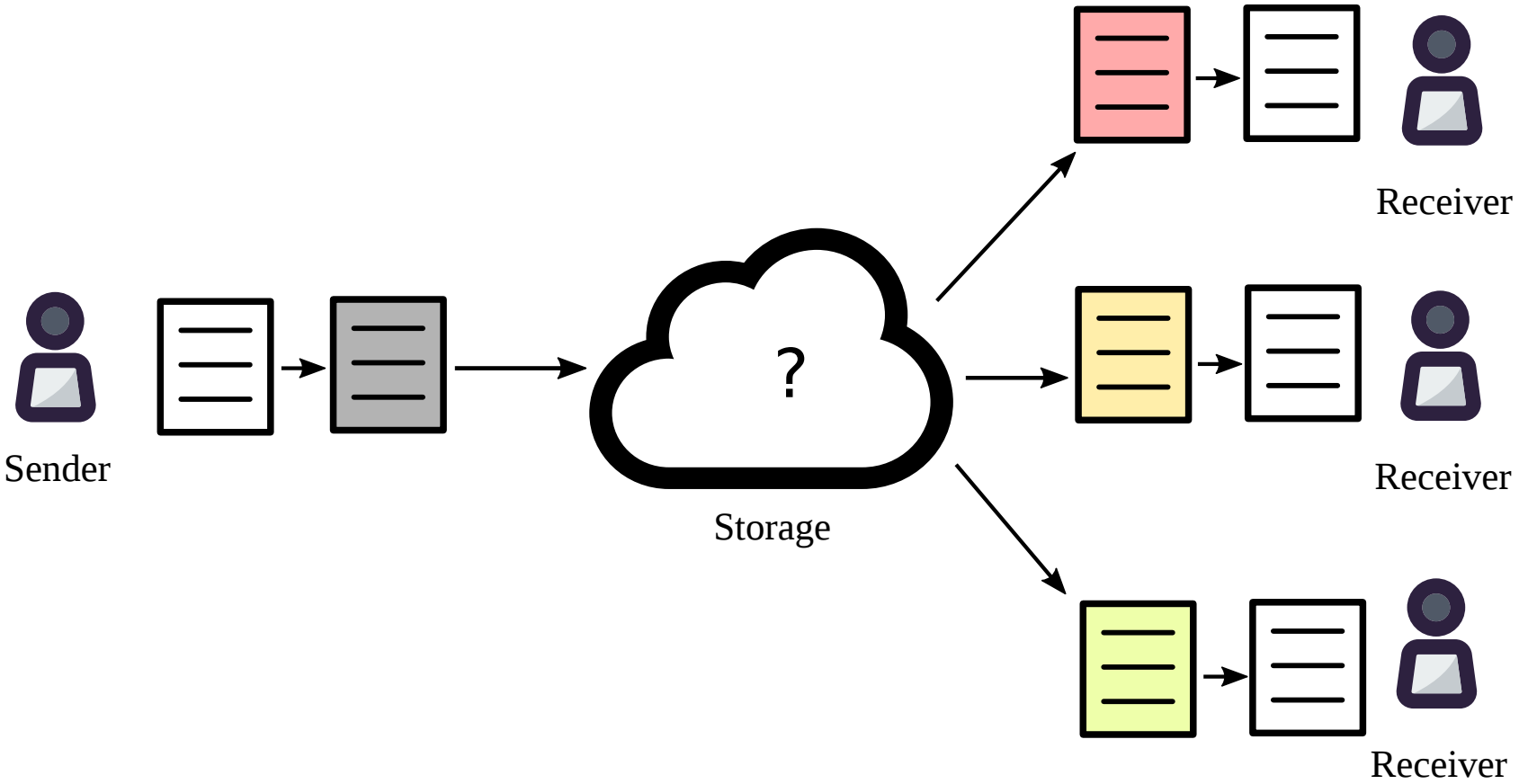
NuCypher KMS: Decentralized Key-Management System

