigned an appropriate amount of bandwidth, claimed by the user in the form of a bandwidth credential.

As a warm up towards the full pricing mechanism, consider the abstraction of a single trusted node with pricing declaration $C(\cdot)$ that handles by itself the total traffic requested to be routed. Suppose that the total demand in an epoch follows some probability distribution. We denote by M the random variable drawn from that distribution. We define the price of the x-th packet (unit of bandwidth) sold in an epoch as:

$$C(x) - C(x-1) + C(0) \cdot \frac{1}{\mathbb{E}[M]}$$

Proposition 1. *Under the above pricing scheme, the expected revenue of the node is* $\mathbb{E}[C(M)]$.

Proof. Summing across all units of bandwidth sold, it holds that the revenue is equal to:

$$M \cdot \frac{C(0)}{\mathbb{E}[M]} + \sum_{x=1}^{M}(C(x) - C(x-1)) = M \cdot \frac{C(0)}{\mathbb{E}[M]} + C(M) - C(0)$$

By linearity of expectation, we conclude the correctness of the statement. □

Given the above one can use properties of the distribution of M and $C(\cdot)$ to argue that the system generates sufficient revenue, i.e., that it is "budget balanced" as a mechanism with high probability. Of course, this only refers to the case of a single hypothetical node that wants to break even, while in our setting we have a large set of profit seeking nodes who do not necessarily agree on their pricing functions $C_i(\cdot)$ and they are organized in a stratified mixnet of L layers.

To address our more general setting, we proceed in two steps. First we consider a combined pricing function $C^*(\cdot)$ that is synthesized in some way based on all the individual $C_i(\cdot)$ functions contributed by the node registrations of those nodes that will populate the mixnet in an epoch. Second, we determine a price per packet function $F(x)$ that takes into account the fact that the mixnet has L layers (hence the work is multiplied by L) while the load is uniformly distributed within each layer among W nodes. The following defines the *fee* for the x-th packet and is parameterized by L, W, M a "surplus" parameter τ and an "average cost" function $C^*(\cdot)$.

$$F(x) := L \cdot \Big(C^*(\lceil \frac{x}{W} \rceil) - C^*(\lceil \frac{x}{W} \rceil - 1) + W \cdot C^*(0) \cdot \frac{1}{\mathbb{E}[M]}\Big) + \tau \tag{1}$$

Note that τ is the parameter of the system controlling the surplus that we wish the fees to produce. We next argue that there is a suitable choice of $C^*(\cdot)$ that combines all operators' individual functions and enables the system to be budget balanced and leave a surplus that is controlled by the parameter τ. For simplicity, in the analysis we assume that M is a multiple of W (note that in any case $M \gg W$ with overwhelming probability).

Theorem 1. *Let* Mix *be the set of nodes selected for the mixnet and* Idl *the set of nodes selected to be idle. Consider the average cost function defined as follows:*

$$C^*(x) = \frac{1}{LW} \cdot \Big(\sum_{i \in \mathsf{Mix}} C_i(x) + \sum_{i \in \mathsf{Idl}} C_i(0) \Big)$$

The total fees collected cover the costs in expectation leaving a surplus of $\tau \cdot \mathbb{E}[M]$*, assuming* $C_i(\cdot)$ *are linear functions.*

Proof. We denote by M_i the packets routed by node i. Without loss of generality we assume $i = 1, \ldots, LW$ are selected to participate in the mixnet, while nodes $K \geq i > LW + 1$ are on reserve.

It holds that $\mathbb{E}[M_i] = \mathbb{E}[M]/W$ for $i \leq LW$ and $M_i = 0$ otherwise. Given this, the expected costs are equal to:

$$\mathbb{E}[\sum_{i=1}^{LW} C_i(M_i) + \sum_{i=LW+1}^{K} C(0)] = \sum_{i=1}^{LW} C_i(\mathbb{E}[M]/W) + \sum_{i=LW+1}^{K} C_i(0)$$

by applying linearity of expectation.

We next compare this to the proceeds from selling the private bandwidth. Let $\ell = M/W$.

$$\sum_{x=1}^{M} F(x) = L \cdot W \cdot (C^*(\ell) - C^*(0)) + L \cdot \ell \cdot W^2 \cdot C^*(0) \cdot \frac{1}{\mathbb{E}[M]} + M \cdot \tau$$

It follows that the expectation of the above expression is equal to $L \cdot W \cdot \mathbb{E}[C^*(M/W)] + \tau \cdot \mathbb{E}[M]$. Observe now the following based on linearity of expectation:

$$L \cdot W \cdot \mathbb{E}[C^*(M/W)] = \sum_{i=1}^{LW} C_i(\mathbb{E}[M]/W) + \sum_{i=LW+1}^{K} C_i(0)$$

Based on this we conclude the proof. □

Remark 1. In light of Theorem 1, in the remaining of the section we will use the assumption that the $C_i(x)$ functions are linear in x.

Remark 2. The parameter $\tau \geq 0$ which controls the surplus is set to some system-wide value which can be updated over time to ensure that there are sufficient funds for participants to cover costs and engage in meaningful delegation. See Section 5.3 for further discussion.

Remark 3. The above dynamic posted-price mechanism does not attempt to perform price discovery. Auction mechanisms are also possible, e.g., running a *multi-unit auction* such as Vickrey, or uniform price [32]. Such mechanisms come with the downside that users will have to engage in more complex bidding processes and wait for the auction to complete in order to obtain their bandwidth allowance (this is in contrast to the posted-price mechanism described above, which processes bandwidth requests as they come).

Remark 4. It is worth noting that the $C_i(\cdot)$ functions are denominated in NYM, nevertheless they reflect real world costs which may be best denominated in fiat currencies (e.g., USD). To accommodate volatility in the exchange rate of NYM, it should be possible for operators to adjust their cost function periodically or, perhaps preferably, incorporate an on-chain oracle that provides the exchange rate and facilitates the cost adjustment automatically.

3.4 Reward allocation mechanism

We denote by R the share of rewards that are available for distribution to the mixnet in an epoch. We recall that R is composed of rewards emitted from the mixmining pool and of (a fraction of) the income from fees. The reward allocation mechanism determines the fraction of R given to each individual mix node, and its subsequent division among the stakeholders (operators and delegates) supporting the node with their NYM token. Recall that one important objective of the mechanism is to compensate the nodes that populate the mixnet for their operational costs. When the i-th node transmits M_i packets in an epoch, $C_i(M_i)$ will be refunded to the operator, while the operator of an idling node i is still refunded an amount equal to $C_i(0)$. The rewards (aggregation of cost refunds plus applicable profits) are transferred automatically to the operators' accounts and to stakeholder accounts (as the operator should not have to be trusted to forward funds to its delegates). In addition to the above, the mechanism is capped so that no node receives more than $\beta \cdot R$ of the rewards, where β is the saturation level parameter.

With foresight, the goal of the mechanism is to incentivize an equilibrium with the following ideal properties:

- There are at all times $N = K$ operational nodes, all of which have an equal amount of reputation (delegated stake plus pledge), where K is a public parameter.
- Delegates who select properly operating nodes receive the same rewards (in expectation) per delegated NYM token.
- More competitive nodes (e.g., those with lower costs and/or higher pledges) are able to translate their competitiveness to higher profit by claiming a larger profit margin.
- Operators who attempt to register multiple nodes either publicly or covertly (in what amounts to a Sybil attack [19]) have to pledge sufficient stake per node to maintain their competitiveness against other nodes. This effect is controlled by a parameter of the scheme denoted by α; the higher the α parameter, the larger the loss of competitiveness experienced by the Sybil attacker when partitioning stake into multiple pledges.

To achieve the above, the mechanism constrains node rewards in a certain manner, taking into account the stake pledged and delegated to the node. The constraint creates a "soft-cap" on how much stake it is rational to pledge or delegate to a node, nudging stakeholders to an equitable organization behind the target number K of mix nodes and preventing centralization of stake (where just a handful of nodes emerges that are insufficient to populate a mixnet of the desired dimensions) as well as fragmentation (where too many weak nodes are proposed and quality of service is severely degraded).

The mechanism is a generalization of the mechanism of Cardano stakepools [7] to a 'proof of work' setting where different amounts of 'work' might be performed by the mix nodes in each

epoch and cost functions are functions of system load per unit of time, as opposed to constant. A node's work relates to the amount of mixnet packets it routes, and recall that the i-th node routes M_i packets incurring a cost $C_i(M_i)$; in contrast, in the modeling of Cardano the costs are independent of actual work invested [7]. Furthermore, given a total amount of traffic routed by the entire mixnet in an epoch, the *share of work* performed by each node depends on whether it has been selected to be *active* in the mixnet, selected to be in *reserve* and is idling, or *not selected* at all in that epoch. As described earlier, the parameter K sets the number of nodes that the stakeholders are incentivized to create. The exact choice of K and of the number of active nodes A and in reserve B, $K = A + B$, depends on the expected demand as estimated by the system. For example, if we want a throughput of 12 Gbps in a mixnet with three layers, with each node offering 100 Mbps, we can choose $K = 720$, which accommodates $A = 360$ operational nodes in a 3x120 mixnet and $B = 360$ idling nodes on reserve. Having $B = 360$ allows the mixnet to double its capacity for the next epoch if demand increases. In any real world deployment, the number of active nodes and reserve will be different and could be based on projected demand and the ability to handle 'bursty' spikes of usage.

A parameter ω_i is defined to specify the share of total network 'work' undertaken by the i-th node, such that $\sum_{i=1}^{K} \omega_i = 1$. In a mixnet with equal number W of nodes and uniform routing through L layers, ω_i is the same for all $A = LW$ active nodes. The $B = K - A$ reserve nodes do not route user traffic in the epoch, but they need to spend resources being online, as their uptime and quality of service is tested throughout the epoch to help determine their performance over time. We establish that the work performed by an active mix is a 10x factor larger that the work of being in reserve (any other factor than 10x may be used if desired — see Section 6 for experimental validation of our choice). For the A active nodes we compute ω_i as:

$$\omega_i = \frac{10}{10A + B} \qquad 1 \leq i \leq A \tag{2}$$

For each of the B reserve nodes, the work ω_i is computed as:

$$\omega_i = \frac{1}{10A + B} \qquad A + 1 \leq i \leq A + B \tag{3}$$

The performance factor ρ_i represents the estimated fraction of packets correctly routed by each node, with $\rho_i = 1$ indicating that the node followed the routing protocol for all the packets it received. ρ_i decreases when the node is down due to a failure, congested due to low throughput and thus dropping some packets, or dropping packets for a malicious purpose. ρ_i can be estimated by sampling via special-purpose measurement authorities, as is the case in Tor [17] or via a decentralized protocol as sketched in Nym [11]. The specific method to establish node performance is out of the scope of this paper, where we assume that ρ_i is available on chain. The performance factor affects nodes' rewards proportionally. When a node frequently has a performance $\rho_i < 1$, delegates are incentivized to move their delegated stake to nodes with better performance in order to maximize their rewards.

Given the above, we now define the reward scheme.

1. The amount of rewards apportioned for the i-th node and its delegates is equal to

$$R_i = R \cdot \rho_i \cdot \frac{\sigma'_i}{\beta} \cdot (\omega_i + \alpha \cdot \lambda'_i) \cdot \frac{1}{1 + \alpha}, \tag{4}$$

where λ_i is the stake that the operator of the i-th node has pledged to their node as a fraction of circulating supply, σ_i is the total stake pledged and delegated also as a fraction of the total circulating supply, and $\lambda'_i = \min\{\lambda_i, \beta\}$ and $\sigma'_i = \min\{\sigma_i, \beta\}$ are capped versions of λ_i and σ_i. We observe the following budget balance property holds:

$$\sum_{i=1}^{K} R_i \leq R.$$

This follows immediately as $\sum_{i=1}^{K} \omega_i = 1$, $\sum_{i=1}^{K} \lambda'_i \leq 1$ and $\sigma'_i \cdot K \leq 1$ for $i = 1, \ldots, K$.

Note that the above is necessary to ensure there are no incentives to delegate more than β of the circulating supply to any one node and thus stakeholders are incentivized to create K distinct nodes; see the next section where we delve deeper into the equilibrium analysis.

2. Given R_i rewards assigned to the i-th node, its **operator** is credited with the following amount:

$$\min\{C(M_i), R_i\} + [(\mu_i + (1-\mu_i) \cdot \frac{\lambda_i}{\sigma_i}) \cdot (R_i - C(M_i))]^+, \tag{5}$$

where $[\cdot]^+ = \max\{0, \cdot\}$, and μ_i is the declared profit margin of the i-th operator.

A node **delegate** with delegated stake s, receives:

$$[(1-\mu_i) \cdot \frac{s}{\sigma_i} \cdot (R_i - C(M_i))]^+ \tag{6}$$

3. The above allocation process may result in leftover funds. Observe that in typical conditions where $\sum \lambda_i < 1$, a certain portion of rewards remain unclaimed and are returned to the reserve. Nodes fail to realize their full reward potential when they are less than "saturated" (i.e., they are supported by a fraction of stake σ_i that is less than β of the available NYM supply) or if their performance ρ_i is below par. The unallocated funds are returned to the reserve, to be distributed in the future. The fact that the mixmining reserve is long lived also helps stabilize rewards in the event of temporary drops of demand (and consequently drops in income from fees), as nodes can remain operational, covering running costs with mixmining pool rewards.

Remark 5. Even though we describe the above mechanism in a "per epoch" fashion, in a real world deployment it is also possible to aggregate rewards for a number of epochs, (e.g., epochs last an hour but rewards are computed in monthly reward intervals, i.e., every 720 epochs). In such case, one can average values across longer intervals for the node performance ρ_i.

3.5 Equilibrium analysis

Family of admissible strategies. We focus our analysis on scenarios where each stakeholder strategically decides to either set up a node or delegate its stake to one or more node operators. More complex strategies can be expressed as coalitions of parties in this mutually exclusive scenario. We assume that the utility of the stakeholders is not affected by any external factors and that the rewards available are always sufficient for at least K stakeholders to become operators. Moreover, delegation incurs no cost, thus all players are either delegators or operators (we revisit this assumption in Remark 7).

The expected *potential profit* associated with the node operated by the i-th stakeholder is equal to:

$$\pi_i = \mathbb{E}[R \cdot (\omega_i + \alpha \cdot s_i) \cdot \frac{1}{1+\alpha} - C_i(M_i)] \tag{7}$$

Note that the above expression sets σ_i to be $\beta = \frac{1}{K}$ (we call such a node "saturated") and, by slightly abusing notation, considers ω_i to be the random variable corresponding to the node's work ratio at a point of "full saturation", i.e., when K nodes have reached stake β. Also recall that M_i is the random variable corresponding to the traffic routed by the node. To simplify the analysis we make the following assumption about the players' parameters: the stake of all stakeholders satisfies $s_i \leq \beta$; for larger players (a.k.a. "whales") whose stake exceeds the bound, one can think of them as being a coalition of a number of smaller players each one with stake obeying the bound.

