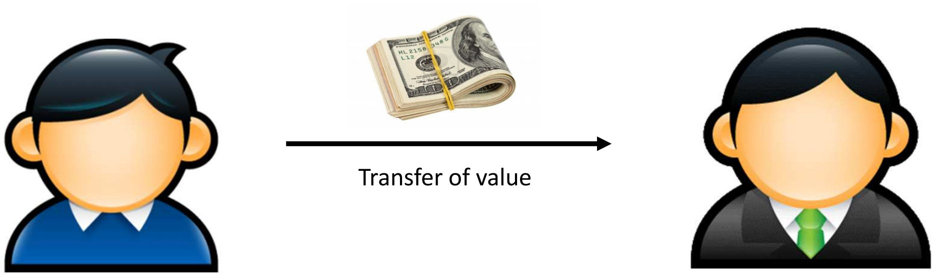
Le Bitcoin et son utilisation par les cybercriminels

Adrien Treccani, Ph.D.

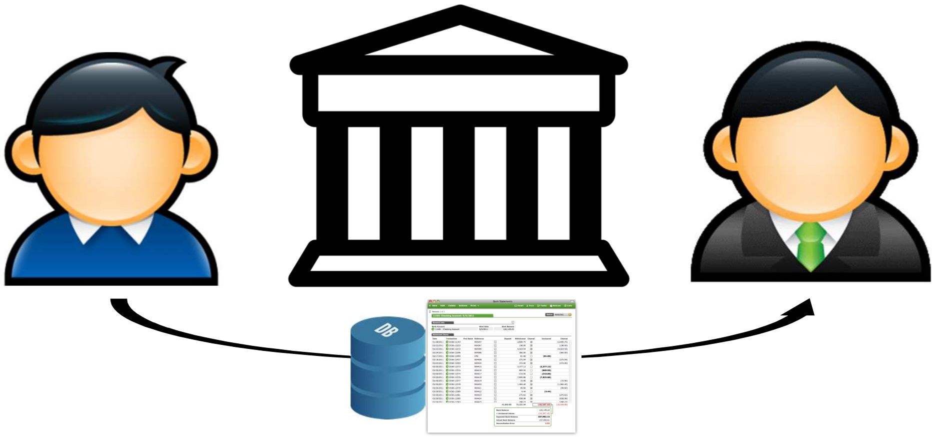
10 novembre 2017

Finance in a nutshell

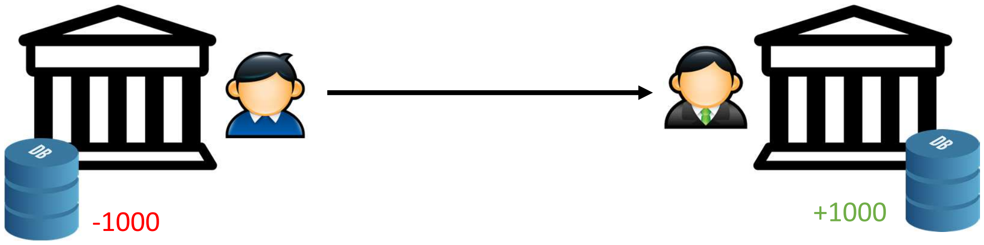


Transfer of value

Electronic transfer (one bank)

