Cryptocurrencies – what are we really talking about?

7.3.2019

Aalto-yliopisto

Cryptocurrencies are virtual currencies that use encryption techniques to achieve decentralized bookkeeping

1. Bitcoin the software
2. Bitcoin the asset
3. Bitcoin the phenomenon

1. Bitcoin the software
2. Bitcoin the asset
3. Bitcoin the phenomenon

Cypherpunk movement

- Ideological movement that advocates the use of cryptography and other privacy-enhancing technologies as a route to social and political change
- Active since the late 1980s

"Privacy is necessary for an open society in the electronic age. ... We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy ... We must defend our own privacy if we expect to have any. ... Cypherpunks write code. We know that someone has to write software to defend privacy, and ... we're going to write it.“

Eric Hughes (1993), *A Cypherpunk's Manifesto*

Bitcoin: A Peer-to-Peer Electronic Cash System

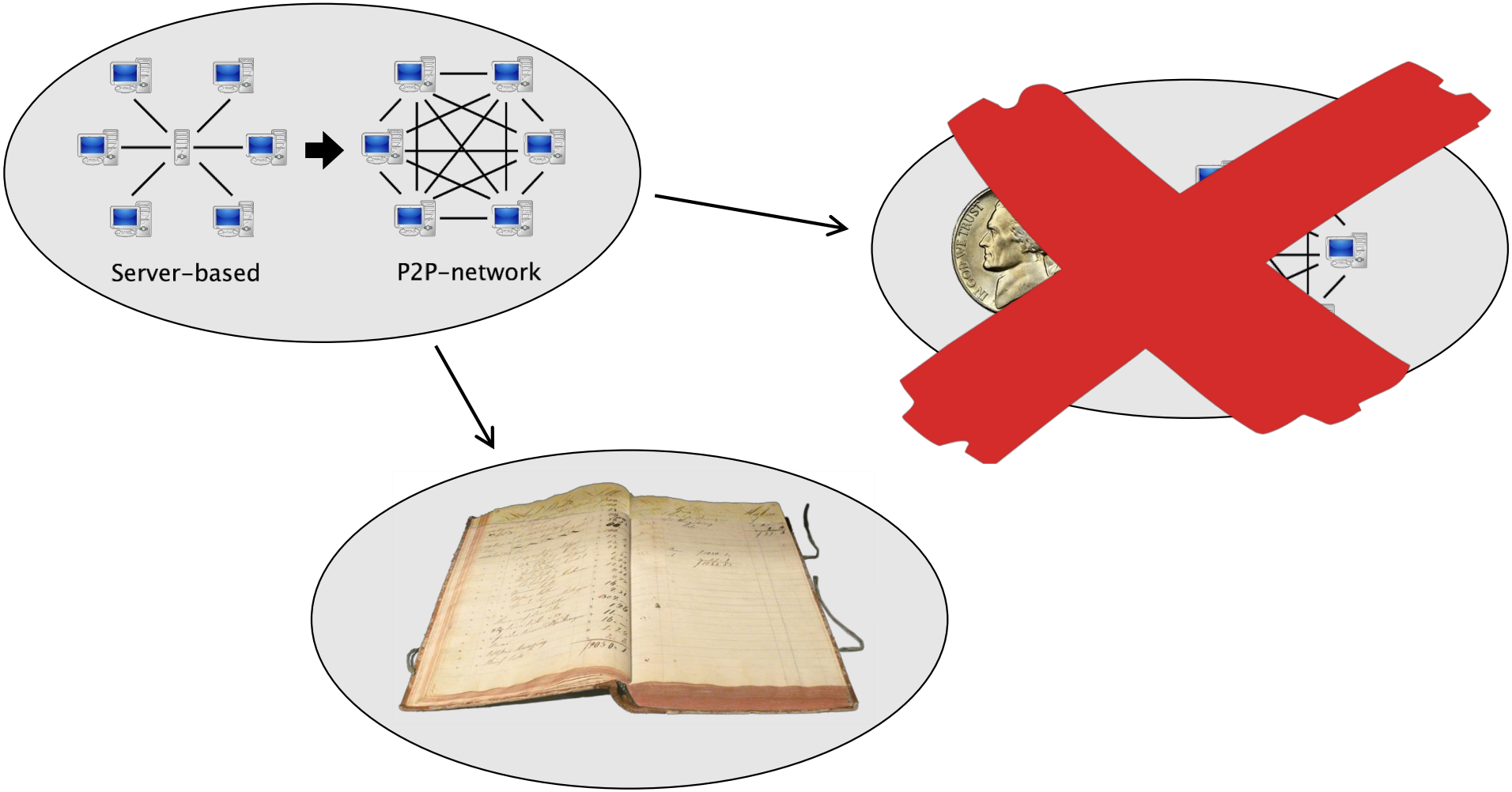
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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

