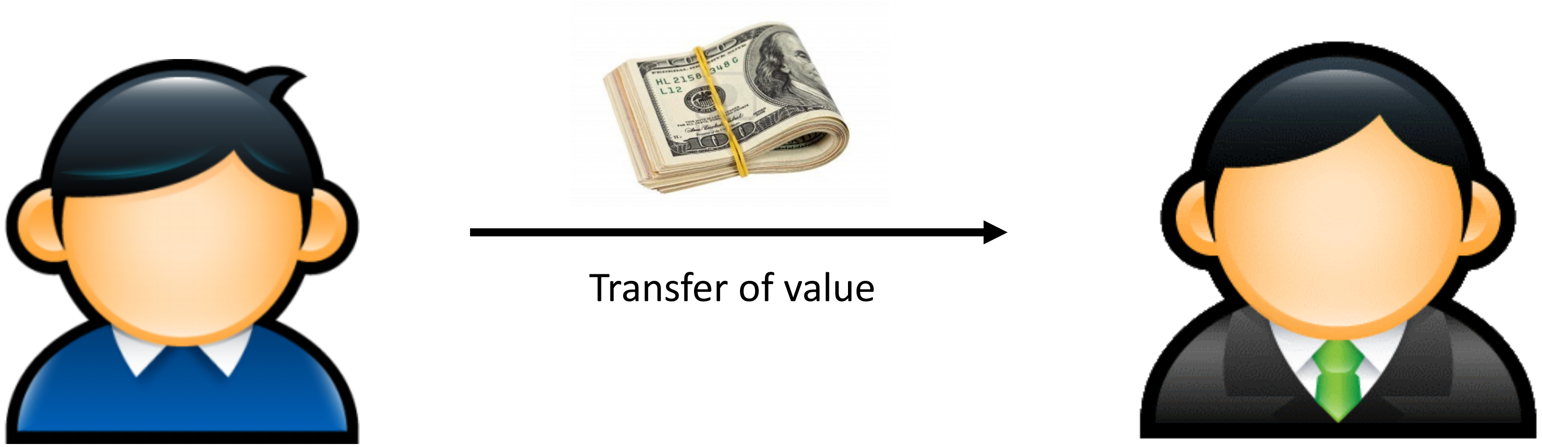
A primer on blockchain technology and its applications

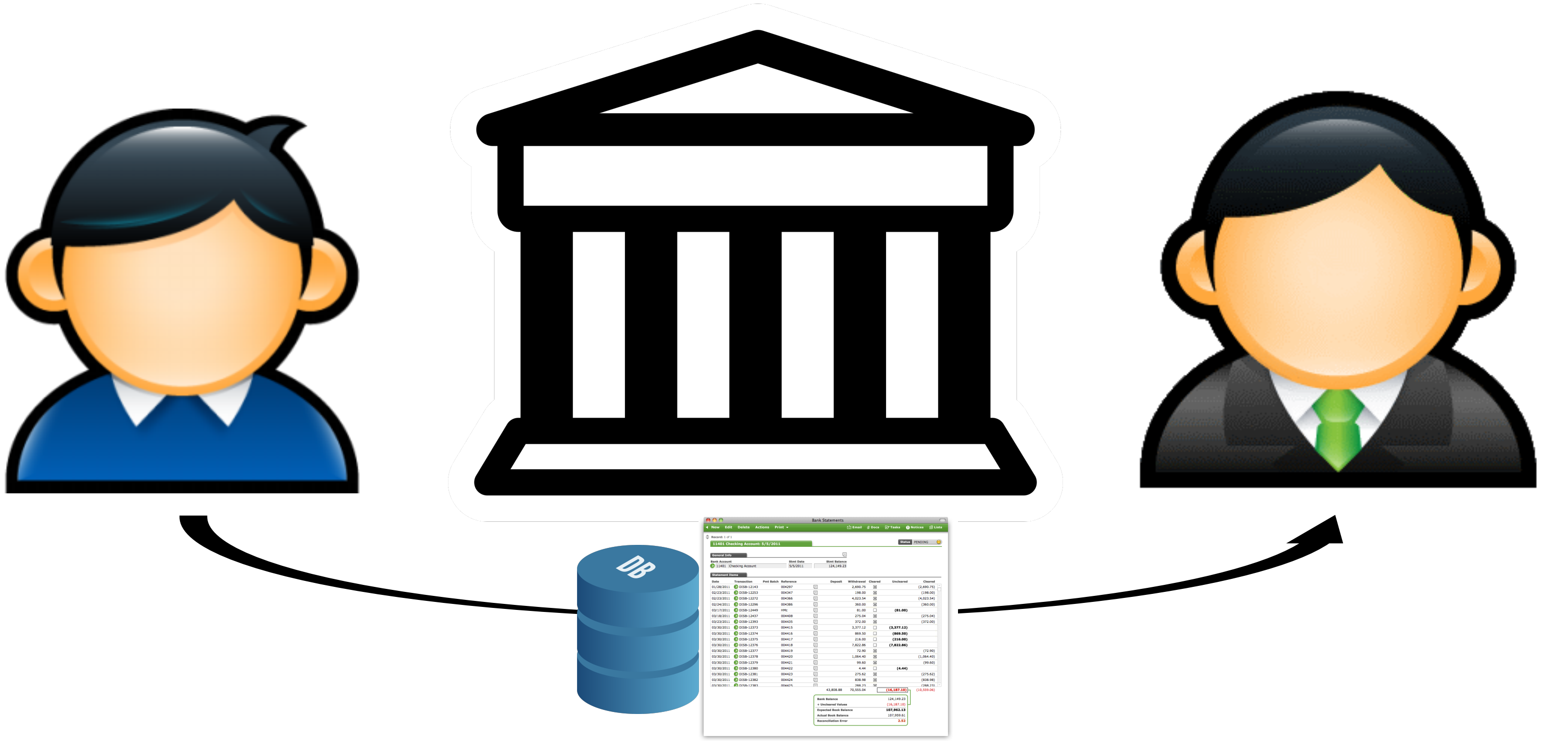
Adrien Treccani, Ph.D.

Swissquote Conference 2017

Finance in a nutshell



Electronic transfer (one bank)



Record: 1 of 1

11401 Checking Account: 5/5/2011

Status PENDING

General Info

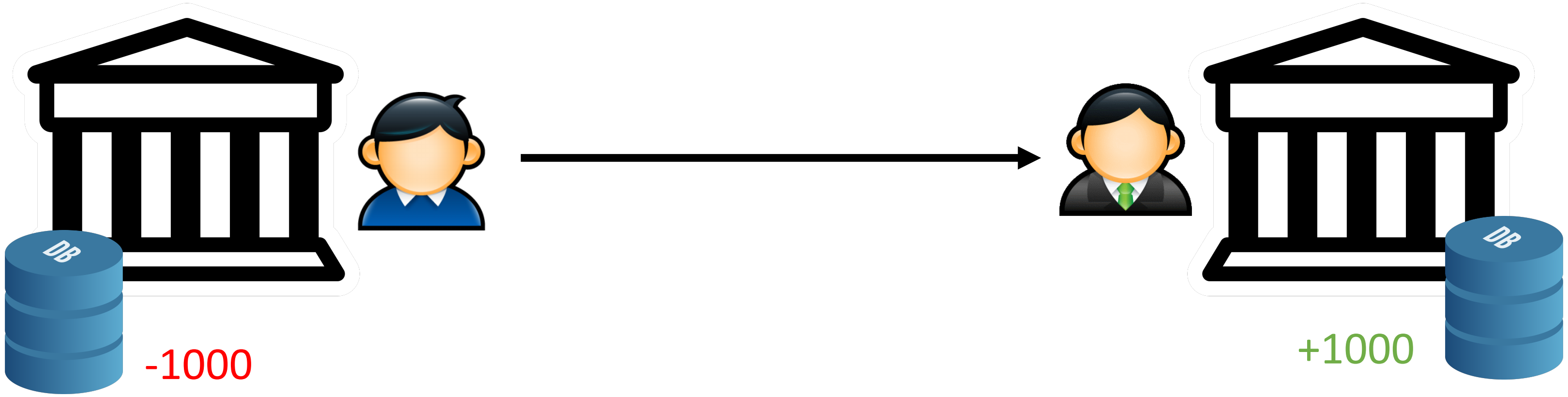
Bank Account: 11401 Checking Account
Stmt Date: 5/5/2011
Stmt Balance: 124,149.23

Statement Items

Date	Transaction	Pmt Batch	Reference	Deposit	Withdrawal	Cleared	Uncleared	Cleared
01/28/2011	DISB-12143		004297		2,690.75	☒		(2,690.75)
02/23/2011	DISB-12253		004347		198.00	☒		(198.00)
02/23/2011	DISB-12272		004366		4,023.54	☒		(4,023.54)
02/24/2011	DISB-12296		004386		360.00	☒		(360.00)
03/17/2011	DISB-12449		HMc		81.00	□	**(81.00)**	
03/18/2011	DISB-12437		004408		275.04	☒		(275.04)
03/23/2011	DISB-12393		004435		372.00	☒		(372.00)
03/30/2011	DISB-12373		004415		3,377.12	□	**(3,377.12)**	
03/30/2011	DISB-12374		004416		869.50	□	**(869.50)**	
03/30/2011	DISB-12375		004417		216.00	□	**(216.00)**	
03/30/2011	DISB-12376		004418		7,822.86	□	**(7,822.86)**	
03/30/2011	DISB-12377		004419		72.90	☒		(72.90)
03/30/2011	DISB-12378		004420		1,064.40	☒		(1,064.40)
03/30/2011	DISB-12379		004421		99.60	☒		(99.60)
03/30/2011	DISB-12380		004422		4.44	□	**(4.44)**	
03/30/2011	DISB-12381		004423		275.62	☒		(275.62)
03/30/2011	DISB-12382		004424		838.98	☒		(838.98)
03/30/2011	DISB-12383		004425		288.23	☒		(288.23)
				43,808.88	70,555.04		**(16,187.10)**	(10,559.06)

