NUCYPHER: ECONOMIC PROTOCOL

THE AUTHOR

1. Context: the Network Service and Workers

The NuCypher network's primary purpose is to provide a *decentralized access control service* to adopters. *Adopters* are a catch-all term for the developers and purveyors of various technological applications and systems, including but not limited to: consumer-facing applications (e.g. a genomic record management app), platforms (e.g. a marketplace for mobile browsing data), Web 3 infrastructure (e.g. a decentralized database-as-a-service), games (e.g. a digital collectible card game) and other multi-endpoint systems (e.g. intra-vehicle data sharing via IOT devices).

NuCypher network nodes, hereafter referred to as *workers*, are an indispensable component of this access control service. Distributed around the world, workers run NuCypher software on their machines in order to facilitate data sharing flows within adopters' applications and systems. This involves enforcing permissions, initially chosen by data owners, that enable access to their encrypted data payloads. More specifically, workers transform ciphertexts associated with the underlying data, such that they are then decryptable by valid recipients. Data owners can also program the enforcement to be based on the fulfillment of certain conditions. In some respects, this service can be compared to a large-scale key management system (e.g. Amazon Web Services KMS), but critically, every sharing flow is end-to-end encrypted and thus does not imply trust in the security or integrity of a centralized third-party or data custodian.

Workers have three main duties:

(1) Being reliably online at all times, in order to respond to access requests or receive new sharing policies
(2) Securely holding onto sharing policies (objects providing the rules and parameters for access to data) and their corresponding *re-encryption key fragments*
(3) Performing *re-encryptions* (enforcing a permission) in response to legitimate access requests

Workers are compensated for these efforts through *fees* (denominated in ETH), paid for by adopters. These costs can optionally be passed on to the end-users of adopting applications. As of April 2019, sharing policies are priced exclusively based on their duration, and one policy is required for each designated recipient (one policy per public key). In practice, this means the cost to an adopter for a given sharing flow depends on the number of recipients and for how long they need access. However, in forthcoming versions, the number of access requests associated with a sharing policy may also influence the sum charged, and a single policy may grant access to multiple recipients. The details of current and future payment models are covered in later sections.

Because some adopters will require sharing policies that last for extended periods (e.g. for over 6 months), it is critical that worker availability is highly predictable. In other words, workers should not be assigned an access management job if they haven't committed to work for at least the duration of the associated sharing policy.

Workers need not be trusted with the underlying private data, given that the objects they hold do not give them this power or permission. Additionally, a single permission update typically involves multiple workers, each of whom only handles fragments of keys and ciphertexts, such that a unilateral refusal to execute one's assignment is almost always inconsequential to the end-user (i.e. the user of an adopting application is unlikely to be affected). Nonetheless, it is possible for workers to *misbehave*, including the following offenses:

(1) Refusing to re-encrypt following a legitimate access request
(2) Generating an incorrect re-encrypted ciphertext for the data recipient
(3) Being offline at any time (hence risking the disruption of a sharing flow or access request)
(4) Colluding with other nodes and the designated recipient(s) to collectively derive a data owners private key (note: the extreme difficulty of orchestrating this attack is detailed in later sections)

2. Objectives of the Economic Protocol

Though the economic protocol is a means to prevent or minimize worker misbehavior introduced in Section 1, this alone is an oversimplification. Economic design choices have a far broader impact, and affect everything from the network's market capitalization to the geographical distribution of workers.
Hence, all economic mechanisms and strategies (already implemented, or to be implemented) should address one or more high-level network objectives. Note that some objectives align, clash or are *sub-goals* of one another; nonetheless, each is evaluated individually here.

(1) **Maximize network adopter acquisition and retention**
Increasing, retaining and diversifying a pool of adopters is the NuCypher network's highest priority. This objective can be broken into the following endeavors:
    (a) Maximizing the quality of service. This sustains the network via retention of satisfied adopters and grows the pool via their recommendations. Service quality can be understood in terms of reliability, security, friction (lack of) and cost-effectiveness, which are explored as distinct objectives later in this section.

(b) Maximizing the network's exposure to non-adopters. For the adopter pool to grow, developers of relevant applications must be aware of the service. A historically popular means of bootstrapping marketing efforts has involved leveraging the network effects of speculation on a freely tradeable native token, where the presence of a liquid asset on exchanges, in media, and on forums/other channels provides free exposure to purportedly relevant audiences. However, prominence of this kind is arguably skewed towards networks with the largest market capitalizations, since they are the most liquid, boast the most interested parties and get disproportionate media coverage as a result. A token with a realistic market cap may be more financially and reputationally sustainable, but may not garner the same notoriety. It's worth noting that for some projects, a large market cap and associated name-recognition has not translated into high-quality adoption, and in some cases ostensible over-valuation has dissuaded developers from building in their ecosystem.

