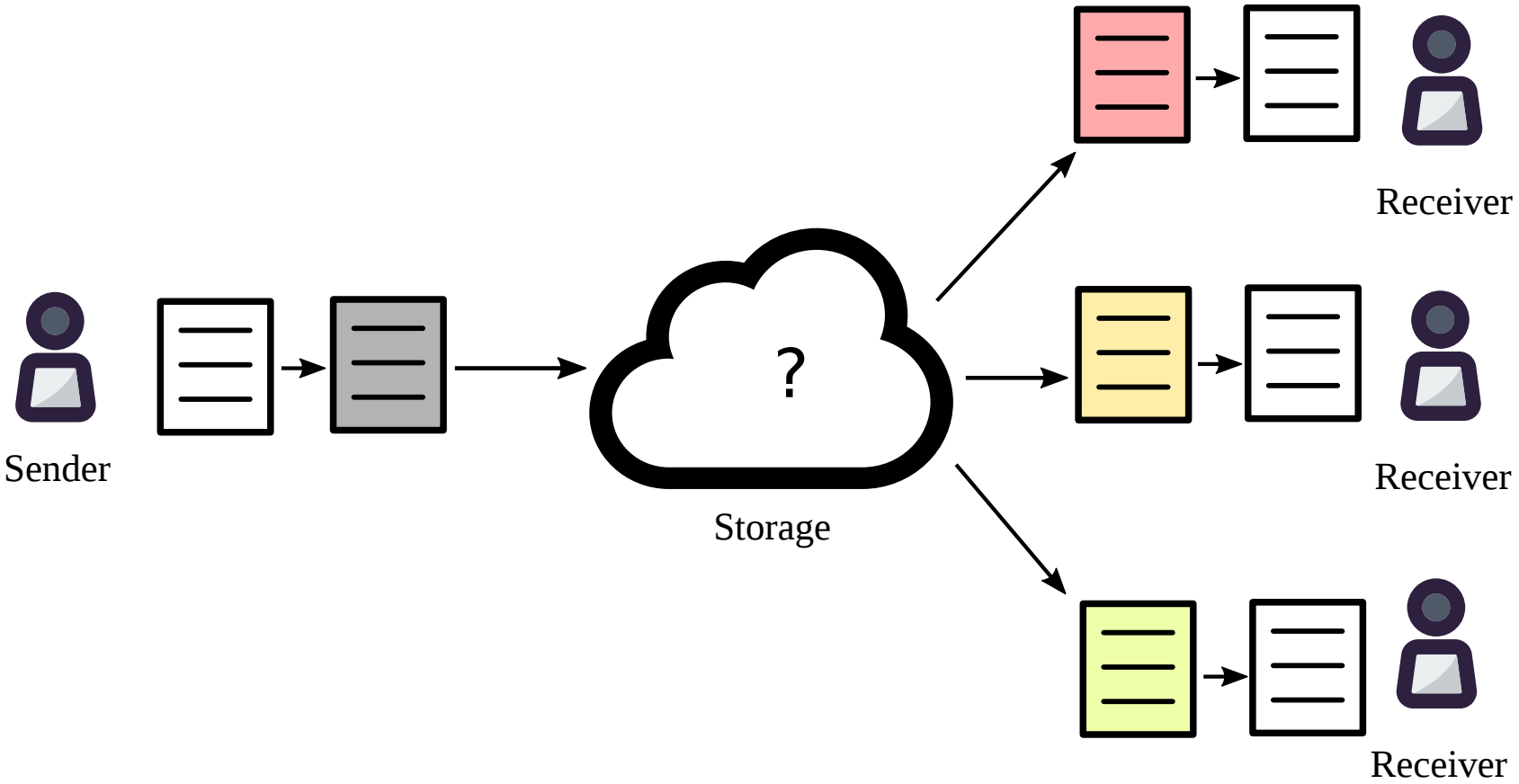
NuCypher KMS: Decentralized Key-Management System

