



It's all in your head – what if
it falls off?
Safekeeping in the digital era

#hcpp19, Pavel



Staying in charge when you cannot be

How?



Staying in charge when you cannot be

How?

DAPP on Ethereum

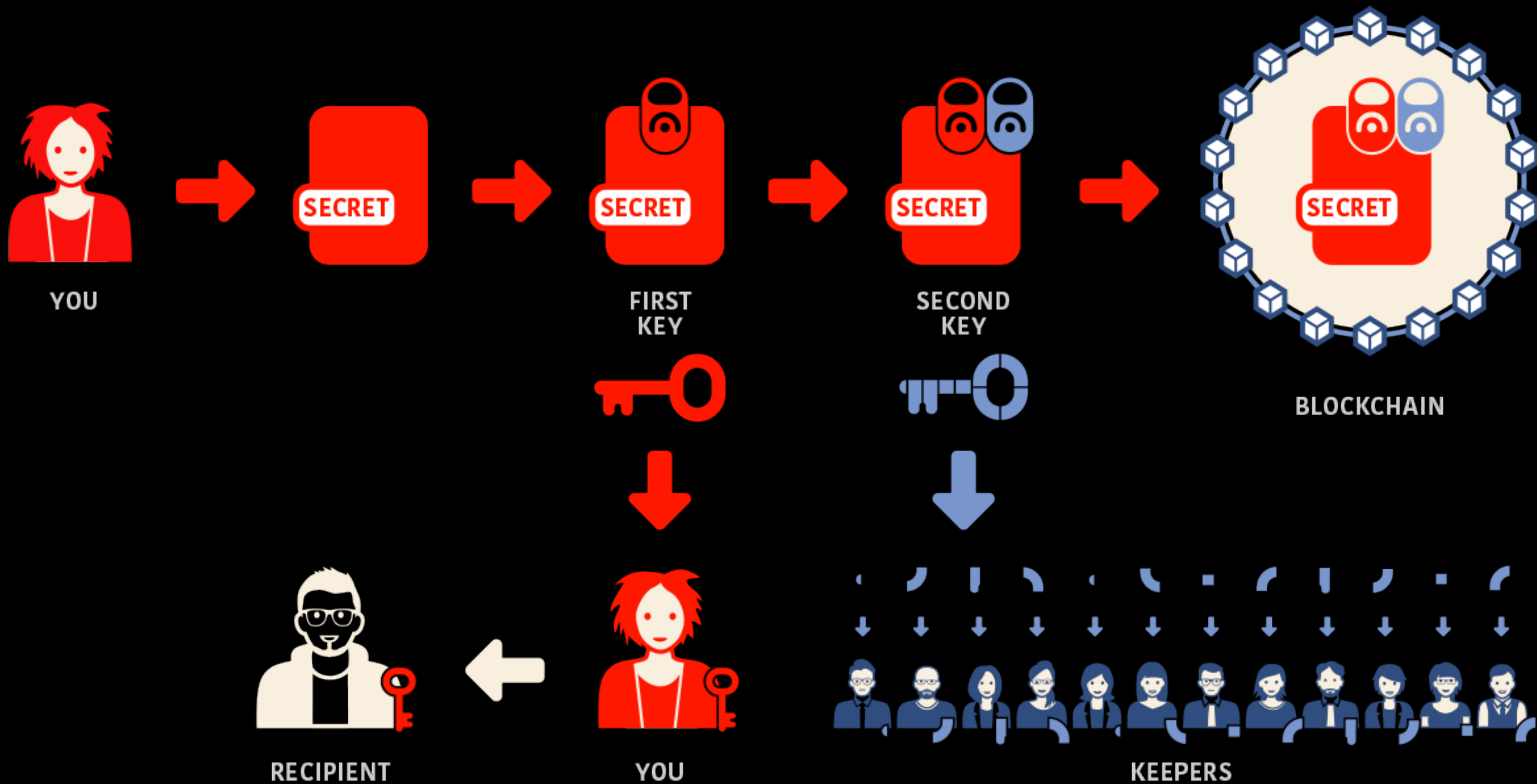
paid keepers

secret split between keepers (Shamir)