(c) Maximize the service's competitive edge. Given that the entirety of NuCypher technology (cryptography, system architecture, code, etc.) is necessarily open source, the barrier impeding a competitor from product replication is rather feeble. A competitive advantage, as perceived by adopters or would-be adopters, is the superior quality of service relative to that of similar or copycat projects. Whether a competitive advantage, such as greater reliability, is realized and maintained, is determined in part by the aggregate decision-making of the network's workers. Moreover, while code can be cloned, competent workers are a finite resource. Operating nodes in multiple networks is possible, but capital and hardware constraints limit this. By way of illustration, imagine if a large swathe of workers decided to abandon the NuCypher network in unison. This would harm the perceived and actual reliability of the service, and potentially boost a competing network via a migration of new service-providers. Conversely, if a large swathe of workers decided to formally commit their efforts to the network for an extended time period, this solidifies the service's perceived and actual reliability, and makes it more difficult for another network to attract those workers (since they now have capital locked up in the NuCypher network). These collective decisions are strongly influenced by the network's economic design.

In summary, the network must aspire towards an inimitable reputation, flexible capacity and recognized stability. These attributes are partially a function of worker decisions (and the alignment of their self-interest with the network's health), the populating and maintenance of whom requires a sensible economic protocol.

(2) **Ensure a highly reliable service (liveness)**

From an adopter perspective, this objective is straightforward to describe. If an access request is submitted to the network, it should be answered immediately and correctly, at or very near network latency, and without fail. From a network perspective, ensuring this level of reliability must take into account, at a minimum, the following factors:

(a) Individual worker behavior or misbehavior. For example, if a set of workers coordinate their refusal to re-encrypt. Alternatively, if a large percentage become apathetic and start cutting corners, for example by confirming their service for an upcoming period but then being offline for all or part of that period.

(b) The overall volume of worker participation. In other words, if demand outstrips supply, then sharing flows may be put on hold. This is unlikely to occur from a pure capacity perspective, but is possible if an adopter requires a large number of independent workers to concurrently manage access in their application.

(c) The distribution of worker commitment. For example, if there are insufficient workers committed to providing the service for a duration required by an adopter.

See objective 5 for more on worker participation.

(3) **Ensure a highly secure service**
In the context of any trustless access control service, the most important notion of *secure* is as follows; private user data cannot be accessed by non-designated parties at any time, including the workers that enforce access. In NuCypher's case, this warranty is achieved via pure cryptographic guarantees, with no direct relation to economics. However, there are secondary security notions germane to economic design; including the mitigation of *denial-of-service* and *censorship* attacks. Furthermore, there is a relationship between the security of a sharing flow and the number of workers assigned the access control job, which means that the overall volume of worker participation can have a bearing on the upper bound of network security.

(4) **Ensure a low-friction and cost-effective service**
This objective refers to the practicality of integrating the network's service into an adopter's application. The manner in which an adopter pays workers is highly relevant here, including the currency in which fees are paid, and the aspects of the service that are chargeable. Zooming out, there is also a natural tension between the affordability of the service to adopters and the affordability/desirability to provide the service as a worker. The exact fee model has huge consequences for the revenue workers can earn from fees (objective 6), which turn impacts the parameterization of mechanisms for worker non-fee compensation, such as rewards. Fee models are explored in greater detail in objective 6.

(5) **Ensure predictable and healthy worker participation/commitment**
A *participating worker* can be defined as one who has committed some minimum sum of capital (denominated in the native token) to the network for some non-trivial period of time (e.g. 1 month). In other words, a service-provider with a

locked security deposit. Overall participation can then be measured in absolute terms, by the total value of committed capital to the network by workers, or in relative terms, by the percentage of the total network capitalization that is committed at a given moment. With regard to the latter, it is unclear what percentage constitutes a *healthy* participation rate. There is a positive relationship between participation and objectives 2 and 3, but overly high participation rates may clash with objective 9, because committed capital is by definition non-liquid. This in turn impacts objective 10, where a lack of freely traded tokens can mean that the total number of independent workers does not grow sufficiently to maintain or increase the network's decentralization. High participation rates also dilute worker income, as explored in objective 6.z'

For a given worker in a given moment, their decisions to participate and for how long, will (at the very least) be influenced by :

(a) Their historical balance sheet, in fiat, with respect to service provision, itself determined by:
   (i) Overheads associated with service provision. This is dominated by 1. changes to the cost of internet connection (i.e. is increased bandwidth required to be a reliable worker) and 2. the cost of electricity to keep a capable machine online at all times.
   (ii) Revenue earned via a combination of rewards and fees.
   (iii) The exchange rate between the multiple digital tokens in which the worker is remunerated and the local fiat currency.