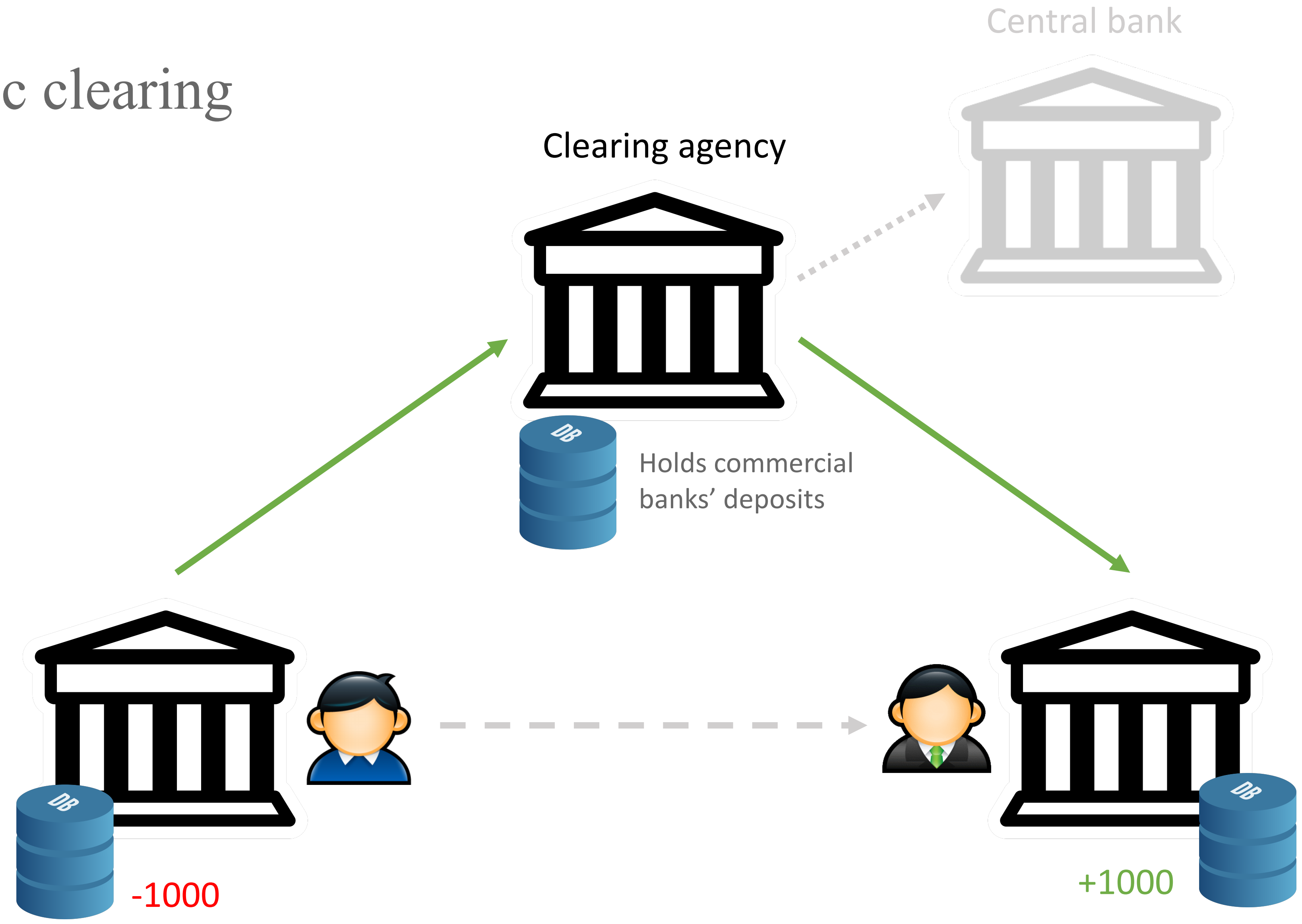
Bank Balance	124,149.23
+ Uncleared Values	(16,187.10)
Expected Book Balance	**107,962.13**
Actual Book Balance	107,959.61
Reconciliation Error	**2.52**

Electronic transfer (two banks)

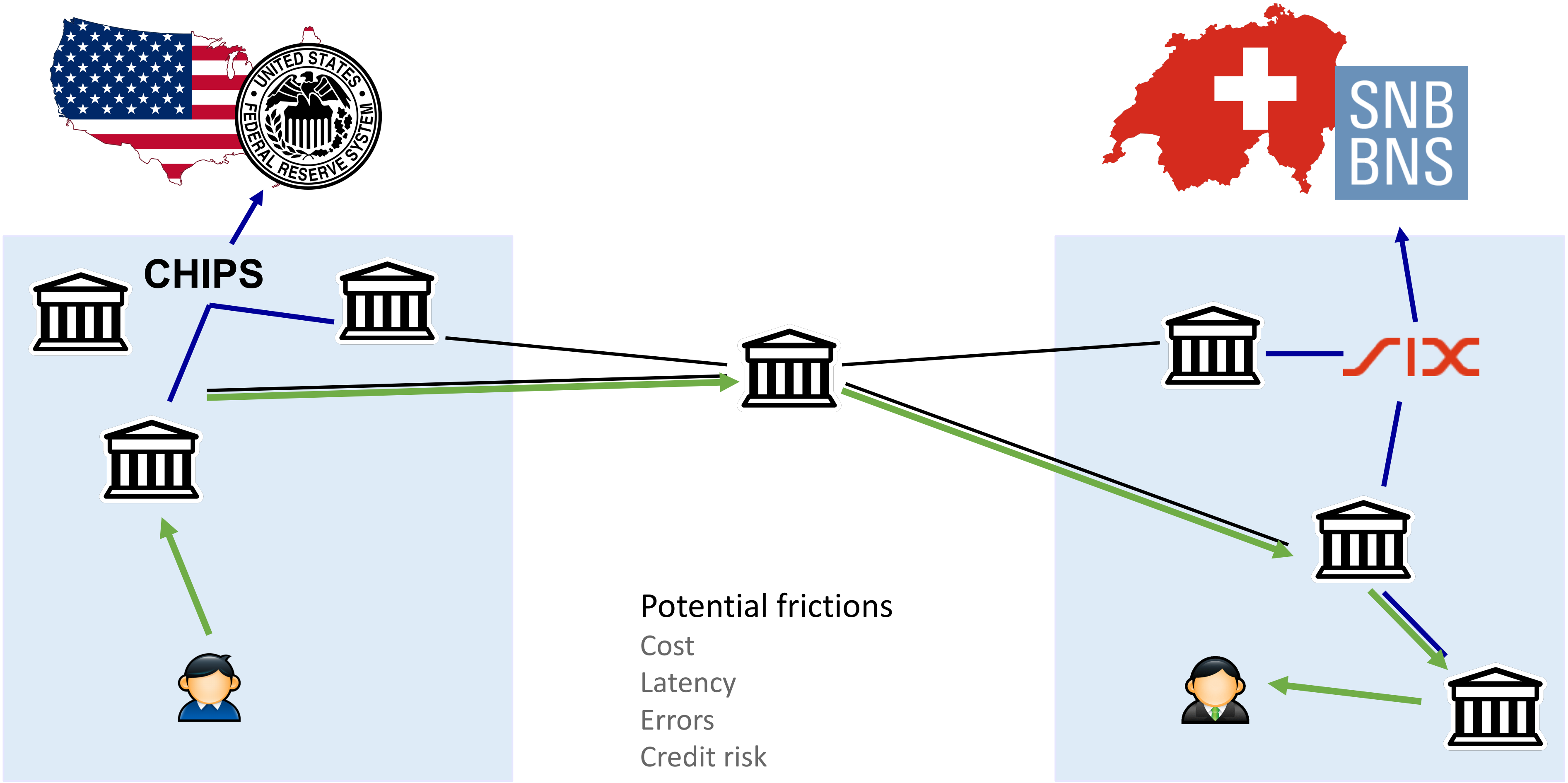


How to make sure consolidated accounting is correct / no fraud?

