Crypto-Currencies and Blockchains Changing Financial Markets

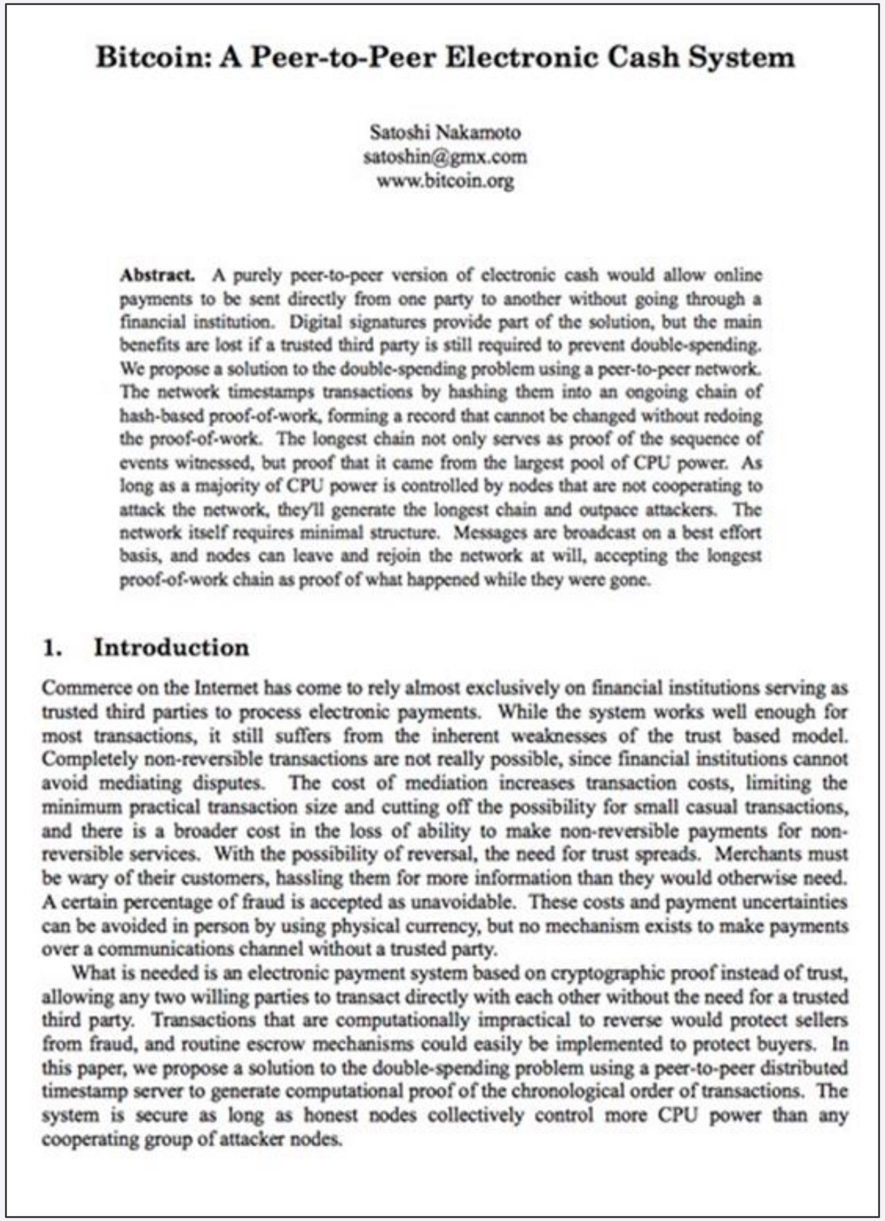
Raghav Chawla

FidelityLabs | FCAT

A Crude History of Money

- Barter
- Precious Metals
- Gold/Silver Coins
- Gold Backed Paper Money
- Fiat Backed Paper Money
- Digitally Recorded Fiat Money
- Digitally Native Money (Bitcoin)

Birth of Bitcoin and Blockchain



Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

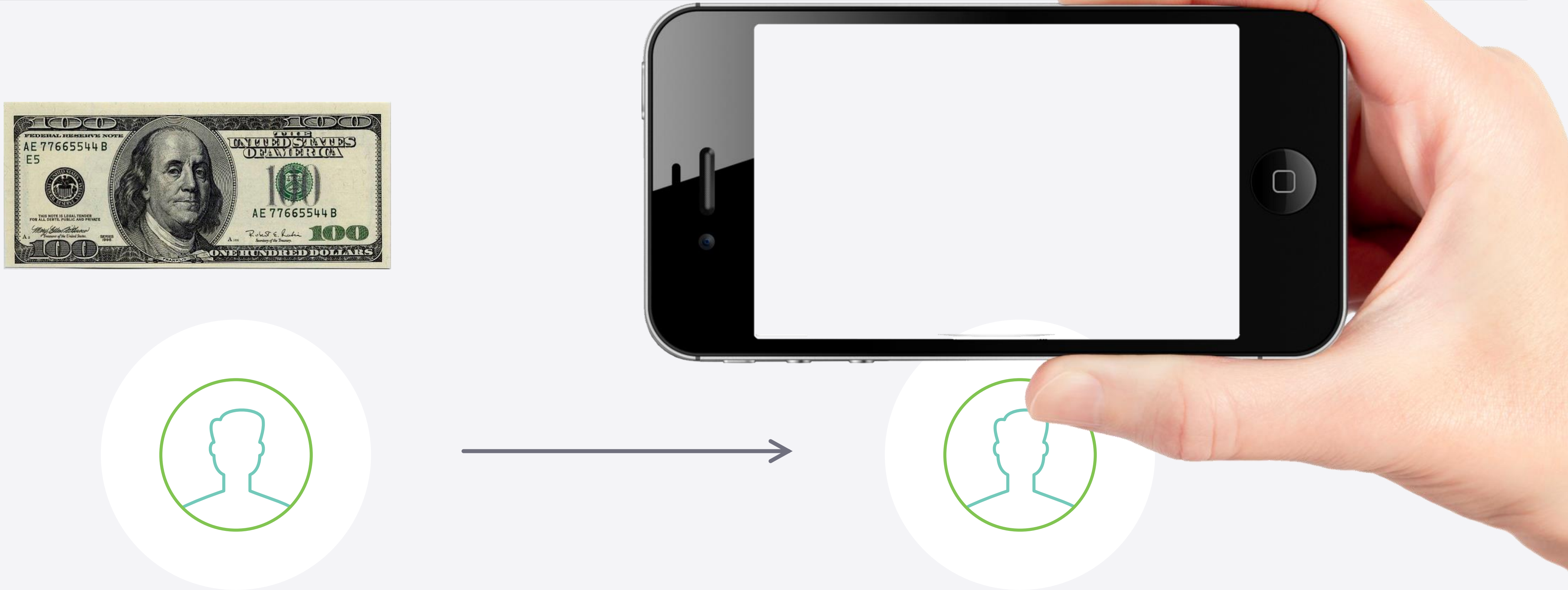
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

