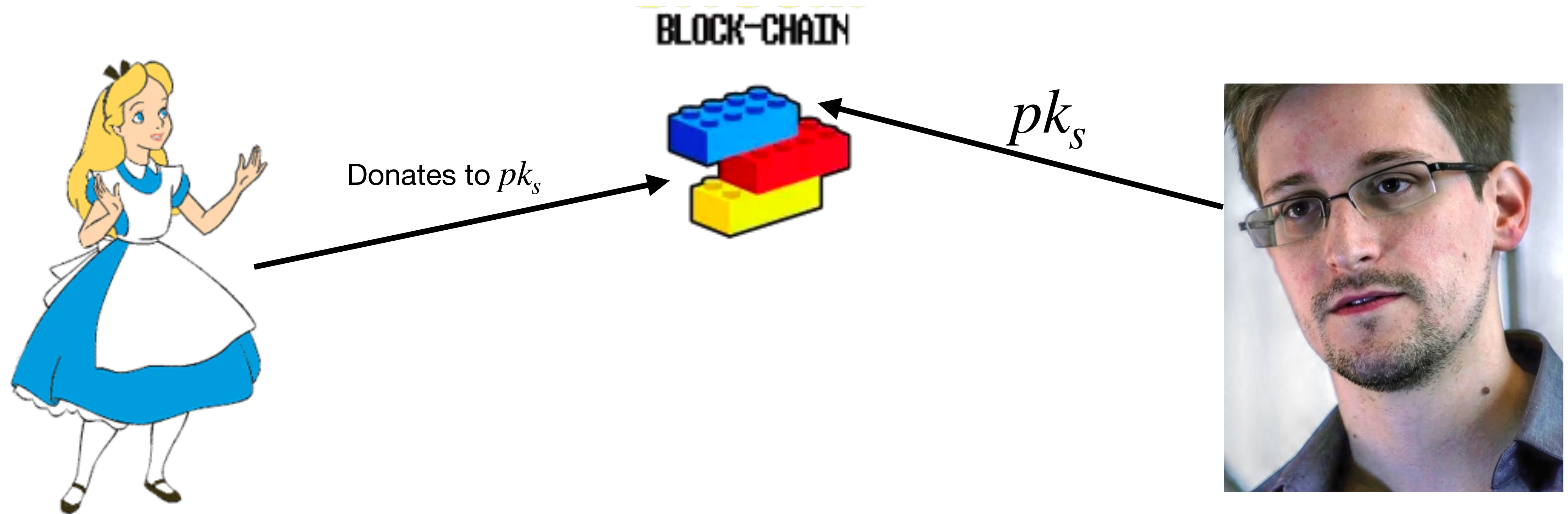


PPS: Privacy preserving Signalling

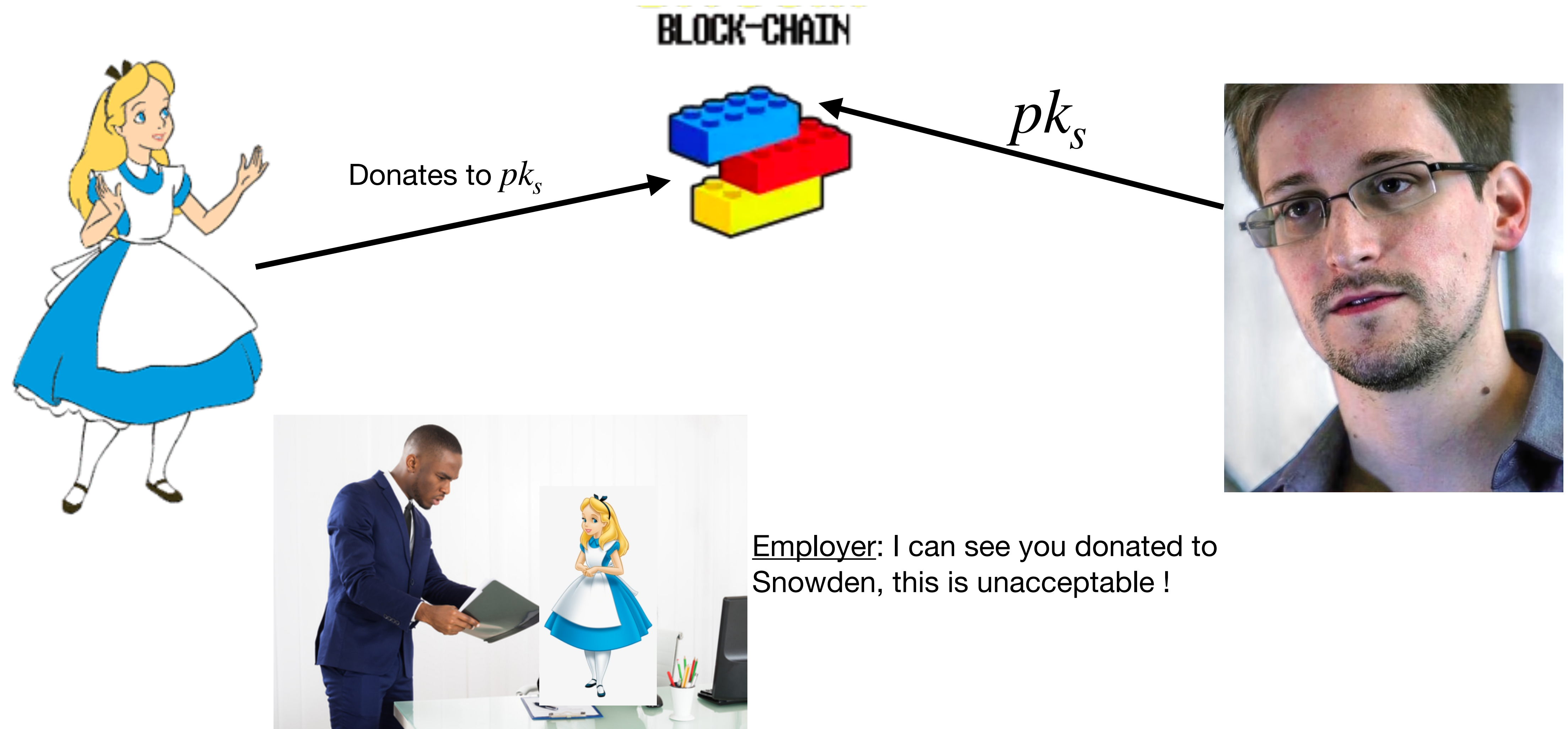