Michael Egorov, CTO

SF Cryptocurrency Devs, 29 Nov 2017

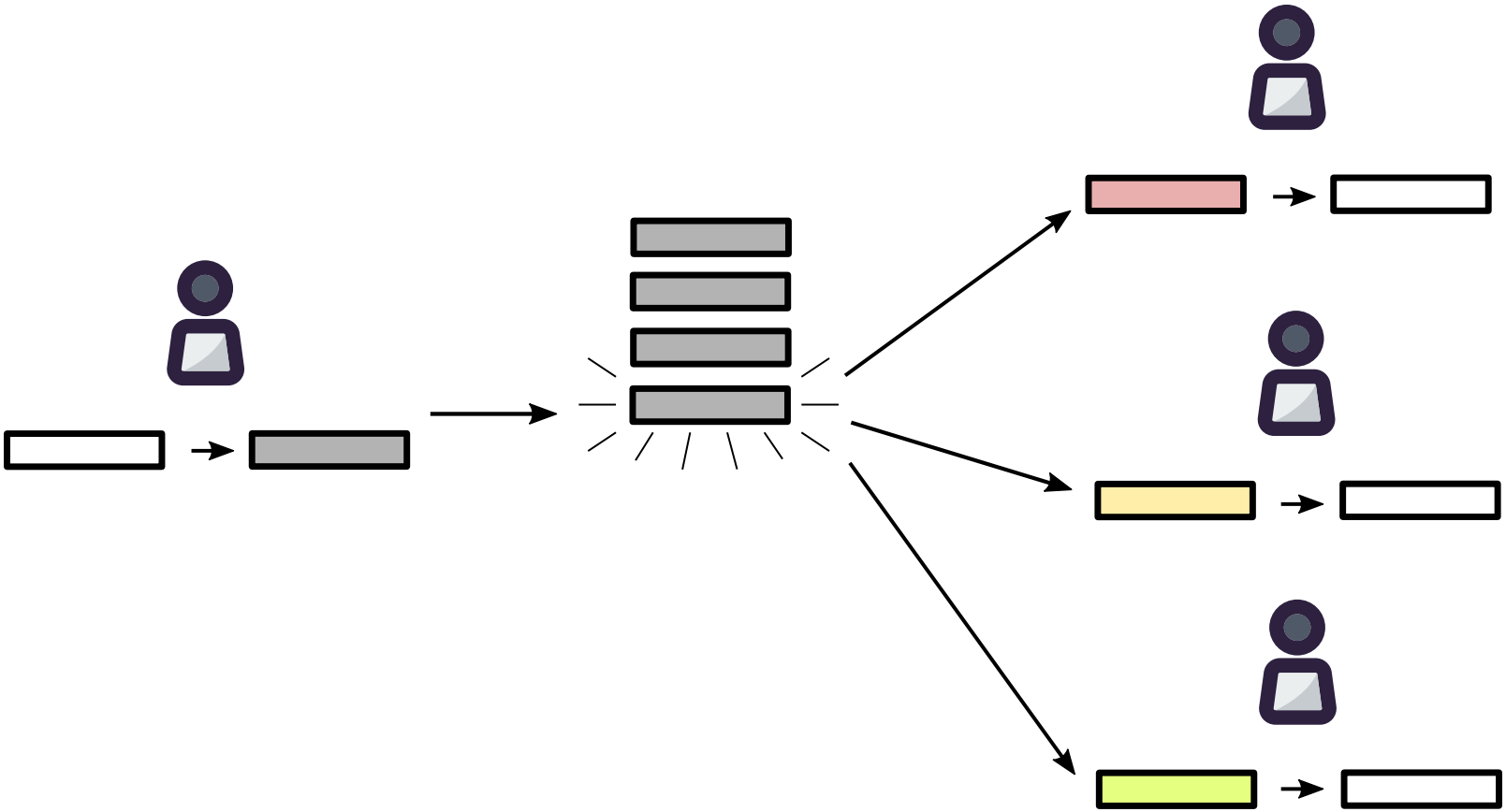
Why

Encrypted file sharing



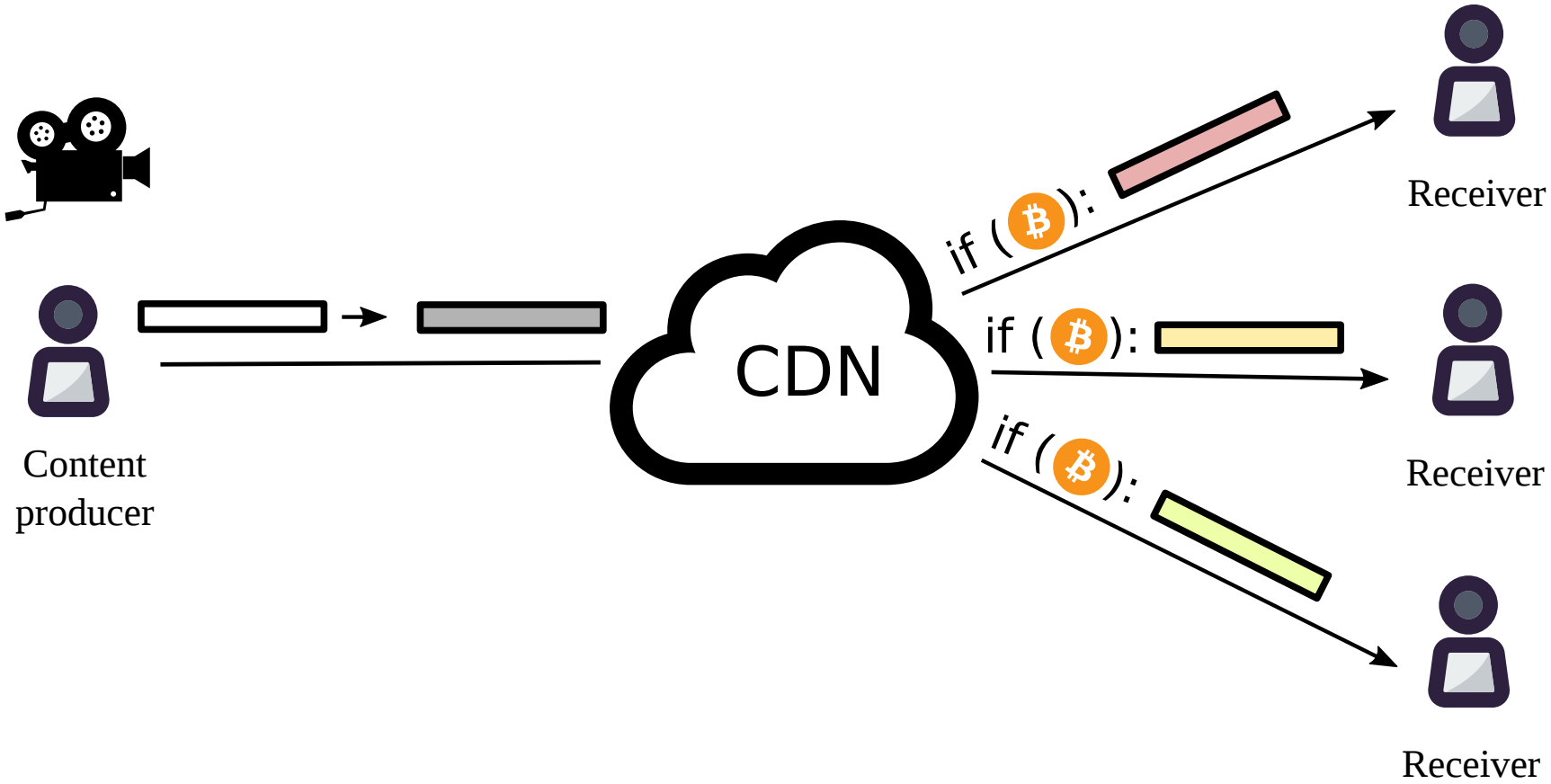
Why

Encrypted multi-user chats