1. Introduction

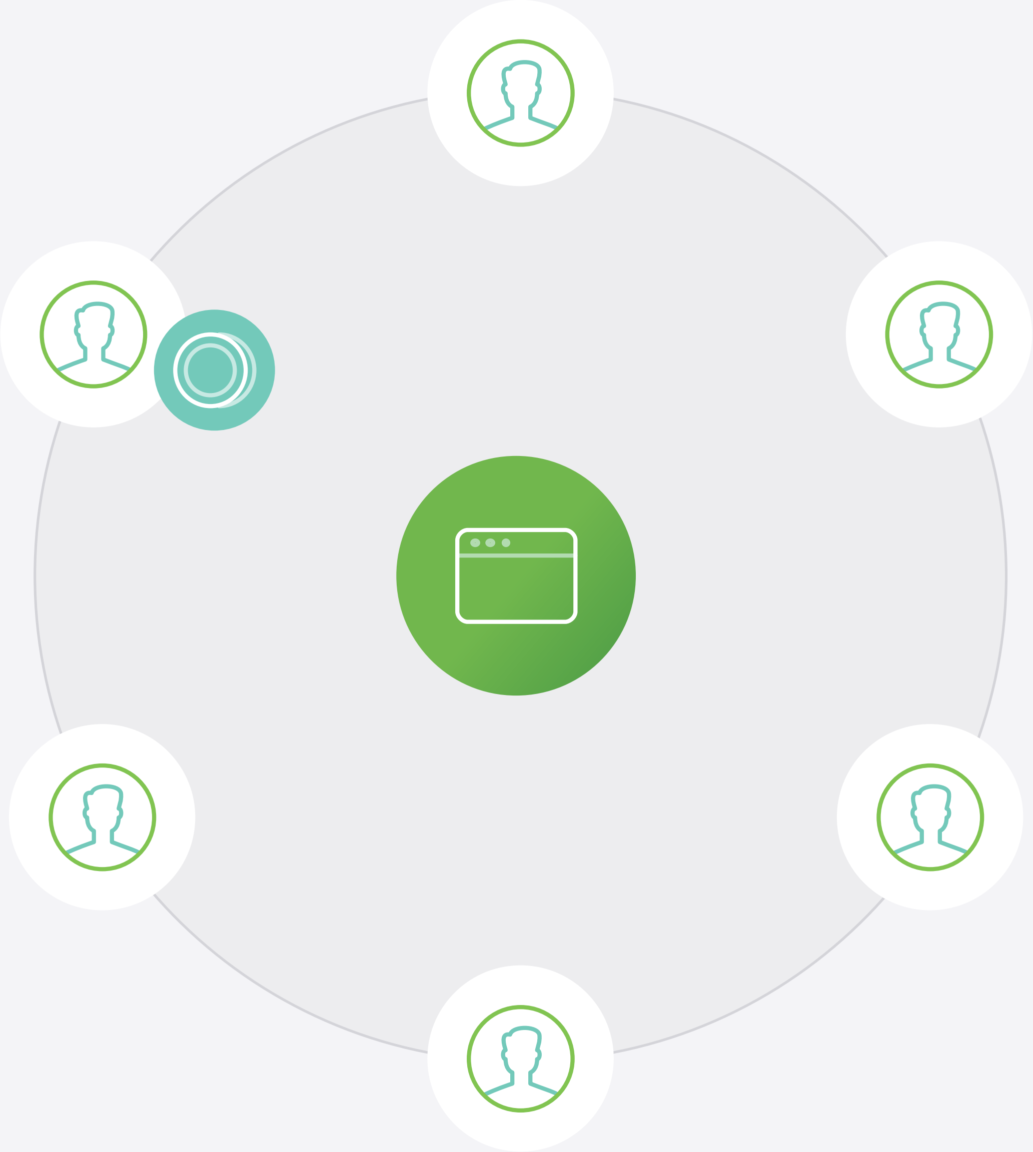
Commerce on the Internet has come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model. Completely non-reversible transactions are not really possible, since financial institutions cannot avoid mediating disputes. The cost of mediation increases transaction costs, limiting the minimum practical transaction size and cutting off the possibility for small casual transactions, and there is a broader cost in the loss of ability to make non-reversible payments for non-reversible services. With the possibility of reversal, the need for trust spreads. Merchants must be wary of their customers, hassling them for more information than they would otherwise need. A certain percentage of fraud is accepted as unavoidable. These costs and payment uncertainties can be avoided in person by using physical currency, but no mechanism exists to make payments over a communications channel without a trusted party.

What is needed is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party. Transactions that are computationally impractical to reverse would protect sellers from fraud, and routine escrow mechanisms could easily be implemented to protect buyers. In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions. The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