FE Hackathon 2021

Team ZenGo X

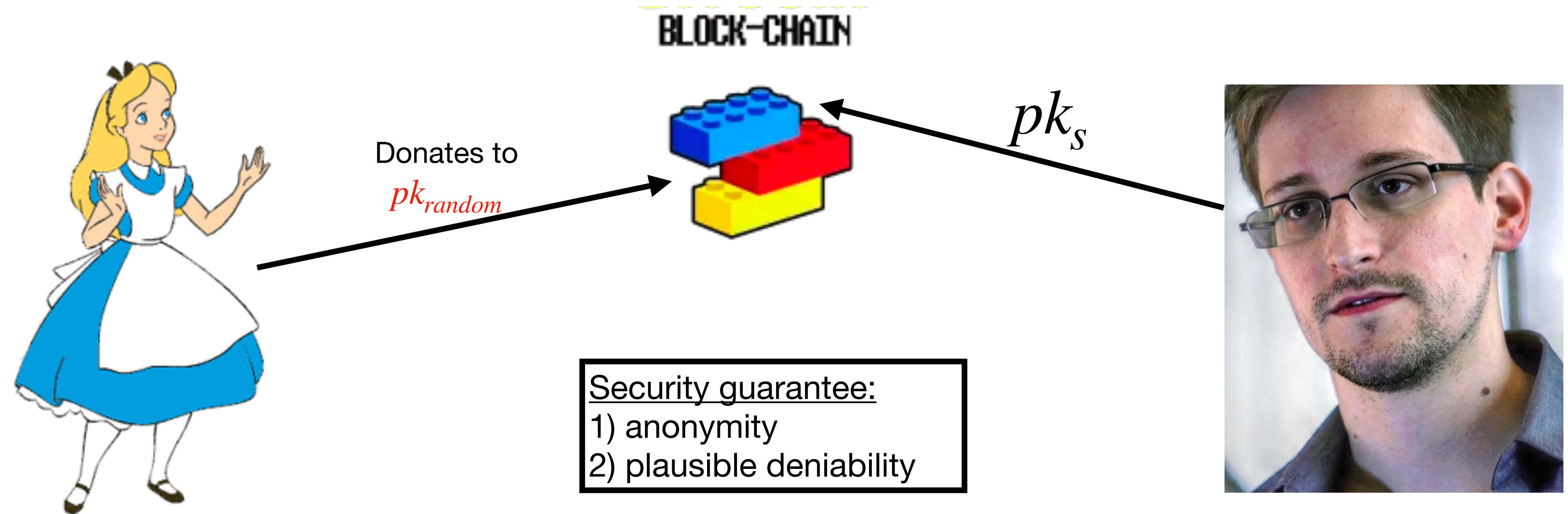
The canonical example: anonymous donations