Electronic clearing



Complex system

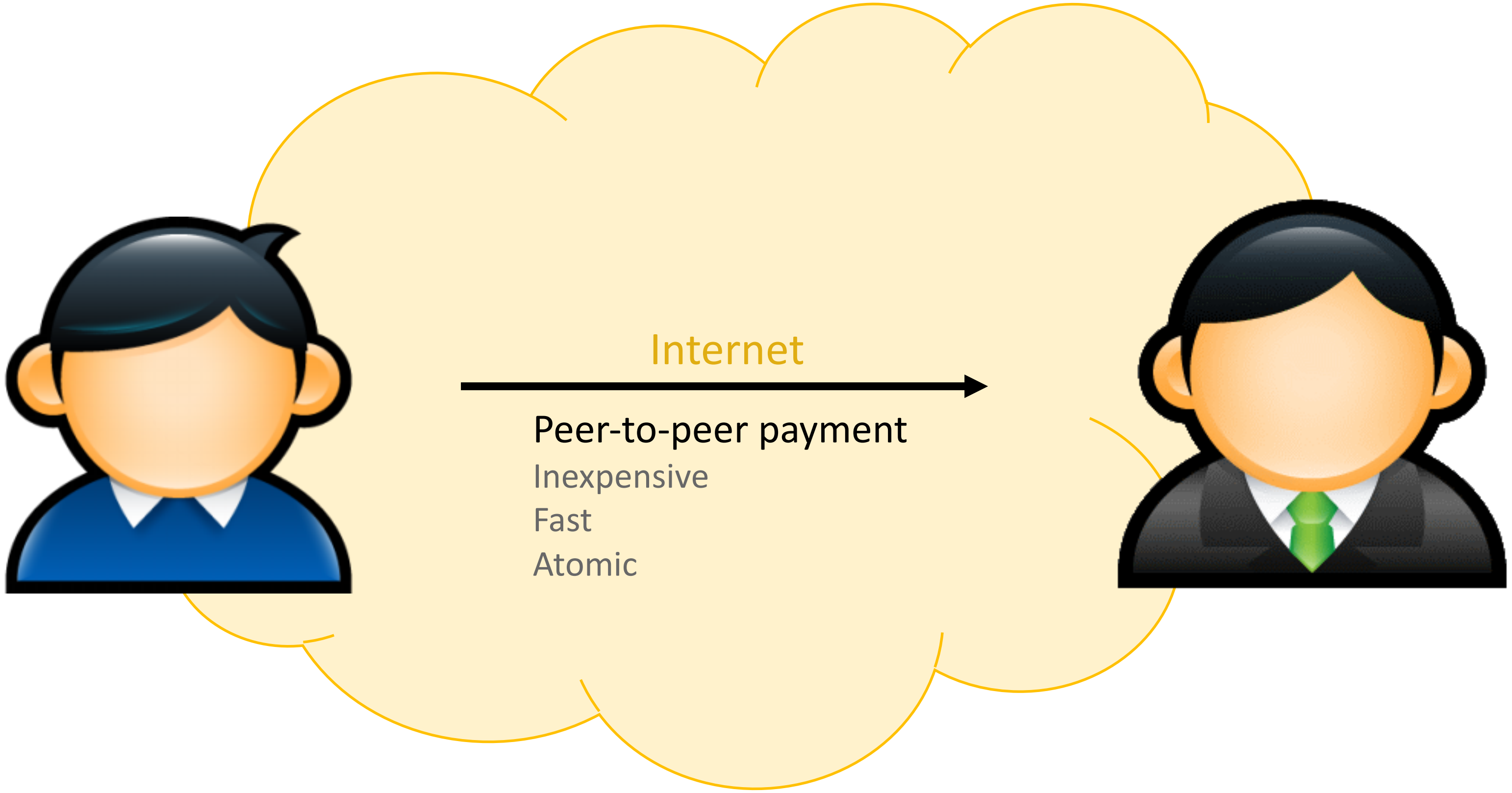


Potential frictions

- 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

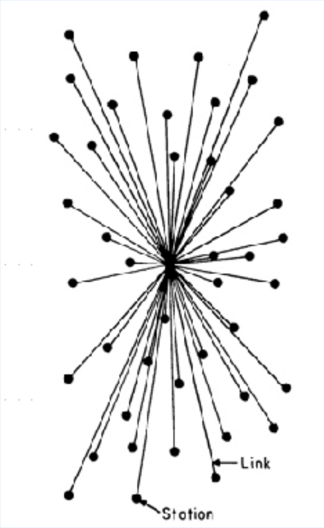
Fast

Atomic

Blockchain motivation (cont'd)