Bitcoin: A Peer-to-Peer Electronic Cash System



P2P network ≠ P2P transaction

Bitcoin's ledger

ACCOUNTS

Account number	Balance
1BvBMSEYstW3	0.023174
1AuF4m4GFg7x	13.990880
1m4GFg7xJ5aN	0.000013
1YstWetSqTF4m	4.290005

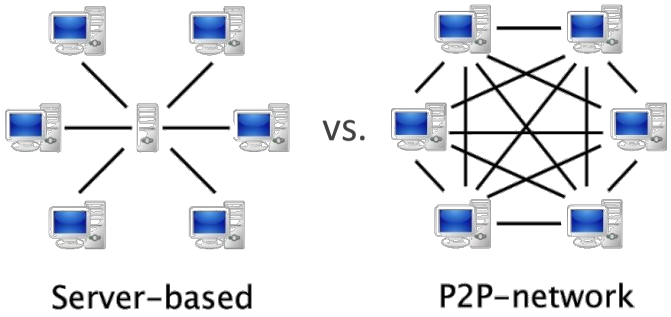
TRANSACTIONS

Sender	Recipient	Amount
1BvBMSEYstW3	1m4GFg7xJ5aN	0.000550
1AuF4m4GFg7x	1m4GFg7xJ5aN	1.000000
1m4GFg7xJ5aN	1YstWetSqTF4m	0.252505
1AuF4m4GFg7x	1YstWetSqTF4m	0.000108

How is this different from a traditional ledger?

Its basic idea is no different, but it is

- Decentralised (P2P network)
- Censorship resistant
- Slow and expensive to operate



Bitcoin's ledger

ACCOUNTS

Account number	Balance
1BvBMSEYstW3	0.023174
1AuF4m4GFg7x	13.990880
1m4GFg7xJ5aN	0.000013
1YstWetSqTF4m	4.290005

TRANSACTIONS

Sender	Recipient	Amount
1BvBMSEYstW3	1m4GFg7xJ5aN	0.000550
1AuF4m4GFg7x	1m4GFg7xJ5aN	1.000000
1m4GFg7xJ5aN	1YstWetSqTF4m	0.252505
1AuF4m4GFg7x	1YstWetSqTF4m	0.000108

Key question:

WHAT IS THE LEDGER KEEPING ACCOUNT OF?

1. Bitcoin the software
2. Bitcoin the asset
3. Bitcoin the phenomenon

What is Bitcoin's ledger keeping account of?

- Initially, the ledger was keeping account of nothing but arbitrary numbers (mining rewards)
- Over time, a secondary market developed
  - Exchanges
  - Over-the-counter trade
- As long as the secondary market is working, Bitcoin is a sort of asset
- Is Bitcoin like gold (or any other commodity)?
  - Bitcoin is like gold in the sense that it's an asset which is nobody's liability
  - Bitcoin is like gold in the sense that it yields no return
  - Bitcoin is not like gold in the sense that it has no industrial use as a raw material
  - Bitcoin is not like gold in the sense that it is not real (it is virtual)
  - According to Klein & Pham-Thu & Walther (2018) Bitcoin, as an asset, doesn't behave like gold or any other asset, and it's pro-cyclical

$$\frac{u(u+1)}{0} \sum_{1=1}^{\infty} = \Lambda dN$$

- 2.1×10^{14} shares issued
- issuer unknown
- $0 equity raised
- no voting rights
- no cashflow

Bitcoin as a payment instrument

- Can be used in private transactions
- Can be used on the Tor network (illegal goods, criminal activity)
- Commonly used in ransomware (criminal activity)
- Online merchant acceptance almost non-existent
- Offline merchant acceptance practically non-existent

Is Bitcoin (the unit) money / a currency?