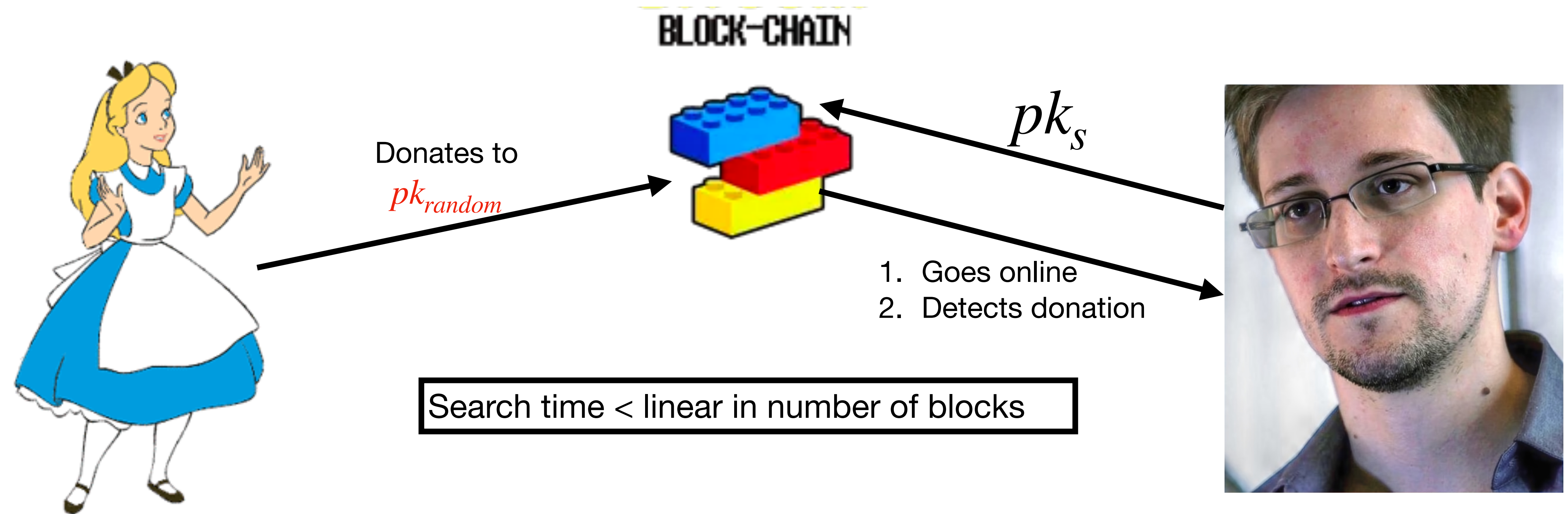
The canonical example: anonymous donations