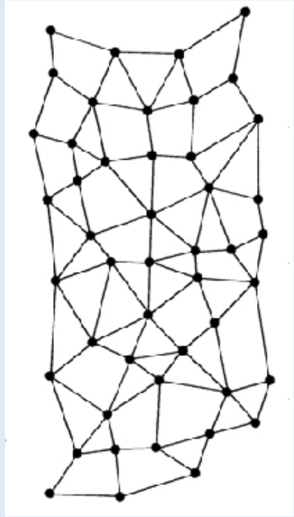
Centralized network

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



Distributed network

Frictionless entry
Democratic governance
Global access
Algorithmic validation



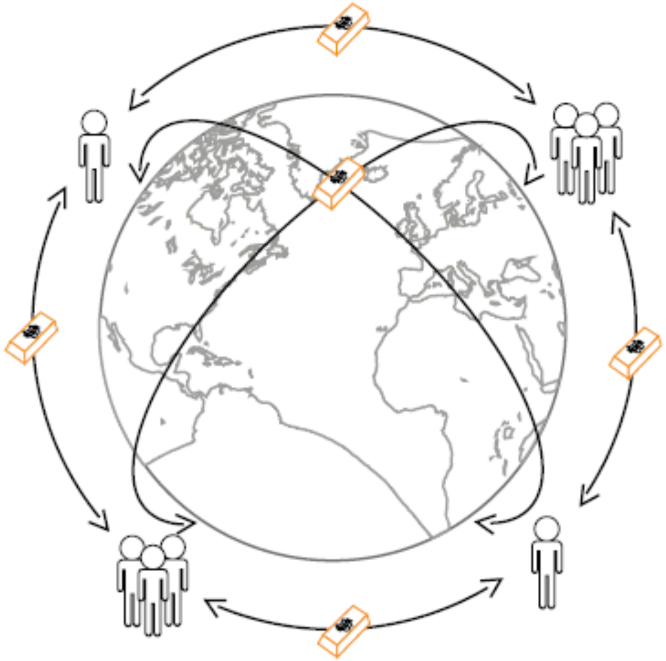
Bitcoin network

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

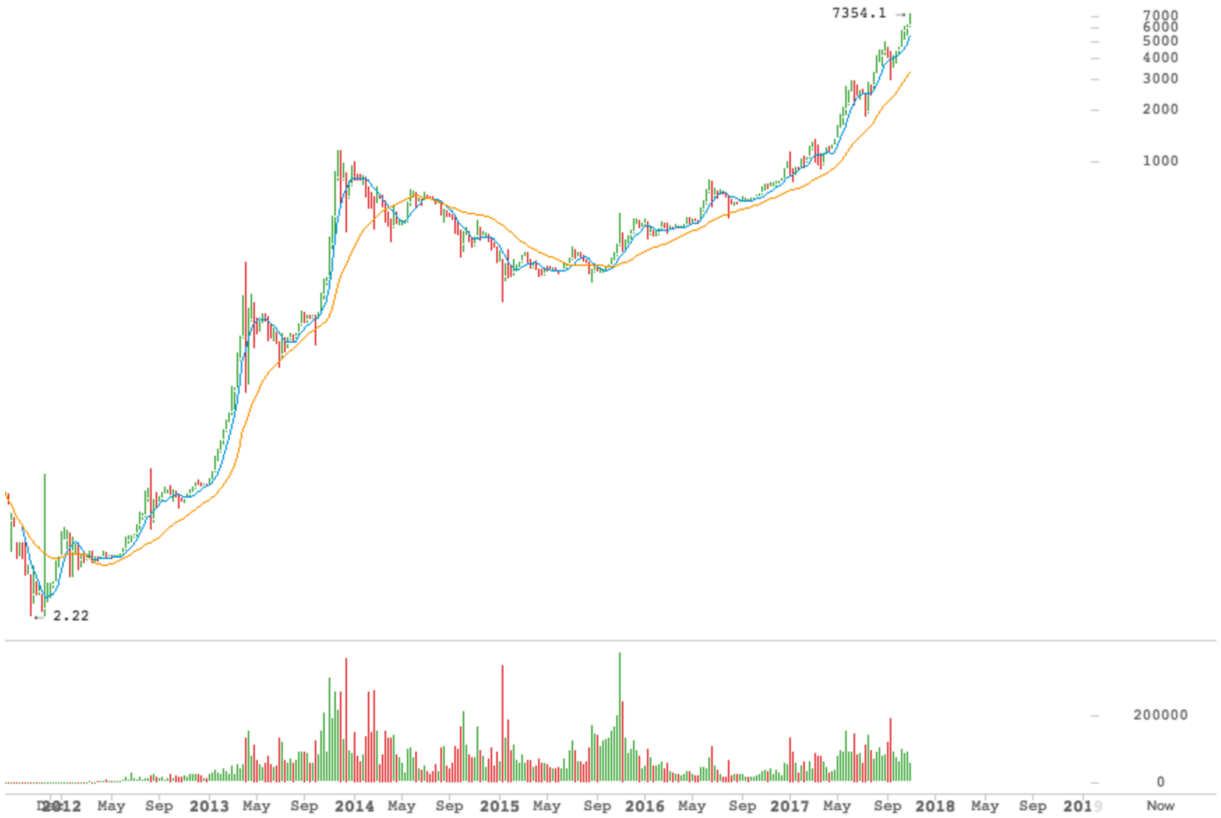
Bitcoin currency

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).*

Double spending problem

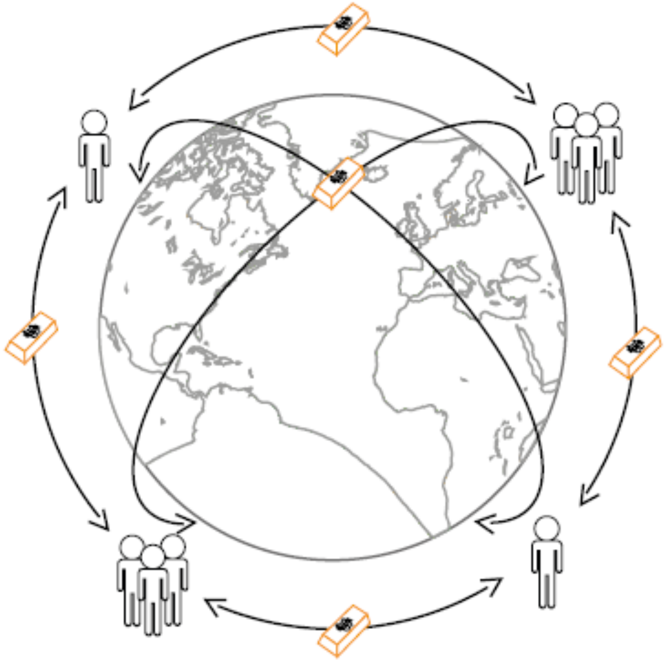
How to avoid users spending the same money twice?

Double spending solution (centralized)

I have canceled your second order.

Don’t ever try again to spend more than you have at my expense.

Double spending (distributed)

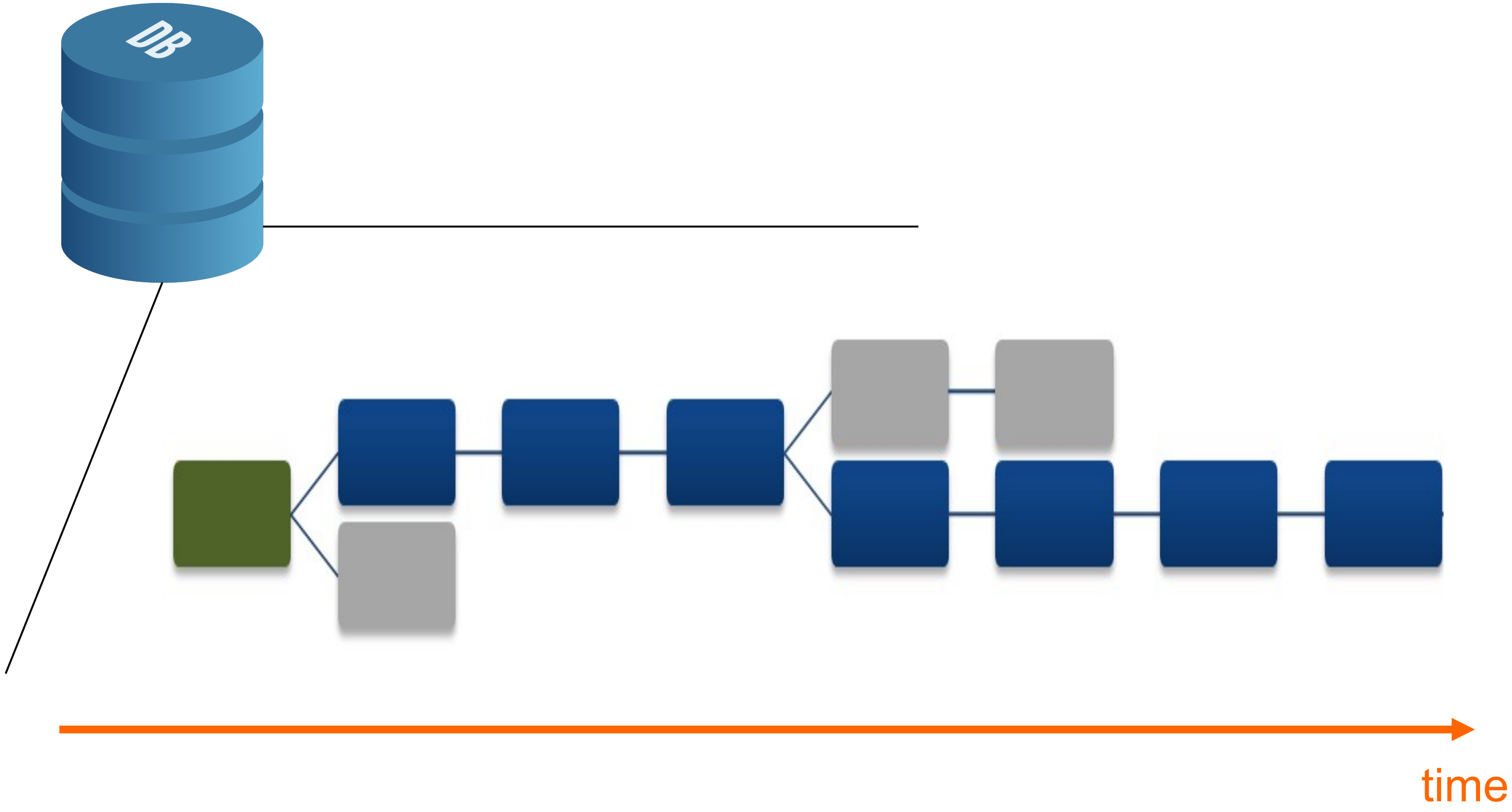


Challenge

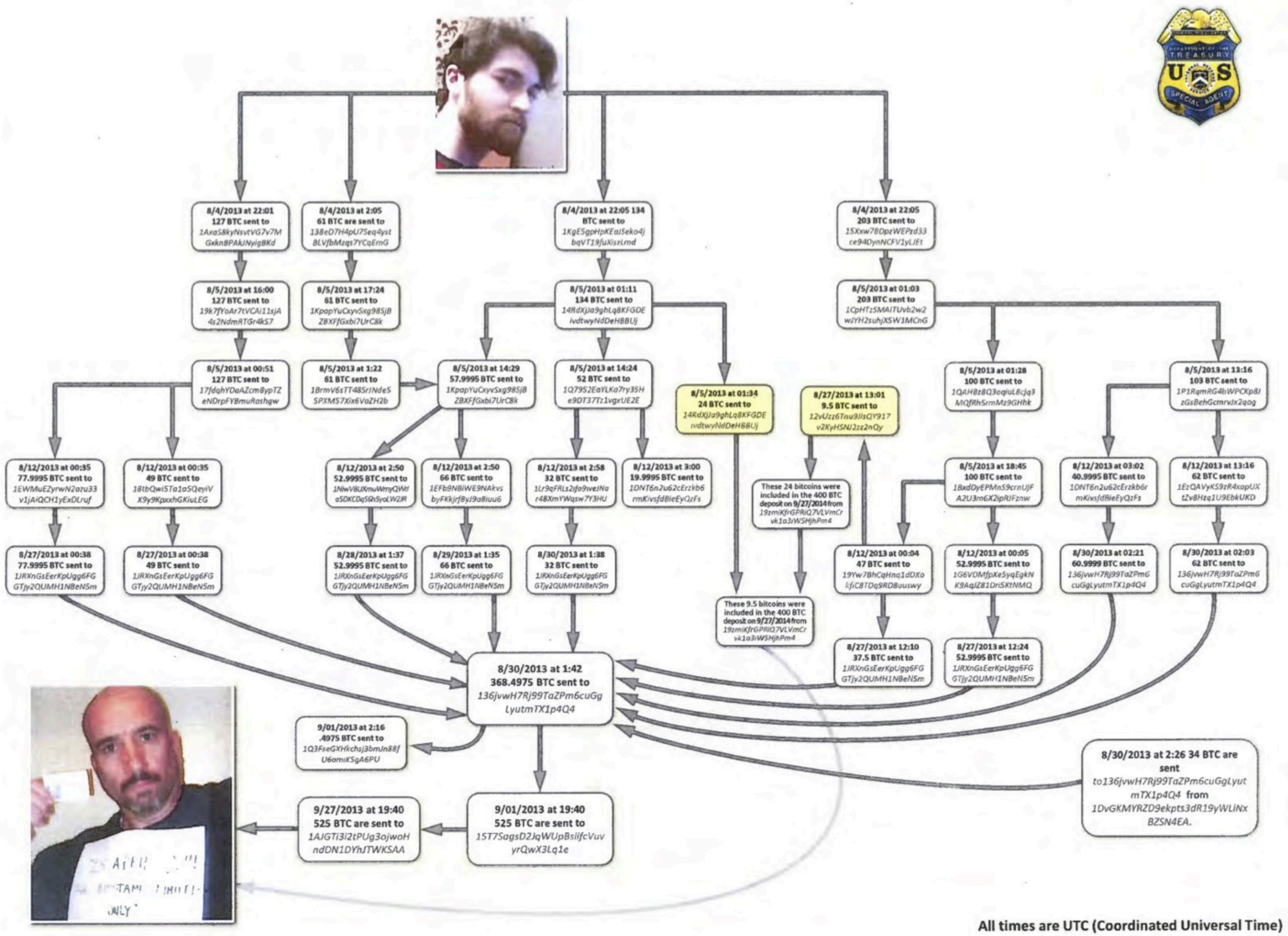
- No central authority
- No chronology
- No trust between users

How to reach an agreement (consensus) on which transactions to validate/ignore?