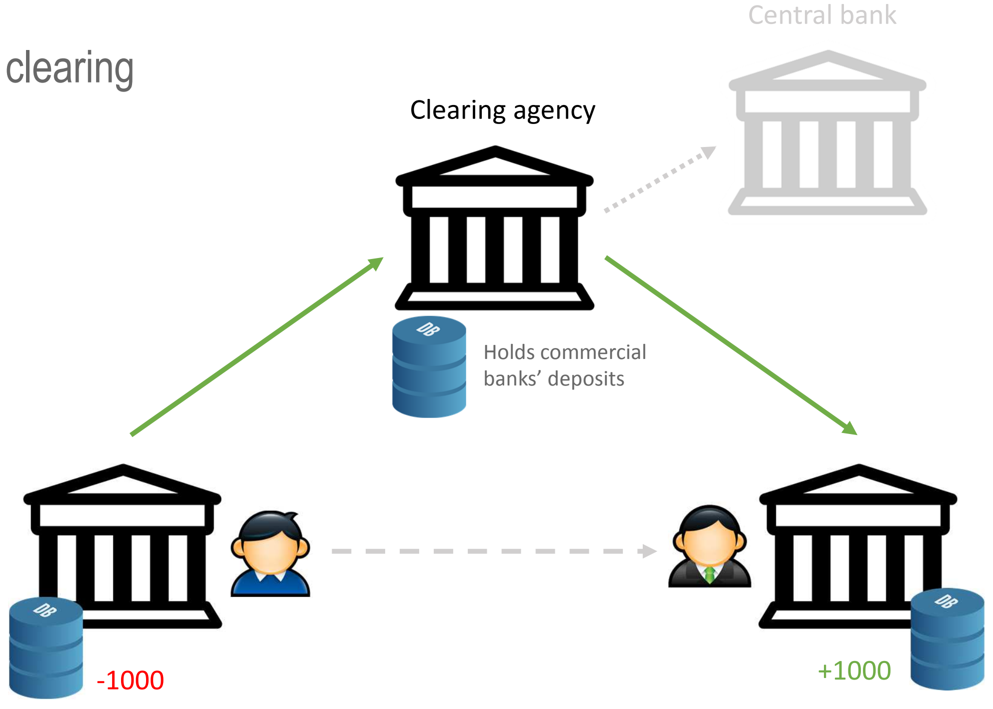


Electronic transfer (two banks)



How to make sure consolidated accounting is correct / no fraud?