Michael Egorov, CTO

Silicon Valley Bitcoin Meetup, 12 Dec 2017

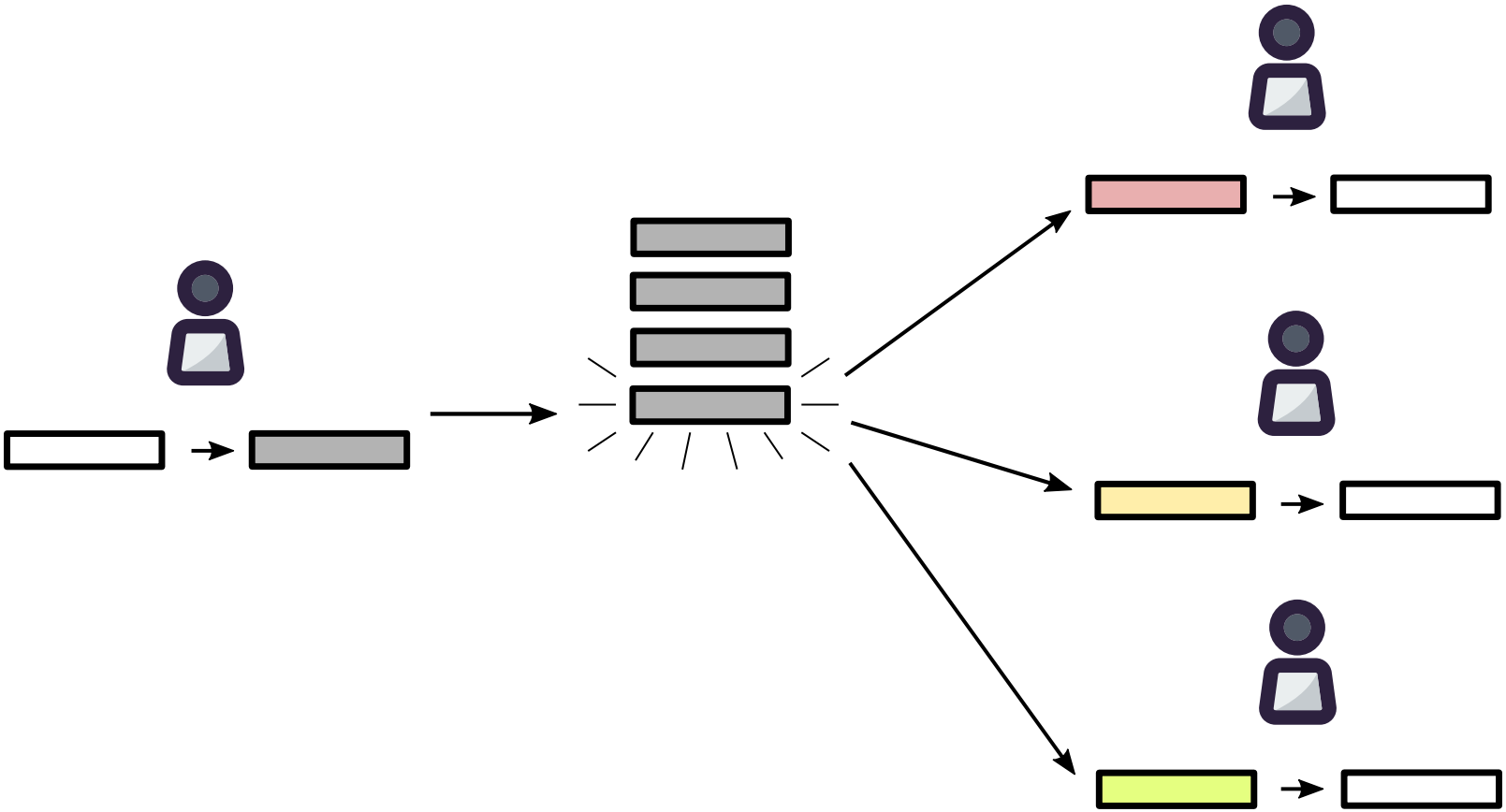
Why