Blockchain *trust machine*



Traceability



8/4/2013 at 22:01
127 BTC sent to
1Axa58kyNsvtVG7v7M
GxknBPAkJNyigBKd

8/4/2013 at 2:05
61 BTC are sent to
138eD7H4pU7Seq4yst
BLVfbMzqs7YCqEmG

8/4/2013 at 22:05 134
BTC sent to
1KgE5gpHpKEaJSeko4j
bqVT19fuXiszLmd

8/4/2013 at 22:05
203 BTC sent to
15Xxw7BDpzWEPzd33
ce94DynNCFV1yLJEt

8/5/2013 at 16:00
127 BTC sent to
19k7fYoAr7tVCAi11sjA
4s2NdmRTGr4kS7

8/5/2013 at 17:24
61 BTC sent to
1KpapYuCxyvSxg98SjB
ZBXFfGxbi7UrC8k

8/5/2013 at 01:11
134 BTC sent to
14RdXjJa9ghLq8KFGDE
ivdtwyNdDeHBBUj

8/5/2013 at 01:03
203 BTC sent to
1CpHTzSMAITUvb2w2
wJYH2suhjXSW1MCnG

8/5/2013 at 00:51
127 BTC sent to
17fdqhYDaAZcm8ypTZ
eNDrpFYBmuRashgw

8/5/2013 at 1:22
61 BTC sent to
1BrmV6sTT48SrJNde5
5PXMS7Xix6VaZH2b

8/5/2013 at 14:29
57.9995 BTC sent to
1KpapYuCxyvSxg98SjB
ZBXFfGxbi7UrC8k

8/5/2013 at 14:24
52 BTC sent to
1Q7952EaYLKa7ry35H
e9DT37Tz1vgxUE2E

8/5/2013 at 01:34
24 BTC sent to
14RdXjJa9ghLq8KFGDE
ivdtwyNdDeHBBUj

8/27/2013 at 13:01
9.5 BTC sent to
12vUzz6Tnu9JisQY917
v2KyHSNJ2zz2nQy

8/5/2013 at 01:28
100 BTC sent to
1QAHBz8Q3aqiuL8cJq3
MQfRh5rmMz9GHhk

8/5/2013 at 13:16
103 BTC sent to
1P1RqmRG4bWPCKp8J
zGsBehGcmrvJx2qog

8/12/2013 at 00:35
77.9995 BTC sent to
1EWMuEZyrwN2azu33
v1jAiQCH1yExDLruf

8/12/2013 at 00:35
49 BTC sent to
18tbQwi5Ta1a5QeyiV
X9y9KpxxhGKiuLEG

8/12/2013 at 2:50
52.9995 BTC sent to
1NiwV8UXmuWmyQWd
a5DKCDq56h5yoLW2JR

8/12/2013 at 2:50
66 BTC sent to
1EFb9NBiWE9NAkvs
byFKkjrf8yJ9a8iuu6

8/12/2013 at 2:58
32 BTC sent to
1Lr9qFRLs2zfo9weJNa
r48XmYWqsw7Y3HU

8/12/2013 at 3:00
19.9995 BTC sent to
1DNT6n2u62cErzkb6
rmKivsfdBieEyQzFs

These 24 bitcoins were included in the 400 BTC deposit on 9/27/2014 from
19zmiKfrGPRiQ7VLVmCr
vk1a3iW5HjhPm4

8/5/2013 at 18:45
100 BTC sent to
1BxdDyEPMn59crnUjF
A2U3m6X2ipRJFznw

8/12/2013 at 03:02
40.9995 BTC sent to
1DNT6n2u62cErzkb6r
mKivsfdBieEyQzFs

8/12/2013 at 13:16
62 BTC sent to
1EzQAVyKS9zR4xapUX
tZv8Hzq1U9EbkUKD

8/27/2013 at 00:38
77.9995 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeNSm

8/27/2013 at 00:38
49 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeNSm

8/28/2013 at 1:37
52.9995 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeNSm

8/29/2013 at 1:35
66 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeNSm

8/30/2013 at 1:38
32 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeNSm

8/12/2013 at 00:04
47 BTC sent to
19Yw7BhCqHnq1dDXo
kfiC8TDq9RD8uuswy

8/12/2013 at 00:05
52.9995 BTC sent to
1G6VDMfpXe5yqEgkN
K9AqJZ81DriSKtNMQ

8/30/2013 at 02:21
60.9999 BTC sent to
136jvwH7Rj99TaZPm6
cuGgLyutmTX1p4Q4

8/30/2013 at 02:03
62 BTC sent to
136jvwH7Rj99TaZPm6
cuGgLyutmTX1p4Q4

These 9.5 bitcoins were included in the 400 BTC deposit on 9/27/2014 from
19zmiKfrGPRiQ7VLVmCr
vk1a3iW5HjhPm4

8/27/2013 at 12:10
37.5 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeNSm

8/27/2013 at 12:24
52.9995 BTC sent to
1JRXnGsEerKpUgg6FG
GTjy2QUMH1NBeNSm

8/30/2013 at 1:42
368.4975 BTC sent to
136jvwH7Rj99TaZPm6cuGg
LyutmTX1p4Q4

9/01/2013 at 2:16
.4975 BTC sent to
1Q3FseGXHkchsj3bmJn88f
U6omiK5gA6PU

8/30/2013 at 2:26 34 BTC are sent
to136jvwH7Rj99TaZPm6cuGgLyut
mTX1p4Q4 from
1DvGKMYRZD9ekpts3dR19yWLiNx
BZSN4EA.

9/27/2013 at 19:40
525 BTC are sent to
1AJGTi3i2tPUg3ojwoH
ndDN1DYhJTWKSAA

9/01/2013 at 19:40
525 BTC are sent to
15T7SagsD2JqWUpBslifcVuv
yrQwX3Lq1e

All times are UTC (Coordinated Universal Time)