To reason about the strategic options of delegation, we define *desirability* of a node as a quantity equal to $(1-\mu_i) \cdot \pi_i$ where μ_i is the profit margin declared by the operator. It expresses the portion of the node's potential profit that the operator distributes to the delegates. In our family of admissible strategies, delegators always delegate to the operators that run nodes with the highest desirability; in other words, a strategy is admissible if all delegated stake is assigned to the most desirable operator; if two or more operators have equal desirability, then delegates are indifferent in their choice between them, unless one of them is saturated while the other is not, in which case the unsaturated node would be preferred. This stems from the fact that once a node is saturated the

rewards stop increasing. Finally, in an admissible strategy, any stakeholder who can be competitive as an operator (in terms of being able to select a profit margin that makes her competitive compared to other stakeholders) runs a node (i.e., we assume that all stakeholders are capable of running nodes) and we have always at least K nodes proposed by stakeholders.

Family of perfect strategies. We next introduce a set of strategies, called "perfect" strategies that we demonstrate are a Nash equilibrium. We assume without loss of generality that players are sorted in a descending order according to expected potential profit. In a perfect strategy, the i-th player operates a node only in case its potential profit is competitive against the $(K+1)$-th stakeholder. The profit margin selected by the player in this case is set to be equal to $1 - \frac{\pi_{K+1}}{\pi_i}$. In case of ties for the K-th position, multiple perfect strategies exist. We observe that in a perfect strategy the node operator $i \leq K$, derives expected utility equal to:

$$(\mu_i + (1-\mu_i) \cdot \frac{s_i}{\beta})\pi_i = (\pi_i - \pi_{K+1}) + \pi_{K+1} \cdot \frac{s_i}{\beta}$$

while delegators investing stake s receive $\pi_{K+1} \cdot \frac{s}{\beta}$. In other words, node operators receive $\pi_i - \pi_{K+1}$ in its entirety and subsequently all involved stakeholders in the node, share according to their contributed stake a portion of π_{K+1}. Observe also that in a perfect strategy the desirability of the first K stakeholders who become operators is exactly π_{K+1}.

The main characteristics of perfect strategies are as follows:

- All stake is either pledged or delegated.
- There are K nodes with exactly $\beta = \frac{1}{K}$ stake staked to them (including pledge and delegation).
- If $\alpha = 0$, for any two players, the one with the lower cost for the work allocated will be necessarily running a node, assuming the other one does. For higher values of α, players backing their nodes with higher pledges gradually become more competitive as α increases.
- Assuming no sub-par performance anywhere in the system, all delegators receive the same rewards equal to $\pi_{K+1} \cdot \frac{s}{\beta}$, where s is their stake relative to the total supply, independently of their choice, where π_{K+1} is the potential profit of the $(K+1)$-th operator.
- The j-th operator receives an additional reward of $\pi_j - \pi_{K+1}$ (on top of its rewards as a delegator to its own node). This is the benefit it receives for being competitive.

Theorem 2. *Every perfect strategy is an equilibrium.*

Proof. Since we are on a perfect strategy, $N = K$, the delegated stake on the node $j \leq K$ is $\beta = 1/K$, the margin $\mu_j = 1 - \frac{\pi_{K+1}}{\pi_j}$ and the desirability of the K operators is the same and equal to π_{K+1}. To prove the theorem, we consider the following cases.

Case I. The stakeholder j is an operator who decreases its margin μ_j to a smaller value μ_j^*. The desirability of the operator remains among the best K and given we are in an admissible strategy the only question is whether the delegated stake makes a difference due to influx of delegates from all the other operators (since we are moving to another admissible strategy where the j-th operator is the most desirable). Note that due to the cap of the reward scheme, the rewards awarded to the j-th operator in total remain the same, however the operator, by decreasing its margin, makes the j-th node more desirable to delegates. The utility of the operator becomes $(\mu_j^* + (1-\mu_j^*)(s_j/\beta))(R_j^* - c_j^*)$, where c_j^* is the expected cost after the switch, while the node rewards are equal to $R_j^* = R \cdot (\omega_j^* + \alpha \cdot s_j)/(1+\alpha) = \pi_j + c_j$, where ω_j^* is the expected weight of the operator after the margin adjustment and c_j the expected cost prior to it; the equality between the two expressions stems from the fact $\mathbb{E}[\omega_j] = \omega_j^*$, which is implied by the fact that the probability of selecting j as an active mixnet node does not change due to the water-filling sampling approach when a node's stake exceeds the saturation level. It follows that the utility of the node is equal to the following expression.

$$(\mu_j^* + (1-\mu_j^*)(s_j/\beta))(\pi_j + c_j - c_j^*)$$

Now observe that it holds $c_j^* \geq c_j$, since the operator's profile and work allocated is maintained; based on this, it follows the utility of the j-th operator cannot increase.

Case II. The stakeholder j is an operator who increases its margin μ_j. This drops its desirability below π_{k+1} and thus the operator runs a node without any delegated stake. This is due to the fact that other stakeholders following the admissible strategy choose to delegate to the original $K-1$ operators while the $(K+1)$-th stakeholder now runs a node as well (by choosing a profit margin of 0 she is as competitive as the $K-1$ original operators who are fully saturated). Running a node without delegates for the j-th stakeholder results in utility $R \cdot (s_j/\beta) \cdot (\omega_j^* + \alpha s_j)/(1+\alpha) - c_j^*$ where c_j^* is the operational cost in this circumstance and ω_j^* the expected weight of the node after increasing the margin. Given that $\omega_j^* \leq \omega_j$ in expectation, this expression is less or equal to $(s_j/\beta) \cdot (\pi_j + c_j) - c_j^* = (s_j/\beta) \cdot \pi_j + (s_j/\beta) \cdot c_j - c_j^*$, where $c_j = \mathbb{E}[C_j(M_j)]$. Recall the utility of the operator prior to the margin increase is $\pi_j - \pi_{k+1} + (s_j/\beta) \cdot \pi_{k+1}$. Subtracting this from the utility after the profit margin increase, we obtain

$$(1 - s_j/\beta) \cdot (\pi_{k+1} - \pi_j) + (s_j/\beta) \cdot c_j - c_j^* \leq 0$$

which follows from the facts (i) $\pi_{k+1} \leq \pi_j$, i.e., the j-th operator was competitive prior to the increase, and (ii) $(s_j/\beta) \cdot c_j - c_j^* \leq 0$ which we argue next.

Let p_j be the probability that the j-th operator is selected. The expected cost is $(1-p_j) \cdot C_j(0) + p_j C_j(\mathbb{E}[M]/W)$ due to the linearity of $C_j(\cdot)$. In the case of c_j, it holds that $p_j = 1$ as there are exactly K nodes with non-zero weight and hence $c_j = C_j(\mathbb{E}[M]/W)$. In the case of c_j^*, where the j-th node is running "solo", we have a configuration where the j-th node is by itself, $K-1$ nodes have total stake $1/K$ and a single node has $1/K - s_j$. It holds that

$$p_j = 1 - \frac{1 - K s_j}{K} \cdot \Big(1 + \sum_{t=1}^{K-1} \prod_{i=t+1}^{K} (1 - \frac{K \cdot s_j}{K - i + 1 + K s_j})\Big)$$

.

It is easy to observe that $p_j \geq K s_j = s_j/\beta$. Putting everything together we have that $c_j^* = (1-p_j) C_j(0) + p_j c_j$ and as a result $(s_j/\beta) \cdot c_j - c_j^* = (s_j/\beta - p_j) c_j - (1-p_j) C_j(0) \leq 0$.

Case III. The stakeholder j stops being an operator and becomes a delegator. In this case its utility equals to $\pi_{k+1} \cdot (s_j/\beta)$ which is no better than the operator utility that includes the additional additive term $\pi_j - \pi_{k+1}$.

Case IV. Consider now a stakeholder j that is a delegator. By definition of the profit margins in the perfect strategy the delegator has to choose profit margin zero. It follows easily that the utility of the player cannot increase in this case.

The above four cases cover all possible deviations within our family of admissible strategies and hence the theorem's statement follows. □

Next we consider the truthfulness of the mechanism, i.e., whether, in a perfect strategy, it makes sense for players to deviate from declaring their true cost. In a nutshell, the following theorem establishes that in a perfect strategy it does not make sense to deviate from being truthful.

Theorem 3. *In a perfect strategy, untruthful cost declarations are not advantageous.*

Proof. Consider the j-th operator making a cost declaration $\hat{C}_j$ that is different from its true cost C_j. In this case, the expected potential profit of the operator would be calculated with the declared cost, as $\hat{\pi}_j = \mathbb{E}[R(\omega_j + \alpha s_j)/(1+\alpha) - \hat{C}_j(M_j)]$. We consider two cases depending on the relation of $\hat{\pi}_j$ and π_{K+1}.

Case $\hat{\pi}_j < \pi_{K+1}$. In this case, the j-th operator declaration makes the operator non-competitive and thus it will not be selected by other delegators who follow the perfect strategy. It follows that the expected utility of the operator in this case is derived by its own stake and is equal to

$$\mathbb{E}[R \cdot s_j/\beta \cdot (\hat{\omega}_j + \alpha s_j)/(1+\alpha)] - c_j \leq (\hat{\pi}_j + \hat{c}_j) \cdot (s_j/\beta) - c_j$$

where $c_j = \mathbb{E}[C_j(M_j)]$, $\hat{c}_j = \mathbb{E}[\hat{C}_j(M_j)]$, and $\hat{\omega}_j$ is the modified expected weight for the j-th node due to the potential change in its total stake, for which we have $\hat{\omega}_j \leq \mathbb{E}[\omega_j]$.

Now recall that $\pi_j = \mathbb{E}[R(\omega_j + \alpha_j)/(1+\alpha)] - c_j$ and as a result $\pi_j + c_j = \hat{\pi}_j + \hat{c}_j$. From this we derive that the expected utility is less or equal to $(\pi_j + c_j) \cdot (s_j/\beta) - c_j \leq \pi_j \cdot (s_j/\beta) \leq$

$\pi_j - \pi_{K+1} + (s_j/\beta) \cdot \pi_{K+1}$, which follows from the fact that $\pi_j \geq \pi_{K+1}$. It follows that the utility is no better than the case of a truthful declaration.

Case $\hat{\pi}_j \geq \pi_{K+1}$. In this case, the j-th operator retains its competitiveness. Recall that its expected utility as a truthful operator is equal to $\pi_j - \pi_{K+1} + \pi_{K+1}(s_j/\beta)$, while the actual expected utility of the operator now would be equal to $(\hat{\pi}_j - \pi_{K+1}) + \pi_{K+1}(s_j/\beta) - c_j + \hat{c}_j$. It is easy to see that the difference between the two is $\pi_j - c_j - (\hat{\pi}_j - \hat{c}_j) = 0$, and hence there is no advantage in this case either (to understand the intuitive reason why, consider that in a perfect strategy, the j-th operator will have to either use (i) a higher margin, when the cost declaration is lower than the true one to cover the costs, or (ii) use a lower margin, when the cost declaration is higher than the true one to remain competitive; in either case, the benefit of lying about the cost is negated by the adjustment in the margin). □

Finally, we discuss the Sybil resilience offered by the mechanism. Specifically we ask how many nodes a large stakeholder, say holding stake χ, can control at the perfect strategy equilibrium. In this case, the stakeholder splits her stake into $\chi_1, \ldots, \chi_t$ portions and operates as t individual stakeholders who create nodes by declaring costs that for the assigned work have expectations equal to $\tilde{c}_1, \ldots, \tilde{c}_t$, splitting the total cost of the Sybil player $\tilde{c} = \sum_{j=1}^{t} \tilde{c}_j$. Suppose that all t nodes are included in the perfect strategy equilibrium and have potential profit $\tilde{\pi}_1, \ldots, \tilde{\pi}_t$ respectively. This suggests that $\tilde{\pi}_j \geq \pi^*$, for some other party's potential profit π^*, i.e., $\mathbb{E}[R(\tilde{\omega}_j + \alpha\chi_j)/(1+\alpha)] - \tilde{c}_j \geq \mathbb{E}[R(\omega^* + \alpha s^*)/(1+\alpha)] - c^*$, where s^*, c^* are the stake and expected cost respectively of the best non-competitive player who is outside the K equilibrium nodes. By summing for all $j = 1, \ldots, t$, we obtain $\mathbb{E}[R(\tilde{\omega} + \alpha\chi)/(1+\alpha)] - \tilde{c} \geq t \cdot (\mathbb{E}[R(\omega^* + \alpha s^*)/(1+\alpha)] - c^*)$, where $\tilde{\omega} = \sum_{i=1}^{t} \tilde{\omega}_j$, from which we have:

$$\chi \geq t\Big(s^* - \frac{\mathbb{E}[\tilde{\omega}]/t - \mathbb{E}[\omega^*]}{\alpha} - \frac{c^* - \tilde{c}/t}{R}(1 + \frac{1}{\alpha})\Big)$$

Based on the above, we observe that when $\alpha \to \infty$ we have $\chi \geq t \cdot s^* - c^*/R$, i.e., the mechanism imposes a lower bound on the Sybil attacker's total stake which has to be approximately t times as large as the stake of the first non-competitive stakeholder assuming $R \gg c^*$.

Remark 6. We note that in practice the system configuration will approximate but may not reach a perfect strategy due to (i) externalities (e.g., an exchange stakeholder who may avoid pledging because it requires high liquidity) (ii) friction and action inertia (e.g., stakeholders who perform a delegation action and subsequently do not engage with the system despite the fact that their delegation choice has in the meantime become sub-optimal).

Remark 7. In a real world deployment, it can be the case that some stakeholders cannot engage in stake delegation. For instance, keys corresponding to wallets might be lost, or tokens might be locked in smart contracts that prohibit their participation in the delegation game. As a result, if at a certain time there is a fraction of stake $\zeta < 1$ that is available for engaging with the mixnet game, then the saturation level β should be set to ζ/K to accommodate for the loss in participation.

4 Economic model simulator

In the previous section we have proven that the reward scheme reaches an equilibrium when participants are perfectly rational and *always* make choices that maximize their financial returns. This ideal behaviour may however not be fully met in practice where, e.g., we can expect a larger number N of registered nodes than the equilibrium value (equal to K rewarded nodes set by the scheme); and that some significant fraction of the token in circulation may not be pledged or delegated, meaning that some stakeholders are taking an opportunity cost compared to the equilibrium, which also results in increased rates of unclaimed rewards that are returned to the mixmining reserve.