Electronic clearing

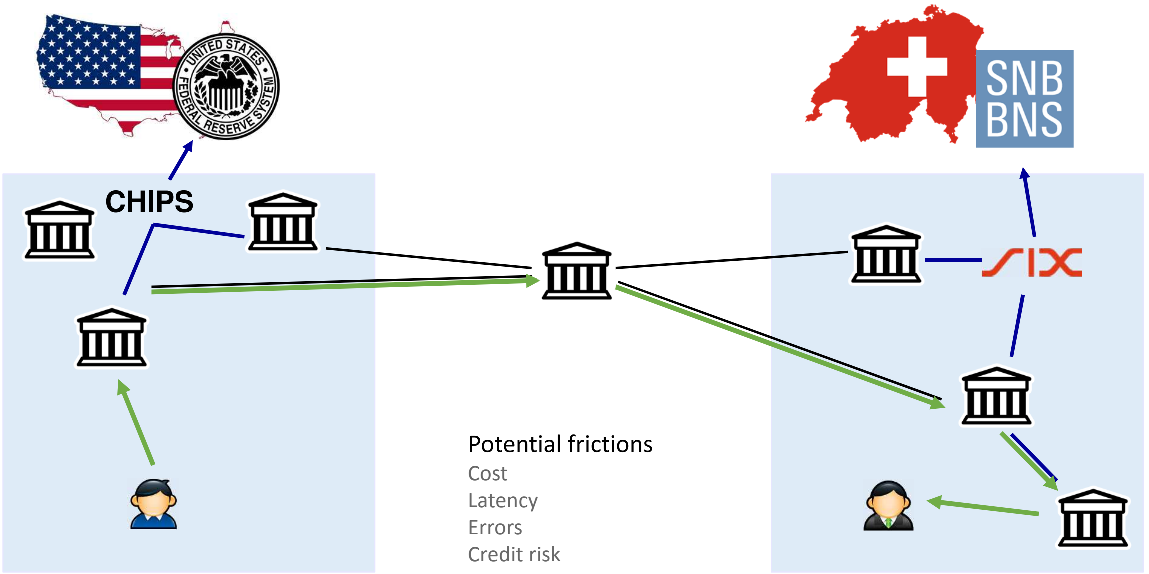


Holds commercial banks' deposits

-1000

+1000

Complex system

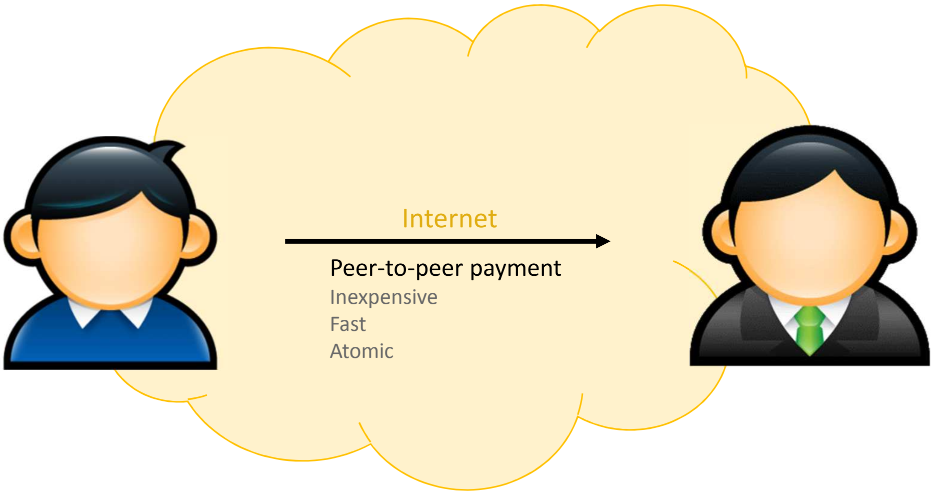


Potential frictions

Cost
Latency
Errors
Credit risk

Blockchain motivation

"Blockchain could reduce banks' infrastructure costs by US$15 – 20 billion per annum by 2022." *Santander Report*



Internet

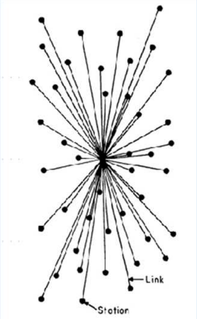
Peer-to-peer payment

Inexpensive
Fast
Atomic

Blockchain motivation (cont'd)

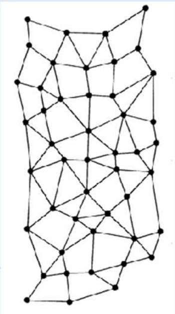
Centralized network

High barrier-to-entry
Pyramidal governance
Oligopolies
Subject to politics



Distributed network

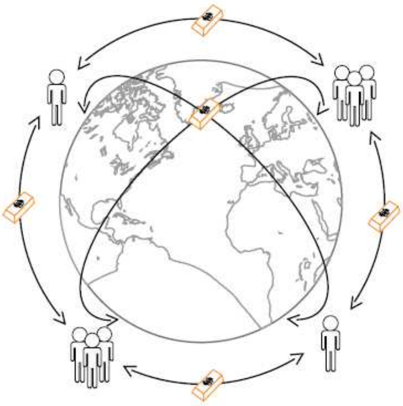
Frictionless entry
Democratic governance
Global access
Algorithmic validation



Bitcoin network

Distributed payment network

Globally available
No central authority (e.g., no bank)
Consensus-based "democracy"