(b) Trends in demand for the service. This is not completely transparent to workers, as fees earned are both a function of demand and the worker's relative ownership of the network. They may be able to glean demand from other sources, such as project announcements and third-party commentary.

(c) The price of the native token and its recent trends.

(d) The attractiveness of other networks with respect to their epoch (a new network may offer greater rewards), general payouts, ease of participation, trends in their demand and other general prospects for growth.

(e) Sunk costs that cannot be re-purposed. Given the limited hardware requirements, much of this cost is time spent on research, financial/risk evaluation, machine set-up and configuration in advance of becoming a network worker.

(f) The current state of the worker's committed capital. In other words, what percentage is convertible into fiat, and what percentage is locked.

(g) The current stage of the reward/inflation schedule, if it is sufficiently predictable.

Note: because workers have the freedom to commit their capital across a range of durations, participation must be measured as the aggregate of capital across the possible units of commitment.

(6) **Ensure meaningful and consistent worker profit**

As covered in objective 5, the month-to-month income for each worker is undoubtedly impactful on participation. But, it may affect their behavior in general, such that losses or low profits lead to apathy or other forms of misbehavior.

Distributing meaningful and consistent profits requires careful reward parameterization and scheduling. And, since access management work is divvied up among participating workers, based on the relative size of their committed capital, worker *employment* is strongly affected by the participation rate, and therefore, so is income from fees. It would be desirable to tune participation such that supply does not dwarf demand for extended periods, particularly at epochs where reward-based incomes are negligible.

(7) **Minimize worker apathy and attrition**

Worker *apathy* is a shorthand for a level of disinterest or non-commitment to the network that can cause a severe behavior change, such as misbehaving or quitting the network. The latter is related to, but distinct from, worker participation, as attrition refers to the percentage of workers who leave their role as a service-provider for good. High attrition rates are particularly risky if the reasons for quitting also repel new workers, or the pool of competent would-be workers approaches an exhausted state.

Attrition may correlate to the size and consistency of worker profits, but is not exclusively driven by this. For example, if rewards are set too high initially, a rational worker may temporarily enjoy large personal gains, but also come to the conclusion that the token supply has been mismanaged, that their prospects for long-term profits are weak, and lose faith in the project altogether.

(8) **Steadily accrue value to native token**

The fiat value of the native token is important because, as explored in objective 5, it strongly affects real-world economic outcomes for workers. It's worth noting that while workers are paid in digital tokens, their overheads (electricity, etc.) are charged in fiat.

The volatility of the token's price is similarly important to workers, as strong uncertainty over the value of future payouts makes planning future service provision very difficult. This uncertainty will be reflected directly in the average duration of capital commitment, if the risks of extreme depreciation render long-term locking of capital an irrational choice.

A steady growth in the value of the native token might be regarded as a by-product of network success, rather than an objective in itself. However, the growth in value is affected by multiple adjustable factors, including the initial token supply, the inflation rate and decay, the payment/fee model, the market formation, and of course the highest-priority objective, the rate of network adoption. The ideal scenario is that the quantity of fees paid into the network grows so large that acquiring the native token in order to become a worker makes economic sense, despite the value it has accrued since network launch.

(9) **Ensure appropriate token liquidity**
Though we may question the link between token liquidity and the acquisition of network adopters, there are firmer reasons for maintaining a sufficiently deep liquidity pool, including:
  (a) Avoiding a general increase in volatility caused by thin markets.
  (b) Avoiding the network being held hostage by a small number of token holders who control a large proportion of the available tokens.
  (c) Allowing new actors to easily, quickly and affordably purchase tokens in order to become workers, thereby increasing network decentralization beyond the initial token distribution.