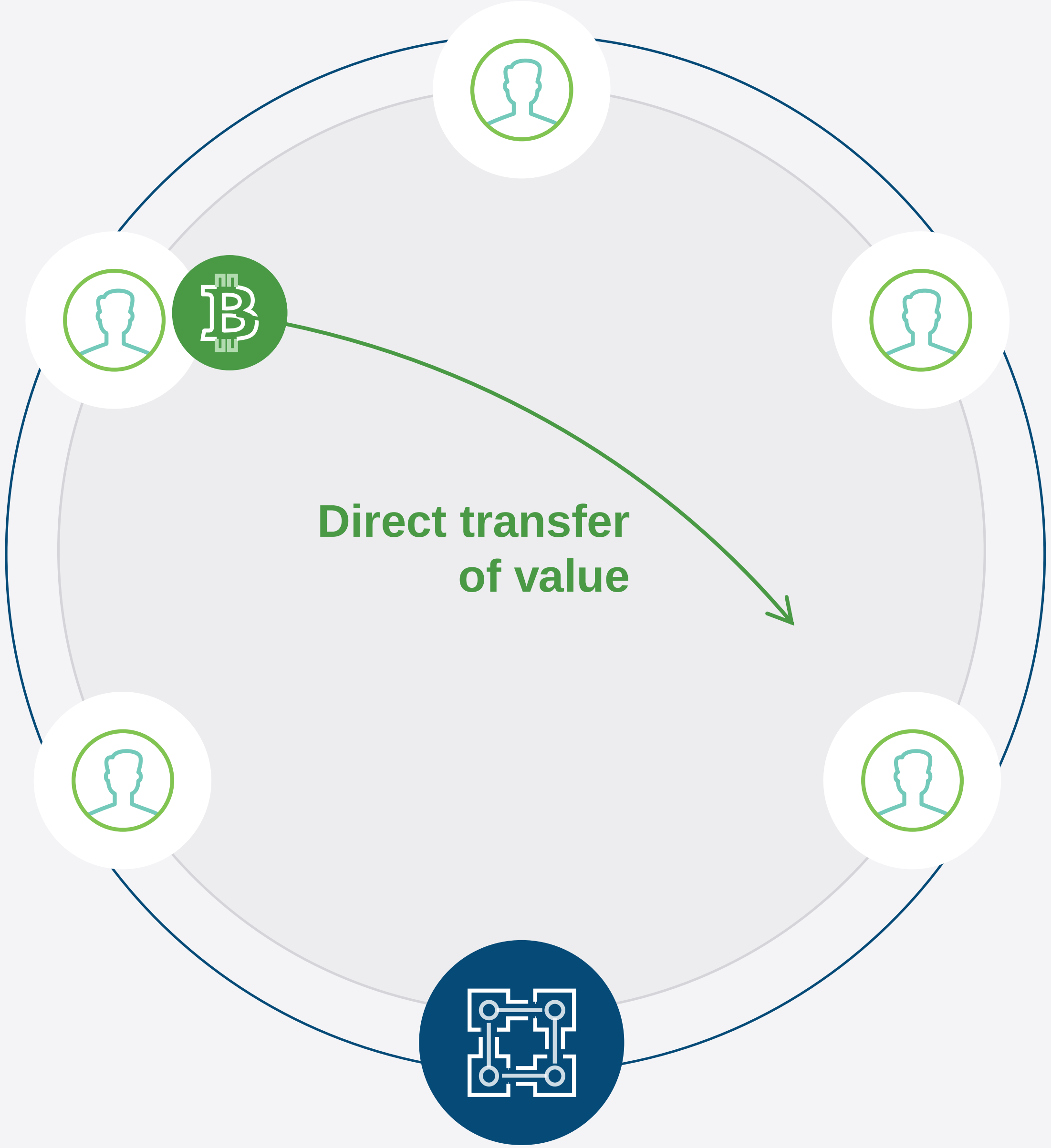
Bitcoin’s Fundamental Breakthrough: Solving for Digital Scarcity