Key numbers

- 20M users
- 4 tx/s
- $250M/day
- ~30 min settlement

Ref: *Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto (2009).*

Use case I: Bankless merchant

Use case II: Remittance

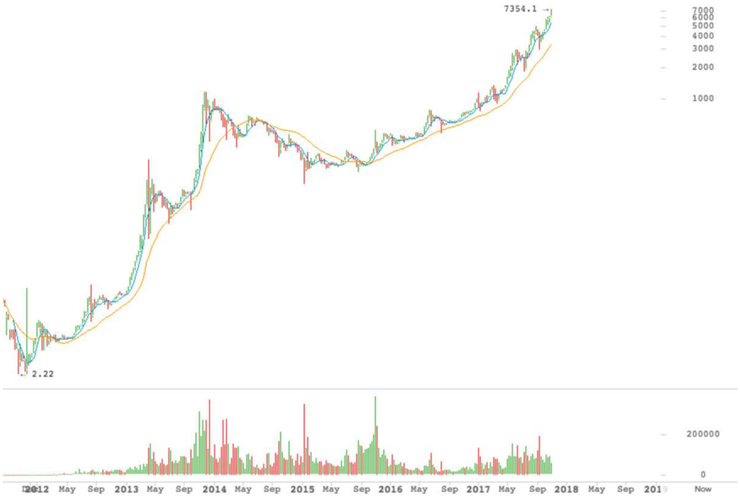
Bitcoin currency

No stabilization policy

Strict 21M cap on bitcoin supply
Deflationary monetary policy

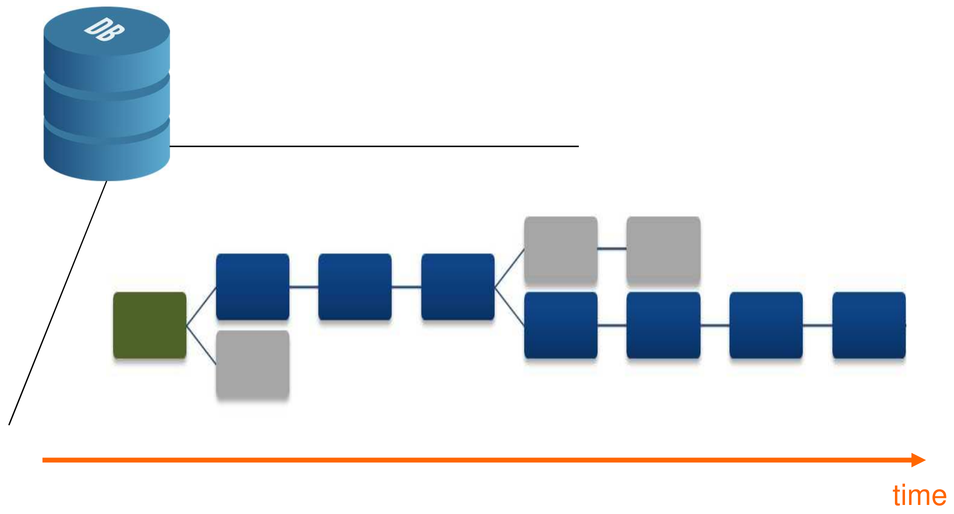
Key numbers

- $100.0B+ market cap
- $7000 ATH price
- 150K merchants



Ref: *Bitcoin: A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto (2009).*

Blockchain *trust machine*



Blockchain storage

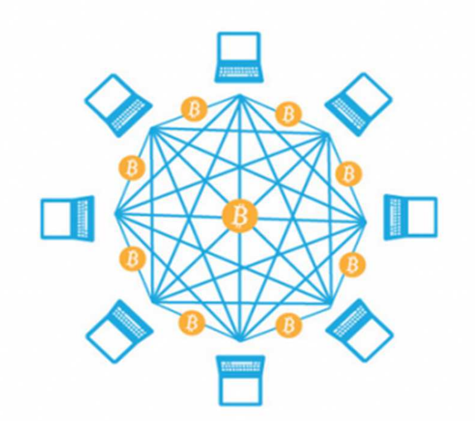
Distributed persistence

Users maintain full copy of the blockchain

- Entire history of transactions
- High redundancy
- Peer-to-peer, public network