- Money is the most liquid asset
  - Money is that for which everything can be exchanged
  - Money can buy anything
  - Money is legal tender
- Money is a general metric for value
  - Prices, wages, taxes, dividends, budgets, bookkeeping, etc.
- Money is an asset with stable value
  - Money can buy more or less the same goods tomorrow as today
  - The value of money doesn't fluctuate
  - Money has an issuer who promises its convertibility and guarantees its value

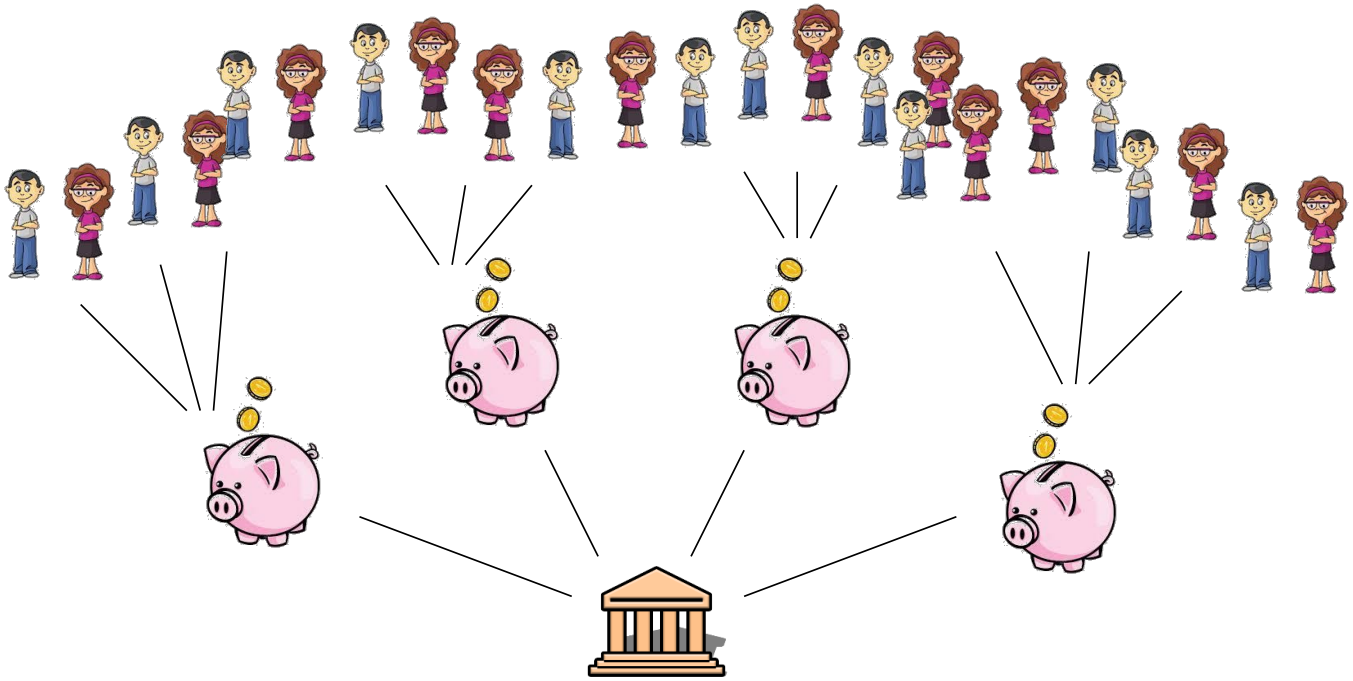
→ **Bitcoin is none of these things**

The modern monetary system

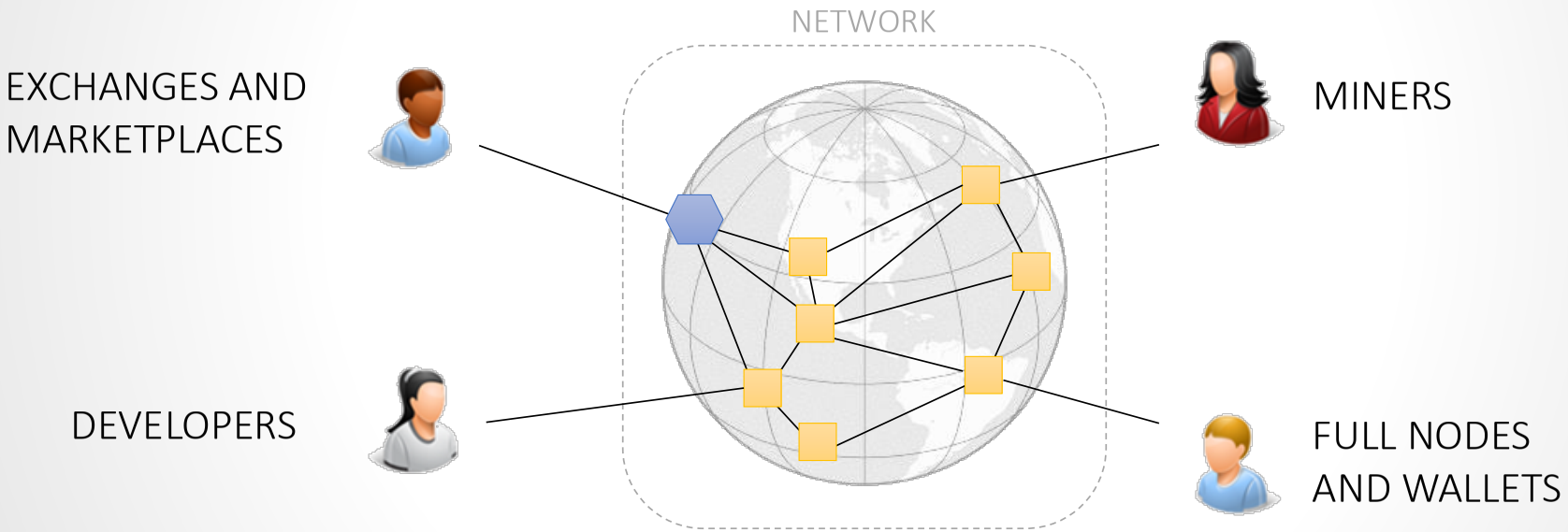
PUBLIC

COMMERCIAL BANKS

CENTRAL BANK



1. Bitcoin the software
2. Bitcoin the asset
3. Bitcoin the phenomenon


NETWORK
EXCHANGES AND MARKETPLACES
DEVELOPERS
MINERS
FULL NODES AND WALLETS

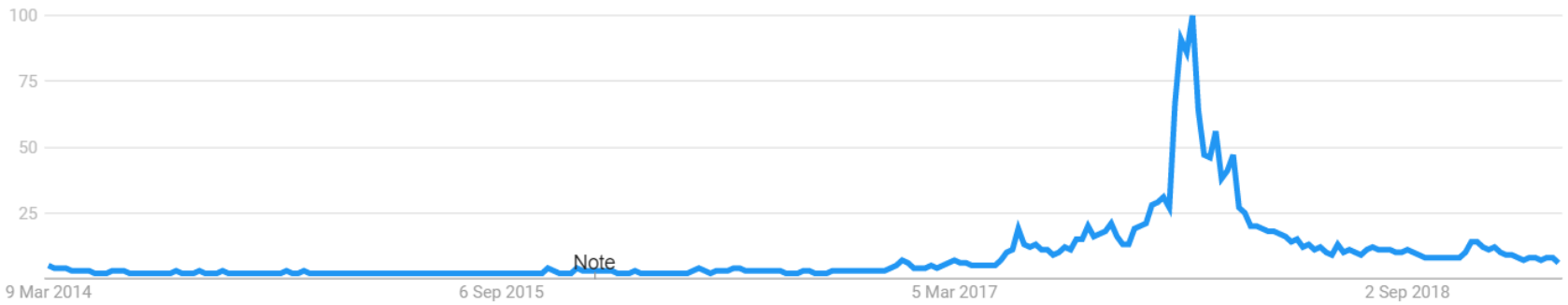
Bitcoin needs more than a ledger to work

1. In a peer-to-peer network, nodes need to be incentivized
   - In BitTorrent, you are incentivized by getting access to content
   - In Bitcoin, you are incentivized by getting mining rewards
2. Bitcoin mining rewards are worth nothing, *unless you can sell them on a secondary market*
3. Why would anyone want to buy (initially worthless) Bitcoin mining rewards?
   - Buyers have been told it gives them privacy
   - Buyers have been told it will become a real-world currency
   - Buyers have been told it's a safe-haven asset
   - Buyers have been told it's cool to own Bitcoin
   - Buyers can use it as a payment method on the Tor network
   - Buyers may be able to sell them later for a profit
4. You need a constant inflow of new buyers, otherwise the market will collapse (every buyer becomes a seller, Bitcoins are never consumed)

4. You need a constant inflow of new buyers, otherwise the market will collapse (every buyer becomes a seller, Bitcoins are never consumed)