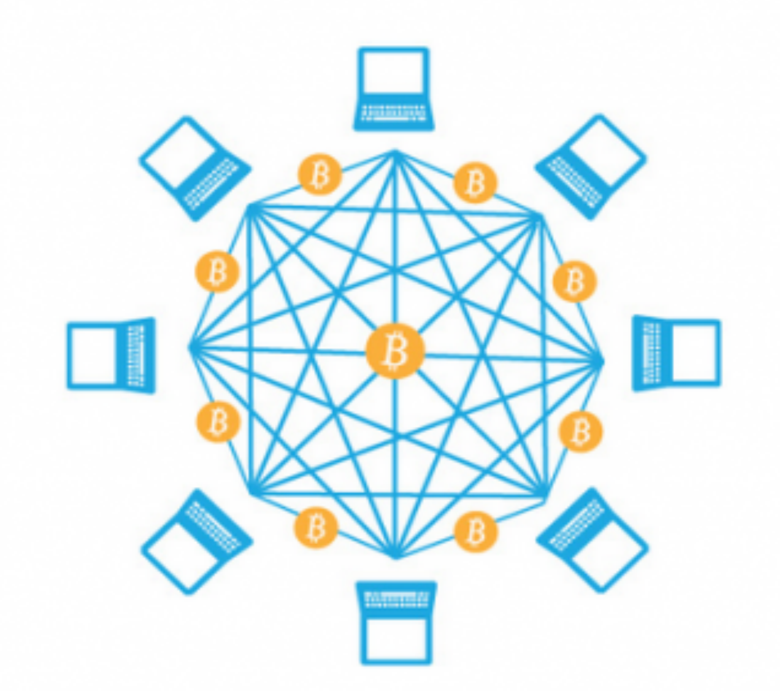
Real-time example

Blockchain storage

Distributed persistence

Users maintain full copy of the blockchain

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



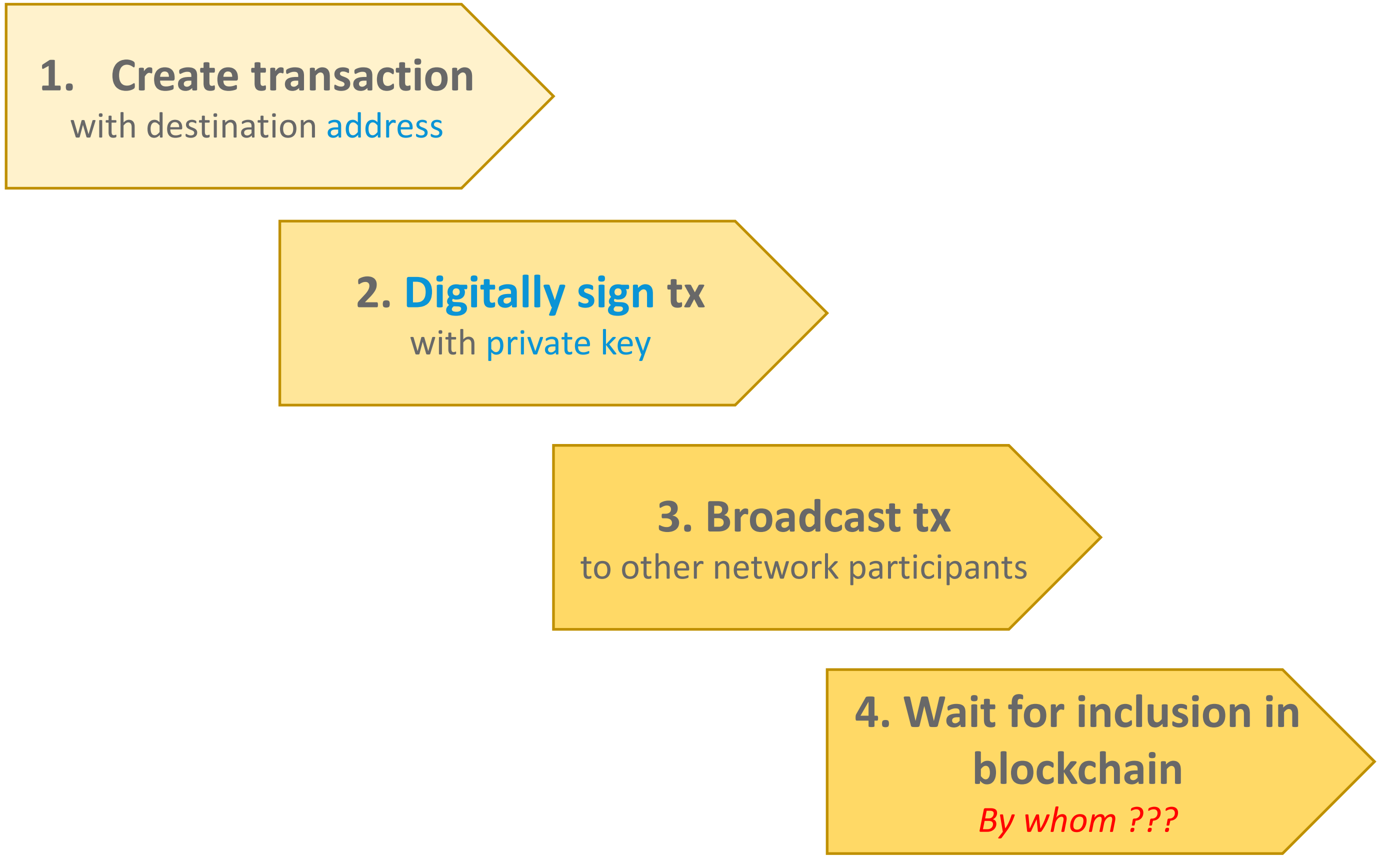
Key numbers

- 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



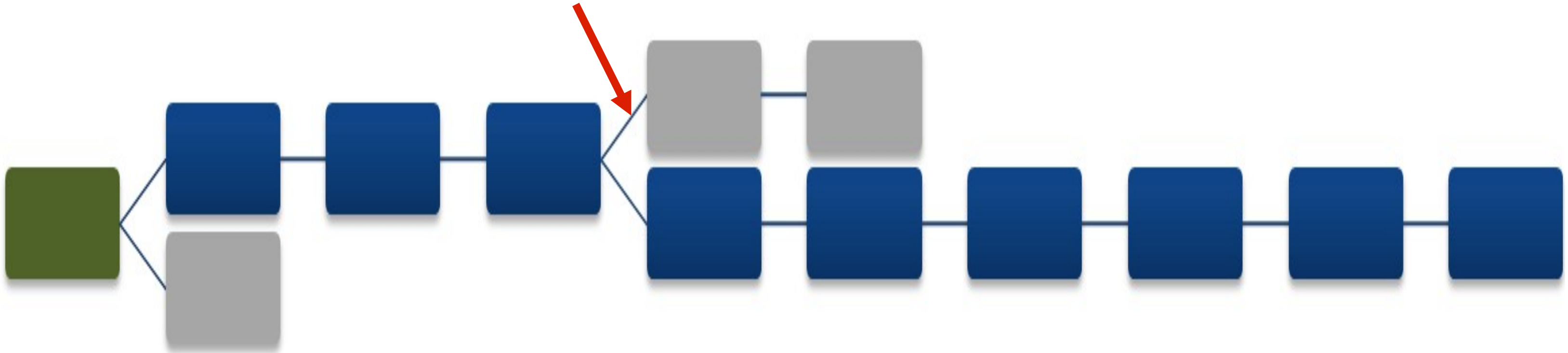
1. **Create transaction**
with destination address

2. **Digitally sign tx**
with private key

3. **Broadcast tx**
to other network participants

4. **Wait for inclusion in blockchain**
By whom ???

Ledger consensus



Miners

Proof-of-work

Stupid *but complex* problem

Miners need to solve proof-of-work problem

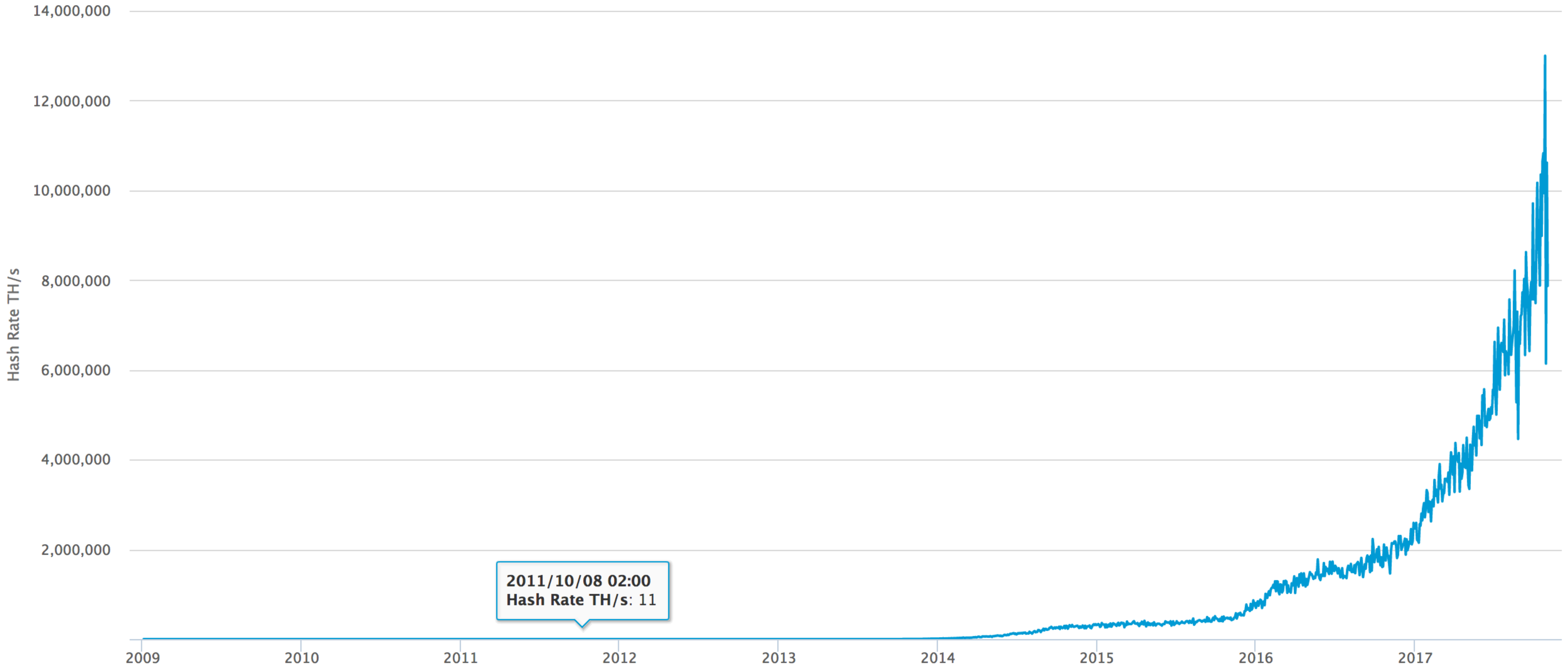
- Required for insertion of new block
- Extremely computationally intensive
- Special hardware + electricity costs