Key numbers

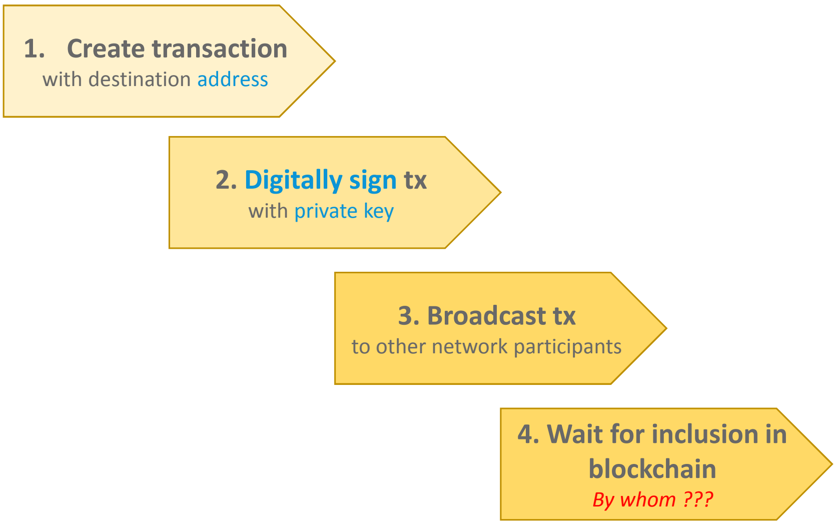
- 5000+ copies
- 140Gb of data
- 280M txs



One-slide cryptography fast-track

	Traditional finance	Bitcoin ecosystem
Account ID *receive payments*	**IBAN number** *GB87BARC20658244971655*	**Address** *1BvBMSEYstWetqTFn5Au4m4…*
Credentials *spend money*	**Card + PIN code + nice smile** *Use your secret PIN and smile to your banker*	**Private key** *5Kb8kLf9zgWQnogidDA76MzPL6T…*
Ownership *prove ownership*	**Bank statement** *Ask your banker for a bank statement*	**Digital signature** *Use private key to prove ownership of address*

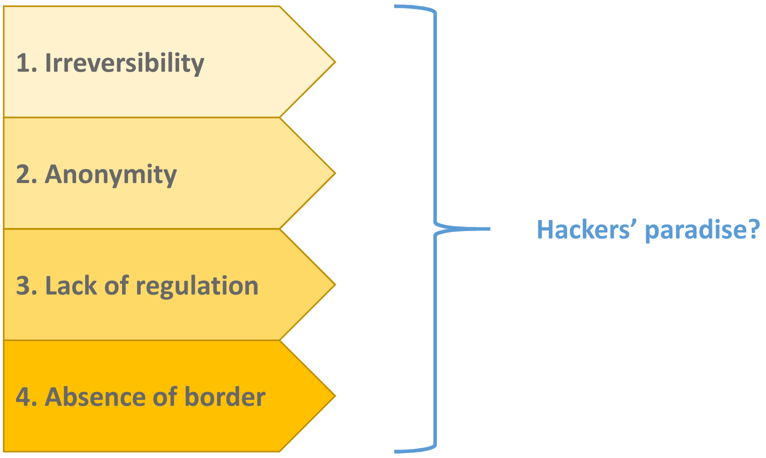
Payment processing



1. **Create transaction** with destination address
2. **Digitally sign tx** with private key
3. **Broadcast tx** to other network participants
4. **Wait for inclusion in blockchain** *By whom ???*

Miners

Hackers’ paradise?



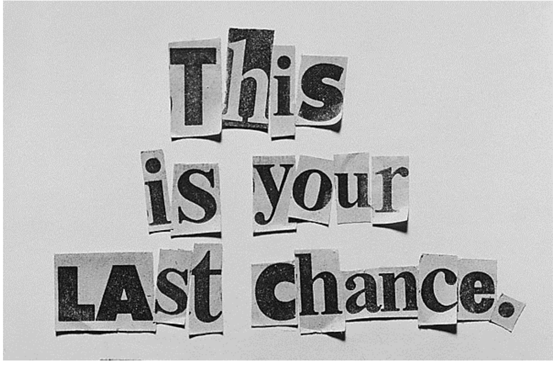
1. Irreversibility
2. Anonymity
3. Lack of regulation
4. Absence of border

Hackers’ paradise?