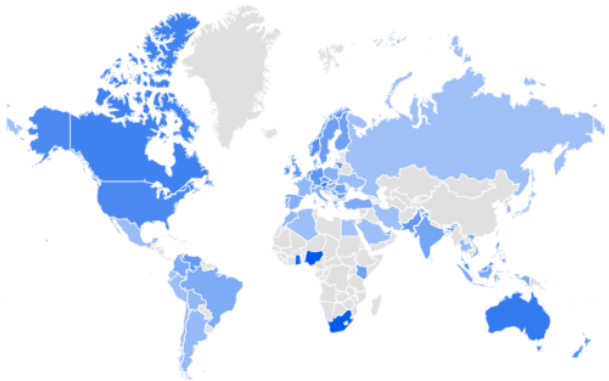

LONDON GRAND EVENT
MONEY MATTERS
BITCOIN
NVESTMENT
KNOWHOW
MADE EASY
COINSMINER
COINS TRADING LIMITED
+447031967430
support@coinsminer.org
Facebook
Viserrys
KIRJAUDU SISÄÄN
REKISTERÖIDY
KOTI
MEISTÄ
LIITTÄÄ
EDUSTAJA
OHJE
UUTISET
TUKI
Finnish
KOLIKOT MINER TRADING LIMITED
INVEST Bitcoin TÄNÄÄN JA Ansaita Voittoa 2 Vuotta
GARANTED
HELPPO
TALLETTAA
INSTANT
PERUUTTAA
ALOITTAA
START YOUR BITCOIN INVESTMENT JOURNEY
INVESTMENT
OFFER
EDIUM
15% HOURLY
6% DAILY
MIN: 5.001 BTC MAX: 50 BTC
PRO
0.21% HOURLY
5.04% DAILY
MIN 50.001 BTC MAX: UNLIMIT
maximum stable Profit
highly qualified financial Experts
friendly customer Service
BITSEA

Interest over time



Interest by region

Region



1	Nigeria	100
2	South Africa	98
3	Ghana	87
4	St Helena	83
5	Slovenia	77

Include low search volume regions

Showing 1–5 of 67 regions

Common misperceptions about Bitcoin

Perception		Reality
Bitcoin is used for payments and more and more merchants and stores accept it	➡	Bitcoin is used almost nowhere for payments, some merchants have tried Bitcoin payments but most have since given up because customers weren't using it
Bitcoin transactions are cheap and quick	➡	Bitcoin is very expensive and inefficient to operate
Bitcoin is a good alternative currency in some poor countries where the domestic currency has crashed (e.g. Venezuela)	➡	Bitcoin requires access to computers or smartphones which most people in poor countries can't afford
Bitcoin is a good investment	➡	Bitcoin yields no return and is therefore entirely speculative
Bitcoin has value because it is scarce	➡	Scarcity sets a lower boundary on market prices but it doesn't make anything valuable
Bitcoin has value because mining Bitcoin consumes energy	➡	The cost of production sets a lower boundary on market prices but it doesn't make anything valuable
Bitcoin represents a new phase in the development of the Internet, the 'Internet of Value'	➡	Bitcoin is just one of many applications using the Internet

There is no such thing as ’Internet of Value’

”Economic value is a measure of the benefit provided by a good or service to an economic agent”