Centralized Solutions to Digital Scarcity

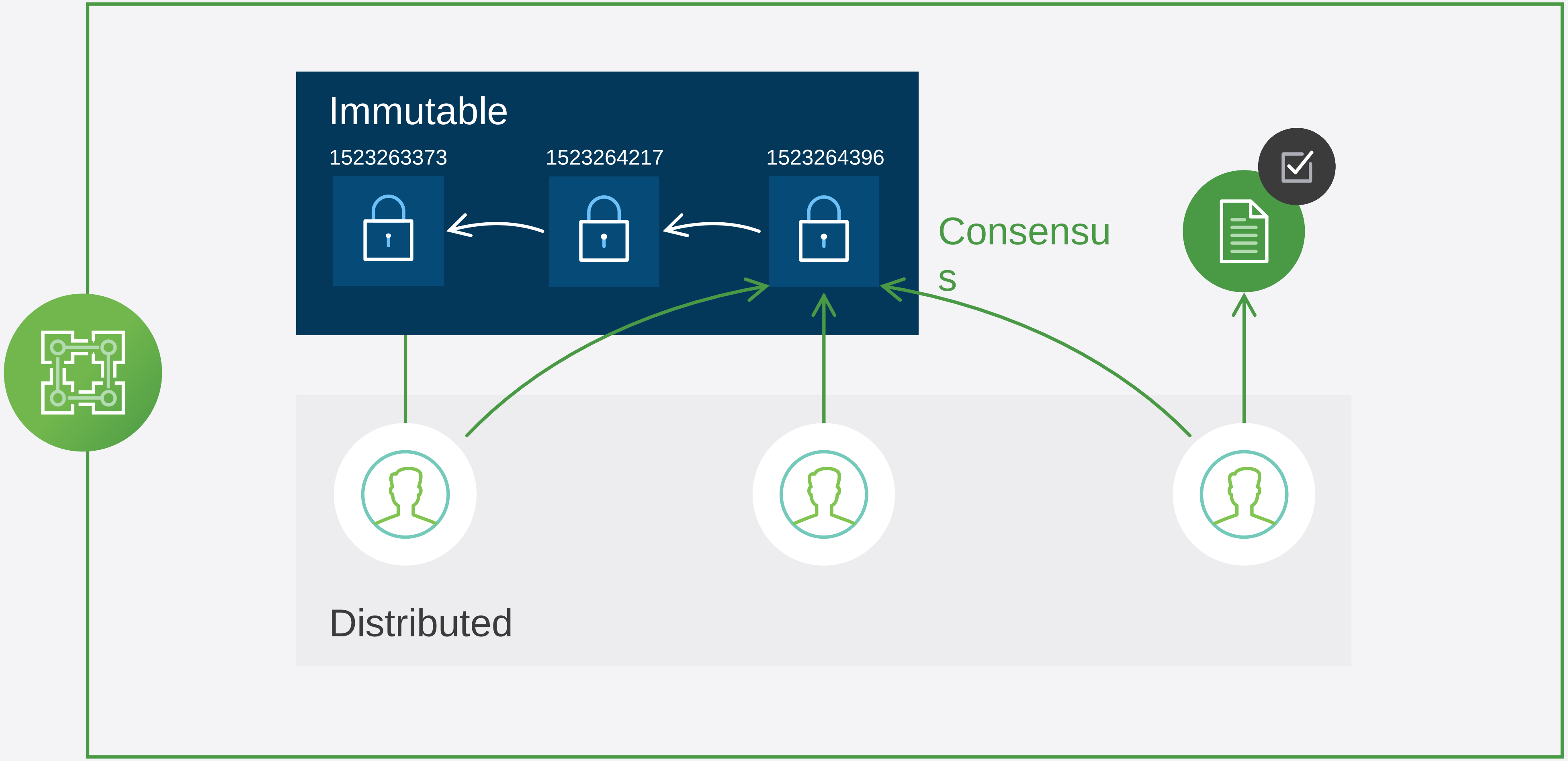


Bitcoin's Fundamental Breakthrough: Solving for Digital Scarcity

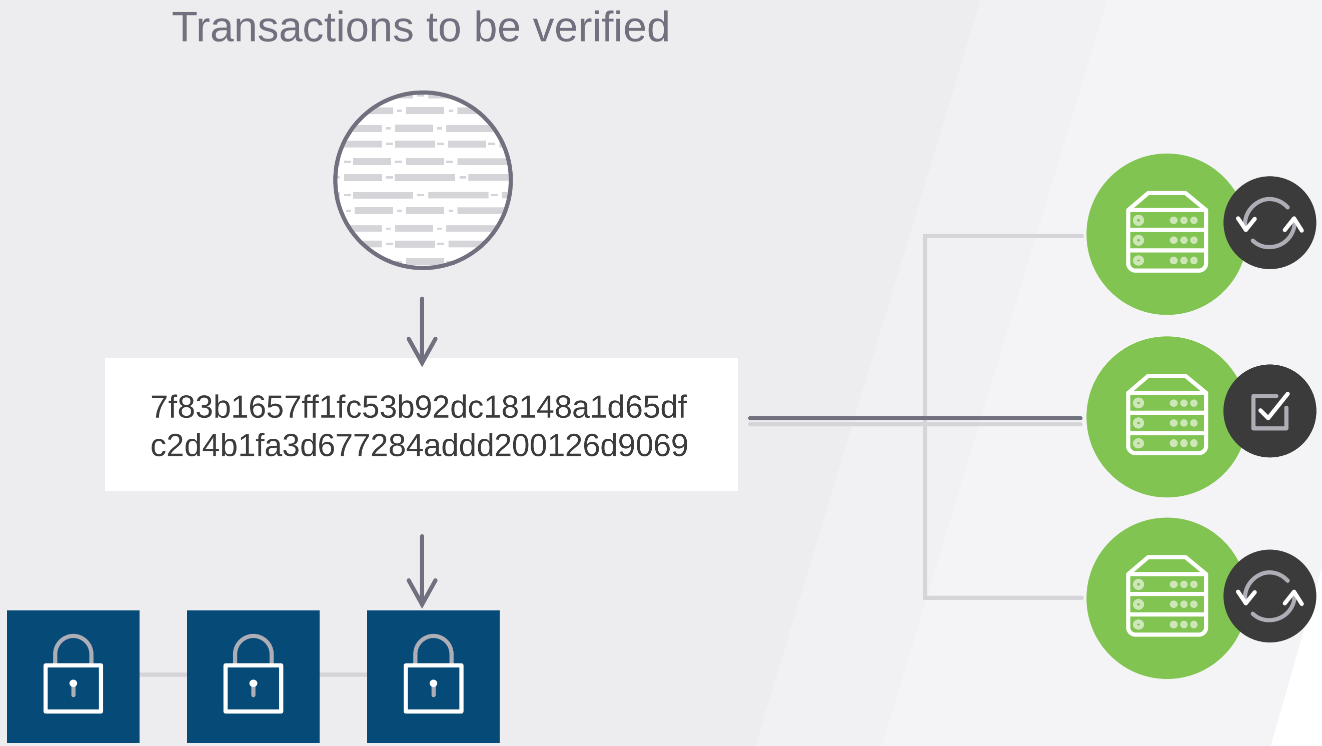


Direct transfer of value

What Is a Blockchain?



Bitcoin Mining



Transactions to be verified

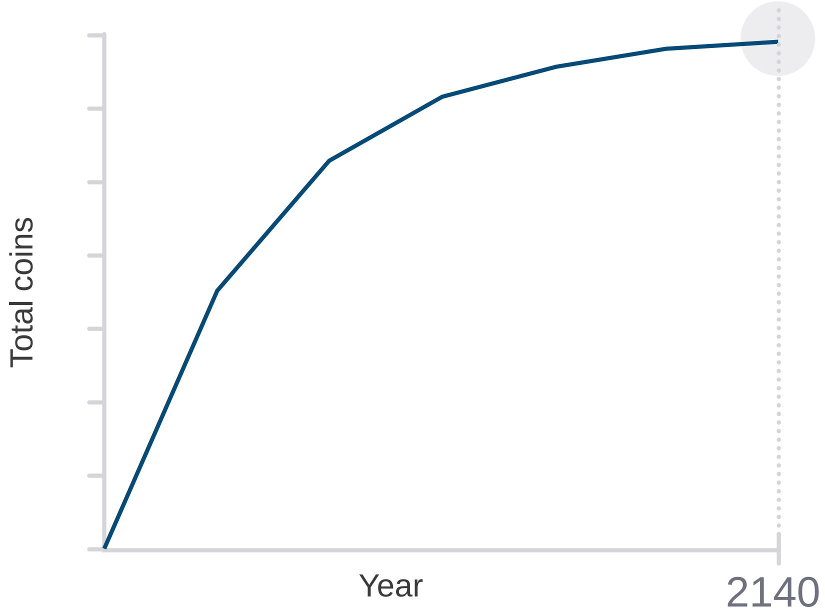
7f83b1657ff1fc53b92dc18148a1d65df
c2d4b1fa3d677284addd200126d9069