Two main attack vectors

Theft : attacker takes the money

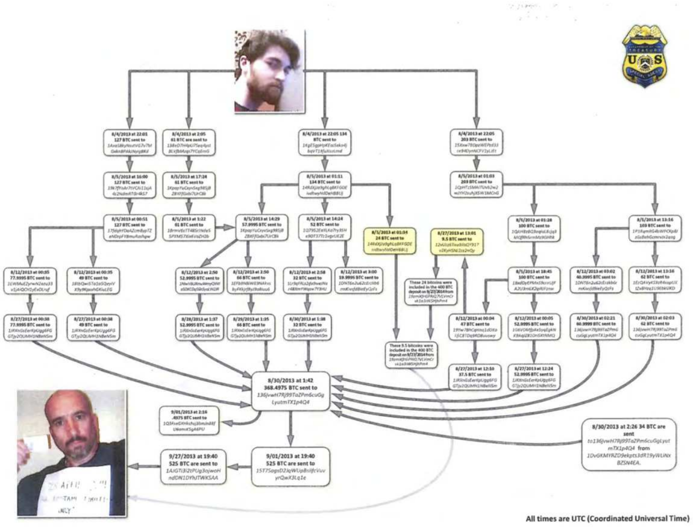
Ransom : attacker kindly asks for the money



Estimation: 1.5m bitcoins stolen *at least once*

Estimation: 40% of businesses affected

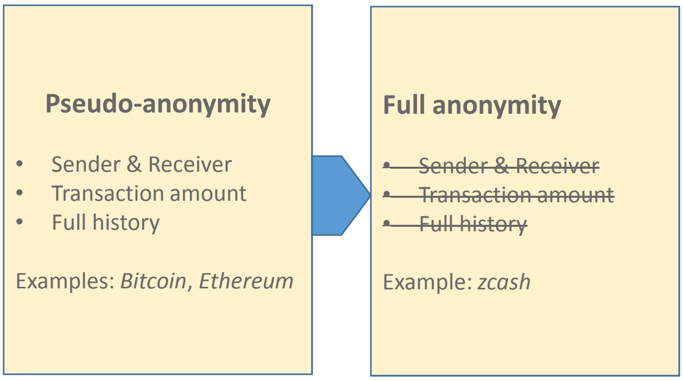
Traceability & KYC


8/30/2013 at 1:42
368.4975 BTC sent to
136jvwH7Rj99TaZPm6cuGg LyutmTX1p4Q4
9/01/2013 at 19:40
525 BTC are sent to
15T7SagsD2JqWUpBsiifcVuv yrQwX3Lq1e
8/30/2013 at 2:26 34 BTC are sent
to136jvwH7Rj99TaZPm6cuGgLyut mTX1p4Q4 from
1DvGKMYRZD9ekpts3dR19yWLiNx BZSN4EA.
These 24 bitcoins were included in the 400 BTC deposit on 9/27/2014
These 9.5 bitcoins were included in the 400 BTC deposit on 9/27/2014
All times are UTC (Coordinated Universal Time)

- IP identification (non trivial)
- Address black listing (non global)
- Regulation of financial intermediaries (hard to enforce)