Encrypted file sharing



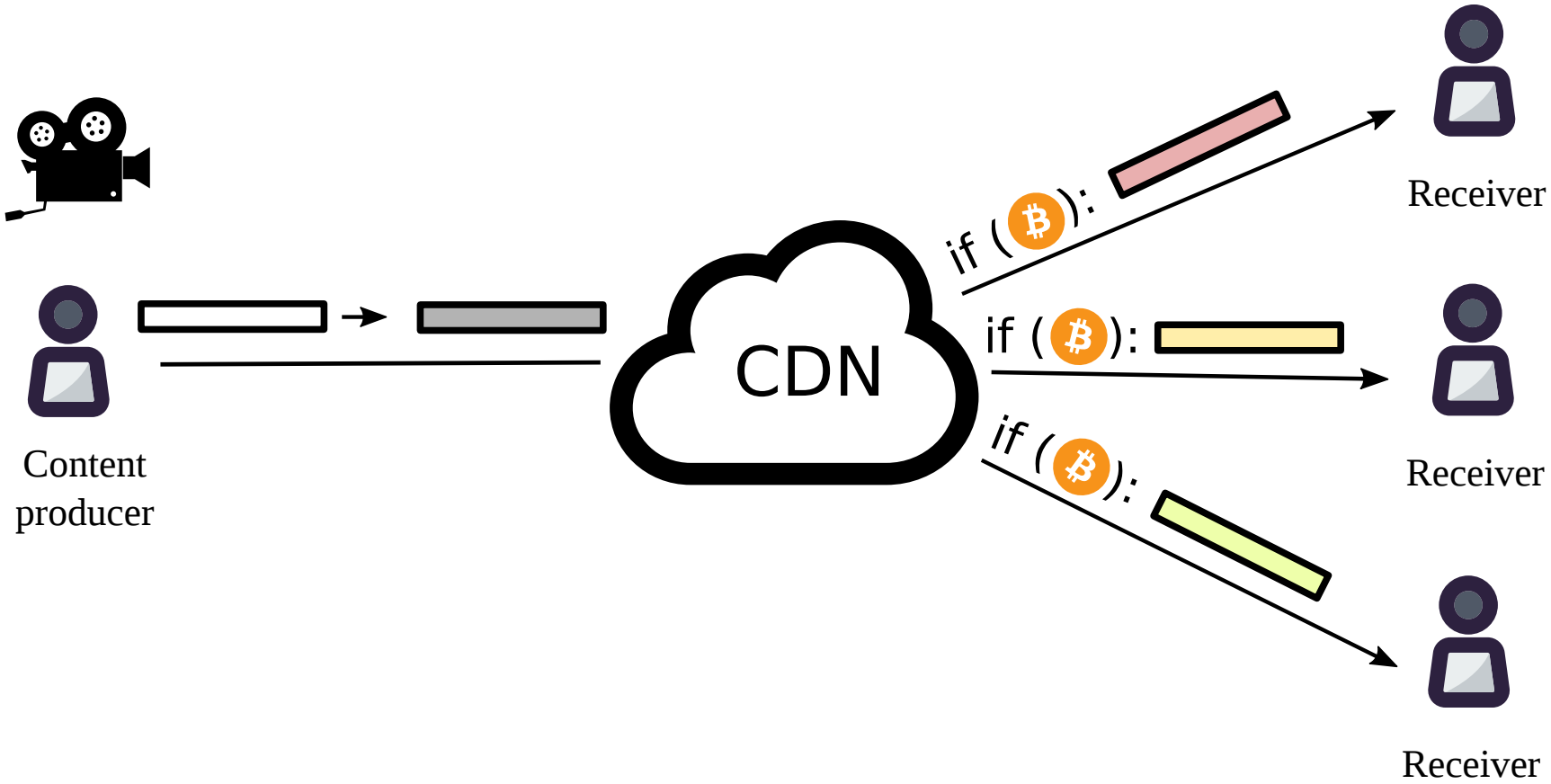
Why

Encrypted multi-user chats