A new block is mined every **10 minutes**

The current block reward is **12.5 BTC**

The block reward halves every **4 years**

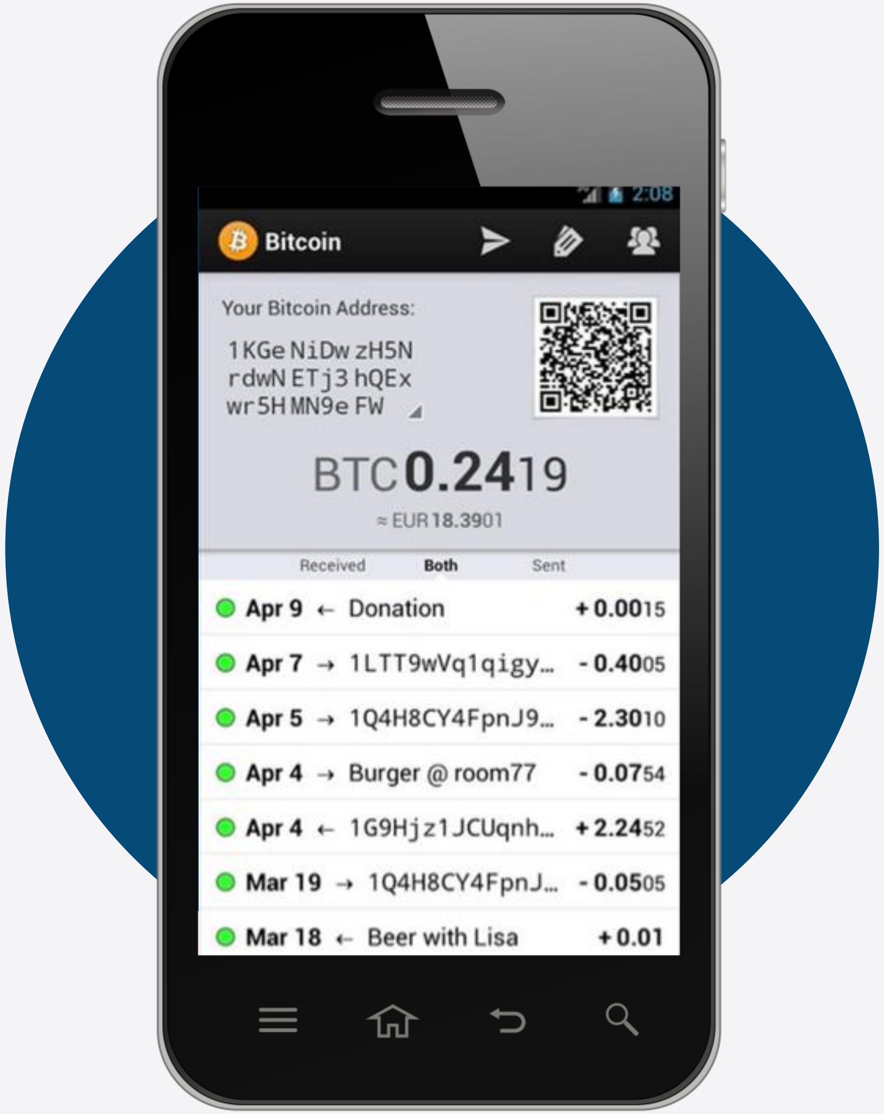
There can only ever be **21 million BTC**



Bitcoin Wallet

Wallet

- Receives bitcoin
- Sends bitcoin
- Monitors your balance
- Keeps track of transactions
- Manages your bitcoin addresses



2:08

Bitcoin

Your Bitcoin Address:

1KGe NiDw zH5N
rdwN ETj3 hQEx
wr5H MN9e FW

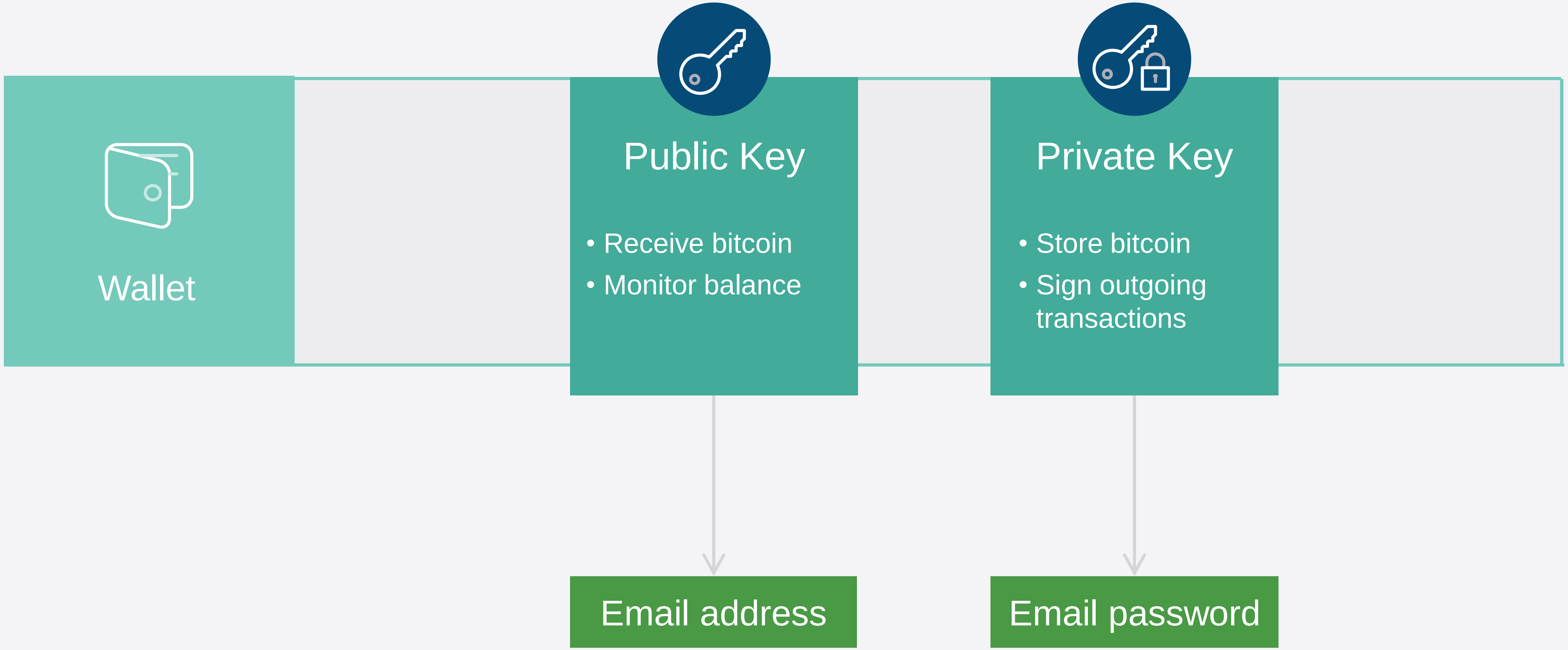
BTC 0.2419

≈ EUR 18.3901

Received Both Sent

Apr 9	←	Donation	+ 0.0015
Apr 7	→	1LTT9wVq1qigy...	- 0.4005
Apr 5	→	1Q4H8CY4FpnJ9...	- 2.3010
Apr 4	→	Burger @ room77	- 0.0754
Apr 4	←	1G9Hjz1JCUqnh...	+ 2.2452
Mar 19	→	1Q4H8CY4FpnJ...	- 0.0505
Mar 18	←	Beer with Lisa	+ 0.01

