NUCYPHER: ECONOMIC PROTOCOL

THE AUTHOR

1. Context: The Service Provided by the NuCypher Network

From a user's point of view, the NuCypher network provides a *decentralized access control service*. Users may include consumer-facing applications (e.g. a medical record management app), platforms (e.g. a marketplace for mobile browsing data), internet infrastructure (e.g. a database-as-a-service) and other multi-user systems (e.g. an intra-vehicle data sharing device).

NuCypher network nodes (hereafter:*workers*) provide this service to users by facilitating sharing flows. This involves updating the permission(s) associated with data payloads. In some ways, the service is similar to that of a large-scale key management system (e.g. AWS KMS), but critically, the sharing flow is end-to-end encrypted and thus does not imply trust in the security or integrity of a centralized third-party or custodian. 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.

Nonetheless, workers are expected to behave properly, and are compensated for their efforts as access managers. In practice, this job involves being reliably online at all times, securely holding onto sharing policies and their corresponding *re-encryption key fragments*, and performing *re-encryptions* (i.e. permission updates) in response to legitimate access requests. This work is remunerated via fees (denominated in ETH), paid by the aforementioned users.

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

Although workers need not be trusted with private data, given that the objects they hold do not give them this power or permission, they can still misbehave: refusing to re-encrypt, producing incorrect re-encryptions, being offline (hence risking the disruption of a sharing flow), and, though extrordinarily difficult to orchestrate, colluding with other nodes and the designated recipient(s) to obtain a data owners private key. To disincentivize misbehaviour, in particular the first two offenses, and reward good behaviour, workers are

required to stake a native token (NU). This allows them to participate in the network and receive access control jobs. Stakes function as a collateral, with one's initial deposit worth a non-trivial sum. Moreover, access control jobs are assigned proportionally to the size of a worker's stake, relative to the aggregate of all current stakes. Similarly, a worker's inflation payout depends on the relative size of their stake with coefficients based on other factors such as the length of their commitment to the network.

Appendix A. The slashing protocol