Bitcoin reward for new blocks

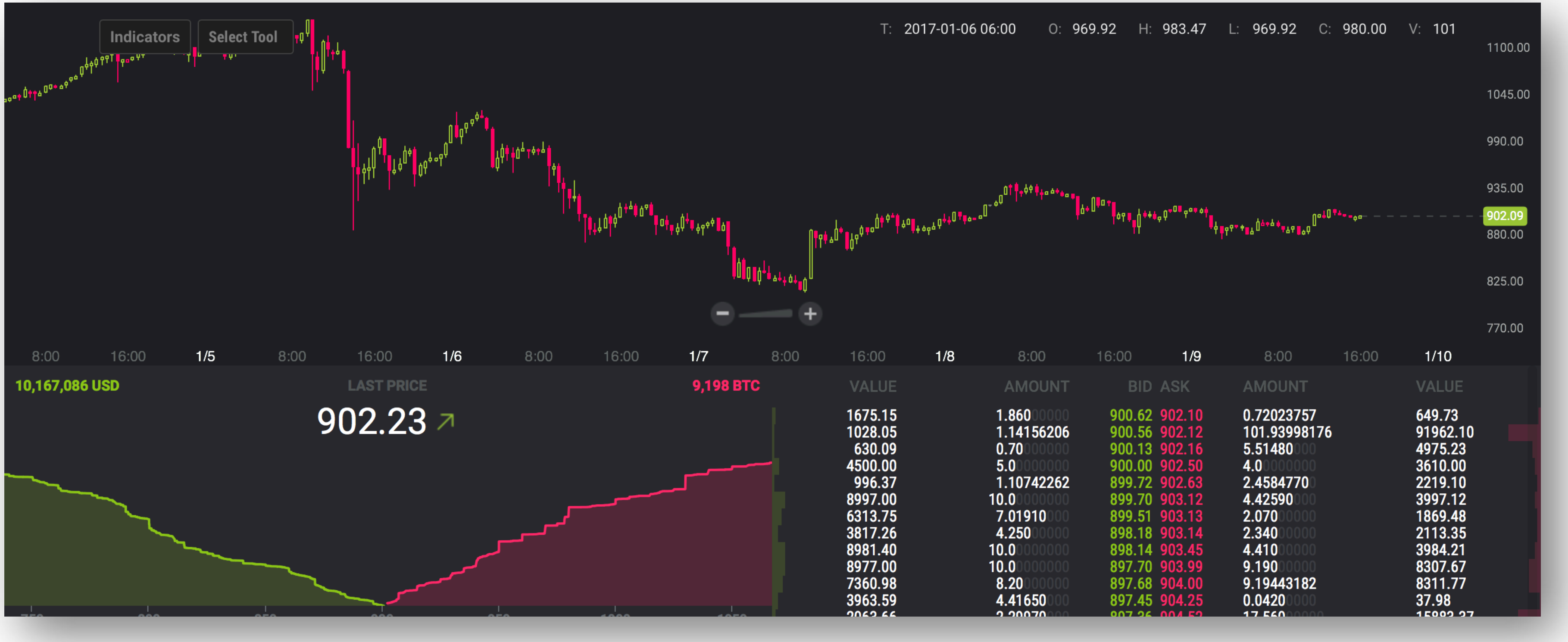
Miners are rewarded with bitcoins

- Freshly created bitcoins (inflation)
- Transaction fees

Network security



Buy bitcoins



T: 2017-01-06 06:00 O: 969.92 H: 983.47 L: 969.92 C: 980.00 V: 101

10,167,086 USD

LAST PRICE

902.23 ↗

9,198 BTC

VALUE	AMOUNT	BID	ASK	AMOUNT	VALUE
1675.15	1.86000000	900.62	902.10	0.72023757	649.73
1028.05	1.14156206	900.56	902.12	101.93998176	91962.10
630.09	0.70000000	900.13	902.16	5.51480000	4975.23
4500.00	5.00000000	900.00	902.50	4.00000000	3610.00
996.37	1.10742262	899.72	902.63	2.45847700	2219.10
8997.00	10.00000000	899.70	903.12	4.42590000	3997.12
6313.75	7.01910000	899.51	903.13	2.07000000	1869.48
3817.26	4.25000000	898.18	903.14	2.34000000	2113.35
8981.40	10.00000000	898.14	903.45	4.41000000	3984.21
8977.00	10.00000000	897.70	903.99	9.19000000	8307.67
7360.98	8.20000000	897.68	904.00	9.19443182	8311.77
3963.59	4.41650000	897.45	904.25	0.04200000	37.98

e.g. bitstamp.net or coinbase.com

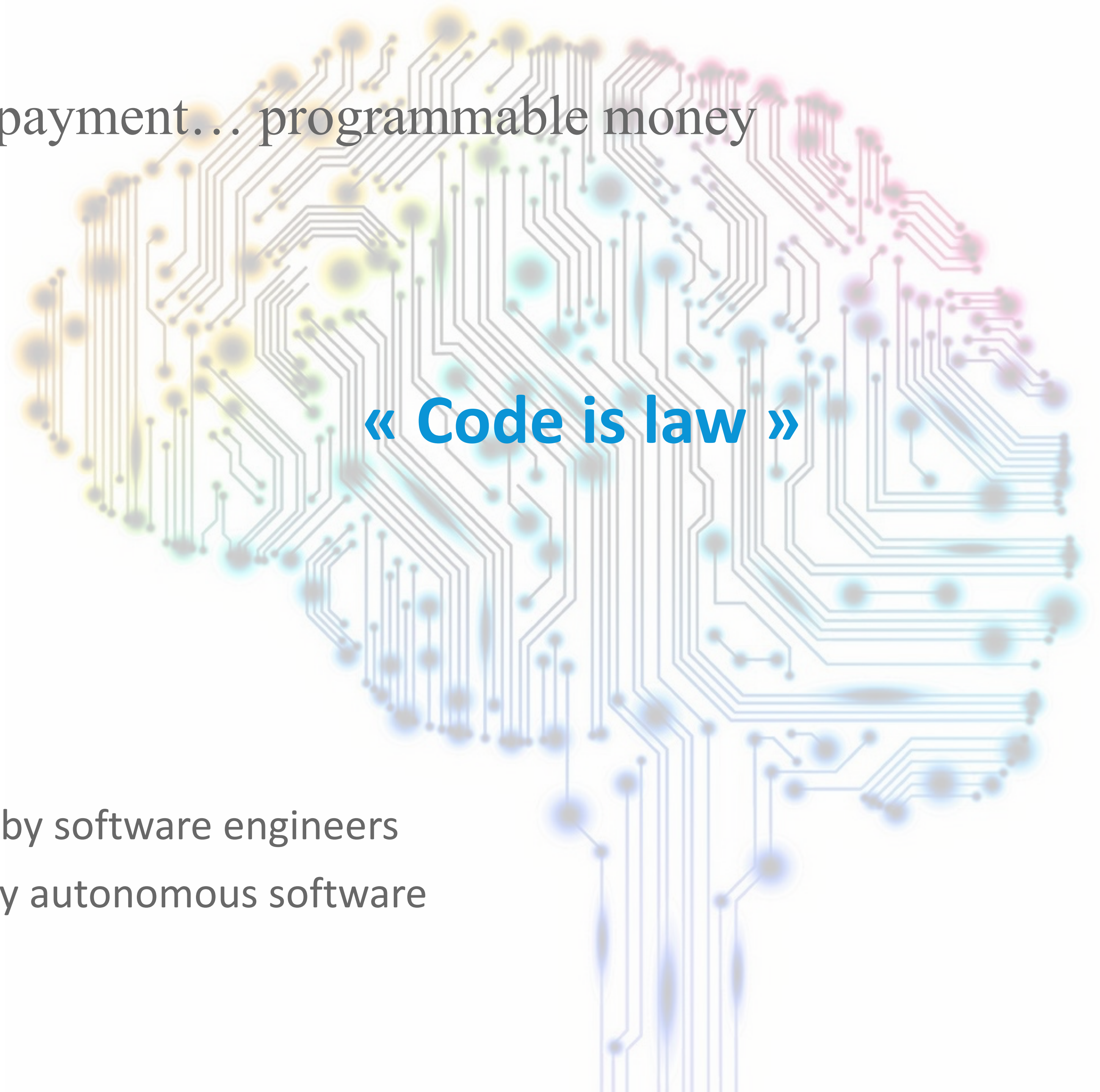
Power consumption

Mining: 350 megawatts and growing (abt consumptions of 290,000 US homes)

Beyond bitcoin currency

METACO

And beyond payment… programmable money



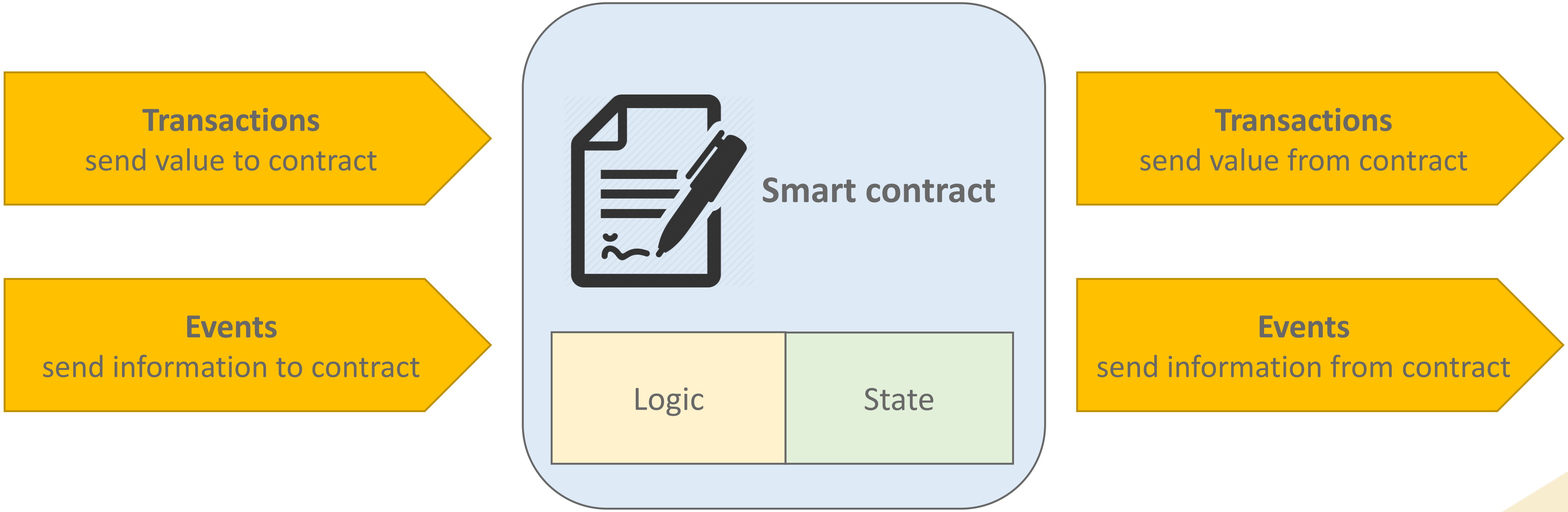
« Code is law »