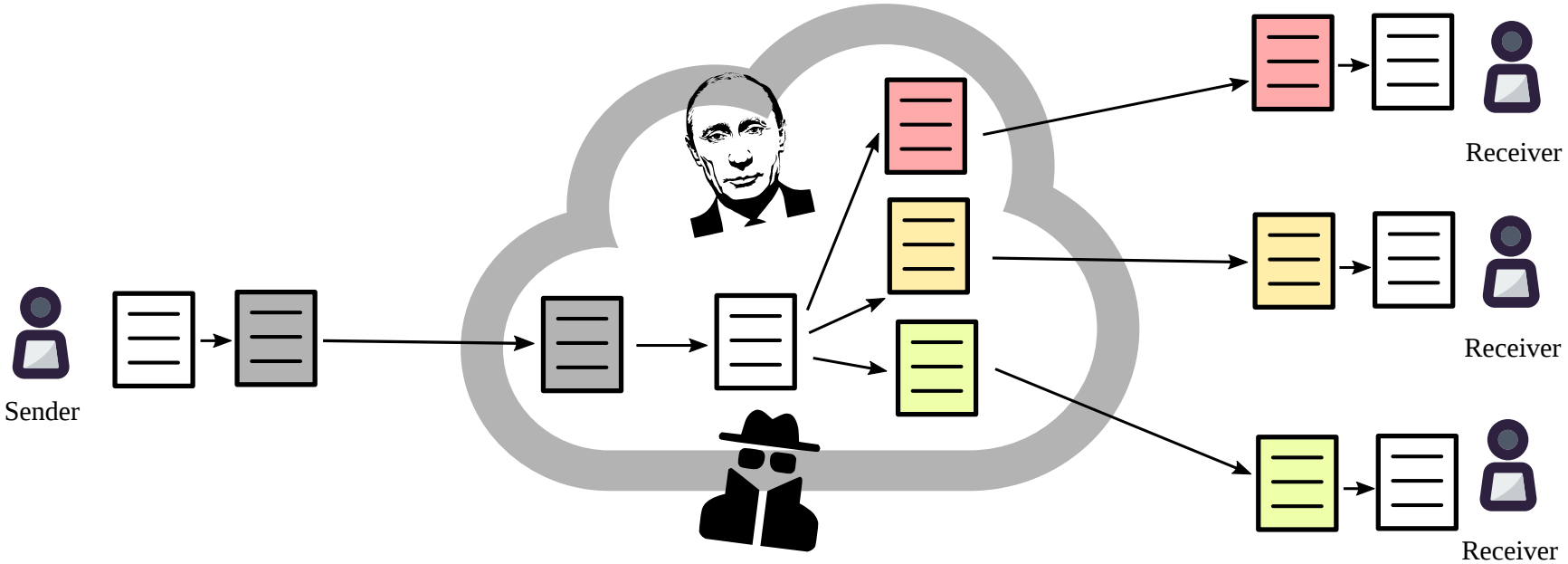
Why

Decentralized Netflix



Central server + TLS

Data vulnerable to hackers, state actors etc



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