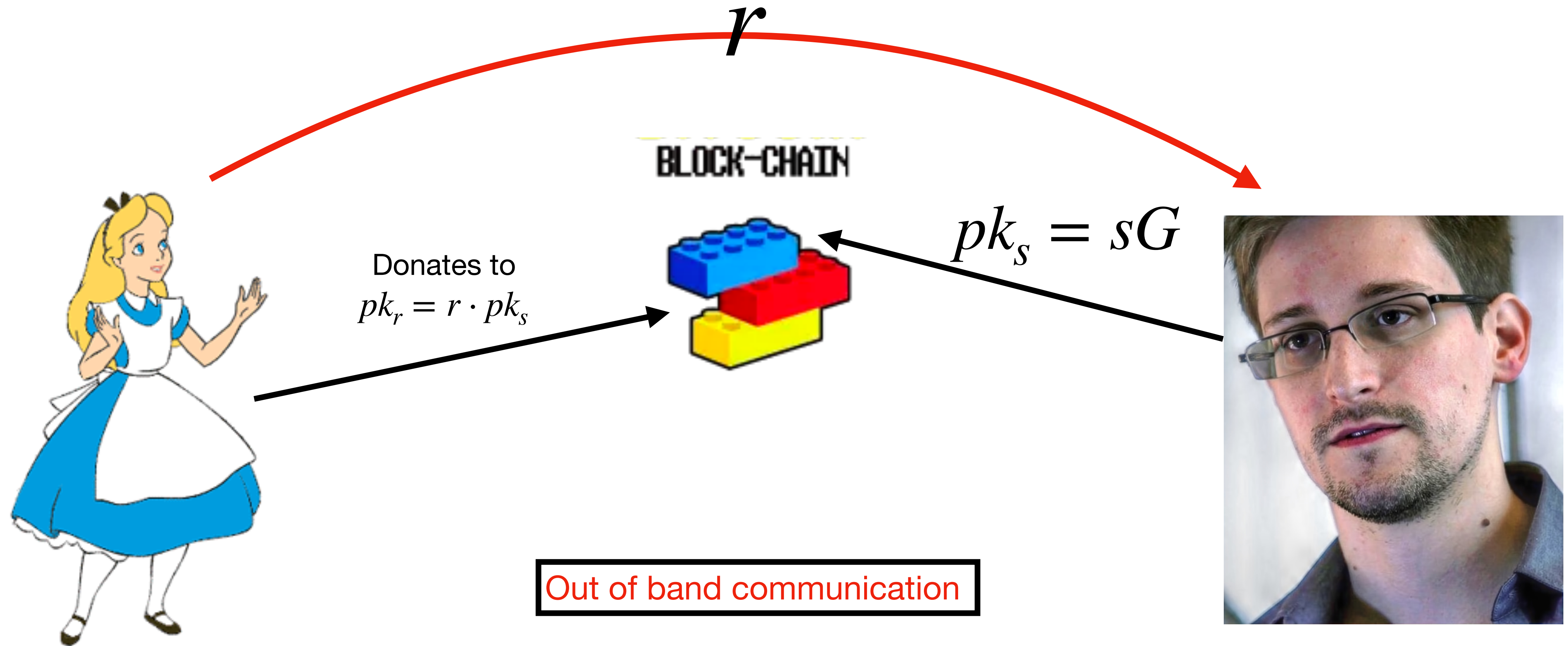
Ideally...