To study the economic viability of the network in practical scenarios, we have implemented in a simulator[8] that models the Nym network and distributes rewards to nodes over time, according to

[8] The main simulation and reward distribution functions are about one thousand lines of code in Python, with an additional thousand lines for selecting and displaying results. The code is publicly available at `https://github.com/nymtech/rewardsharing-simulator`.

the proposed reward scheme. This simulator allows us to evaluate rewards in non-ideal conditions and compare returns for node operators and delegates in different scenarios. The simulator takes as inputs the system configuration parameters and parameters on the behaviour of participants. It runs the reward distribution scheme with those parameters and participant behaviours for a configurable number of intervals (where each interval corresponds to a month), evolving the state on a per-interval basis to account for token flows (e.g., updates to the mixmining pool size considering past emissions and returned unclaimed rewards) and system updates (e.g., increased number K of mix nodes required to serve a growing demand).

To capture a wider set of possible configurations we do not assume that the system has converged to the perfect strategy equilibrium (cf. Section 3.5), and instead consider nodes with varying pledge sizes, amounts of delegation and resulting reputation scores. Moreover, in line with Remark 7 only a fraction of the available token supply is staked in the network. The simulator computes the per-interval distribution of rewards to each participant as well as a variety of parameters of interest, such as the share of work performed per node in the interval. We use this simulator to study the economic viability of the mix network in different conditions and deployment scenarios.

To be clear, this is an academic paper and not an investment prospectus or financial advise. We use the term 'return on stake' in a loose generic sense, and are relying on hypothetical scenarios using experimental technology. Actual results using the technology will vary widely. It's quite possible that this venture could result in loss of monetary funds for anyone who uses the software. Any participant in an actual network is expected to do their own research rather than relying on these simulation-based experiments.

5 Experimental setup

Using the simulator, we study the reward allocation to participants over a five-year period, considering the configurations described in this section and the parameter values summarized in Table 1. It should be emphasized that our simulations consider hypothetical scenarios to obtain indicative results useful to fine-tune the scheme's parameters; they however provide no guarantee on the reward amounts that may be obtained by nodes or the return rates that delegates can expect in the actual world, where parameter values will vary and not reproduce the exact same configurations considered in these simulations.

5.1 Reference mix node

In our experiments we consider that all the available nodes are identical in terms of operational cost, packet processing capacity, performance and declared profit margin. Fixing $C_i(\cdot)$, ρ_i and μ_i, allows us to focus on the effects of pledge and reputation on the node's rewards, λ'_i and σ'_i, which we vary per node. We represent these values as fractions over the stake saturation point of nodes, considering saturation $\beta = \frac{1}{K}$, i.e., the reputation level of node i is given by $\sigma'_i \cdot K$ and its pledge saturation level by $\lambda'_i \cdot K$.

Based on estimated commercial costs for computation and bandwidth we consider that a mix node with up to 16 CPU cores and unlimited network data can be operated for a flat monthly cost of \$200.[9] The mix node **cost function** is thus simply modeled as $C(x) = 200$ for all nodes (cf. Section 3.1). We assume that these monthly operational costs remain constant over the five-year period. Since computation and networking costs are likely to decline over time, this is a conservative assumption.

In terms of mix node **capacity**, based on current implementation benchmarks[10], we assume a CPU core[11] can process 3125 mixnet packets per second, while the size of the packet payload has little impact on processing time. We consider mix nodes that parallelize packet processing over

[9] Linode's shared CPU plan at `https://www.linode.com/pricing/` quotes \$5 per month for a 1 CPU Core and 1 GB RAM. We additionally consider a \$120 flat monthly fee for unlimited bandwidth and transaction fee expenses in the Nyx blockchain.

[10] Note that the implementation performance may improve over time, and current benchmarks were done in September 2021 using `https://github.com/nymtech/nym/tree/develop/mixnode`

[11] AMD EPYC 7601 with a base clock rate of 2.2GHz.

Table 1: Parameters of the experimental setup

Name	Value	Notation	Notes
Reference Mix Node			
Minimum node pledge	1000 NYM		Constant
Number CPUs per node	16		Constant
Peak packets/second per CPU	3125 p/s		Grows 1% monthly (12.7% yearly)
Monthly costs per node	\$200	$C_i(\cdot)$	Constant
Node performance	1.0 (100%)	ρ_i	Constant
Node profit margin	0.1 (10%)	μ_i	Constant
Mixnet parameters			
Layers of mixnet	3	L	Constant
Width of mixnet	≥ 120	W	Proportional to demand
Active nodes	≥ 360	A	$A = L \cdot W$
Idle (reserve) nodes		B	$B = A$
Rewarded nodes	≥ 720	K	$K = A + B = 6 \cdot W$
Total node candidates	≥ 1440	N	$N = 2 \cdot K$
Average mixnet load	20%		Network absorbs 5x peaks
Simulation parameters			
Epoch	1 hour		
Reward interval	1 month	t	720 hours (epochs)
Simulated period	60 months (5 years)		
Data routed per interval		$M(t)$	Dependent on Scenario S_0, S_1
Scenario S_0 "low demand"	$M_0(0) = 0$	S_0	$M_0(t) = 0$ p/month
Scenario S_1 "growing demand"	$M_1(0) = 500 \cdot 10^9$	S_1	$M_1(t+1) = 1.06 \cdot M_1(t)$ p/month
Exchange rate NYM	1 NYM = \$1		Constant
Price for users	\$1 for 10^6 packets		Constant
Income from fees in S_0	$F_0(0) = 0$	S_0	$F_0(t) = 0$ NYM/month
Income from fees in S_1	$F_1(0) = 500 \cdot 10^3$	S_1	$F_1(t+1) = 1.06 \cdot F_1(t)$ NYM/month
Token distribution and staking parameters			
Mixmining pool reserve	$P(0) = 250$m NYM	$P(t)$	$P(t+1) = P(t) - 0.02 \cdot P(t) + U(t)$
Monthly pool emissions	2%		$0.02 \cdot P(t)$
Budget rewards entire mixnet		$R(t)$	$R(t) = 0.02 \cdot P(t) + 0.6 \cdot F(t)$
Rewards for node i (out of K)		$R_i(t)$	Eq. (4)
Unclaimed rewards		$U(t)$	$U(t) = R(t) - \sum_i R_i(t)$
Available staking supply	initial: 750m NYM		1 billion minus $P(t)$
Per-node stake saturation point	initial: 1.04m NYM		Available supply divided by K
Pledged stake	0.15		Constant at 15% of available stake
Delegated stake	0.6		Constant at 60% of available stake
Unallocated stake	0.25		Constant at 25% of available stake
Sybil resilience parameter	0.3	α	Constant

up to 16 CPU cores and thus can process up to 50k mixnet packets per second. We consider a moderate increase in processing power per CPU core of 1% monthly (12.7% annually), which after 5 years takes the peak capacity per core slightly above 5600 packets per second.

In our simulations we consider that nodes have perfect **performance** $\rho_i = 1$, while noting that any decrease in performance would proportionally scale down a node's rewards in line with Eq. (4).

We also consider that nodes declare a **profit margin** of 10%,[12] i.e, $\mu_i = 0.1$. In practice (given comparable systems such as Cosmos and Cardano), profit margins are likely to vary widely and the parameter is a point of competition between nodes to attract delegates as seen in the perfect strategy described in Section 3.5. Recall that the profit margin only affects the split of a node's rewards between its operator and delegates, but has no impact on the total rewards R_i received by the node. In addition, note that the effect of μ_i is mainly relevant for nodes with low pledge and high delegation ($\sigma'_i \gg \lambda'_i$); for nodes with small amounts of delegation ($\sigma'_i \approx \lambda'_i$), variations in μ_i will not make much difference to the raw profit of the operator, which is in such cases mainly determined by the operator's pledge (λ'_i).

5.2 Mixnet parameters

The mixnet has three layers ($L = 3$) and a variable width W that is dependent on the traffic demand M. Given an expected $\hat{M}$ packets in the next epoch, the mixnet width W is chosen so that mixes are on average at 20% of their peak capacity (of 50k p/s), and can thus absorb sudden increases in demand of a factor 5x over the average load. Thus, mix nodes route on average 10k p/s, and a total of $M_e = 36$ million packets per one-hour epoch. Given an expected $\hat{M}$, W is computed as $W = \lceil \frac{\hat{M}}{M_e} \rceil$.

As explained in Section 3.4, the network also keeps a reserve of B idling nodes that can be used to grow the network in the next epoch. We consider that the number of reserve nodes is chosen as $B = A = LW$, meaning that the total number of nodes is $K = A + B = 6W$ and the network can be doubled in size if needed. Thus, for an expected traffic load $\hat{M}$, the network is dimensioned so that the available nodes can route up to $10 \cdot \hat{M}$ when all are active and used at peak capacity.

In order to bootstrap a network that provides sufficient usage capacity (more than a million mixnet packets per second) from the start and that sustains a sizeable community of operators, we set a minimum value for the mixnet width of $W = 120$ nodes (even if in the beginning there is very little or no traffic), which results in $K = 720$ nodes, of which $A = 360$ are active across 3 layers and the other $B = 360$ are in reserve. We note that Nym uses cover traffic that makes up for low user traffic, so that $W = 120$ does not result in poor anonymity due to thin traffic per node, and also that mix nodes may run on fewer than 16 CPU cores until the network is functioning at capacity for $W = 120$.

Finally, we assume that at all times there is an excess of mix node candidates to sample from, i.e., $N > K$. In our experiments we consider $N = 2K$ total registered nodes, meaning that in each epoch half the nodes are selected for rewards. We discuss the effects of this parameter choice in Section 5.5.

5.3 NYM exchange rate and service pricing

Token exchange rates are notoriously volatile and hard to predict, often due to speculation. To factor out exchange rate effects (which are extraneous to the reward scheme and would obscure rather than enlighten the dynamics of the scheme itself) and simplify our study, we consider that the exchange rate of NYM and USD is constant at parity, i.e., 1 NYM = \$1. In terms of the overall effects of variations in the exchange rate, we can say that a highly valued token makes the mixmining reward pool emissions be worth more and thus increases the desirability of participation (both for operators and stakeholders) regardless of fee income, while a low token price would diminish the value of pool emissions (the 'subsidy' would be worth very little) and make the system wholly dependent on user fees, which are expected to remain stable in fiat (converted to NYM) because they depend on node operational costs and user willingness to pay, both of which are tied to fiat.

[12] Although this is relatively high, it is in line with profit fees taken from networks such as Cosmos, available at `https://cosmos.fish/leaderboard/all`.

In terms of pricing, we consider that users are willing to pay $1 per million anonymous mixnet packets. With the current deployed size of 2 KB per packet, this corresponds to up to 2 GB of anonymized user data for $1 (which, depending on the underlying application, can be significant throughput, e.g. for Ethereum transactions assuming an average size of 500 bytes, this would translate to 4M transactions). Note that the ideal packet size is dependent on the applications used over Nym, and thus if applications accessible through Nym require exchanging large volumes of data, larger packet sizes may be introduced to lower the cost per byte for users. For example, large mixnet packets of 1 MB would enable users to send up to 1 TB for $1. This would be effective because the mixnet performance bottleneck is the processing power required for public key operations per packet header, while being mostly insensitive to packet payload size. If the applications that use Nym involve short exchanges of data, e.g., sending blockchain transactions or text messages, then packet sizes of just a few KB utilize bandwidth more effectively. In our simulations we consider just the number of packets. We assume for simplicity that the price of $1 per million packets remains constant over time, i.e., that the system adjusts the parameter τ (Eq. (1)) if needed to keep user prices constant at that level.[13] Of course, these assumptions in terms of user fees and payment are vast simplifications and need in-depth investigation in future research.

In terms of the interaction between the NYM exchange rate and Nym service pricing, we expect service prices (as well as operational costs) to remain stable in fiat, while adjusting for the exchange rate of NYM if it fluctuates. Beyond accounting for exchange rate adjustments however, we note that an appreciation in value of the NYM token allows for setting a lower τ (even $\tau = 0$), as the mixmining rewards alone provide strong incentives for participation in the system, while a low exchange rate for the NYM token may require raising τ to ensure mix nodes receive enough rewards after covering costs to be willing to continue to provision the service.

5.4 Available mixnet rewards

The budget of rewards $R(t)$ available to the mixnet per monthly interval t is the aggregation of two sources of income: the emissions of the mixmining pool, which per interval amount to 2% of the funds in the pool $P(t)$, and 60% of the total income from mixnet usage fees $F(t)$. Setting monthly pool emissions at 2% makes the reserve deplete slowly, lasting multiple years, while at the same time it provides enough rewards from the start to sustain a large enough set of operators: with 250m NYM allocated to the pool, the emissions in the first month amount to 5m NYM, and after one year the pool still emits about 4m NYM per month, i.e., 80% of the initial value. When considering $K = 720$ nodes, 5m NYM results in almost 7k NYM per node per month in the equilibrium, and about 0.7% monthly (8% annualized) returns for NYM stakeholders supporting the node. In terms of bandwidth fees, we note that packets typically travel five hops, with the first and last hop being a gateway and the three middle hops corresponding to nodes in each of the three mixnet layers. Therefore allocating 40% of the income to gateways and 60% to the mixnet is a fair split that reflects each party's contribution to the service provisioning. Thus, the budget of rewards available for distribution to the mixnet in interval t is:

$$R(t) = 0.02 \cdot P(t) + 0.6 \cdot F(t) \tag{8}$$

This budget $R(t)$ is distributed among individual mix nodes, each receiving a share $R_i(t)$ depending on their parameters, according to Eq. (4).

Mixmining pool. The mixmining pool is initialized with $P(0) = 250$ million NYM, and updated per interval as:

$$P(t+1) = P(t) - 0.02 \cdot P(t) + U(t), \tag{9}$$

where $0.02 \cdot P(t)$ is the inflation emitted by the pool and $U(t)$ are the rewards available for distribution to the mixnet that remain unclaimed and are returned to the pool, computed as:

[13] Although there are no direct comparables for charging for anonymized data via a mixnet, for packet sizes of a few KB this simplified price is in line with estimates from VPN monthly pricing: `https://www.codeinwp.com/blog/how-much-does-a-vpn-cost/`.