Not much to do for small thefts…

Anonymity of cryptocurrencies



Pseudo-anonymity

- Sender & Receiver
- Transaction amount
- Full history

Examples: *Bitcoin*, *Ethereum*

Full anonymity

- ~~Sender & Receiver~~
- ~~Transaction amount~~
- ~~Full history~~

Example: *zcash*

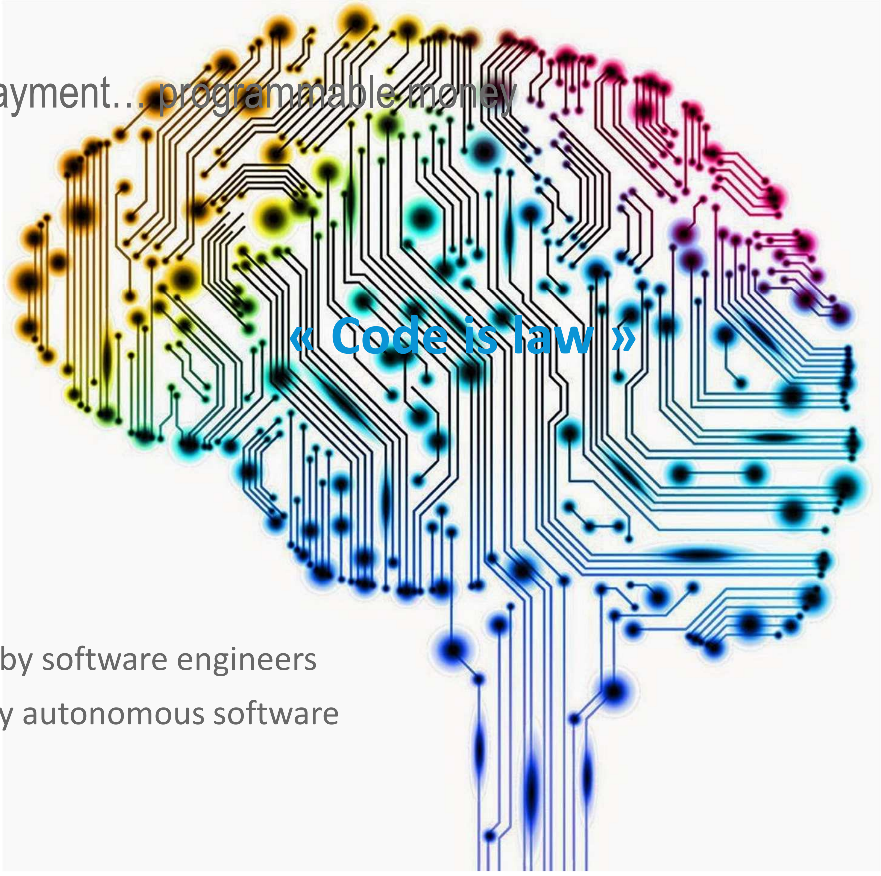
Solution against theft

Solution against ransomwares?

No magic solution

- Better computer security & system upgrades
- Data backups
- Network isolation

And beyond payment… programmable money



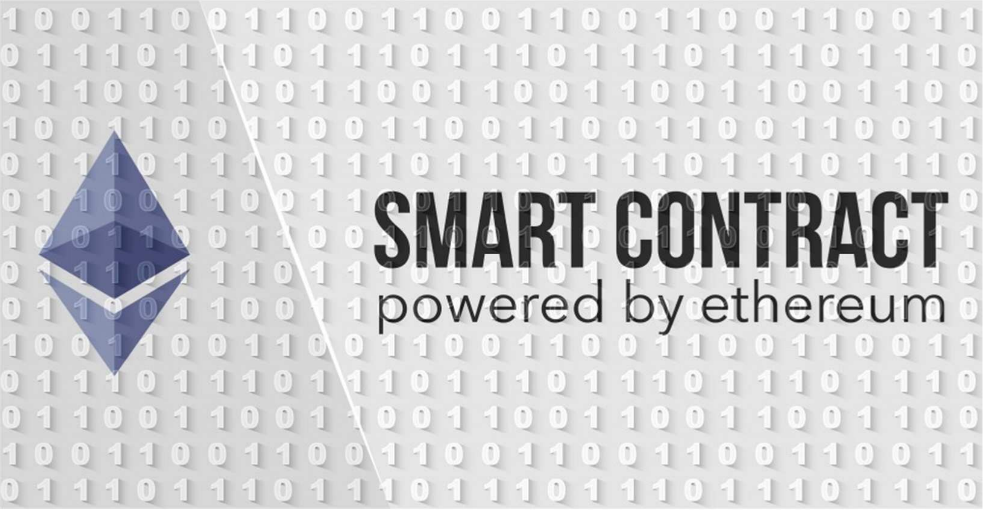
« Code is law »