Anatomy of a Bitcoin Wallet



Wallet

Public Key

- Receive bitcoin
- Monitor balance

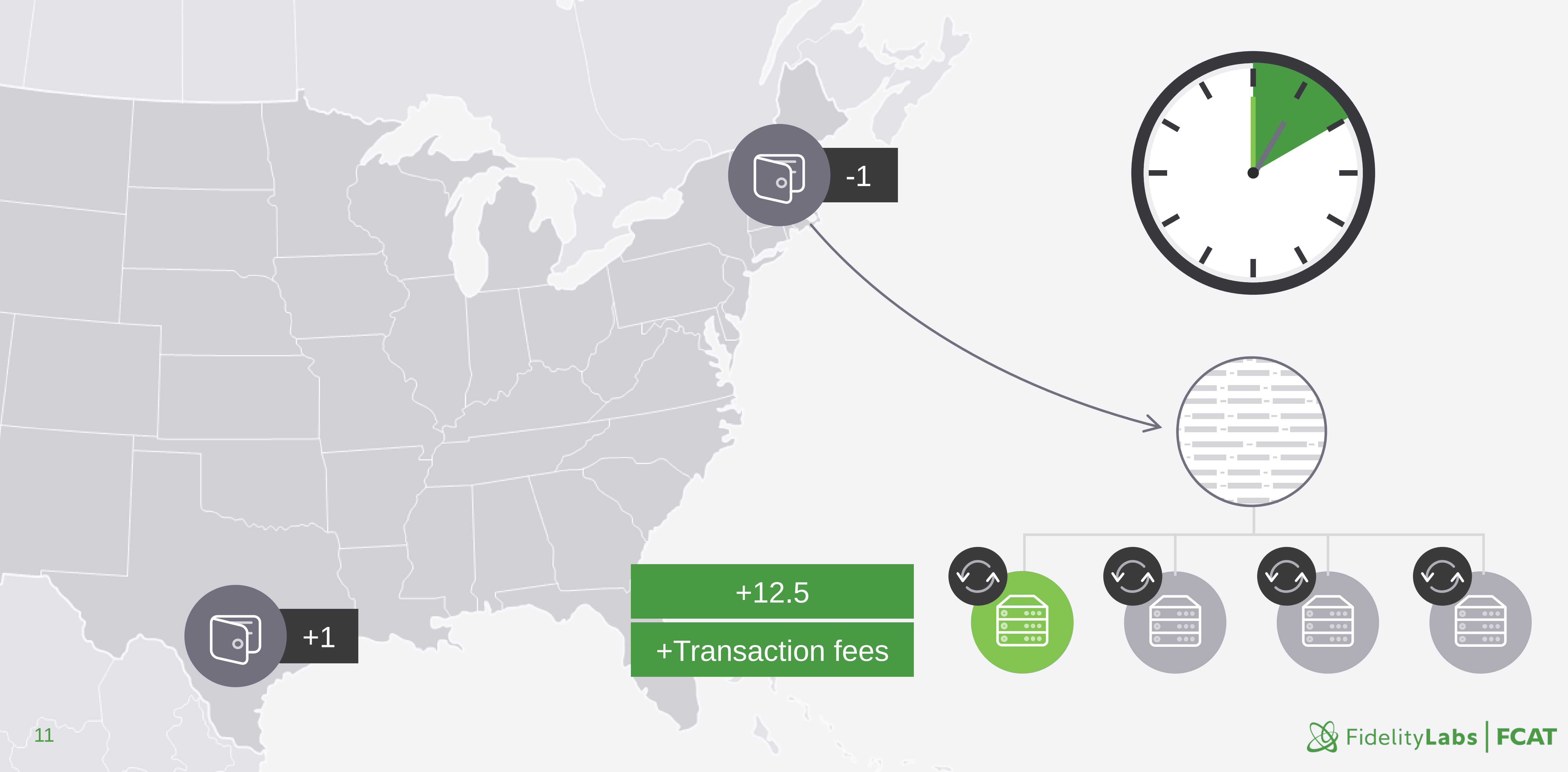
Private Key

- Store bitcoin
- Sign outgoing transactions

Email address

Email password

Putting it All Together: A Transaction

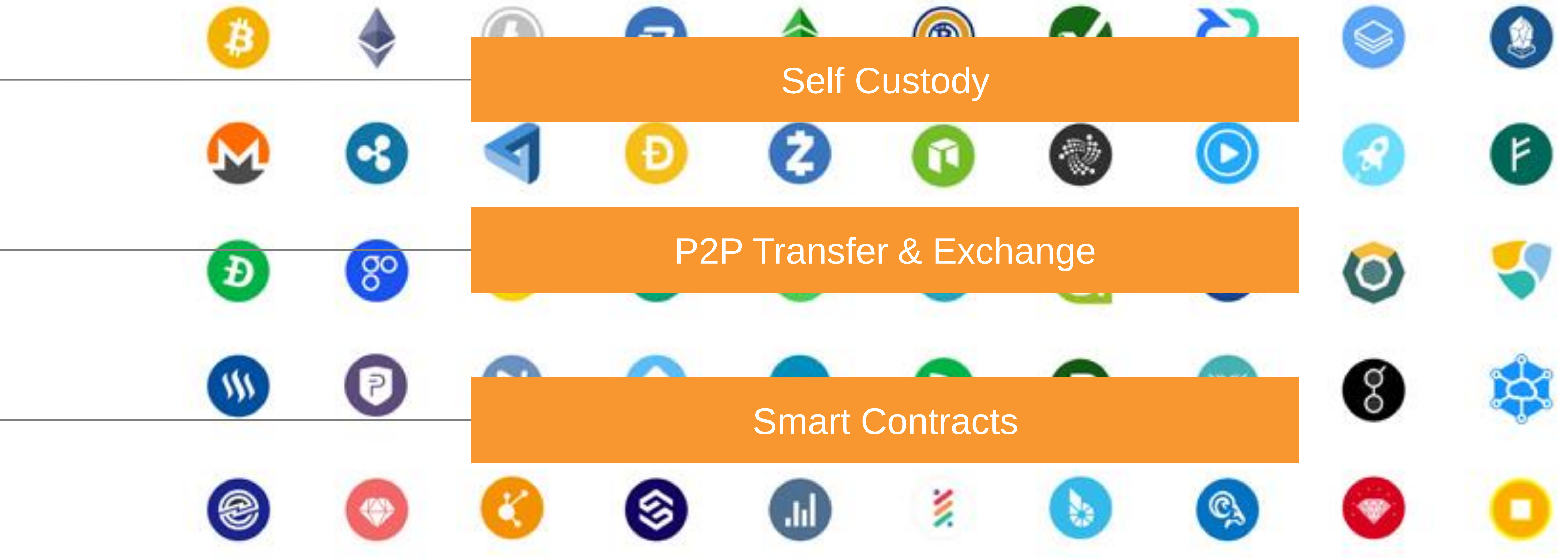


Meets Traditional Criteria of a Currency

	Gold	Fiat	Bitcoin	
Scarcity:	A	F	A+	Only 21m will ever be created
Verifiability:	B	B	A+	Cannot be counterfeited
Fungibility:	A	B	B	One bitcoin is worth the same as any other
Divisibility:	C	B	A+	Denominated in amounts up to 8 decimal places (0.00000001)