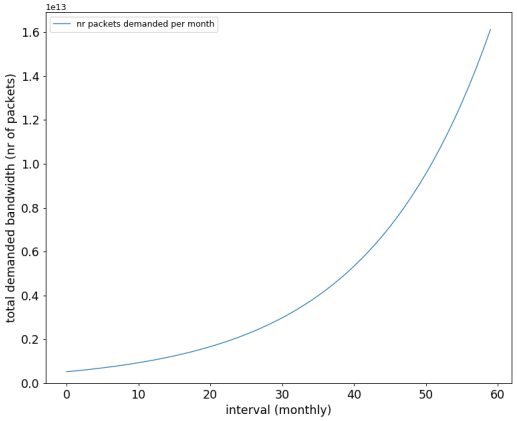
$$U(t) = R(t) - \sum_i R_i(t) \tag{10}$$

$R(t)$, $R_i(t)$ and $U(t)$ are computed by the simulator based on the system and node parameters that determine the rewards distribution. The interval rewards $R_i(t)$ per node are the aggregate of the rewards allocated by our scheme to the node per epoch (cf. Eq. (4)), considering 720 epochs (hours) per interval (month), and sampling (proportionally to reputation), on a per-epoch basis, A nodes to be *active* and B nodes to be in *reserve*, for a total of $K = A + B$ sampled nodes that are *rewarded*. These K nodes are sampled from a larger set of $N > K$ registered node candidates. Updates to W (and consequently updates of A, B, K, and N) happen in the change of interval, whenever needed to serve increased demand. Accordingly, we show results at monthly (or yearly) granularity rather than per epoch. When computing rewards for an interval with 720 epochs, the scheme accounts for the number of epochs in the interval that a node was selected as active (the node was one of the first A sampled nodes, and is rewarded at the 'active' work rate), selected as reserve (the node was one of the last B sampled nodes, and is rewarded at the 'reserve' work rate), or not selected for rewards (the node receives zero rewards for those epochs).

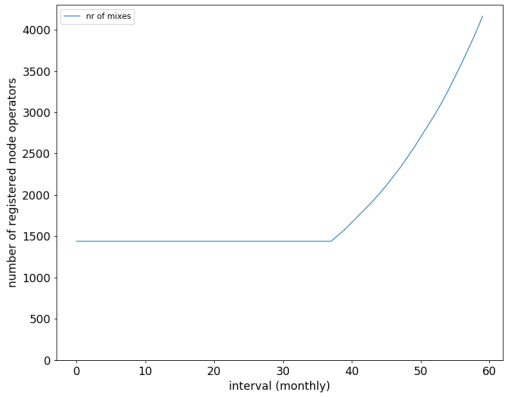
Income from fees. For the income from fees $F(t)$ we consider two extreme scenarios to explore a wide range of possible reward outcomes for participants:

1. **Scenario S_0:** "low demand" is a scenario with low income from fees which, without loss of generality, we will assume to be the worst possible case, namely $F_0(t) = 0$. Scenario S_0 provides the horizon of viability of a mixnet that relies on the mixmining pool alone. We consider the scheme rewards $K = 720$ nodes, of which half are active in the mixnet at any time, and another half are kept in reserve ($A = B = 360$ and $W = 120$), while $N = 1440$ candidate nodes are available to sample from at any time.
2. **Scenario S_1:** "growing demand" is a scenario with 6% growth of demand per monthly interval, i.e., $F_1(t + 1) = 1.06 \cdot F_1(t)$, which about doubles demand every year. $F_1(0)$ is the income corresponding to an initial average load of 200k packets per second, which amount to $0.5 \cdot 10^{12}$ packets in the first month, as shown in Figure 3a. With fees priced at 1 NYM per million packets, $F_1(0) = 0.5$ million NYM, of which 200k NYM are taken by gateways leaving 300k NYM to the mixnet (note that $P(0) = 5$ million NYM, and thus initially usage fees provide just 6% of the mixnet budget). After 5 years, in this scenario the network routes $16 \cdot 10^{12}$ packets per month, amounting to almost ten million NYM in fees for the mixnet. Compared to less than four million NYM of monthly pool emissions, in S_1 fees provide more than 70% of the mixnet income by the end of year five, with the mixmining pool providing the remaining 30%. As shown in Figure 3b, the exponentially increasing demand triggers a scaling up of the mixnet in the beginning of the fourth year (month 38), from the configured initial size of $K = 720$ rewarded nodes up to more than two thousand, allowing us to study network growth funded by fees. Note that we consider N to be double the number K set by the reward scheme as optimal for the equilibrium, and thus the number N of node candidates shown in the figure is double of K.

Figure 4 shows for both scenarios S_0 and S_1 the evolution of the mixmining pool emissions ($0.02 \cdot P(t)$), the mixnet income fees ($0.6 \cdot F(t)$), and their aggregation as available rewards $R(t)$, of which $\sum_i R_i(t)$ are distributed to mix nodes and $U(t)$ remain unclaimed. As shown in Figure 4a, in S_0 all the network income is due to pool emissions, which slowly diminish over time (the green line representing fee income is at zero and not visible, while the blue and orange lines overlap). After five years, the monthly emissions have declined in this scenario to about half the initial monthly amount of 5 million. With the considered distribution of pledges and delegation (described in detail in the next section), slightly more than half the available rewards are distributed to nodes in this scenario while the rest is returned to the pool as unclaimed. Figure 4b shows the total budget of rewards in S_1 increasing over time due to the growing income from fees, which overtake pool emissions as the main source of income after three years (month 42). In the last year of the simulation (from month 45), the amount of unclaimed rewards is larger than the pool emissions, meaning that the pool is replenished for a few intervals. This replenishment would stop once fee income stabilizes at

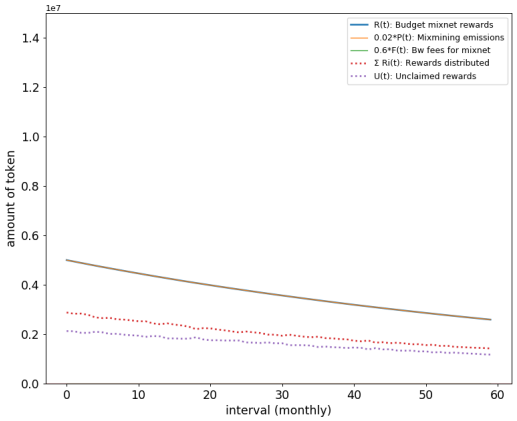


(a) Bandwidth demand in S_1 (packets per month).

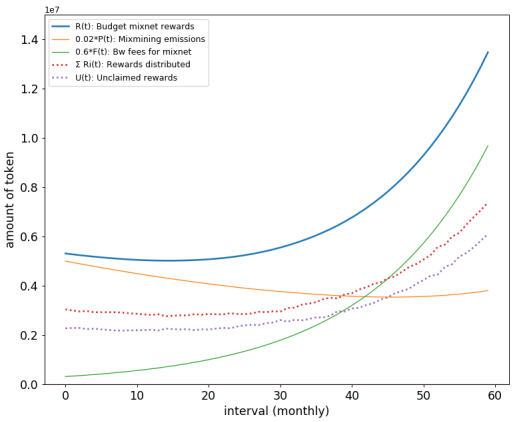


(b) Number N of registered mix node candidates over time in S_1, considering $N = 2K$ and an initial $K = 720$.

Fig. 3: Scenario S_1: exponential growth in demand and mixnet size over five years (60 months).



(a) Rewards budget in scenario S_0



(b) Rewards budget in scenario S_1

Fig. 4: Evolution over 60 months in S_0 and S_1 of: pool emissions $0.02 \cdot P(t)$, mixnet income fees $0.6 \cdot F(t)$, available rewards $R(t)$, distributed rewards $\sum_i R_i(t)$ and unclaimed rewards $U(t)$.

some level or stakeholder engagement increases (which would reduce the proportion of unclaimed rewards), leading again to shrinking of the mixmining reserve. The reserve thus acts as a buffer that depletes when needed to subsidize network operations, and replenishes if the network income grows steeply without stakeholders being fully engaged in contributing to node reputation.

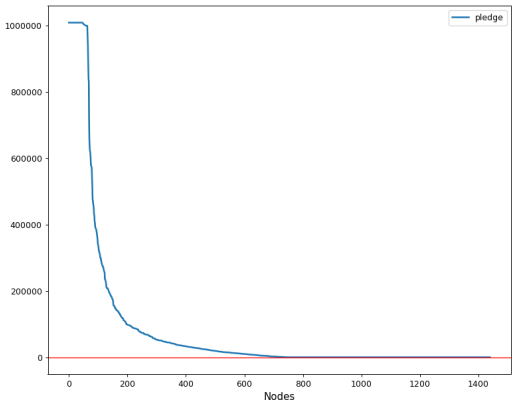
5.5 Staking distribution and parameters.

The NYM total supply is **constant** at one billion token, all of which are created at genesis. Initially, the NYM supply available for pledging and delegation amounts to 750 million token, with the other 250 million token being in the mixmining pool and thus unavailable. The per-node **stake saturation point** is given by the available stake uniformly distributed over K nodes, i.e., by $750 \cdot 10^6 \cdot \frac{1}{K}$. For the initial $K = 720$ nodes this amounts to a saturation point of 1.04 million NYM per node. As the mixmining reserve funds are released, the total NYM supply available for pledging and delegation increases accordingly, and so does the saturation point. Conversely, when the number K of rewarded nodes increases, the saturation point decreases.

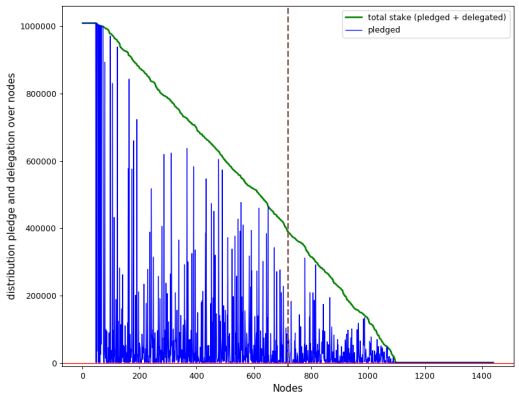
The equilibrium analysis presented in Section 3.5 shows that in an ideal frictionless world, the system has an equilibrium state with all available stake evenly distributed among exactly K nodes, all of which are at saturation point (maximum reputation of one) and operated by the stakeholders with the largest stake to pledge. In real-world settings however, we can expect deviations from the ideal world. For example, we can expect a larger number N of registered nodes than the equilibrium

value K, as is currently the case in comparable deployed systems such as Cardano, where most candidate nodes are unsaturated and there is a long tail of nodes that have minimal pledging and no delegation. Furthermore, not all stakeholders stake all their token, leaving a fraction unallocated (cf. Remark 7), and for a variety of reasons some large stakeholders may prefer to delegate their stake rather than pledge it to operate themselves a node. Finally, due to all sorts of externalities (e.g., popularity, community dynamics), stakeholders in practice pursue strategies that deviate from purely maximizing returns to prioritize support of nodes they like; and due to action inertia they may fail to act in a timely fashion as the system re-configures, leaving their stake sub-optimally allocated. We attempt to capture these aspects in our simulations in order to evaluate the reward scheme in realistic conditions.

Of the available NYM token (initially 750 million), we consider that stakeholders dedicate 15% of their total combined stake to pledging and 60% to delegation, with the remaining 25% of available stake being unallocated.[14] These pledged and delegated NYM are spread over N node candidates, each with an aggregate amount between the minimum pledge and the saturation point. We consider distributions of pledging and delegation that are in line with what can be observed in existing staking systems such as Cardano.[15] We take into account that pledges are constrained by how stake is distributed among stakeholders, with a small number of large stakeholders (e.g., investors and other 'whales' that have acquired large amounts of NYM) who can saturate their pledges to maximize rewards, and a large number of stakeholders with a limited budget to pledge. We aim to study the reward outcomes for participants with a wide range of budgets (pledge) and reputation (aggregate of pledge and delegation). For this, and in line with other research in the space [7], we consider a very skewed Pareto distribution of pledges with a few saturated nodes (pledges of 1m NYM) and a long tail with the minimum pledge of 1000 NYM, as shown in Figure 5a.



(a) Distribution of node pledges in a network with $K = 720$, $N = 1440$, and 15% of available token supply dedicated to pledging. Ordered by pledge.



(b) Distribution of reputation (pledge+delegation) in a network with $K = 720$, $N = 1440$, 15% of available token supply dedicated to pledging and 60% delegated. Ordered by reputation (pledge+delegation).

Fig. 5: Distribution of pledges and reputation (snapshot for an epoch).

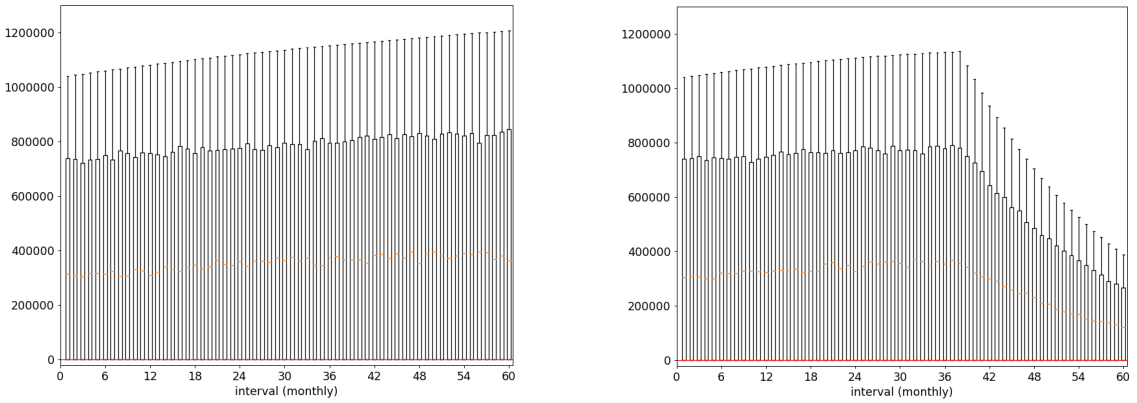
We further consider that 60% of the NYM supply is delegated to registered nodes. We allocate delegated token to nodes in a randomized manner (uniform amount of delegation between zero and the saturation point minus the pledge), choosing first the nodes whose pledge is larger than the minimum until the delegation budget is exhausted. As shown in Figure 5b, this results in part – but not all – of the nodes with minimum pledge receiving delegation, some even up to the saturation point, allowing us to study a broad range of pledge-delegation combinations. Once all the delegated stake has been allocated, there remains a tail of nodes with minimal pledge and no delegation. Given that the minimal pledge is much smaller than the saturation point, this

[14] Note that 66% is the target amount of Cosmos for staking and 75% is in line with other projects like Polkadot: `https://w3f-research.readthedocs.io/en/latest/polkadot/overview/2-token-economics.html`

[15] See for instance, `https://pooltool.io`.

amounts to negligible reputation. Considering $N = 2K$, three quarters of registered nodes have non-negligible reputation while the last quarter has negligible reputation. Increasing N to account for more nodes with negligible reputation does not change the reward dynamics, since nodes with negligible reputation are (almost) never selected, and even when they are, they receive a small amount of rewards and thus have no impact on the rewards of nodes with non-negligible reputation. In other words, nodes with negligible reputation are practically irrelevant, and the existence of a smaller or larger set does not make a difference for nodes with non-negligible reputation. The value of $N = 2K$ should however be taken into account when interpreting results that show boxplot distributions over the set of nodes: the bottom quarter (third quartile) of nodes have negligible reputation (and consequently negative profits due to low rates of selection and rewards), while the median corresponds to the K-th highest reputation node. Larger values of N, e.g., $N = 10K$, would result in the vast majority of nodes having negligible reputation and, when depicting distributions, only the outliers would show meaningful results for the high-reputation nodes that are actually players in the network.