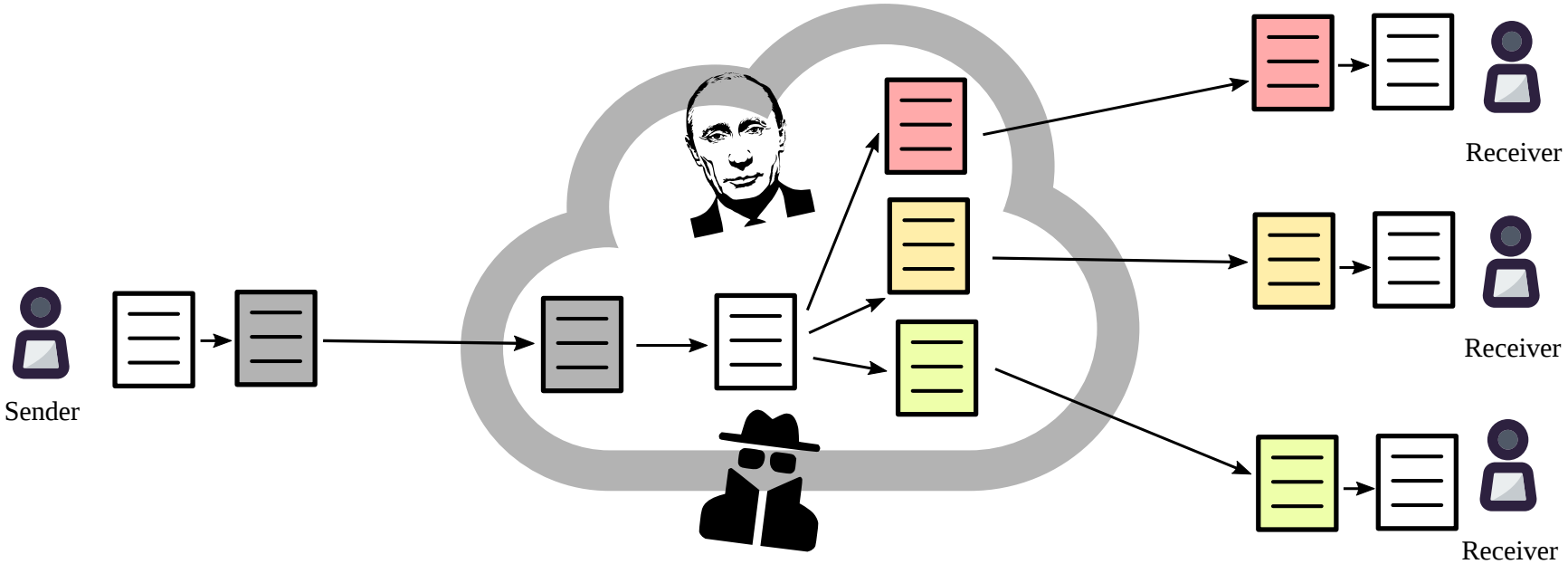
Why

Decentralized Netflix



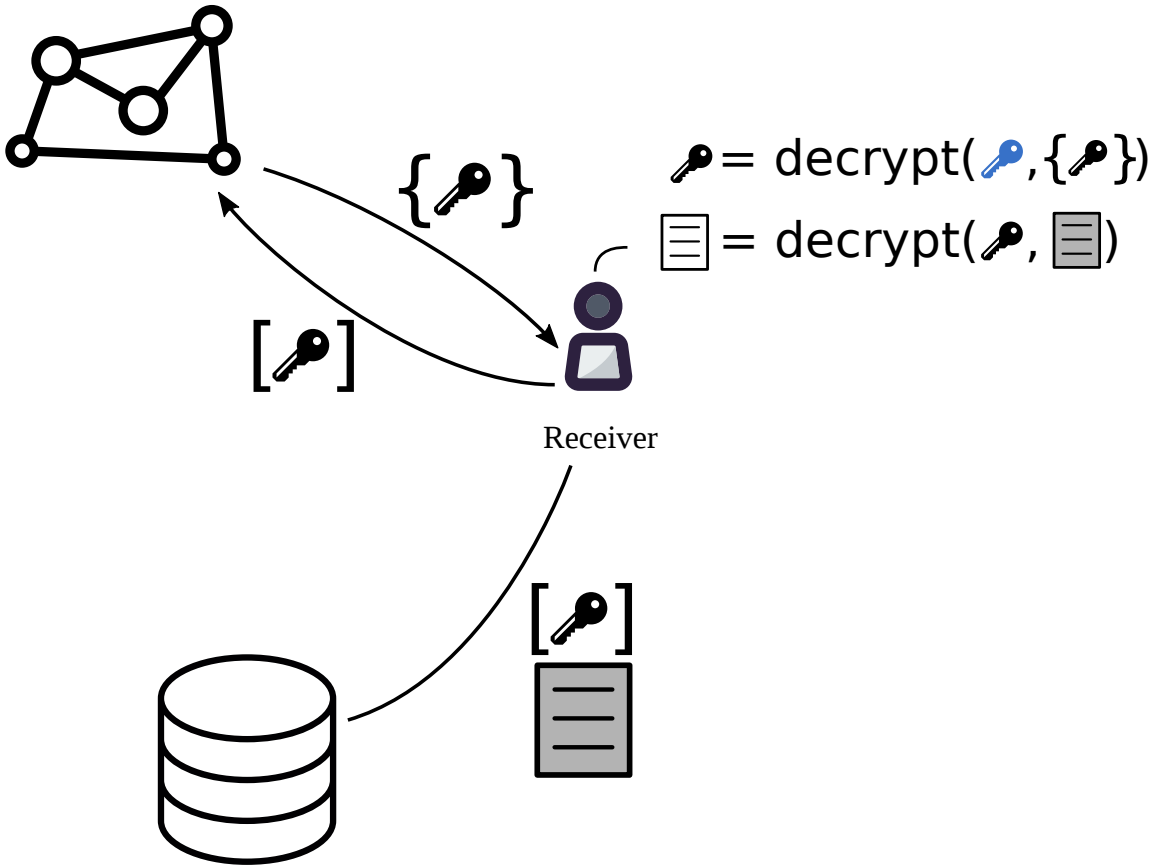
Central server + TLS

