NuCypher KMS: Decentralized Key-Management System

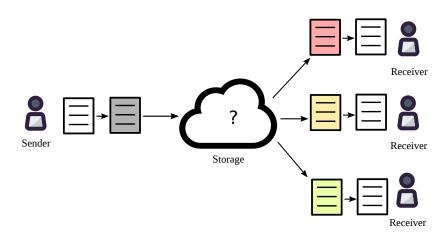
Michael Egorov, CTO

SF Cryptocurrency Devs, 29 Nov 2017



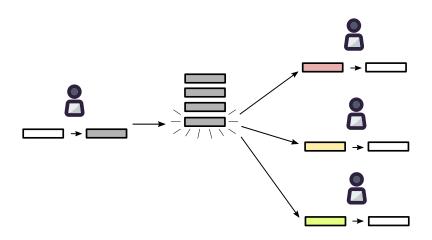
Why

Encrypted file sharing



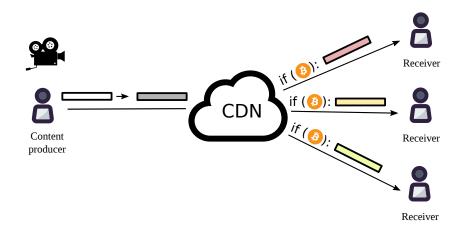
Why

Encrypted multi-user chats



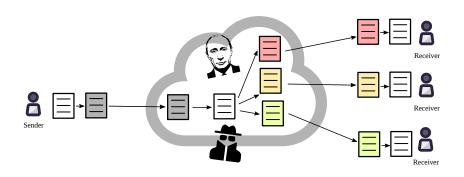
Why

Decentralized Netflix



Central server + TLS

Data vulnerable to hackers, state actors etc



5 / 17

Michael NuCypher KMS 29 Nov 2017

Solution

Proxy re-encryption + decentralization



 Michael
 NuCypher KMS
 29 Nov 2017
 6 / 17

What is proxy re-encryption (PRE)



 Michael
 NuCypher KMS
 29 Nov 2017
 7 / 17

PRE demo



8 / 17

Michael NuCypher KMS 29 Nov 2017

Centralized KMS using PRE

Still too much power



 Michael
 NuCypher KMS
 29 Nov 2017
 9 / 17

Threshold split-key re-encryption (Umbral)



Michael NuCypher KMS 29 Nov 2017 10 / 17

Decentralized KMS network



 Michael
 NuCypher KMS
 29 Nov 2017
 11 / 17

KMS token



Michael NuCypher KMS 29 Nov 2017 12 / 17

KMS token

Mining



 Michael
 NuCypher KMS
 29 Nov 2017
 13 / 17

Investors



14 / 17

Early users



Team



16 / 17

How to contribute, learn



 Michael
 NuCypher KMS
 29 Nov 2017
 17 / 17