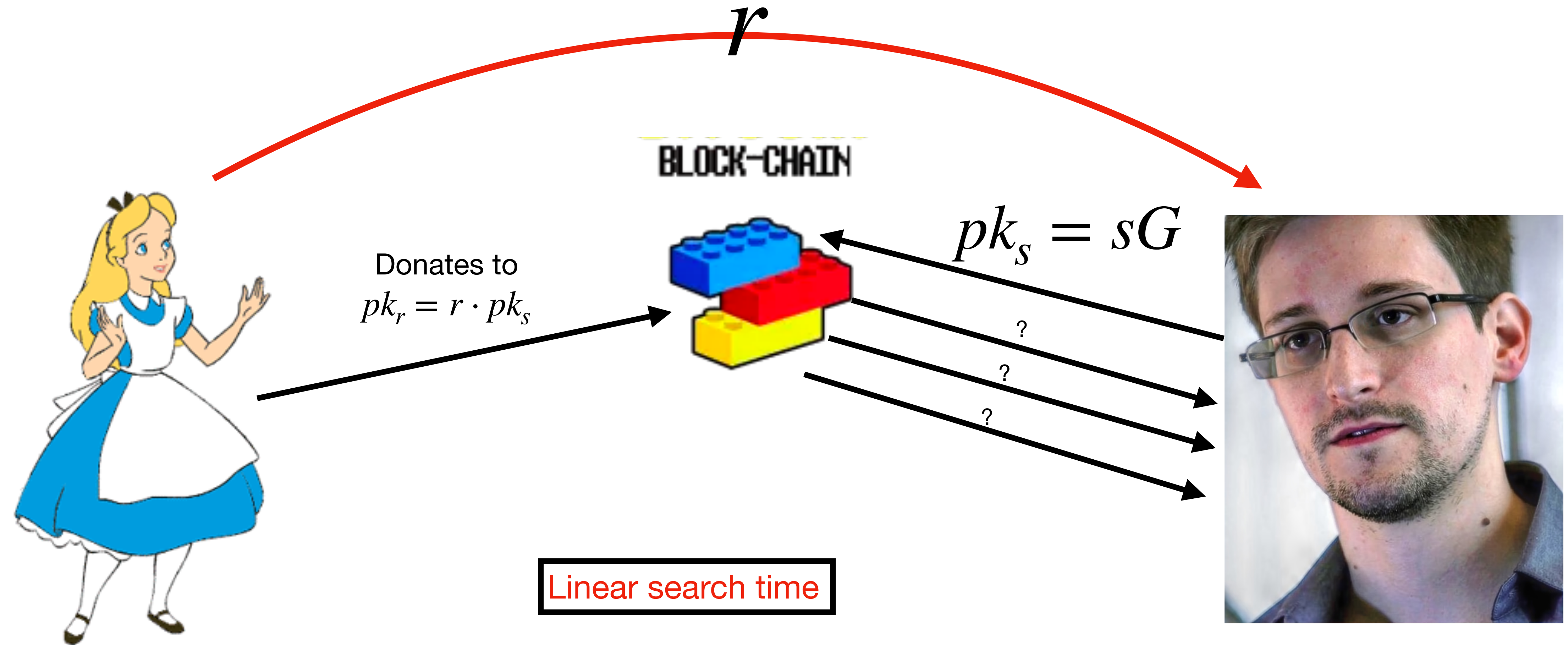
Ideally...



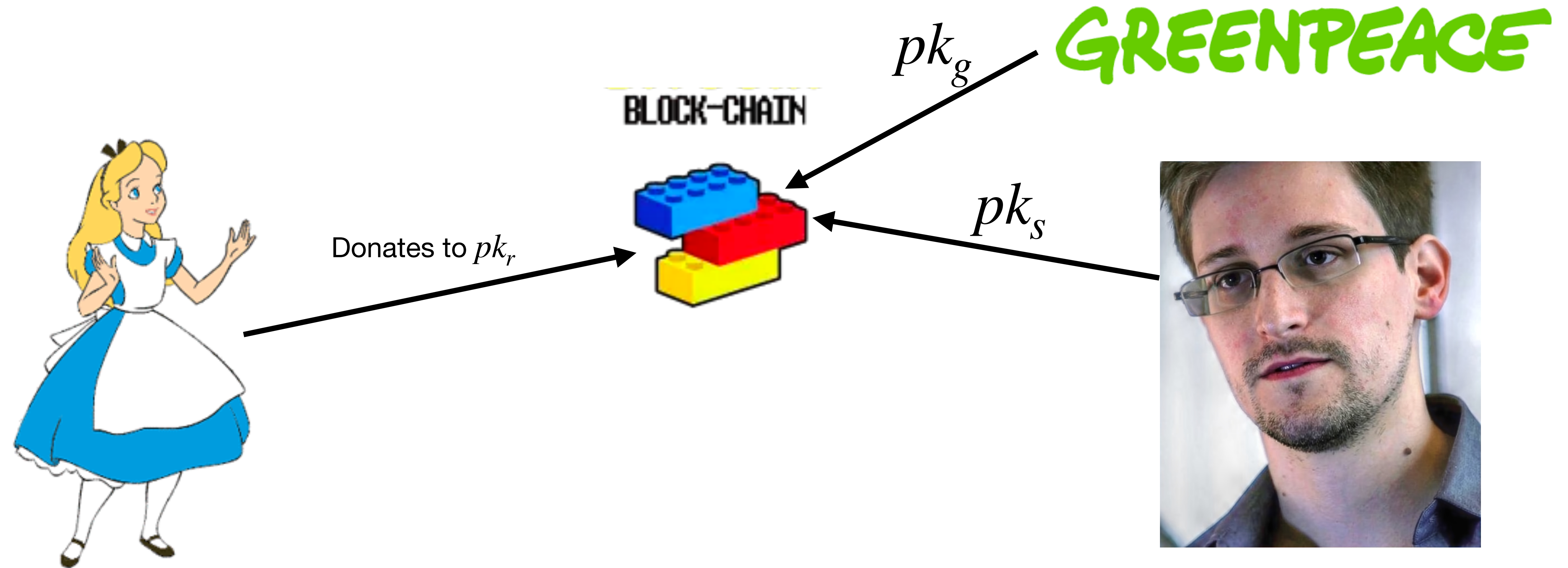
Best solution today :