We recall that the per-epoch selection of nodes is proportional to their reputation expressed as stake saturation level, i.e., the fraction of pledge and delegated token of nodes relative to the stake saturation point. For example, if the stake saturation point is reached at 1 million NYM, a node that aggregates 200k NYM between pledge and delegation has a reputation or saturation level of 0.2, or 20%. Considering $N = 2K$, only half the nodes are selected for rewards in each epoch, and given that more than half have non-negligible reputation (marked with the vertical dotted line in Figure 5b), not all nodes with non-negligible reputation are selected in every epoch for rewards.



(a) Scenario S_0.

(b) Scenario S_1.

Fig. 6: Boxplots with the distribution of node reputation (pledge+delegated token) over the set of N node candidates and its evolution on a monthly basis for 5 years (60 months). In both scenarios 15% of available token supply is dedicated to pledging and 60% is delegated.

In Figure 6 we show how the distribution of node reputation evolves over time in scenarios S_0 and S_1. We represent each interval's distribution of aggregate pledge and delegation as a boxplot[16] where the top values mark the per-node saturation point in that interval (initially at 1.04m NYM). Note that each individual boxplot can be represented as Figure 5b, where the median is marked by a vertical dotted line and the maximum values are on the left of the x axis. In S_0 the network size is constant and thus the distribution remains stable, with a slight increase in values over time due to the increased circulating supply (caused by the emissions of the mixmining reserve). In S_1 we can observe that the amount of token staked per node decreases from the fourth year (month 38), as from that moment the mixnet size grows every month and the token supply is redistributed among a larger number of nodes to account for network scaling, which lowers the per-node saturation point.

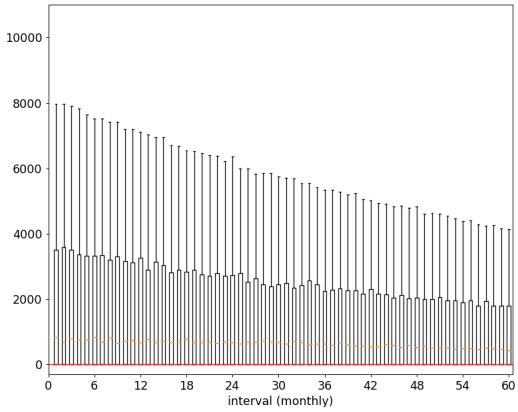
[16] In each boxplot, 50% of the the data is within the box, the orange line is the median, the whiskers show the range of the data, and outliers (if any) are plotted as dots.

6 Experimental results

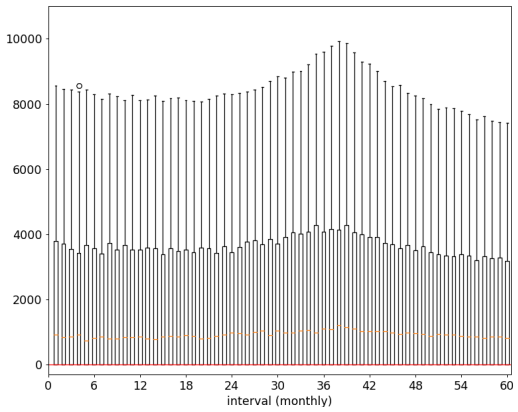
We run our simulator in the described experimental setup and study participant rewards. In all the figures we show on the left results for the S_0 (low demand) scenario, and on the right for S_1 (growing demand). We recall that these results are illustrative of the functioning of the scheme but provide no guarantees or even likelihood on the rewards that stakeholders can expect in any deployment in the real world.

6.1 Distribution of node rewards

First we examine the distribution of rewards over nodes per interval. Figures 7a and 7b show boxplots with the distribution of monthly rewards to nodes over a 5-year period. The top whisker per box corresponds to the rewards of the most rewarded node in the interval; the top of the box marks the first quartile of the distribution; the median is marked with an orange line; and the bottom whisker corresponds to the rewards of the least rewarded node, which is usually zero considering there is a tail of nodes with minimal reputation, unlikely to be selected for rewards.



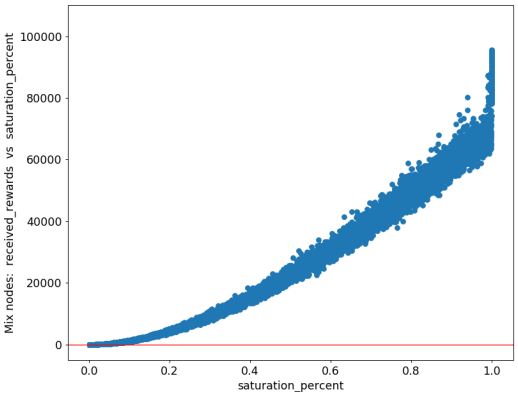
(a) Monthly rewards received by nodes in S_0 over five years.



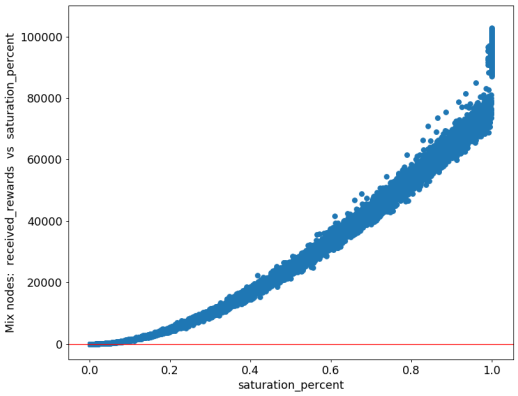
(b) Monthly rewards received by nodes in S_1 over five years.

Fig. 7: Distribution of monthly rewards to nodes over five years (60 months), considering $K = 720$ minimum rewarded nodes per epoch and $N = 2K$ total node candidates.

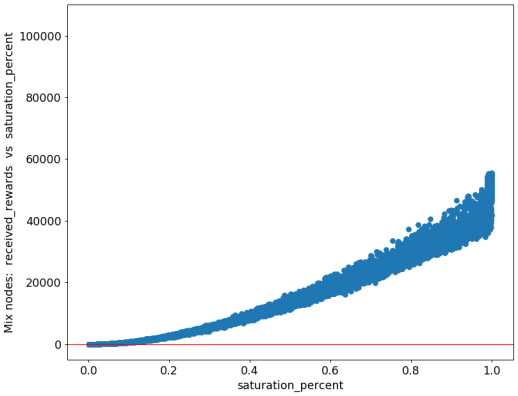
We can see that in both scenarios the node median rewards are stable at around 1k NYM per month, though slightly lower in S_0, particularly after some time. As we are considering $N = 2K$ total node candidates, the median (orange line) corresponds to the K-th most rewarded node, which in a situation of equilibrium would be the last existing node, while the first quartile (top of the box) represents the $\frac{K}{2}$-th node, which would be the median node in a situation without excess candidates. In S_0, the most rewarded nodes (those with maximum reputation) initially receive 8k NYM per month, slowly declining to about 4.5k NYM per month after five years. In S_1, as result of the exponential growth in demand (and corresponding income from fees), the rewards per node do not diminish even as there are more nodes to reward. The peak at month 38 corresponds to the network taking fees at capacity for $K = 720$, when bandwidth demand has grown to fully utilize the initial capacity, but right before additional demand makes the mixnet increase over the initial size (thus increasing the number of nodes over which to spread rewards). Once the network starts scaling, the per node rewards stabilize around 3.5k NYM for the first quartile and 8k NYM for the top rewarded nodes, with the median remaining at 1k NYM per month. Thus, as long as the NYM exchange rate does not diminish to the point of making the mixmining rewards worthless, these results indicate that under this model, the network can operate and remain viable for a few years, even with low income from usage. This provides the system with ample time to integrate applications and grow the user base – keeping in mind that long-term sustainability is only possible with eventual income from fees.



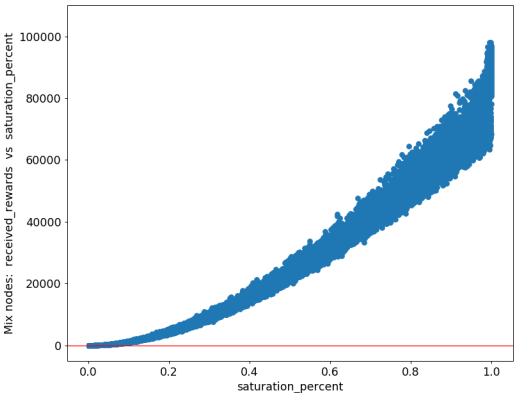
(a) Annualized node rewards in S_0 (first year).



(b) Annualized node rewards in S_1 (first year).



(c) Annualized node rewards in S_0 (fifth year).



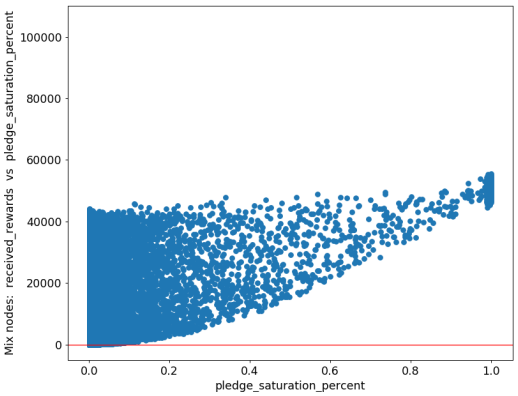
(d) Annualized node rewards in S_1 (fifth year).

Fig. 8: Annualized node rewards relative to node reputation (stake saturation level of the node).

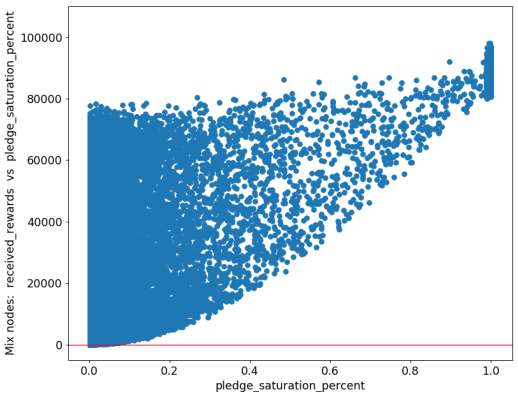
To better understand the relationship between node reputation and received rewards, i.e, which nodes are at the top of the boxplot and which at the bottom, we take snapshots of the network in the first and fifth years of simulation, for both S_0 and S_1. The results are in Figure 8, where we show a scatterplot of the annualized rewards received by nodes relative to their reputation level; i.e., each dot with coordinates (x, y) is a sample from a node in the simulation, the x coordinate is the node reputation and the y coordinate the annualized rewards received by the node. As we can see in Figure 8a and Figure 8b, the results are similar for both scenarios in the first year of operation.

The difference between the two scenarios becomes visible by the fifth year of operation, shown in Figure 8c and Figure 8d, for S_0 and S_1, respectively. In S_0 rewards have diminished and, for the same level of reputation, nodes are receiving about half the amount of rewards compared to the first year of operation. In S_1 on the other hand, for a level of reputation nodes still receive the same amount of rewards as they did in the first year. Note that due to growing demand in S_1 the network has become larger after five years (higher W, K and N), which lowers the per-node stake saturation point, and results in more nodes having high reputation levels. This is visible in Figure 8d with a higher density of samples in the higher saturation values, meaning that not only nodes keep receiving the same level of rewards for a saturation level, but also that more nodes are being rewarded at high levels.

In all depicted cases there is an obvious strong positive correlation between node reputation and received rewards. Nodes with a reputation level below 10% barely receive any rewards. On the other extreme, we can observe some variance within the set of nodes with maximum reputation of 100%, with two groups being distinguishable in Figure 8b. This difference relates to the size of the nodes' pledge, weighed by the parameter α in our reward scheme (Eq. (4)). The nodes receiving higher rewards are those with large pledges that significantly contribute to the reputation of the node. Those operators are compensated for the opportunity cost of locking up a large amount of token



(a) Received node rewards in S_0, fifth year.



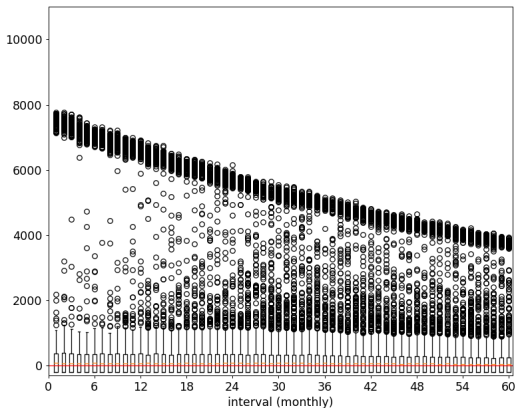
(b) Received node rewards in S_1, fifth year.

Fig. 9: Annualized node rewards (fifth year) relative to the level of pledge saturation.

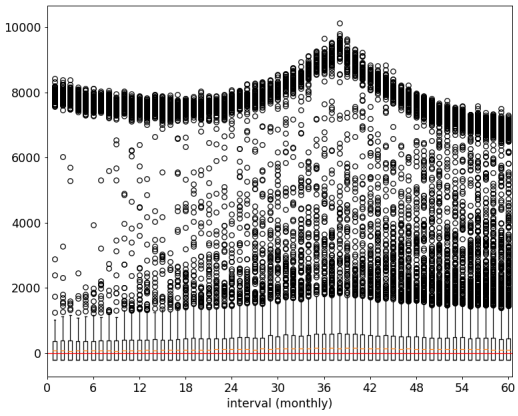
and for having more 'skin in the game'. The set of nodes receiving lower rewards are those with small pledges, which reach saturation primarily with delegated stake. This is illustrated even more clearly in Figure 9, where we show node rewards relative to the level of pledge saturation (ignoring delegation), and we clearly see the cluster of highest rewards corresponding to nodes whose pledge fully saturates the node. For low pledges, the variance in node rewards is very significant as it depends on the reputation of the node. As we can see in Figure 9b, a node with minimal pledge (saturation barely above zero) may receive up to 80k NYM per year if it becomes fully saturated and reaches maximum reputation, and as little as zero if it receives no delegation from other stakeholders; while a node with 60% of pledge saturation receives a minimum of 40k NYM when it receives no additional delegation, and up to 85k NYM when it becomes fully saturated thanks to delegation. Nodes with fully saturated pledges are the best rewarded with between 80k and 100k NYM per year.

6.2 Distribution of node operator profits

From the amount of rewards allocated to a node (shown in the previous figures), our scheme first subtracts and refunds the node's operational costs ($C(\cdot) = 200$ in the considered case). The remainder represents the node's *profit*, and it is split between the operator and the delegates according to Eq. (5) and Eq. (6).

