NuCypher KMS: Decentralized Key–Management System

Michael Egorov, CTO

SF Cryptocurrency Devs, 29 Nov 2017

Why

Encrypted file sharing

Why

Encrypted multi-user chats

Why

Decentralized Netflix

Why

Too much power in hands of state actors

Solution

Proxy re-encryption + decentralization

What is proxy re-encryption (PRE)

PRE demo

Centralized KMS using PRE

Still too much power

Threshold split-key re-encryption (Umbral)

Decentralized KMS network

KMS token

KMS token

Mining

Investors

Early users

Team

How to contribute, learn