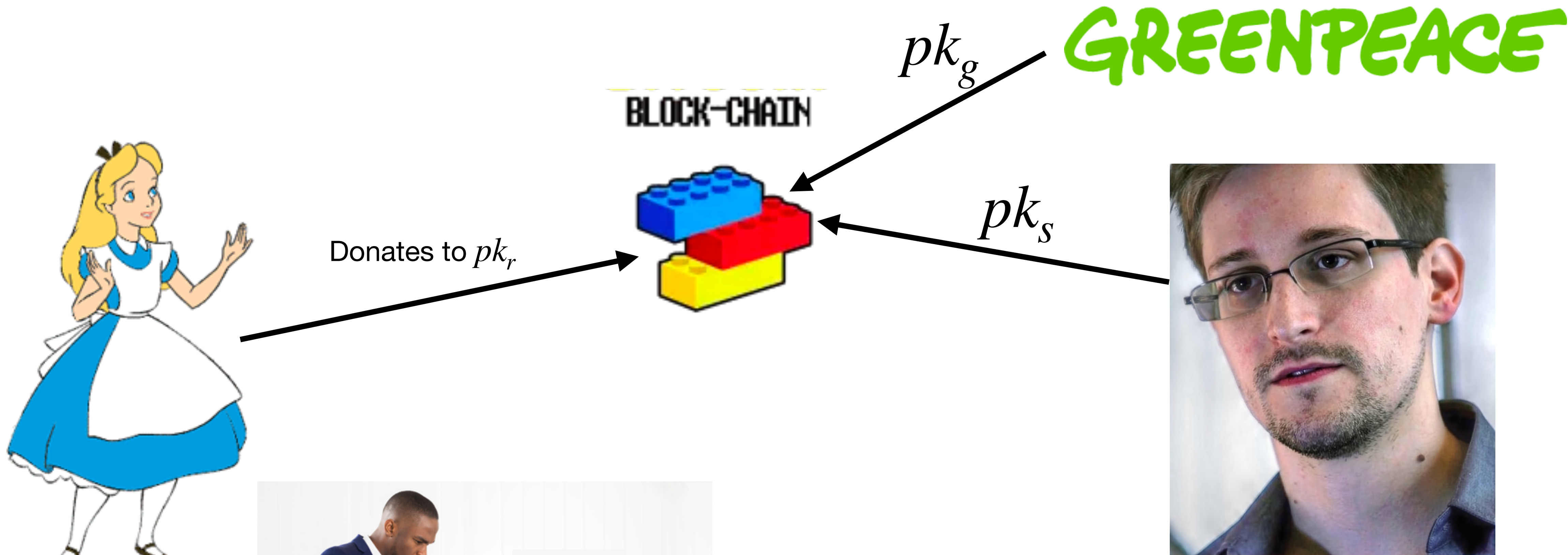
Best solution today :