Liquidity is partially determined by many external and non-controllable factors, such as the actions of third-party exchanges. However, token holders can be discouraged from trading tokens if the allure of locking the capital is too great, given the size of payouts or other incentives. Some token-holders are already geared towards trading rather than service provision, but it's worth remembering that the practical hurdles to switching between the two are not particularly high from a hardware or expertise point of view. Therefore, it is worth weighing the possible returns from trading and/or market making, against the equivalent from service provision as a worker, to avoid pulling all token holders into one camp or another.

(10) **Maximize and maintain network decentralization and openness**
This objective refers to the heterogeneity of active workers, with respect to their geographical location, and to a lesser extent to their capabilities (hardware and skills). Of equal importance is the distribution of wealth, (measured by the *Gini coefficient*), where a concentration of tokens in few hands is highly undesirable.

A large number of workers, located in a wide variety of political, economic and social circumstances, bestow the network strong resilience along a number of planes. From a security point of view, a key threat to the network (detailed in objective 11) becomes exponentially more difficult to orchestrate when workers are broadly distributed around the world. Looking at worker participation, if workers represent a set of countries with diverse purchasing power (or a similar metric like average salaries), this increases the network's ability to survive periods of low payouts. Revenue which would be irrelevant to some workers is economically worthwhile to those with far lower overheads and alternative incomes.

The decentralization of workers is greatly affected by the token distribution mechanism chosen at network launch, during which the goal is generally to get tokens into as many hands as possible. However, subsequent mechanisms can also provide an antidote to poor initial distributions but will tend to rely on sufficient token liquidity.

(11) **Minimize or extinguish security threats to network**
Although some threats to the network can be regarded as *unknown unknowns*, and are therefore difficult to legislate against, we can begin with plausible adversarial motives. One such motive may be to impede the users of specific adopting applications from sharing data. For instance, let's examine a case where an undercover journalist is attempting to share data with a news outlet, and there are a set of workers controlled by the adversary, an evil regime. To have a chance of blocking the story from being shared, they would need to control a large proportion of the network otherwise theres no way to ensure their workers will be assigned the relevant sharing policy. In theory, if the first message is blocked, the journalist could repeatedly re-issue sharing policies, each with a new, random set of workers and eventually the message would be re-encrypted by an honest/uncontrolled worker. The cost and difficulty of controlling a sufficient number of workers depends on the networks stage of growth, but this prerequisite prices out most adversaries. The adversary may instead attempt to bribe as many workers as possible. This is logistically more feasible, as it does not depend on each target workerss willingness or ability to sell their tokens at a given moment (their tokens may be locked for a time period so long as to render the attack pointless). Bribe recipients may demand compensation equal to the loss of expected income (rewards + fees), plus some motivating premium.
Regardless of how the adversary seeks control, they will need to identify and convince existing workers to cooperate (selling their tokens or accepting a bribe). In both cases, this attack is easier to achieve earlier in the lifetime of the network, when there are fewer workers to approach, they are less spread out, and the total market cap, and therefore cost of attack, is likely to be lower. Importantly, in all these cases, it would be expedient for the attacker to instruct their bribed workers to simply go offline, rather than re-encrypt incorrectly, since the protocol cannot (yet) differentiate between lazy, DDoS-ed and malicious workers who fail to answer requests, and this approach costs the corrupt workers far less while achieving the adversary's goal.

(12) **Maximize network protocol upgradeability**

(13) **Ensure decentralized governance**

3. Staking, Payouts and Slashing: Overview

Initially, payouts from fees alone are unlikely to incentivize a sufficient number of would-be workers to join the network. Though the cost of performing re-encryptions are quite low, in the early stages of the network, so too will the revenue from fees. Hence, until demand for decentralized access control has reached a stable growth phase, an inflation-based subsidy is necessary to motivate workers.

To incentivize predictable behavior, and disincentize misbehavior, in particular the first three offenses listed in Section 1, workers are required to stake a native token (*NU*) by locking it for a predefined time period. This commitment of capital, which cannot be reversed until the chosen unlock date, enables them to participate in the network and receive access control jobs. Stakes function as a collateral that can be reduced (hereafter: *slashed*) in the event of a provable offense.

Stakes represent an initial deposit of non-trivial value, and will increase in value if rewards are *re-staked* by the worker over time. Access control jobs are assigned proportionally to the size of a worker's stake, relative to the aggregate of all current stakes in the network. Similarly, a worker's reward payout depends on the relative size of their stake, with coefficients based on other factors such as the length of their committed service to the network.

4. Evaluation of Existing and Historical Economic Protocols

Appendix A. The slashing protocol