Data vulnerable to hackers, state actors etc

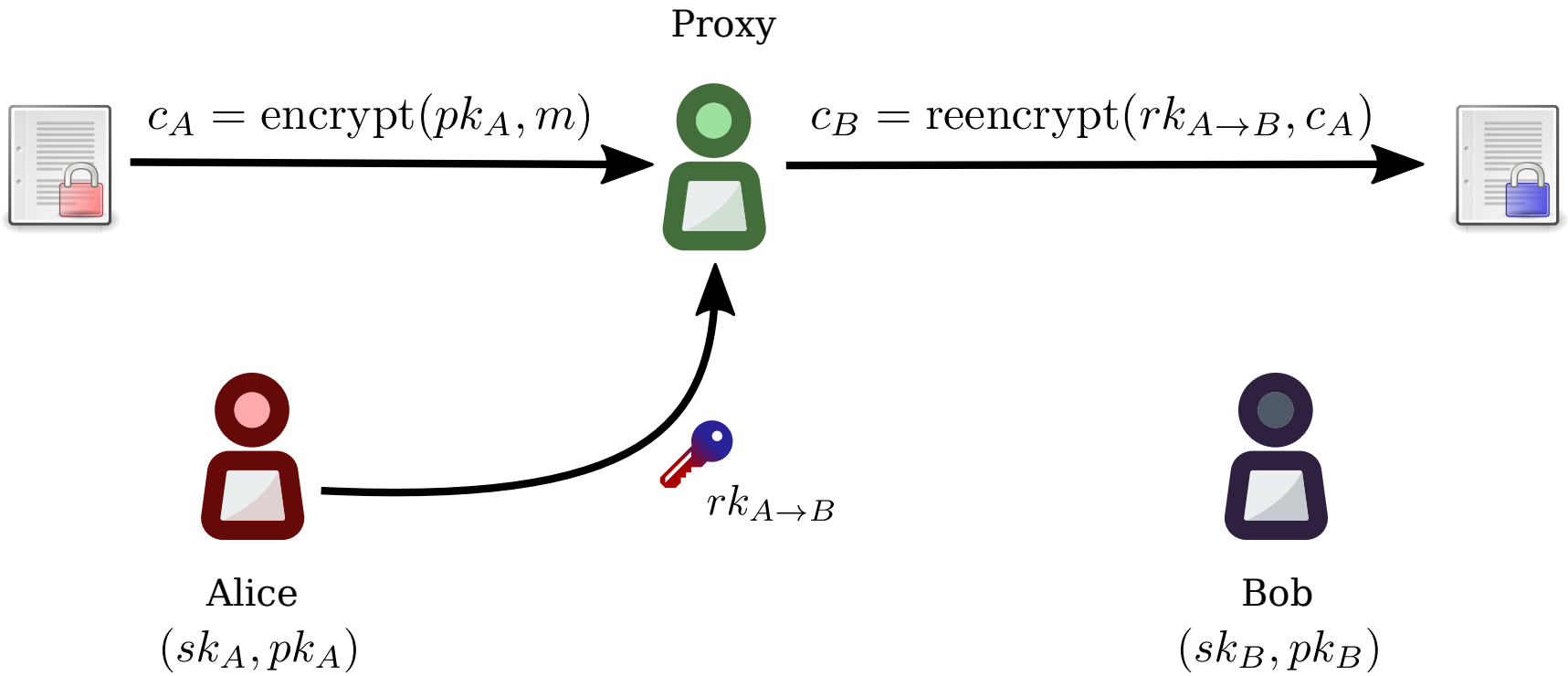


Solution