Our solution : FE-PPS

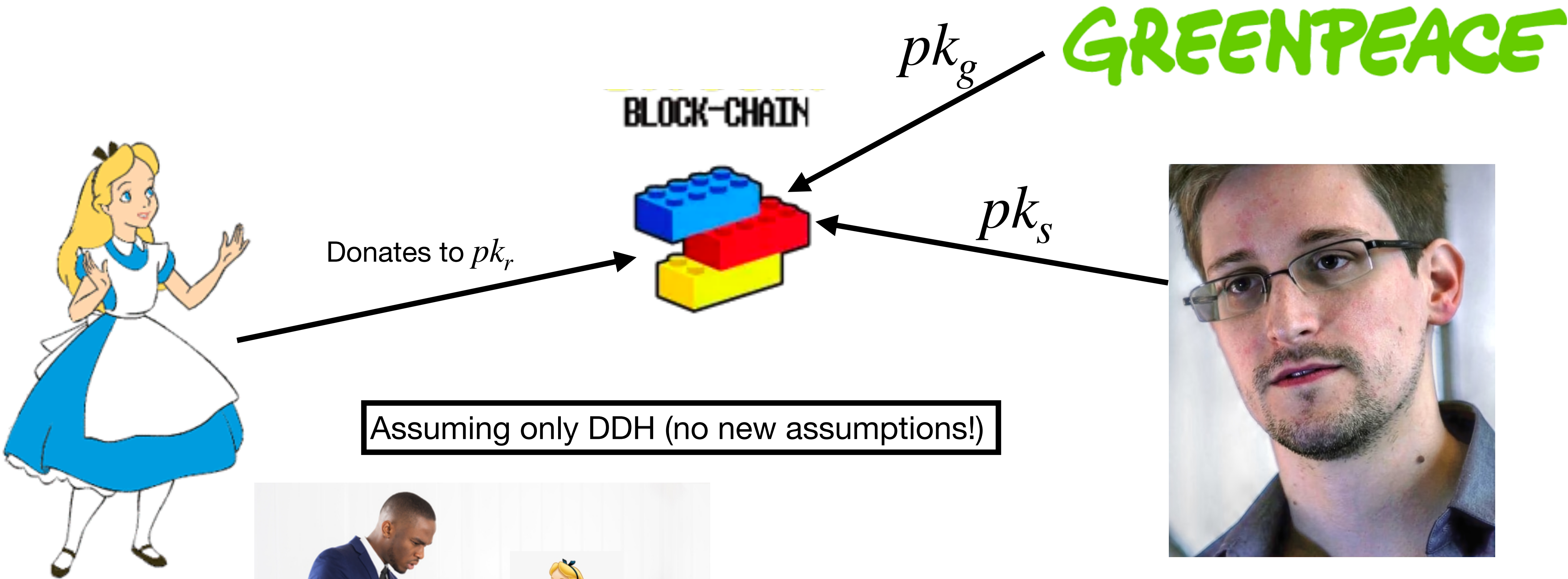


Our solution : FE-PPS



Employer: I can see you made a donation to either Snowden or Greenpeace or xxx or yyy or... very good!

Our solution : FE-PPS



Employer: I can see you made “A” donation to either Snowden or Greenpeace or xxx or yyy or... very good!