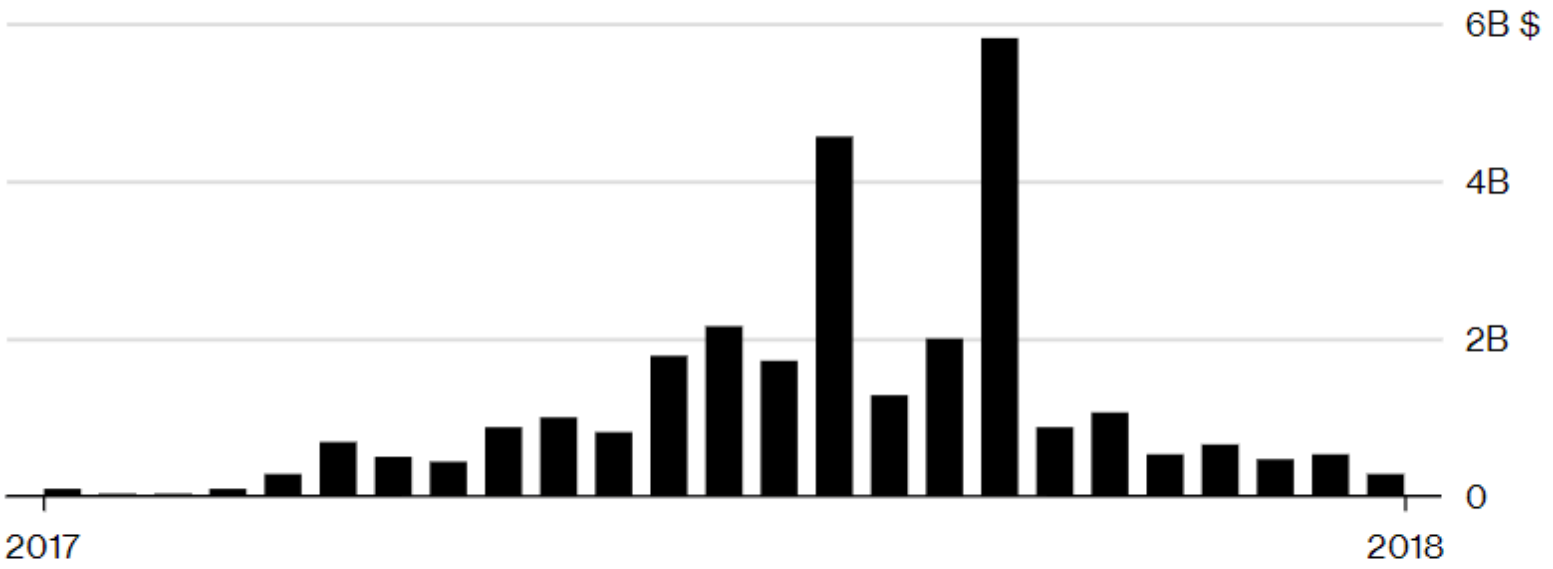
- Wikipedia

Value is not a thing, it’s an attribute!

- There is only one kind of Internet, the Internet of *data*
- The Internet is a *messaging network*, it can only relay messages, nothing else
- Valuable things like money, share certificates, and land deeds are kept in *depositories and managed by custodians* (banks, CSDs, land registries, etc.)
- Depositories and bank accounts *record ownership of assets*
- Assets are not messages and cannot be digitised
- Instructions to transfer ownership are messages and can be digitised
- Messages get sent around, but the assets stay where they are

Funds Raised via ICOs by Month

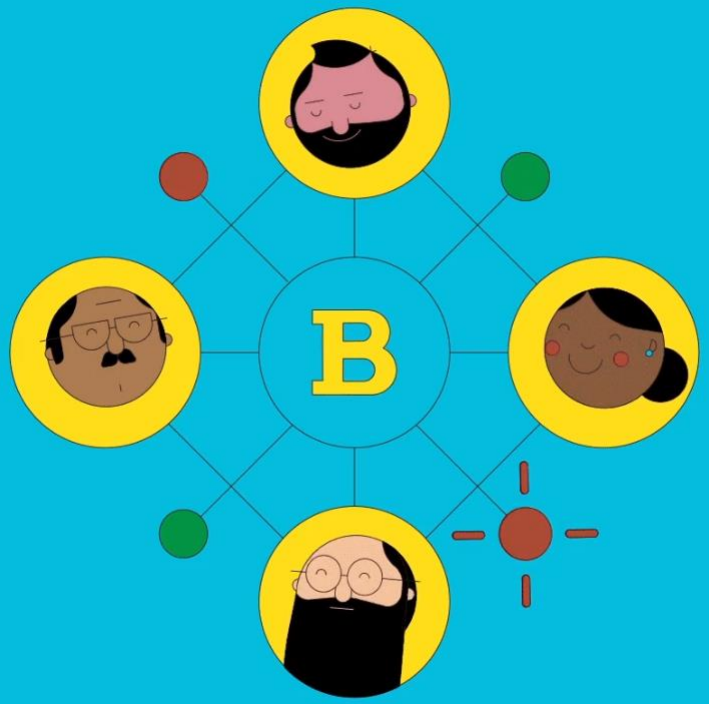
In U.S. dollars



Source: CoinSchedule.com

Despite the blockchain hype—and many experiments—there's still no "killer app" for the technology beyond currency speculation.

WIRED



The only blockchain project that has crossed over into mainstream recognition so far is Bitcoin.

The New York Times

Aleksi Grym
aleksi.grym@bof.fi
 @aleksigrym