Proxy re-encryption + decentralization



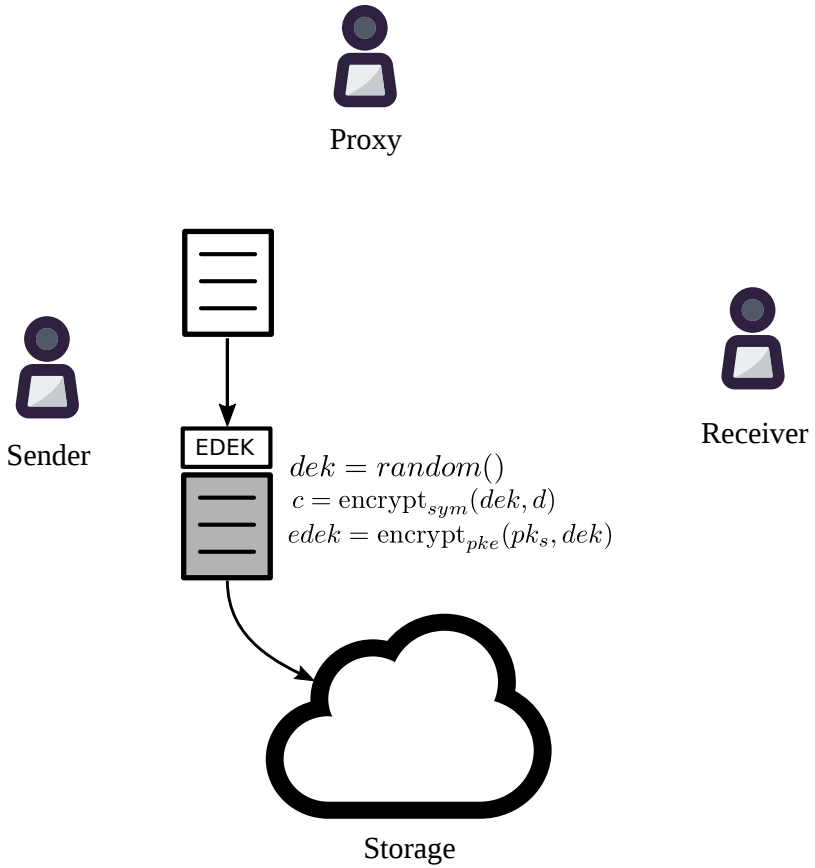
What is proxy re-encryption (PRE)