Ambition

Replace lawyers by software engineers

Replace courts by autonomous software

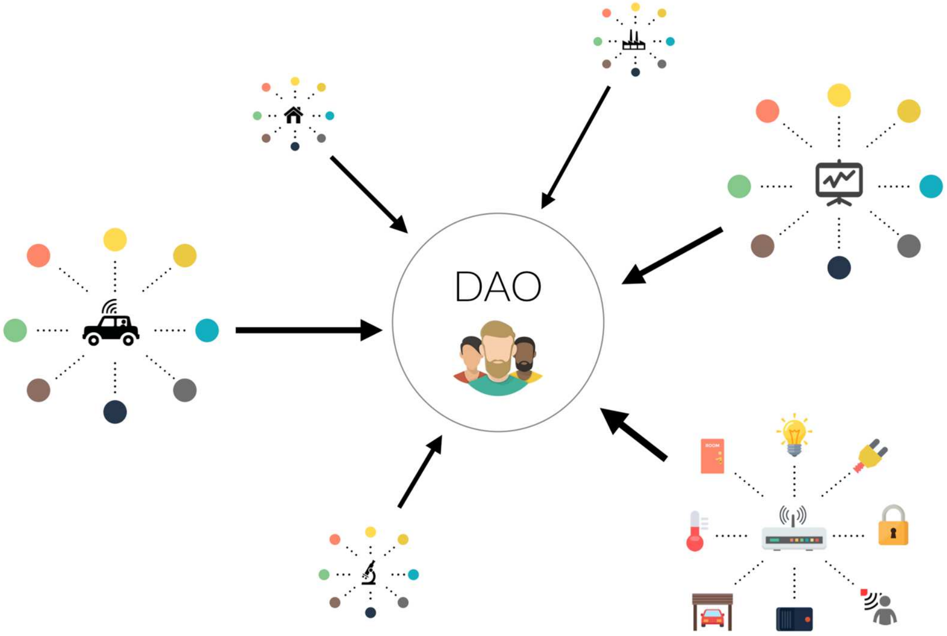
Smart contract platform



Case study: The DAO

“Do smart contracts remove all form of risk?”

Case study: The DAO

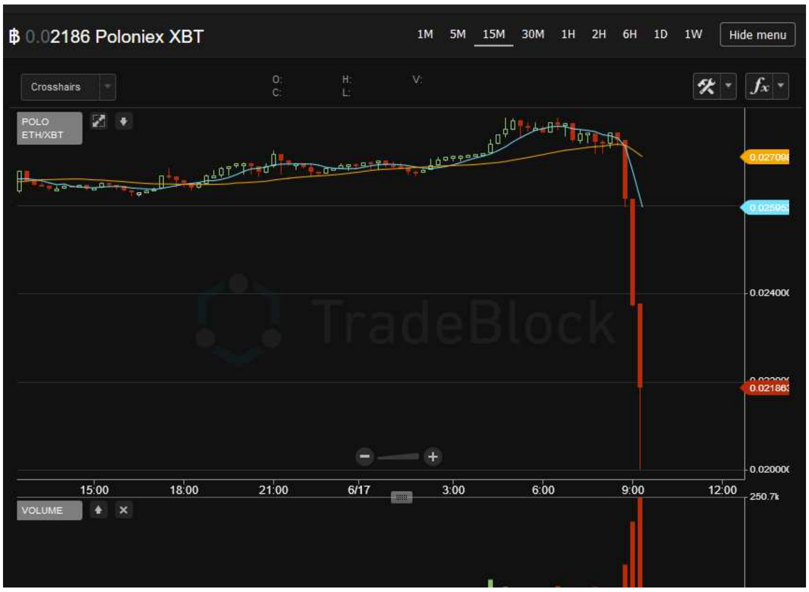


Case study: The DAO

THE DAO IS CODE.

GET DAO TOKENS

Case study: The DAO



METACO

Questions & Answers

For further discussion: **treccani@metaco.com**

METACO