Explosion of Digital Assets

Crypto-Currencies | Utility Tokens | Security Tokens



Self Custody

P2P Transfer & Exchange

Smart Contracts

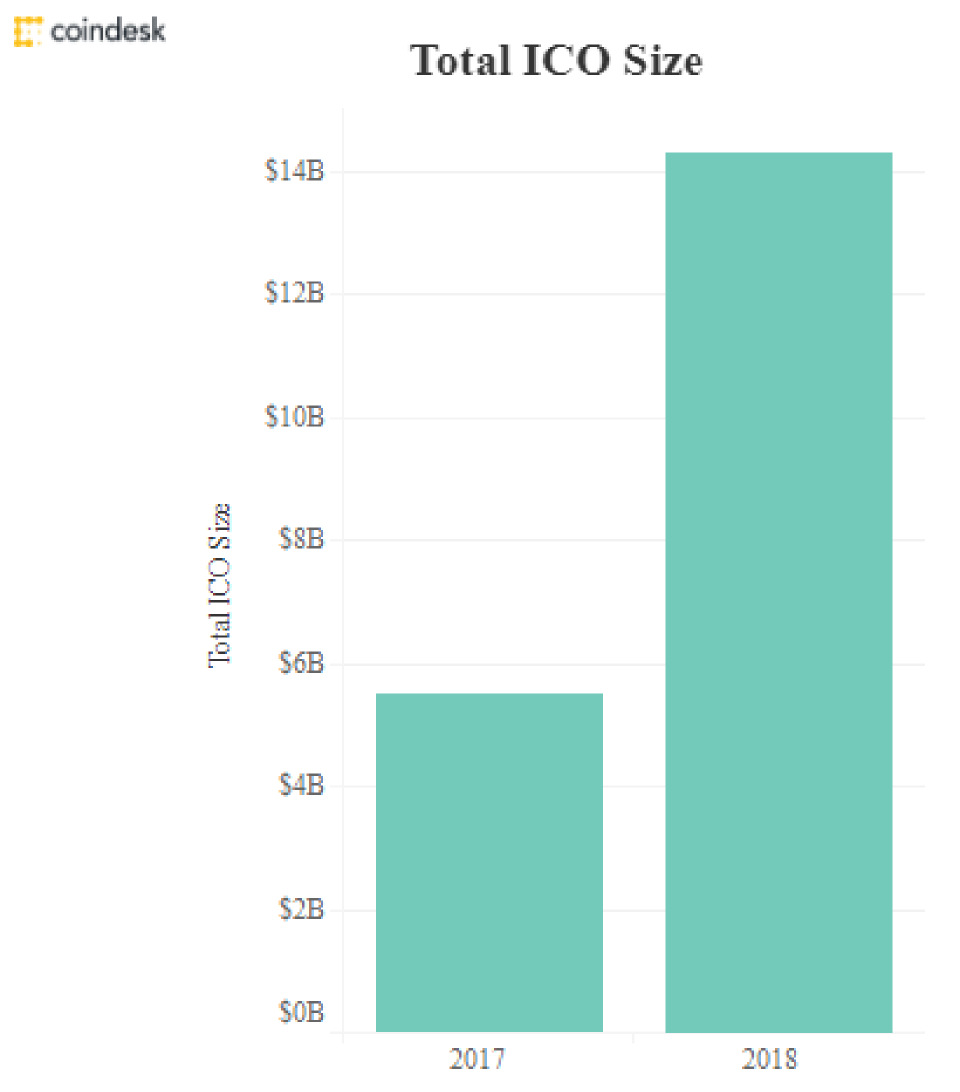
ICO Token

Buy ICO Tokens

1 ETH= 25 ICO tokens

0x6Aa179bfAB9708FE91695a351691e78a48ec007e

Initial Coin Offerings



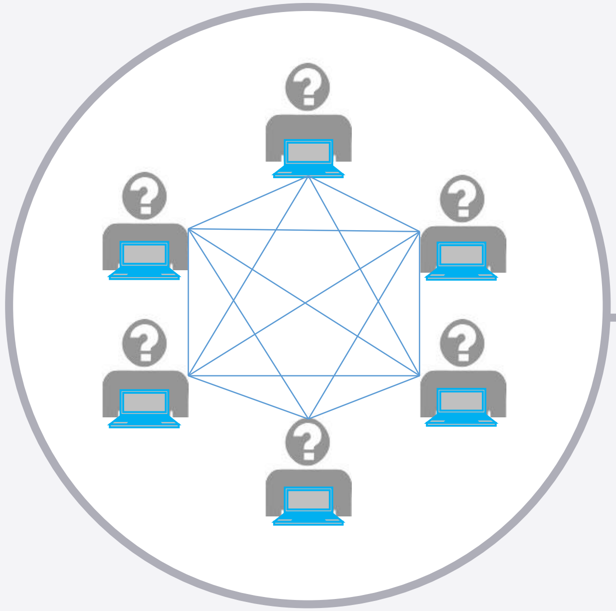
Challenges

Scalability

Privacy

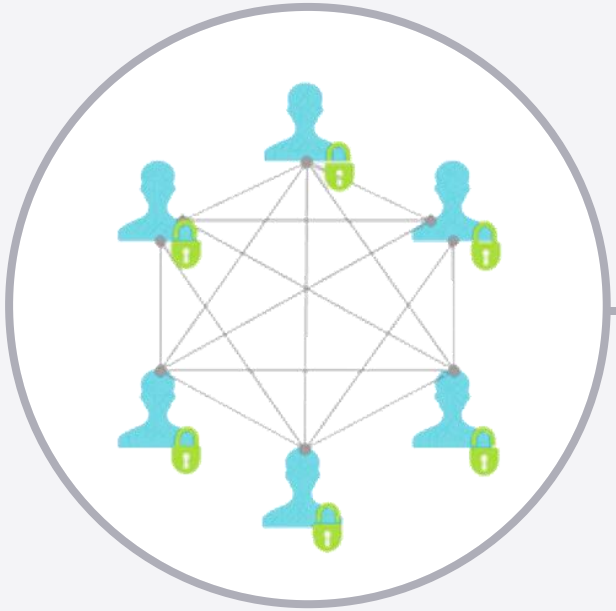
Usability

Regulations



Public Blockchain

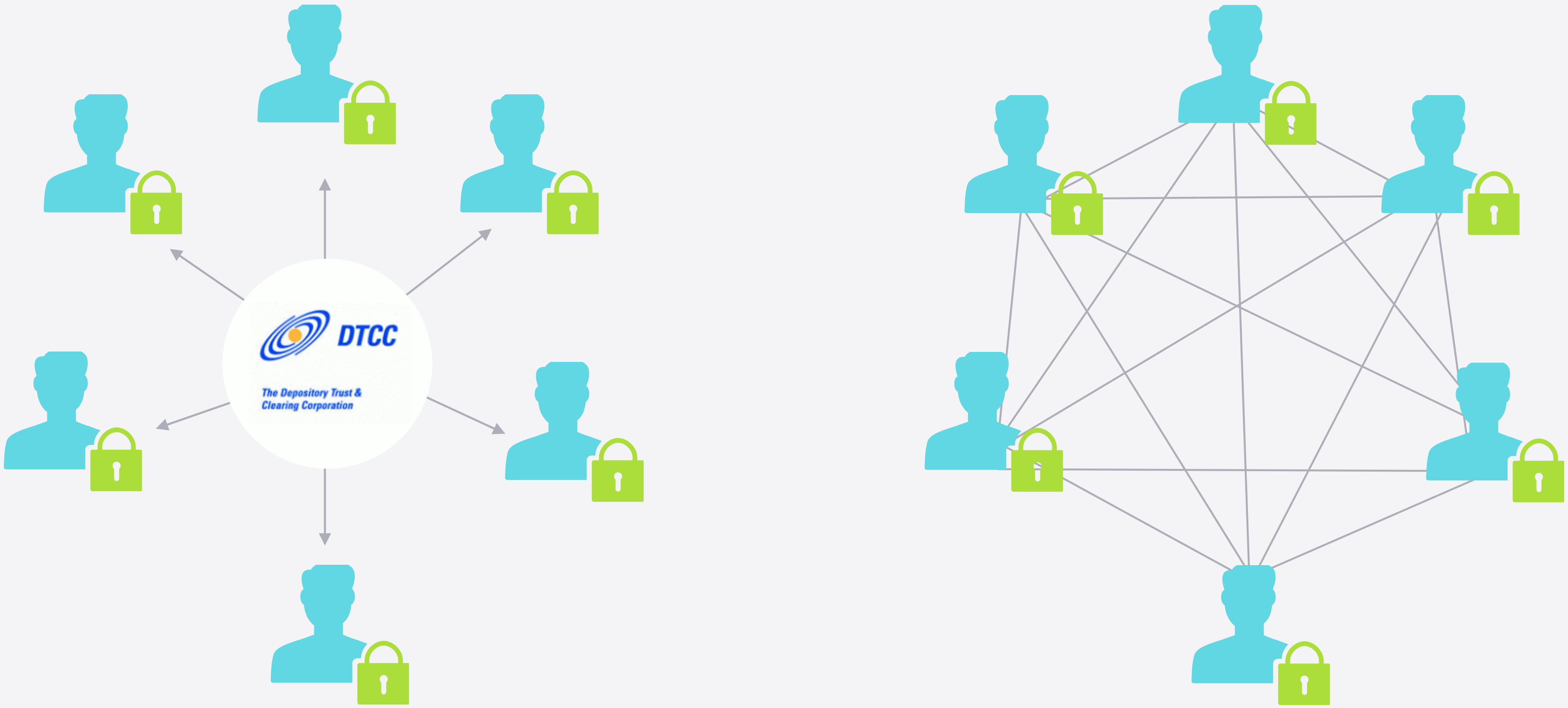
Open, permissionless network that anyone can join, read and write to without the permission of another entity



Private Blockchain

Closed, permissioned network that restricts access to only known, authorized, and trusted participants

Private Blockchain Use Case



Conclusion

- Bitcoin – alternative store of value
- Digital Assets – P2P issuance, custody, transfer, and exchange
- Initial Coin Offerings vs PE, VC and IPOs
- Private/Permissioned blockchains

Thank you!

Let’s stay in touch

raghav.chawla@fmr.com