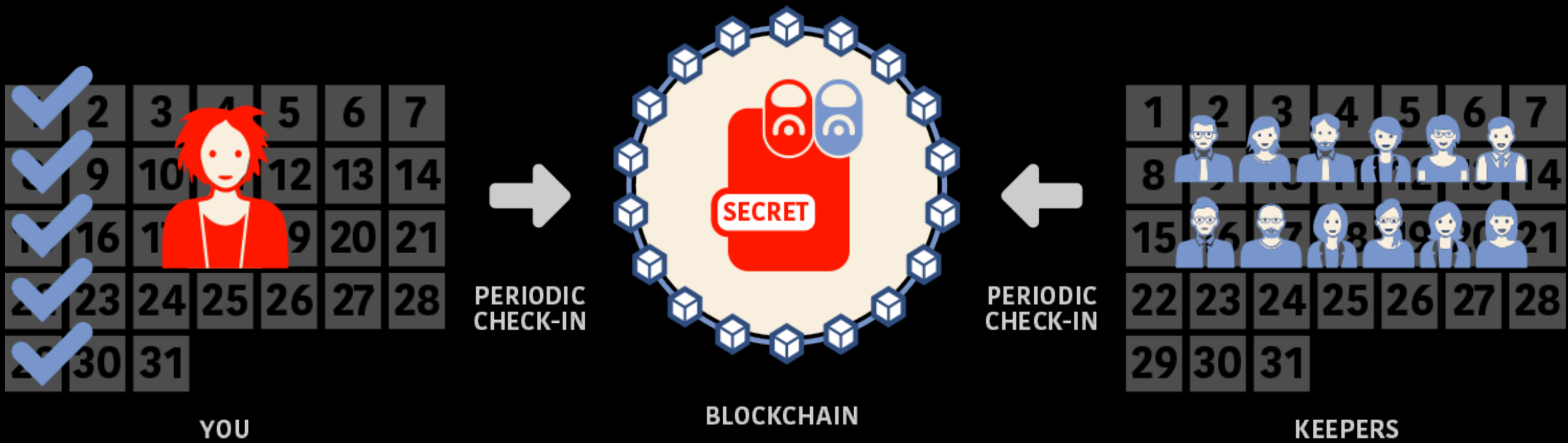
keepers publish secret once you drop out

publication is inevitable and unstoppable

Bitcannery



How it works



How it works

1	2	3	4	5	6	7
8	9	10		12	13	14
15	16	17		19	20	21
22	23	24	25	26	27	28
29	30	31				

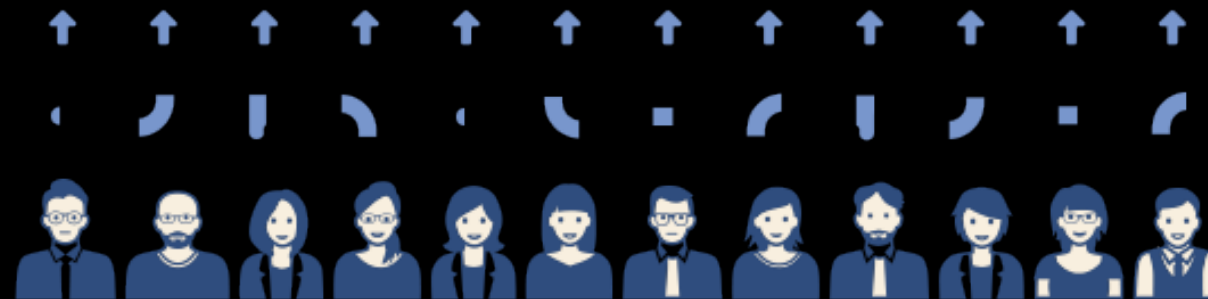


YOU MISSED CHECK-IN



BLOCKCHAIN

SECOND
KEY



KEEPERS

How it works

Opt out from services:

- notaries

- human agents

- centralised password storage

Rely on:

- cryptography

- proper system design

Open source:

- audit the code!

Bitcannery



Your Secrets (3)

[+ Deploy New Secret](#)

SECRETS	STATUS	CHECK-IN DATE	PAYMENT	KEEPERS	ACTIONS
sleepy_goldberg_28 Rinkeby 3 oct 13:47	Check-in missed	— Last check-in	— Check-in cost	3/3 received <div></div>	
jovial_mendel_22 secret	Deploying	— Last check-in	— Check-in cost	—	Continue Deploy
inspiring_chandrasekhar_74 hccp19	Check-in missed	— Last check-in	— Check-in cost	3/3 received <div></div>	

How it looks



Deploy New Secret

You're about to set up a new secret. Secret sharing is powered by the Ethereum blockchain, so you'll need to send two Ethereum transactions in the process.

Secret

Secret is a message you're sharing. It'll be encrypted twice: first time with a public key of the recipient, and the second time with a custom AES key to prevent them from getting the message too early.

Description to remember what it is about (stored locally)

Secret Text

How it looks

Recipient

Recipient's ECC public key

Check-In Interval

Check-in interval, e.g. 1 min, 1 day or 1 month

Keepers

AVERAGE KEEPER PRICE

0.05 ETH (Based On Historical Data)
Per Keeper Per Month

KEEPERS

2



ESTIMATED TOTAL

0.1 ETH
Total Per Month

Request Keepers

How it looks

Get in touch

<https://t.me/bitcannery>

pavel@bitcannery.net

<https://twitter.com/emdin>

References

<https://bitcannery.net>

<https://bitcannery.github.io/bitcannery-dapp/>

<https://github.com/bitcannery>

<https://www.gwern.net/Self-decrypting-files>