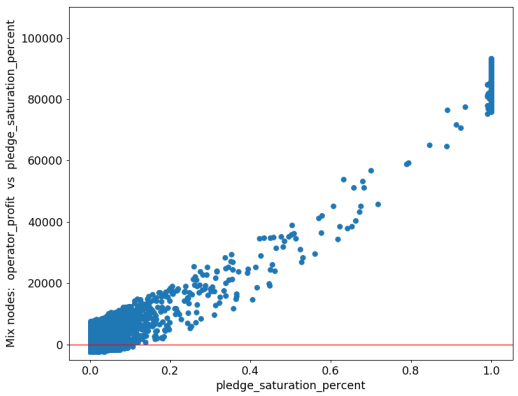


(a) Monthly operator profits in S_0.

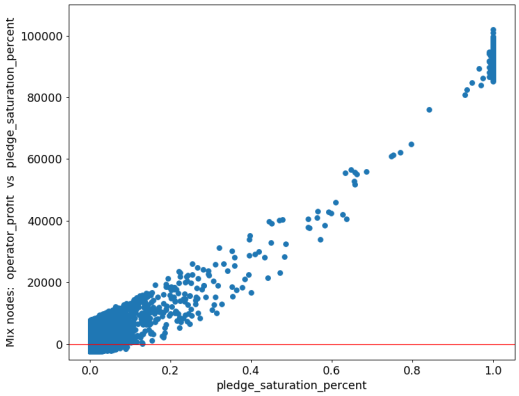


(b) Monthly operator profits in S_1.

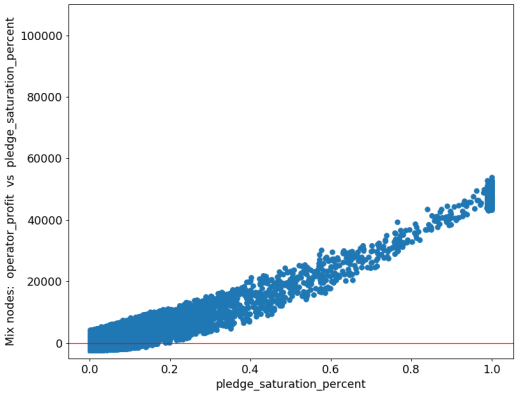
Fig. 10: Distribution of monthly profits to node operators over five years (60 months), considering at least $K = 720$ rewarded nodes per epoch and $N = 2K$ total node candidates.



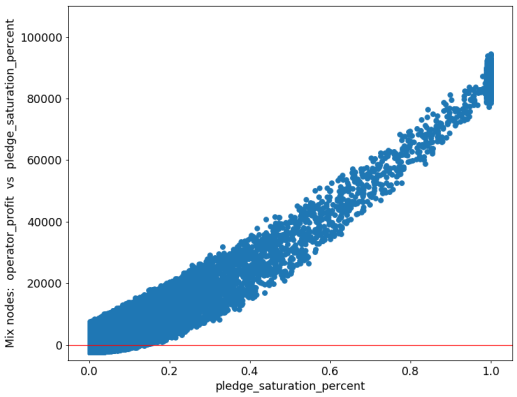
(a) Annualized operator rewards in S_0 (first year).



(b) Annualized operator rewards in S_1 (first year).



(c) Annualized operator rewards in S_0 (fifth year).



(d) Annualized operator rewards in S_1 (fifth year).

Fig. 11: Annualized operator rewards relative to the level of pledge saturation.

The net amount of rewards given to the operator *after* refunding costs are the *operator profits* (a node's profit is negative when the operational costs of running the node for a month are higher than the monthly rewards it has received). We show these profits for our studied scenarios in Figure 10, again as boxplots with the distribution of per-node monthly profit for the set of N candidate nodes. In both S_0 and S_1 the outliers at the top represent nodes run by 'whales' who can afford to fully saturate nodes with their pledge alone, and thus receive all the node's rewards (note that those outliers match the top values in Figure 7). The profit of these participants in both scenarios starts at around 8k NYM per month and after five years is at 4k−8k NYM, depending on the demand scenario. The first quartile node, which is the $\frac{K}{2}$-th node in terms of operator profit, makes around 400 NYM net per month in both scenarios, with operator profits slowly decreasing in S_0 over time, down to 200 NYM per month after costs. The median node, which is the K-th node in terms of operator profit, makes a modest but positive net profit in both S_0 and S_1, even at the end of the five year period. Even though the majority of nodes make a profit in both S_0 and S_1, we can see that some nodes take a loss, as the lower part of the boxplots (between the median and the third quartile) are below the red line marking zero, indicating loss (down to a loss of \$200). This is the case for nodes that have very low reputation and thus are rarely sampled as part of the K rewarded nodes — and even when they are, they receive small rewards, which at the end of the month are insufficient to compensate for the operational costs of running a node, estimated at \$200 per month.

Similarly to before, we study the relationship between node operator rewards and node pledge, where the pledge is represented by its corresponding saturation level, i.e., if the per-node saturation point is 1 million NYM, then a pledge of 250k NYM corresponds to a pledge saturation level of 0.25 (25%). Our results for the first and fifth years of simulation, for both S_0 and S_1, are shown in Figure 11. As expected, in all scenarios node operator rewards are proportional to the node's pledge, with rewards per saturation level being sustained over time if the network receives income

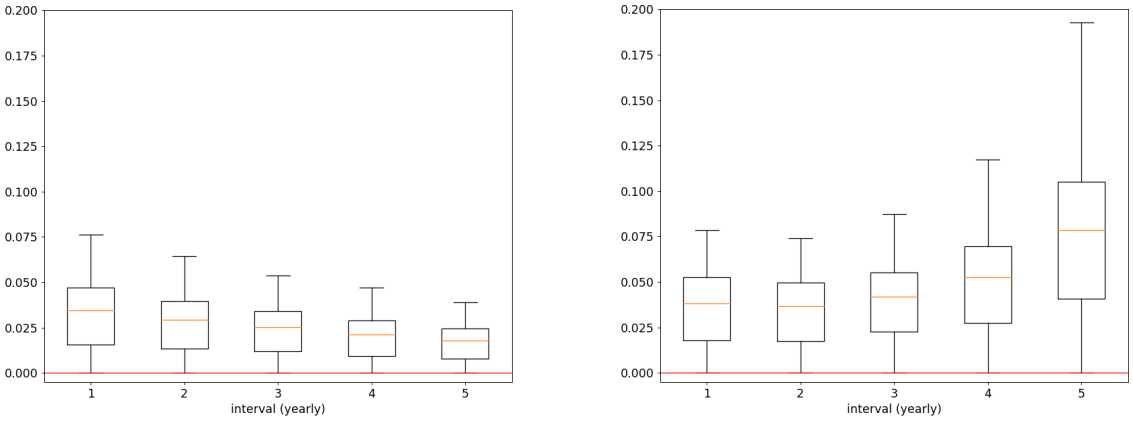
from fees (S_1) – but decaying to about half the amount after five years if the network fails to attract fees and is entirely reliant on the mixmining reserve for rewarding nodes (S_0). Compared to Figure 9, we can see that operators obtain the lower band of the rewards minus the costs, while the excess rewards (if any), which are proportional to delegation to the node, are distributed among the delegates.

We also observe in all four cases that some nodes with low pledge have a negative profit (dots below the red line), meaning that their rewards are insufficient to cover operational costs. In the worst case a node's yearly net profit may be $2400 negative, when the node receives zero rewards and pays operational costs of $200 every month. This lack of profitability only affects nodes with both pledge saturation below 0.2 and low rates of delegation resulting in low reputation. Note that the median (K-th) node considered in our setting has a reputation level of 0.4 (40%), as shown by the dotted line in Figure 5b.

6.3 Distribution of returns to node delegates

We now turn our attention to the returns received by stakeholders that delegate their stake rather than operate a node themselves. Our scenarios consider that all N candidate nodes have identical operational cost, profit margin, and performance; while differing in their pledge and reputation, as before, to isolate the impact of pledging and delegation on rewards.

The distributions of yearly returns for delegates are shown as boxplots in Figure 12, with each sample correspoding to the rewards received by a node in the simulation. We compute the annualized ROS (Return On Stake) without taking into account compounding effects, i.e., simply multiplying monthly ROS by 12. The monthly ROS samples include all nodes with a non-zero amount of delegation, with the ROS value computed by dividing the rewards given to a node's delegates by the total amount delegated to the node. For example, if a node has 500k NYM in delegated token, and it distributes 2k NYM in a month to its delegates, the ROS value for that node in that month is $\frac{2 \cdot 10^3}{500 \cdot 10^3} = 0.4\%$, which corresponds to 4.8% annualized ROS.[17]



(a) Annualized ROS for delegates in S_0.

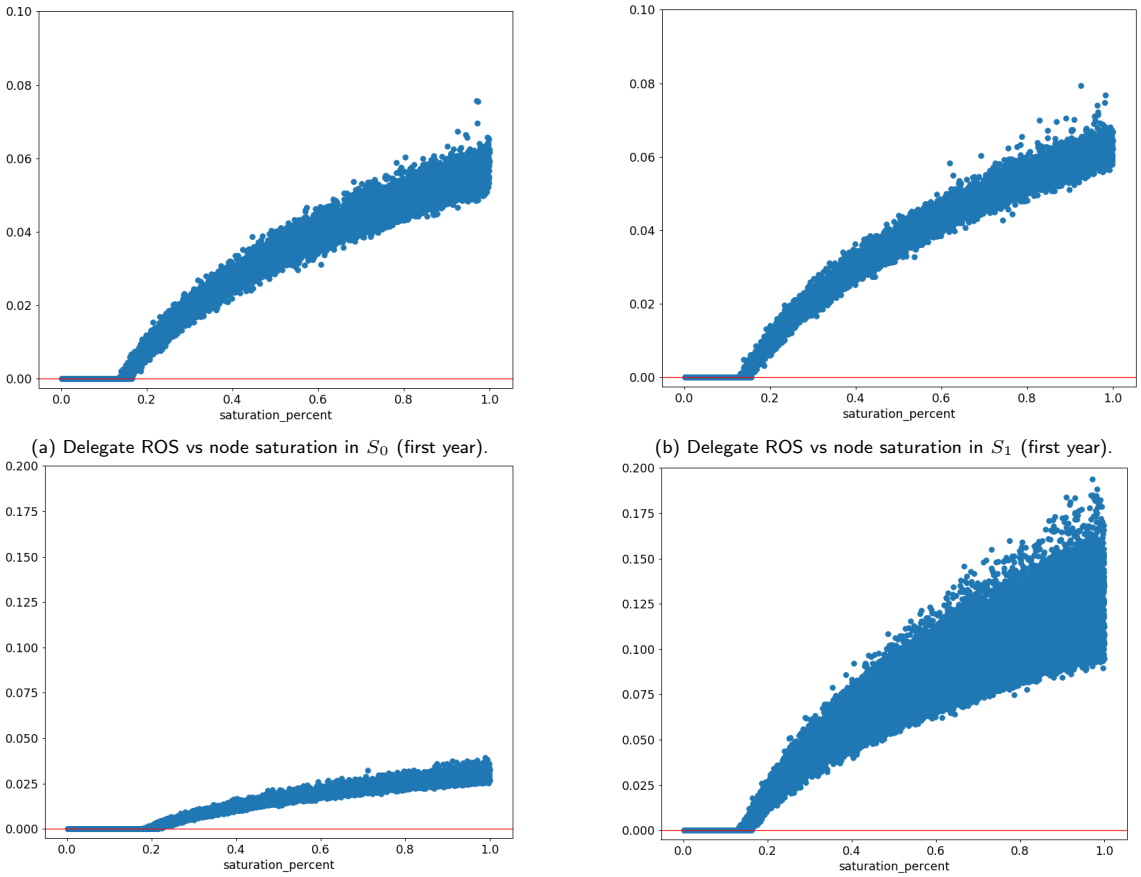
(b) Annualized ROS for delegates in S_1.

Fig. 12: Distribution of ROS (Return On Stake) to node delegates over five years.

Figure 12a shows that in S_0 the annualized ROS for delegates starts with a median of 3.5% and a maximum for the best performing nodes of 7.5%, which is comparable to the ROS that would be attained in the equilibrium. Without any fee income, the ROS declines over time to a median of 2% and a maximum of 4% per year, after five years. As depicted in Figure 12b, in S_1 returns start at a level just slightly above S_0 but, over time, they increase with user demand to a median of 8% and a maximum of 20% per year. The reason for this increase is that the amount of token

[17] We emphasize that the ROS is denominated in NYM and the results shown here are a product of simulations under the assumptions put forth in Section 5. Actual returns in fiat may vary widely - what is presented here should not be construed as investment advice!

available to pledge and delegate to nodes remains relatively constant, while the rewards allocated to the set of stakeholders are significantly multiplied due to the fees taken by the network, leading to higher rewards (returns) per unit of stake.



(a) Delegate ROS vs node saturation in S_0 (first year).

(b) Delegate ROS vs node saturation in S_1 (first year).

(c) Delegate ROS vs node saturation in S_0 (fifth year).

(d) Delegate ROS vs node saturation in S_1 (fifth year).

Fig. 13: Scatterplot of ROS (Return On Stake) vs node saturation, in S_0 and S_1 in the first and fifth years of operation.

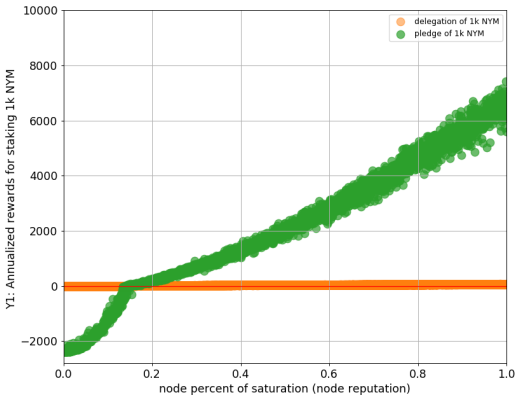
In both S_0 and S_1 scenarios there is a wide spread of ROS between the highest value (corresponding to the delegates of the node that provided the best ROS) and the lowest, which is zero for the fraction of nodes that use all received rewards to cover costs and do not distribute anything to their delegates. We show in Figure 13 the relationship between the ROS offered by a node to its delegates, and the node's reputation level, for both scenarios S_0 and S_1 in the first and fifth years of operation. As we can see in all figures, the returns are highly correlated with the node reputation. Nodes with reputation levels below 20% give zero returns to delegates. Above this threshold, the returns increase up to the maximum return rate, achieved at reputation 100%, which corresponds to the stake saturation point. This illustrates the strong incentives of the scheme towards clustering delegate support on nodes that already have a significant reputation, in other words, collectively reaching consensus on a set of reputable nodes. The ROS for delegates is comparable in the first year for both scenarios (slightly higher for S_1 as there is additional income), as shown in Figure 13a and Figure 13b, where delegates of fully saturated nodes obtain a yearly ROS in the range 5%-7%. In the fifth year however, the returns are vastly different for S_0 and S_1, as illustrated in Figure 13c and Figure 13d. In S_0 the returns decline to half their initial value, while in S_1 they increase very significantly up to a maximum of nearly 20% annual ROS for the best performing nodes, and up to 10% for nodes with medium levels of reputation.