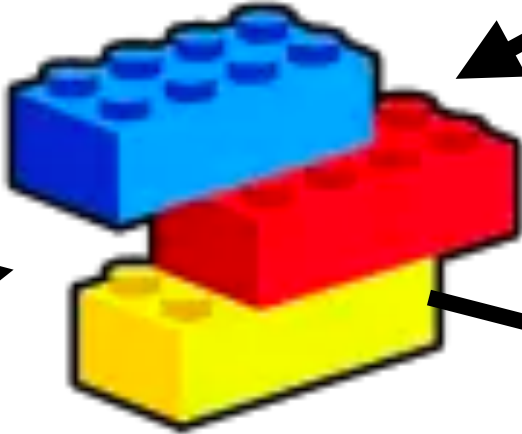
Our solution : FE-PPS

GREENPEACE



Donates to pk_r

BLOCK-CHAIN



pk_g

pk_s

- 1. Goes online
- 2. Detects donation

Search time = $\mathcal{O}(\log(t))$, t = number of blocks



Our API

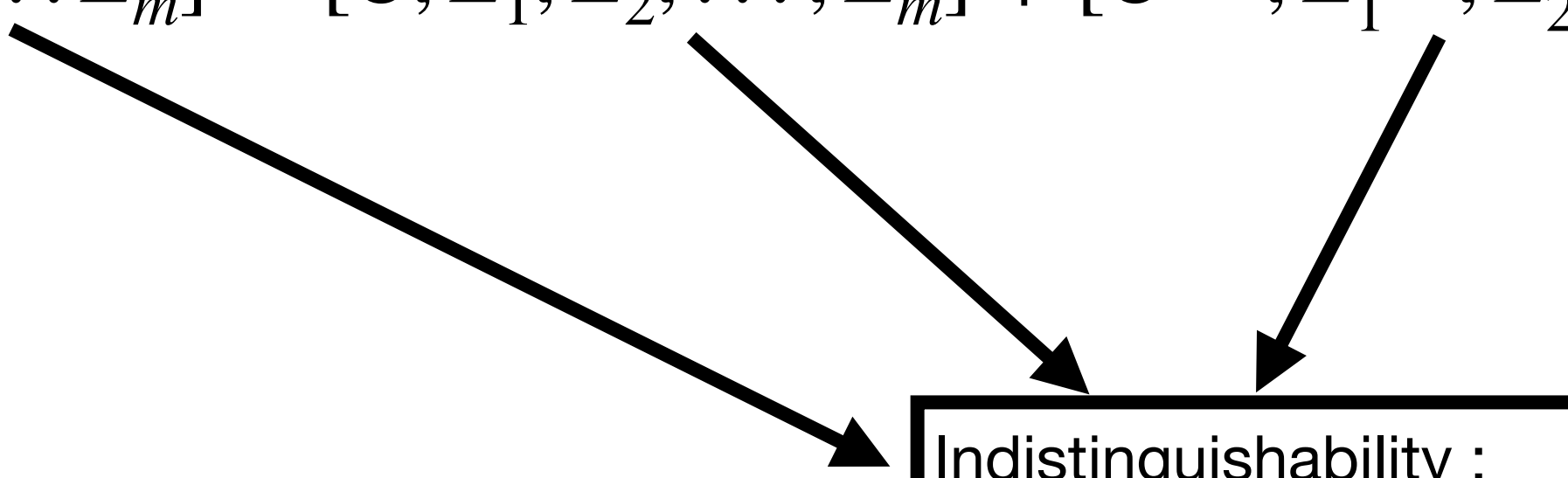
We use simple.DDH (Simple Functional Encryption Schemes for Inner Products)

- **Setup** (assume m receivers):
 - wraps [Setup](#) and [KeyDer](#)
 - no trusted party is needed
- **Send** (Alice):
 - Wraps [Encrypt](#)
 - Reads state from the blockchain $(C^{i-1}, E_1^{i-1}, E_2^{i-1}, \dots, E_m^{i-1})$
 - Updates ciphertext state $[C^i, E_1^i, E_2^i, \dots, E_m^i] = [C, E_1, E_2, \dots, E_m] + [C^{i-1}, E_1^{i-1}, E_2^{i-1}, \dots, E_m^{i-1}]$
 - Publish new state to the blockchain
- **Search** (Snowden):
 - Wraps [Decrypt](#)
 - Binary search for first signal in a range of blocks
 - Collect donation, repeat

Our API

We use simple.DDH (Simple Functional Encryption Schemes for Inner Products)

- **Setup** (assume m receivers):
 - wraps **Setup** and **KeyDer**
 - no trusted party is needed
- **Send** (Alice):
 - Wraps **Encrypt**
 - Reads state from the blockchain $(C^{i-1}, E_1^{i-1}, E_2^{i-1}, \dots, E_m^{i-1})$
 - Updates ciphertext state $[C^i, E_1^i, E_2^i, \dots, E_m^i] = [C, E_1, E_2, \dots, E_m] + [C^{i-1}, E_1^{i-1}, E_2^{i-1}, \dots, E_m^{i-1}]$
 - Publish new state to the blockchain
- **Search** (Snowden):
 - Wraps **Decrypt**
 - Binary search for first signal in a range of blocks
 - Collect donation, repeat



Indistinguishability :

- E_i contains a signal
- E_j contains a signal

Future steps

- Support EC groups in GoFE
- Write down a smart contract and ship it live
- Explore building it on Bitcoin (ciphertexts are EC points)
- adjust to work as a Mixer (receivers are also senders)
- take advantage of the inner product: enable auditability for designated authorities
- Malicious security: Zk proof of correct update

Thank you!

DEMO