The NuCypher Network: A decentralized cryptological network offering accessible, intuitive, and extensible runtimes and interfaces for secrets management and dynamic access control

Michael Egorov,* David Nuñez,† and MacLane Wilkison‡
NuCypher

(Dated: September 11, 2019)

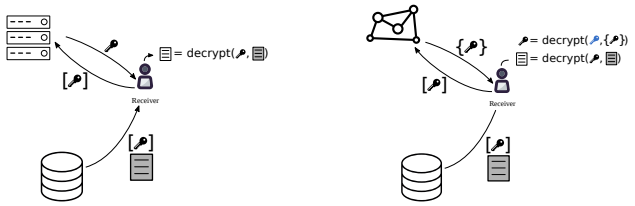
The NuCypher Network provides accessible, intuitive, and extensible runtimes and interfaces for secrets management and dynamic access control. It's accessible by virtue of being decentralized, permissionless, and censorship-resistant: there are no gate-keepers and anyone can use it. It's intuitive thanks to the classic character-based narrative of Alice and Bob (with the introduction of additional cryptological characters where appropriate), that permeates the code-base and helps developers write safe, misuse-resistant code. It's extensible as it currently supports proxy re-encryption but can be extended to provide support other cryptographic primitives.

The NuCypher Network enables developers to manage secrets and dynamically grant and revoke access to sensitive data in public networks.

CONTENTS

I. INTRODUCTION

A key management system (KMS) is an integrated approach for generating, distributing, and managing cryptographic keys for devices and applications (Fig. 1). A KMS includes the backend functionality for key generation, distribution, and rotation as well as the client functionality for injecting, storing, and managing keys on devices [1].



(a) Centralized KMS (b) PRE-based KMS

FIG. 1: Difference between a centralized key management system (KMS) and one which uses proxy re-encryption (PRE)

As the root of trust, it's critical that a KMS is appropriately configured, managed, and protected. Historically, this has meant deploying a KMS on-premises in hardware security modules (HSM) [2] or using tools like HashiCorp's Vault [3]. However, this requires a high degree of technical sophistication as well as upfront capital investment. To ease the technical burden and provide more competitive pricing, vendors like Amazon CloudHSM [4], Google Cloud KMS [5], Azure Key Vault [6] and TrueVault [7] have begun offering KMS as a service. However, KMS as a service offerings necessitate placing an undue level of trust in the service provider,

* michael@nucypher.com
† david@nucypher.com
‡ maclane@nucypher.com

which may be inappropriate for security-critical applications.

Public consensus networks, such as Bitcoin and Ethereum, are a promising solution to this centralization problem. But the limitations of public consensus networks in performing cryptographic operations that involve the manipulation of secret data are well-established [8]. Consensus networks employ a volunteer network of nodes, which is subject to constant churn and not as reliable as central infrastructure when it comes to availability and enforcing access management rules.

The NuCypher Network uses a decentralized network to remove the reliance on central service providers, proxy re-encryption for cryptographic access control, and a token incentive mechanism to ensure reliability, availability, and correctness. Because of the use of proxy re-encryption, an unencrypted symmetric key (which gives the ability to decrypt private data) is never exposed server-side (Fig. 1), and there is no single point of security failure. Even if compromised, hackers would only get re-encryption keys but access to the file is still protected.

II. NETWORK

III. SMART CONTRACT LAYER

IV. NU TOKEN AND STAKING ECONOMICS

V. CHARACTERS

VI. CONCLUSION

[1] Wikipedia, "Key management — Wikipedia, the free encyclopedia," (2017).

[2] Wikipedia, "Hardware security module — Wikipedia, the free encyclopedia," (2017).

[3] HashiCorp Inc., "Vault by hashicorp," (2017).

[4] Amazon Inc., "Aws cloudhsm," (2017).

[5] Alphabet Inc., "Cloud key management service," (2017).

[6] Microsoft Inc., "Key vault," (2017).

[7] TrueVault Inc., "Hipaa compliant api & secure data store," (2017).

[8] Gabriel Kaptchuk, Ian Miers, and Matthew Green, "Managing secrets with consensus networks: Fairness, ransomware and access control," Cryptology ePrint Archive, Report 2017/201 (2017).