Taking these results into account together with those of the previous section, we can see that in low-demand scenarios (S_0) the mixmining subsidies can sustain the network for some years while demand slowly takes off — as long as the subsidies remain valuable, which are tied to the value of the NYM token. During this time, a sufficient number of node operators are refunded for costs and additionally receive a net profit of several hundred NYM, while delegates make modest returns on their investment. With high demand (S_1), a growing number of operators can be adequately funded by the network as it scales, while delegate return rates *increase* significantly with the network's turnover, strengthening the incentives for stakeholders to engage with the network by pledging or delegating their token.

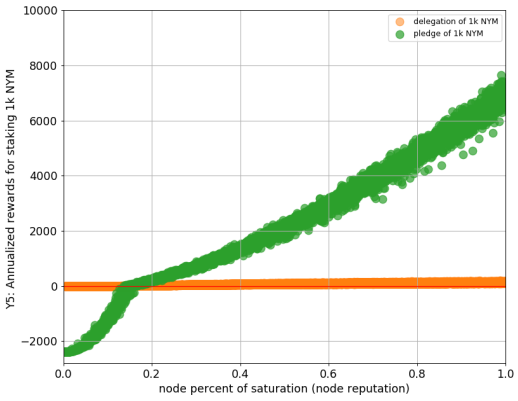
6.4 Return On Stake (ROS) for pledging vs delegation

Finally, we consider stakeholders deciding whether to pledge or delegate their NYM stake, and study the rewards they would receive in the simulated scenarios for pledging versus delegating 1k, 10k, and 100k NYM to nodes with varying levels of reputation. For brevity we only show results for the first year of scenario S_0 (which are almost identical to the results for the first year of scenario S_1) and the fifth year of scenario S_1. The results for the fifth year of S_0 differ in expected ways, consistent with the results shown in previous sections: rewards become half the amount they were in the first year of S_0.

We show in Figure 14 the simulated returns for pledging and delegating 1k NYM in the considered scenarios. Each dot at coordinates (x, y) is a sample taken from a node in the simulation, with the x being the node's reputation, and the y being the rewards obtained from pledging (green dots) or delegating (orange dots) 1k NYM to that node. In the case of pledging (green dots), we only sample nodes with a comparable pledge, defined as within 20% of the considered amount, i.e., for 1000 NYM, we only sample operator ROS (node operator profit divided by the node pledge) for nodes whose pledges are between 800 NYM and 1200 NYM, and multiply their operator ROS by 1000 to obtain the returns for the considered 1k NYM pledge. In the case of delegation (orange dots), we sample the delegates' ROS (total delegate rewards divided by total delegated stake) of all nodes with an amount of delegation equal or superior to the considered amount (i.e., for 1k NYM we consider nodes that have at least 1k NYM delegated to them) and multiply their delegate ROS by 1000 NYM to obtain the rewards corresponding to the delegation of 1k NYM to that node.



(a) Simulated returns for pledging and delegating 1k NYM in S_0 (first year).

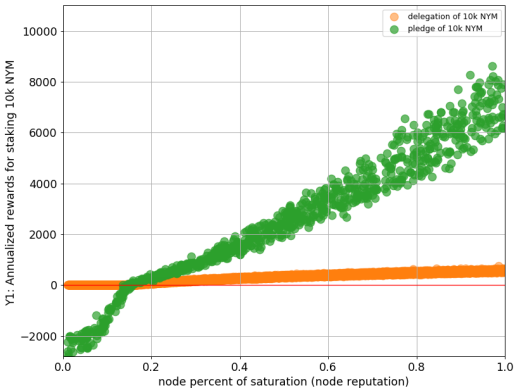


(b) Simulated returns for pledging and delegating 1k NYM in S_1 (fifth year).

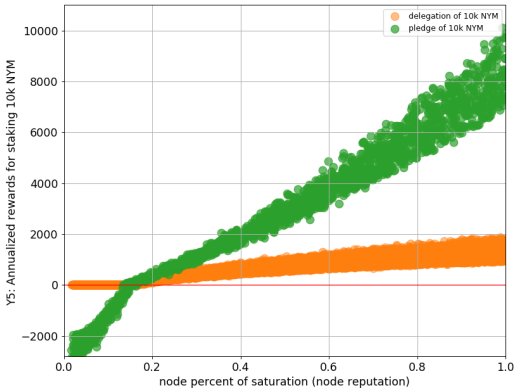
Fig. 14: Simulated annual rewards when pledging and delegating 1k NYM in the considered scenario.

As we can see in Figure 14a and Figure 14b, for a given level of node saturation a pledge of 1k NYM leads to rather similar rewards in both cases, even though the considered underlying scenarios are vastly different. Pledging 1k NYM to a node that becomes fully saturated with delegated stake results in returns of 6k-8k NYM per year for the node operator in the considered scenario. On the other hand, if the node saturation level is below 0.2 (20%), rewards will not be sufficient to offset operational costs, resulting in a negative net balance for the operator. If the stakeholder decides

to delegate rather than pledge the 1k NYM, in S_0 they initially receive about 75 NYM per year in rewards when the node they delegate to is fully saturated. This compares to up to 200 NYM per year for delegating to fully saturated nodes in S_1 in the fifth year. Nodes with lower levels of saturation give lower rewards to their delegates, and even no rewards when the saturation level is below 0.2 (note that this threshold may be different in scenarios with different rates of pledge and delegation by stakeholders). Delegates do not contribute to operational costs and thus never have a net negative profit – at worst they receive zero rewards.



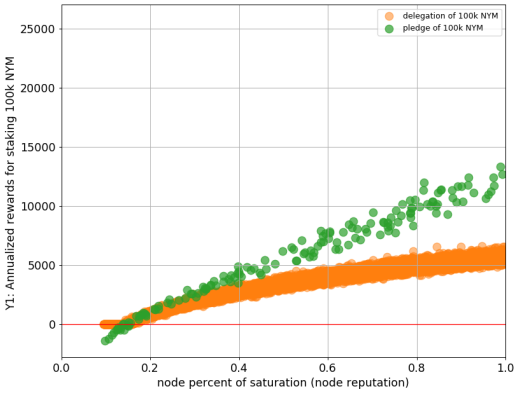
(a) Simulated returns for pledging and delegating 10k NYM in S_0 (first year).



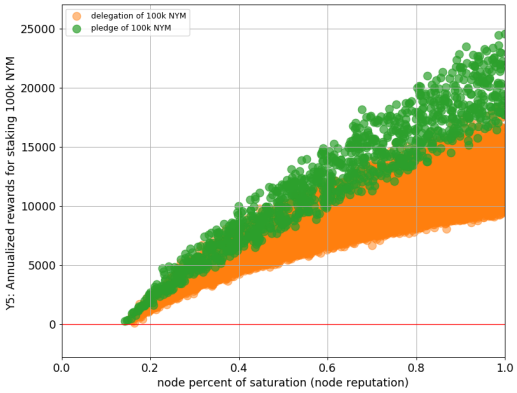
(b) Simulated returns for pledging and delegating 10k NYM in S_1 (fifth year).

Fig. 15: Simulated annual rewards when pledging and delegating 10k NYM in the considered scenario.

Figure 15 shows the results for pledging and delegating 10k NYM. In Figure 15a we can see that the operator returns for pledging 10k are only marginally higher than for pledging 1k (Figure 14a). In the high-income scenario depicted in Figure 15b, the operator returns for pledging 10k NYM are about 20% higher compared to a 1k pledge (Figure 14b). Taking into consideration that the pledge is ten times larger, this is a modest increase in returns. The difference in returns is however very significant when looking at the rewards obtained from delegating 10k compared to delegating 1k, which are roughly proportional to the amount of delegated NYM and thus increase by an order of magnitude.



(a) Simulated returns for pledging and delegating 100k NYM in S_0 (first year).



(b) Simulated returns for pledging and delegating 10k NYM in S_1 (fifth year).

Fig. 16: Simulated annual rewards when pledging and delegating 100k NYM in the considered scenario.

In our third and last example, shown in Figure 16, we examine the returns obtained for pledging and delegating 100k NYM. For S_0 (Figure 16a), we can see that the returns for pledging increase

with respect to smaller pledges, but moderately so. A 100-fold increase from pledging 1k NYM to pledging 100k NYM only increases operator rewards from a maximum of 7.5k NYM per year to a maximum of 14k NYM per year, which is less than double. In the case of S_1 (Figure 16b) the pledging rewards for 100k increase more than double compared to just pledging 1k (Figure 14b), still making the increase in returns modest compared to the increase in pledge. In the case of delegation however, we can see that stakeholder returns increase proportionally to the delegated amount. In Figure 14b, the growth in returns for delegates reduces the differential in returns compared to pledging, as stakeholders pledging a large amount can make just slightly lower returns by delegating their token, without the need to spend time and effort operating themselves a node.

In summary, our mixnet reward scheme prioritizes in first instance the viability of mix node operators, ensuring that they cover operational costs and make a sufficient additional profit to be incentivized to operate. Even if their own NYM pledge is very small, as long as their overall reputation is high (meaning that their node has a high saturation level due to delegated stake), nodes receive a consistent amount of NYM rewards even if the network has low usage in the first few years. Once sufficient rewards have been dedicated to ensure operator incentives and viability, the scheme compensates stakeholders proportionally to their support of well-performing, high reputation nodes. The rate of returns for delegates is more sensitive to the network income than the operator returns. When the network income increases, the number of rewarded nodes increases accordingly (the per-node saturation point decreases with the inverse of this number), while the per-operator rewards remain stable and the per-staked-token returns increase proportionally to the network income.

We note that the scheme's incentives for stakeholders change with the amount of NYM they have. A stakeholder with just 1k NYM to pledge or delegate makes a choice between: (i) safely earning a few dozen NYM over the year by delegating the 1k to high-reputation, well-performing nodes; or (ii) pledging that amount to their own node, and potentially making thousands of NYM in returns over the year if the node attracts enough delegated stake, i.e., if it becomes a high reputation node; but also potentially failing to attract enough delegated stake and thus getting no rewards, while still having costs to pay for operating the node. In contrast, a stakeholder with 100k NYM chooses between: (i) safely earning thousands of NYM in returns by delegating to high-reputation, well-performing nodes; and (ii) obtaining up to double the amount rewards by pledging to their own node instead, assuming that that node is successful in becoming saturated with delegated stake — if the node is unsuccessful in attracting delegated stake, the stakeholder may end up with fewer rewards than if the 100k had been delegated to someone else with more reputation. From this perspective, larger stakeholders may have more of an opportunity cost from pledging than smaller stakeholders, and if they are successful after taking a risk, they can *at best double* their returns. In contrast, small stakeholders have a higher-risk and higher-reward choice to make: they can get returns that are *two orders of magnitude larger* if they pledge and operate a successful (high reputation) node, compared to delegating to someone else. We can thus expect that small stakeholders will be strongly incentivized to operate high-quality nodes in order to multiply their rewards, which is favourable for network operator diversity, competitiveness and growth. To encourage large stakeholders to also become operators and pledge large sums of stake, note that the scheme's parameter α gives a rewards premium to large stakeholders for pledging and operating high-quality nodes. At the same time, note that the target number of operational mix nodes sets a limit on the number of mix nodes that is profitable to operate. If too many stakeholders pledge to propose mix nodes (i.e., if $N >> K$), reputation is spread thin and most nodes incur in losses and most delegates get zero returns. This is due to the system state being too far from the equilibrium. This encourages the cancellation of unprofitable nodes until a subset of nodes emerge accumulating significant reputation, thus bringing the state closer to the equilibrium and improving rewards for stakeholders.

7 Related work

The questions of reputation, rewarding participation, and payments for anonymity networks such as mixnets are longstanding research problems that pre-date the invention of Bitcoin and Tor [23]. In 2000, the Canadian privacy technology company Zero Knowledge Systems developed and deployed an anonymity network called the Freedom Network, which took user payments in return

for provisioning network privacy. The Freedom Network failed to reach widespread adoption partly due to lack of a usable and privacy-friendly payment mechanism [3]. In another example of incentivized privacy network, the Free Haven design also included rewards for service in maintaining file storage anonymously [14].

Mixnets, invented by Chaum [8], prevent the linking of the sender and receiver of a message given a reliable mixnet. Early designs for mixnet reputation used trusted witnesses to rate mix node reliability in free-route networks and prevent packet loss [13], similar to the concepts used in Nym. Later work used reputation ratings by the mix nodes themselves in a cascade [18]. However, reputation was in all of these systems non-fungible and not explicitly related to payments, as the idea of reputation-based currency as a reward payment was theorized but considered too difficult [16]. A number of reputation systems were considered [9, 28, 36] but not added to Tor as they could lead to new attacks and transitioning a volunteer-run altruistic network into an incentive-based network could alienate altruistic node operators while incentivizing adversarial behavior, potentially damaging the Tor network. Nevertheless, the lack of rewards in Tor leads to nearly half of relay operators having financial concerns over their running of nodes [27]. Nym is launched as an incentivized and decentralized mixnet, which avoids some of these issues, and our game-theoretic analysis shows that our proposed reward-sharing system encourages honest behavior from all parties in order to maximize individual rewards.

In terms of cryptocurrency, payment for anonymous routing has been suggested utilizing Bitcoin [5], privacy-enhanced cryptocurrencies like ZCash [29], or even proposals for Tor-specific coins [25] as well as payment of the guard [37]. However, this prior work neither includes a game-theoretic analysis nor addresses practical deployment issues such as how the necessary nodes are recruited and vetted, how nodes that are temporarily unused are paid in case they may be needed for routing in the future, how rewards maintain the global system over time even during low-usage periods, and how to determine a fair payment amount for all nodes in the system, including those that are not routing traffic at a given moment.