PRE demo

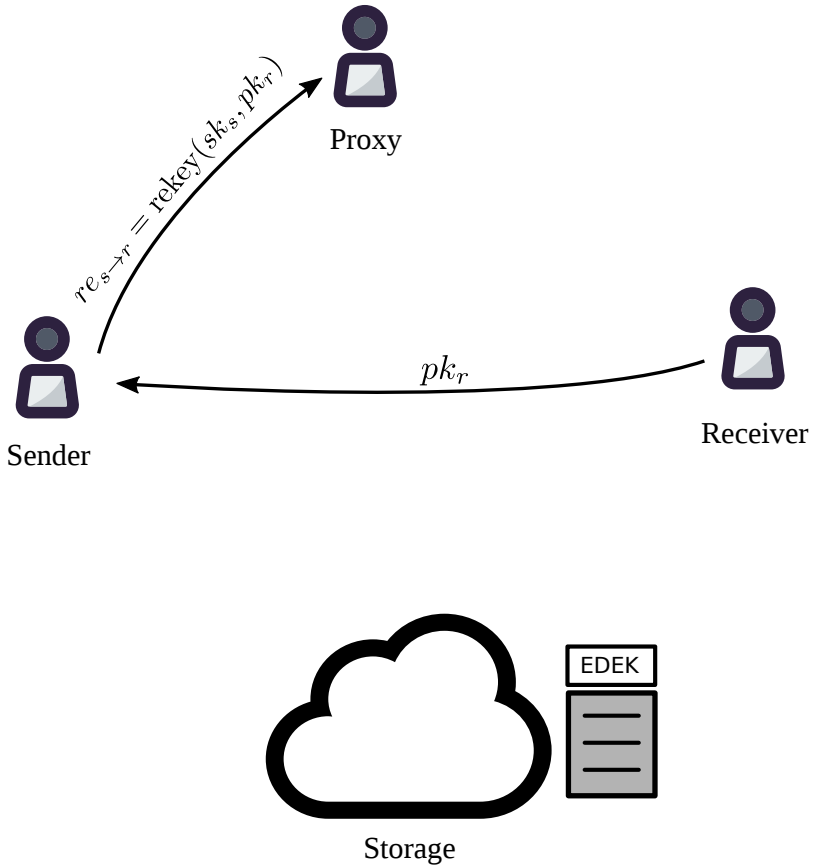
Centralized KMS using PRE

Encryption



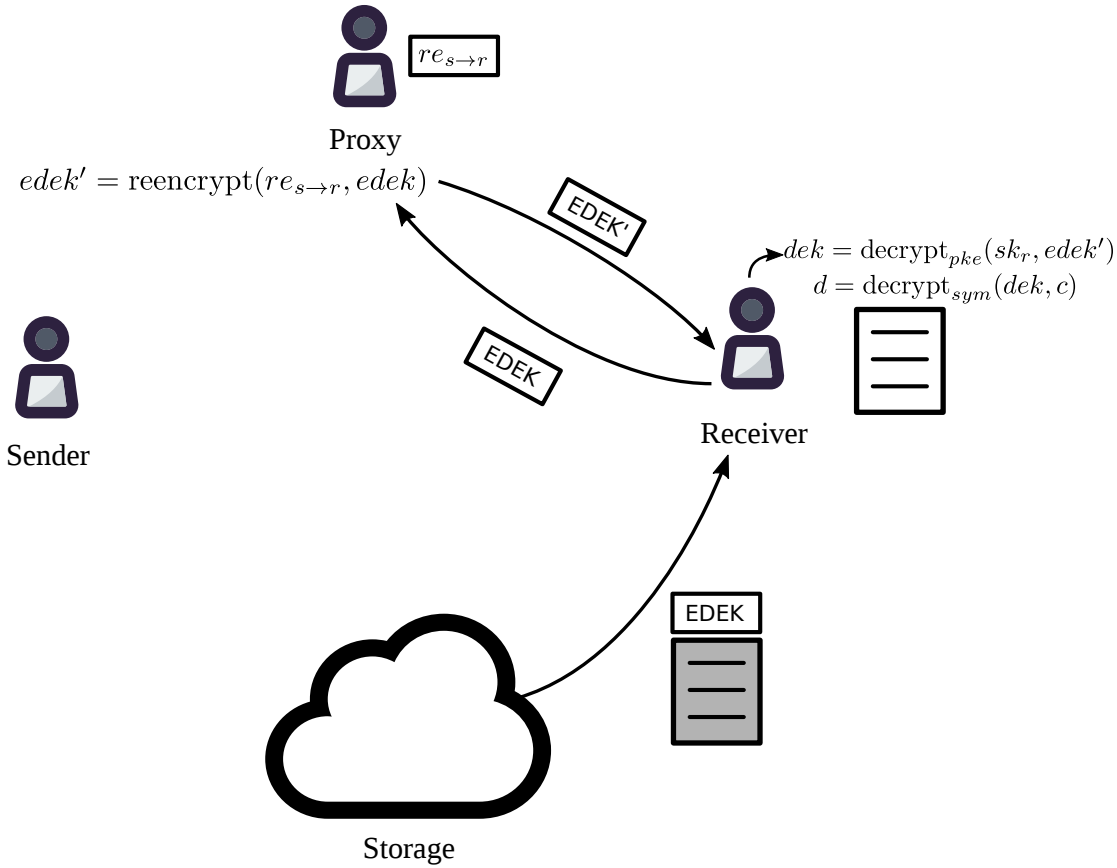
Centralized KMS using PRE

Access delegation



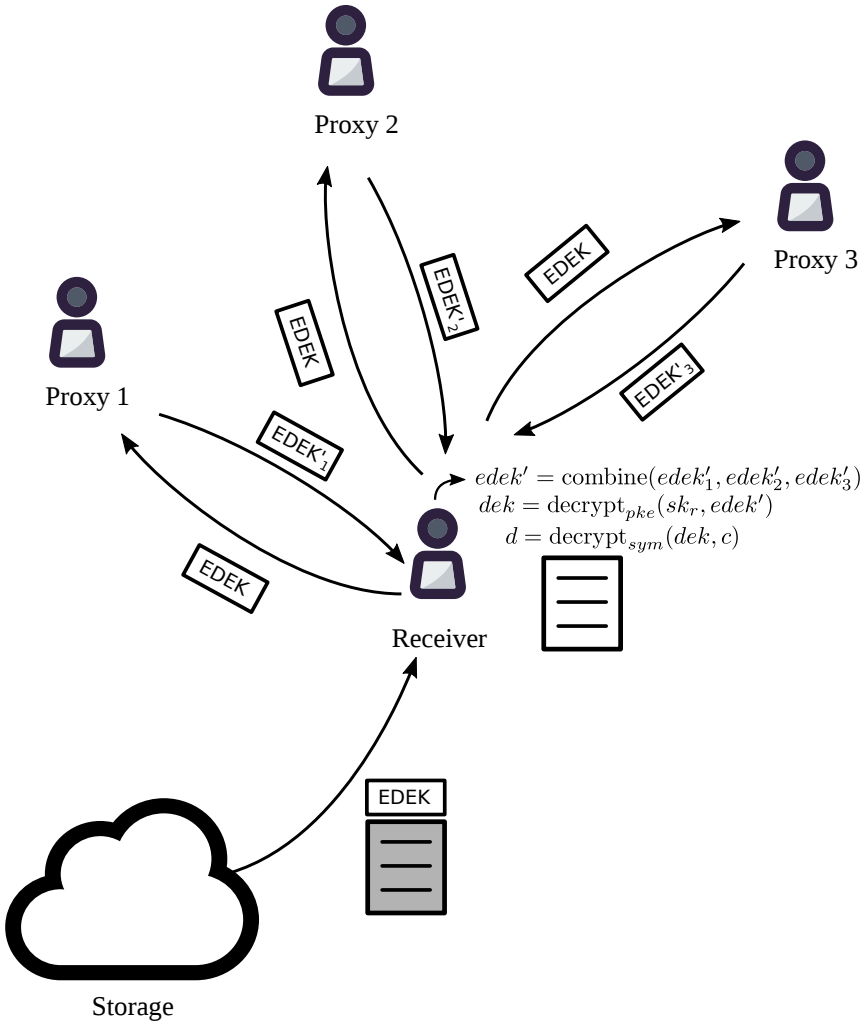
Centralized KMS using PRE

Decryption



Decentralized key management

Using threshold split-key re-encryption (Umbral)



https://github.com/nucypher/nucypher-kms/

https://github.com/nucypher/nucypher-pre-python/

KMS token

Purpose

- Splitting trust between re-encryption nodes (more tokens = more trust and more work);
- In-network means of payment for deploying policies;
- Proof of Stake for minting new coins according to the mining schedule;
- Security deposit to be at stake against malicious behavior of nodes

KMS token

Mining

Mining reward:

$$\text{reward} = \frac{\text{locked\_tokens} \times \text{reward\_rate}}{\sum_{\text{all miners}} \text{locked\_tokens}} + \sum_{\text{this miner}} \text{miner\_fees}$$

Unexpected bonus use cases

Delegate access to Bitcoin funds with proxy re-signature:

$$\text{sig}_a = \text{re-sign}(\text{re}_{ba}, \text{sign}(\text{priv}_b, \text{tx})).$$

Dead man's switch to give access to data or Bitcoin keys:

```
if (now - last_transaction) > 100 * days:
    c_b = reencrypt(re_ab, c_a)

else:
    raise LifeError("The man isn't dead yet")
```

Early users

Decentralized marketplaces:

- Datum;
- Helios.

Decentralized databases:

- Bluzelle;
- Fluence;
- Wolk.

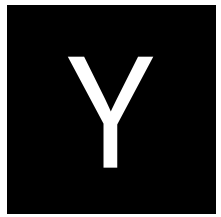
Medical data sharing

- Medibloc;
- ZeroPass;
- Wholesome.

IoT

- Spherity (together with BigchainDB).

Investors



Blockchain Partners Korea

Team

Founders

Advisors

How to contribute, learn

Website: `https://nucypher.com/blockchain.html`
Github: `https://github.com/nucypher/`
Slack: `https://nucypher-kms-slack.herokuapp.com/`
Whitepaper: `https://arxiv.org/abs/1707.06140`