We build our reward-sharing scheme for mixnets on game theoretic mechanisms in cryptocurrency (cf. [2]), inspired in particular by the combination of a pool of inflationary rewards to bootstrap the nodes and transaction fees to sustain the network in the long term, similarly to Bitcoin [35]. These features allow to achieve globally desired properties, such as rewarding desirable behavior via stable returns at a Nash equilibrium [33]. However, Bitcoin's "proof of work" reward-sharing scheme has also led to considerable centralization [24] of Bitcoin mining, and a game-theoretic equilibrium analysis shows this is indeed rational [31] and potentially unavoidable in general [34]. Yet, even though Bitcoin still works [4], misjudging the exact amount of rewards to be shared among different components with (crypto)economic incentives can still have catastrophic consequences. For example, one of the reasons that Tor does not implement economic rewards in its own currency is that prior attempts to do so for file-sharing such as Mojonation had a reserve of inflation that was open to attacks that led to hyperinflation [45]. The problems of compounding centralization due to inadequate reward-sharing have been endemic in 'proof of stake' networks [21] and more widely in 'proof of work' systems as well [30]. There is only one prior reward-sharing scheme that reaches a game-theoretic equilibrium achieving a certain target of decentralization via delegated stake [7]. We build on this construction, which is tailored to the setting of ledger maintenance, showing how to apply it to mixnets settings. A number of challenges had to be tackled to make this happen, including taking into account that costs are proportional to the work allocated to nodes (they were assumed constant per epoch per player in [7]) and activity assignments in the mixnet are a random variable (some nodes are idling while others are processing traffic in each epoch, while all nodes have the same exact role in [7]). Developing the rewards system to incorporate these mixnet specific considerations required a novel game-theoretic analysis for mixnet nodes that has never been applied to anonymous routing before, along with simulations that demonstrate the financial sustainability of the entire mix network under plausible assumptions.

8 Conclusion and future work

We have presented a reward sharing scheme for paid anonymity networks such as the Nym mixnet, and proven via a game-theoretic analysis that it promotes decentralization while having good Sybil-resistance properties. Our reward sharing scheme, together with a bootstrapping reserve and

a pricing mechanism for mixnet bandwidth, enables a market for private communications that can scale, as it can convert the demand from users into increased capacity for service provisioning via recruiting more mix node operators. Given an excess of mix node candidates, the selection of nodes for the mixnet at each epoch is proportional to mix node reputation, with high-reputation nodes having higher chances of selection than low-reputation nodes. A node's reputation is proportional to the aggregate amount of NYM pledged and delegated to it, and it signals the confidence of stakeholders (including the operator) in the good performance of the node: regardless of reputation, nodes that fail to deliver packets when selected for the mixnet are penalized with diminished rewards, which encourages stakeholders to move their support (and associated reputation) to more reliable nodes, thus contributing to the overall health and performance of the network.

We have presented simulation-based empirical results to illustrate the functioning of the scheme in non-ideal conditions, where there is an excess of mix node candidates, some stakeholders fail to engage and others fail to make optimal choices that maximize their rewards. Our results indicate that the scheme can enable a viable network that covers operational costs and where stakeholders are sufficiently incentivized to engage and take actions that are beneficial to the quality and performance of the whole system.

The economic viability of the system crucially depends on some assumptions. Notably, the value of the mixmining reserve used to bootstrap the system is dependent on the value of the NYM token. If the NYM token depreciates, so does the mixmining reserve and the rewards it releases, even to the point where mixmining rewards may not cover mix node operational costs, which are tied to fiat, making the network unsustainable. On the contrary, a more valuable NYM token increases the value of the mixmining reserve and the rewards it releases, making it more attractive for stakeholders to engage with the system by pledging or delegating to mix nodes. In the case of user fees, they should not fluctuate with the value of the NYM token. Usage fees can be priced in fiat or a stablecoin and converted to NYM via an automatic conversion oracle that accounts for current exchange rates. Similarly, mix node costs can be recorded in fiat and automatically converted to NYM when distributing rewards.

The percentages of NYM dedicated to pledging and delegating to mix nodes are also influential in the results. In our experimental setup we have assumed that 15% of the available supply is pledged and 60% delegated, with the remaining 25% of stake being unallocated. This results in roughly half the available rewards remaining unclaimed and being returned to the mixmining pool. A higher percentage of pledging and delegation would increase the amount of distributed rewards, while lower levels of stakeholder engagement would lead to more unclaimed rewards being returned to the pool. Similarly, we have assumed perfect performance for all mix nodes, and any loss in performance would increase the unclaimed funds returned to the pool for later distribution. This dynamic protects the mixmining pool from depletion by lowering the distributed rewards when mix node performance is poor or stakeholders are disengaged in large proportions. The pool depletes at maximum rate when all mix nodes have perfect performance and all stakeholders are engaged and following a perfect strategy (i.e., in the equilibrium), and at a slower rate (i.e., more rewards remain unclaimed and are returned to the pool) the more they deviate from the equilibrium. We plan to publicly release the simulation code so that everyone can test out reward distributions in different scenarios.

Our scheme opens new possibilities for deploying incentivized mixnets. However, there is still more work to be done to orchestrate and scale anonymous communication networks while providing long-term predictable service for users and earnings for node operators. Our game theoretic results are proven for "single shot" strategies and it would be interesting to consider iterated variants of the basic delegation game, where stakeholder strategies statefully adapt over time, as well as analyze the game theoretic incentives of coalitions of players to validate the robustness of our game equilibria in this setting. While we have proven the existence of favorable equilibria for decentralization and Sybil resilience, this does not exclude the existence of other less favourable equilibria and computing metrics such as the price of anarchy would be useful. Despite these limitations, our simulation analysis shows that long-term financial sustainability can be established under a wide set of plausible parameters in terms of user growth and stake distributions. Future empirical analyses can incorporate utility-maximizing agents and study individual node strategies with diverse costs and profit margins, as well as adapting the scheme to different kinds of decentralized systems besides mixnets. An important next step is to specify a decentralized scheme for mix node performance

measurement that can provide trustworthy values to the reward sharing mechanism. Finally, we would like to study the sensitivity of network viability to macroeconomic parameters, as well as the impact of a fluctuating token exchange rate. As Nym and other networks launch in the real world and scale, feedback from the real-world deployment of the reward-sharing scheme for mixnets can be further used to refine the analysis.

References

1. Nikolaos Alexopoulos, Aggelos Kiayias, Riivo Talviste, and Thomas Zacharias. MCmix: Anonymous messaging via secure multiparty computation. In *USENIX Security Symposium*, pages 1217–1234. USENIX Association, 2017.
2. Sarah Azouvi and Alexander Hicks. Sok: Tools for game theoretic models of security for cryptocurrencies. *Cryptoeconomic Systems*, 1(1), 2021.
3. Adam Back, Ian Goldberg, and Adam Shostack. Freedom 2.1 security issues and analysis. `http://www.cypherspace.org/adam/pubs/freedom-21.pdf`.
4. Christian Badertscher, Juan Garay, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. But why does it work? A rational protocol design treatment of Bitcoin. In *Annual international conference on the theory and applications of cryptographic techniques*, pages 34–65. Springer, 2018.
5. Alex Biryukov and Ivan Pustogarov. Bitcoin over Tor isn't a Good Idea. In *IEEE Symposium on Security and Privacy (S&P)*, pages 122–134. IEEE, 2015.
6. Rainer Bohme, George Danezis, Claudia Diaz, Stefan Kopsell, and Andreas Pfitzmann. Mix Cascades vs. Peer-to-Peer: Is One Concept Superior? In *Proceedings of Privacy Enhancing Technologies (PETs)*, pages 243–255, 2004.
7. Lars Brünjes, Aggelos Kiayias, Elias Koutsoupias, and Aikaterini-Panagiota Stouka. Reward sharing schemes for stake pools. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P)*, pages 256–275. IEEE, 2020.
8. D. Chaum. Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM*, 24(2):84–88, 1981.
9. Yao Chen, Radu Sion, and Bogdan Carbunar. Xpay: Practical anonymous payments for tor routing and other networked services. In *Proceedings of the ACM Workshop on Privacy in the Electronic Society (WPES)*, pages 41–50, 2009.
10. George Danezis and Ian Goldberg. Sphinx: A compact and provably secure mix format. In *Proceedings of the IEEE Symposium on Security and Privacy (S&P)*, pages 269–282. IEEE, 2009.
11. Claudia Diaz, Harry Halpin, and Aggelos Kiayias. The Nym Network. `https://nymtech.net/nym-whitepaper.pdf`, February 2021.
12. Claudia Diaz, Stefaan Seys, Joris Claessens, and Bart Preneel. Towards measuring anonymity. In *Proceedings of the 2nd International Conference on Privacy Enhancing Technologies (PETs)*, pages 54–68, 2002.
13. Roger Dingledine, Michael J Freedman, David Hopwood, and David Molnar. A reputation system to increase mix-net reliability. In *International Workshop on Information Hiding*, pages 126–141. Springer, 2001.
14. Roger Dingledine, Michael J Freedman, and David Molnar. The Free Haven project: Distributed anonymous storage service. In *Designing Privacy Enhancing Technologies*, pages 67–95. Springer, 2001.
15. Roger Dingledine and Nick Mathewson. Anonymity loves company: Usability and the network effect. In *Workshop on the Economics of Information Security (WEIS)*, 2006.
16. Roger Dingledine, Nick Mathewson, and Paul Syverson. Reputation in p2p anonymity systems. In *Workshop on economics of peer-to-peer systems*, 2003.
17. Roger Dingledine, Nick Mathewson, and Paul Syverson. Tor: The second-generation onion router. In *USENIX Security Symposium*, pages 303–320, 2004.
18. Roger Dingledine and Paul Syverson. Reliable mix cascade networks through reputation. In *International Conference on Financial Cryptography and Data Security (FC)*, pages 253–268. Springer, 2002.
19. John R Douceur. The sybil attack. In *International workshop on peer-to-peer systems*, pages 251–260. Springer, 2002.
20. Pavlos S. Efraimidis and Paul (Pavlos) Spirakis. Weighted random sampling. In *Encyclopedia of Algorithms*, pages 2365–2367. 2016.
21. Giulia Fanti, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang. Compounding of wealth in proof-of-stake cryptocurrencies. In *International conference on Financial Cryptography and Data Security (FC)*, pages 42–61, 2019.

22. Giulia Fanti, Shaileshh Bojja Venkatakrishnan, Surya Bakshi, Bradley Denby, Shruti Bhargava, Andrew Miller, and Pramod Viswanath. Dandelion++: Lightweight cryptocurrency networking with formal anonymity guarantees. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, 2018.
23. Elke Franz, Anja Jerichow, and Guntram Wicke. A payment scheme for mixes providing anonymity. In *Trends in Distributed Systems for Electronic Commerce*, pages 94–108. Springer, 1998.
24. Adem Efe Gencer, Soumya Basu, Ittay Eyal, Robbert Van Renesse, and Emin Gün Sirer. Decentralization in bitcoin and ethereum networks. In *International Conference on Financial Cryptography and Data Security*, pages 439–457, 2018.
25. Mainak Ghosh, Miles Richardson, Bryan Ford, and Rob Jansen. A TorPath to TorCoin: proof-of-bandwidth altcoins for compensating relays. Technical report, Naval Research Lab, 2014.
26. Harry Halpin. Nym Credentials: Privacy-preserving decentralized identity with blockchains. In *Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 56–67. IEEE, 2020.
27. Hsiao-Ying Huang and Masooda Bashir. The onion router: Understanding a privacy enhancing technology community. *Proceedings of the Association for Information Science and Technology*, 53(1):1–10, 2016.
28. Rob Jansen, Nicholas Hopper, and Yongdae Kim. Recruiting new Tor relays with BRAIDS. In *Proceedings of the ACM conference on Computer and Communications Security (CCS)*, pages 319–328, 2010.
29. George Kappos and Ania M Piotrowska. Extending the anonymity of Zcash. *arXiv preprint arXiv:1902.07337*, 2019.
30. Dimitris Karakostas, Aggelos Kiayias, Christos Nasikas, and Dionysis Zindros. Cryptocurrency egalitarianism: A quantitative approach. In *International Conference on Blockchain Economics, Security and Protocols (Tokenomics)*, pages 1–21, 2019.
31. Aggelos Kiayias and Aikaterini Panagiota Stouka. Coalition safe equilibrium with virtual payoffs. In *ACM Conference on Advances in Financial Technologies (AFT)*, 2021.
32. Paul Klemperer. *Auctions: Theory and Practice*. Princeton University Press, 2018.
33. Joshua A Kroll, Ian C Davey, and Edward W Felten. The economics of bitcoin mining, or bitcoin in the presence of adversaries. In *Proceedings of Workshop on the Economics of Information Security (WEIS)*, volume 2013, page 11, 2013.
34. Yujin Kwon, Jian Liu, Minjeong Kim, Dawn Song, and Yongdae Kim. Impossibility of full decentralization in permissionless blockchains. In *Proceedings of the ACM Conference on Advances in Financial Technologies (AFT)*, pages 110–123. ACM, 2019.
35. Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. `https://bitcoin.org/bitcoin.pdf`, 2008.
36. Tsuen-Wan Ngan, Roger Dingledine, and Dan Wallach. Building incentives into Tor. In *International Conference on Financial Cryptography and Data Security (FC)*, pages 238–256, 2010.
37. Paolo Palmieri and Johan Pouwelse. Paying the guard: An entry-guard-based payment system for Tor. In *International Conference on Financial Cryptography and Data Security (FC)*, pages 437–444, 2015.
38. Andreas Pfitzmann and Marit Hansen. Anonymity, unobservability, and pseudeonymity — a proposal for terminology. In *International Workshop on Designing Privacy Enhancing Technologies (PETs): Design Issues in Anonymity and Unobservability*, pages 1–9, 2001.
39. Ania M Piotrowska, Jamie Hayes, Tariq Elahi, Sebastian Meiser, and George Danezis. The Loopix anonymity system. In *USENIX Security Symposium*, pages 1199–1216, 2017.
40. Joseph Poon and Thaddeus Dryja. The Bitcoin Lightning Network: Scalable off-chain instant payments. `https://lightning.network/lightning-network-paper.pdf`, 2016.
41. Andrei Serjantov and George Danezis. Towards an information theoretic metric for anonymity. In *Proceedings of the International Conference on Privacy Enhancing Technologies (PETs)*, pages 41–53, 2002.
42. Piyush Kumar Sharma, Devashish Gosain, and Claudia Diaz. On the anonymity of peer-to-peer network anonymity schemes used by cryptocurrencies. arXiv preprint arXiv: 2201.11860, 2022.
43. Alberto Sonnino, Mustafa Al-Bassam, Shehar Bano, and George Danezis. Coconut: Threshold issuance selective disclosure credentials with applications to distributed ledgers. In *Proceedings of the Network and Distributed System Security Symposium (NDSS)*. Internet Society, 2019.
44. Ewa Syta, Philipp Jovanovic, Eleftherios Kokoris Kogias, Nicolas Gailly, Linus Gasser, Ismail Khoffi, Michael J Fischer, and Bryan Ford. Scalable bias-resistant distributed randomness. In *IEEE Symposium on Security and Privacy (S&P)*, pages 444–460. IEEE, 2017.
45. Bryce Wilcox-O'Hearn. Experiences deploying a large-scale emergent network. In *International Workshop on Peer-to-Peer Systems*, pages 104–110. Springer, 2002.