Ambition

Replace lawyers by software engineers

Replace courts by autonomous software

Smart contract



Transactions
send value to contract

Events
send information to contract

Smart contract

Logic

State

Transactions
send value from contract

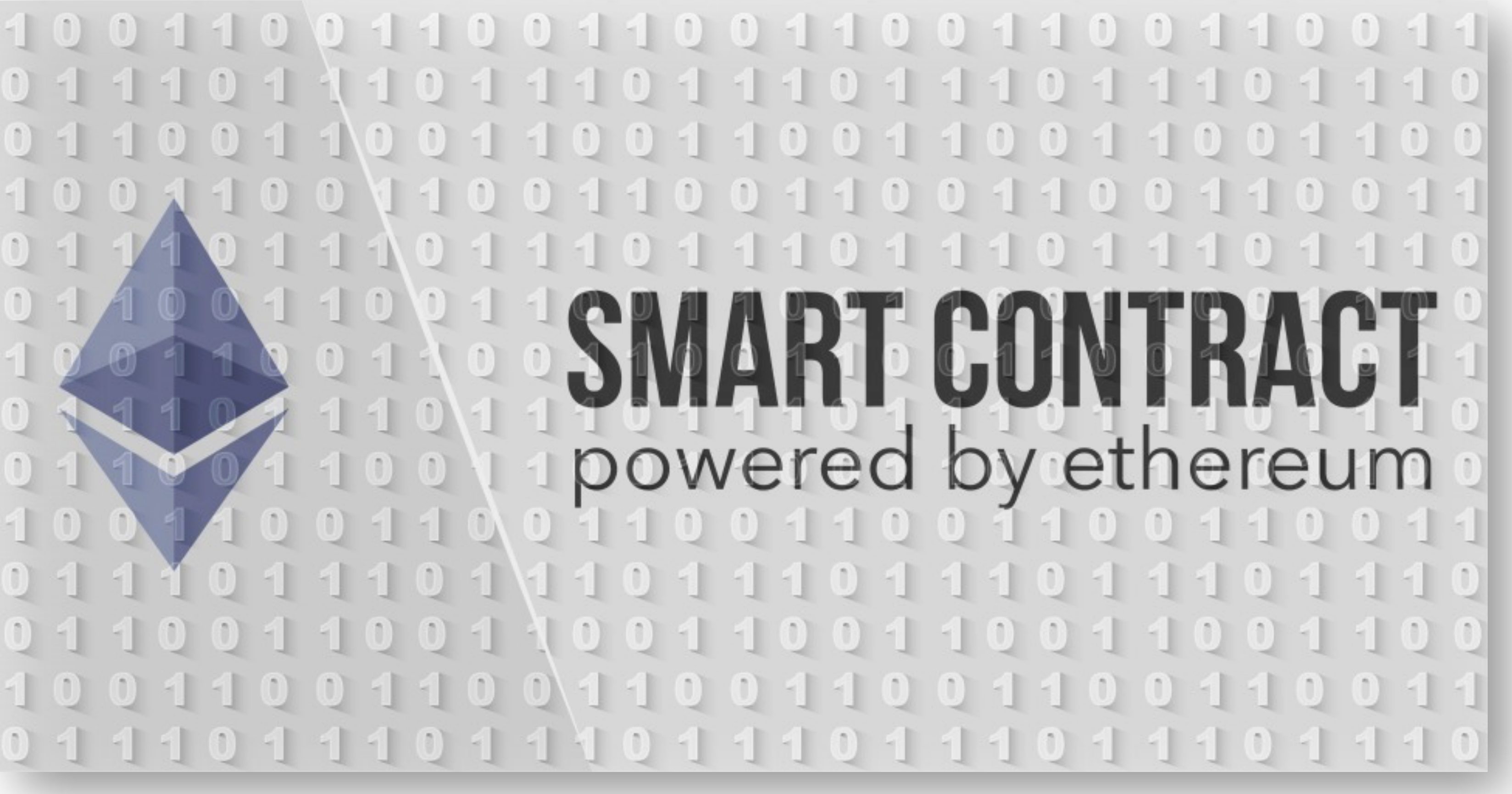
Events
send information from contract

Use case: Multi-signature account

Multi-signature

Logic	**Allow withdraw if and only if** 1. CEO orders withdraw, or 2. 2 out of 3 assistants order withdraw and volume smaller than 1M a day
State	• Balance of the contract • Authorized assistants • Amount withdrawn in last 24h

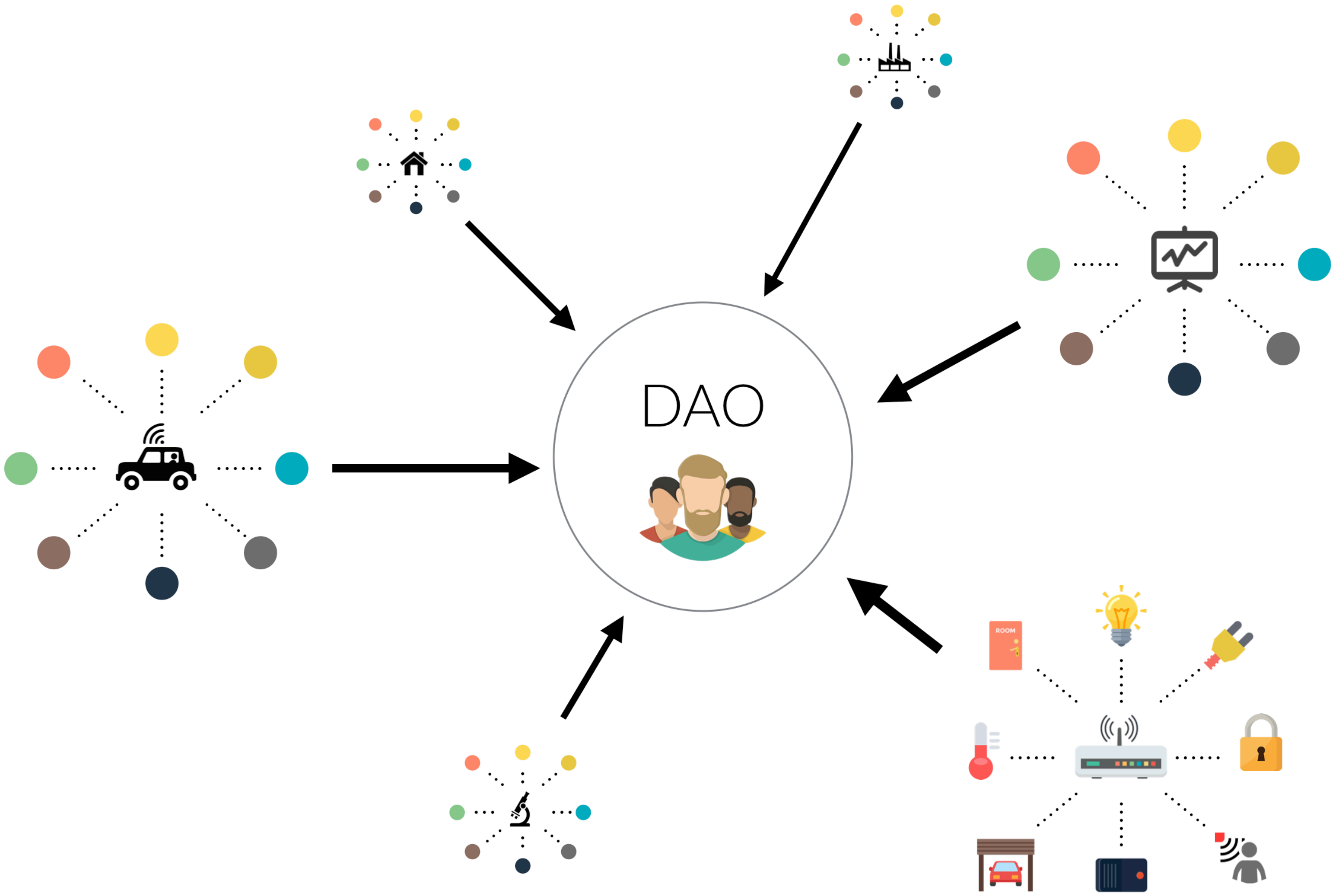
Smart contract platform



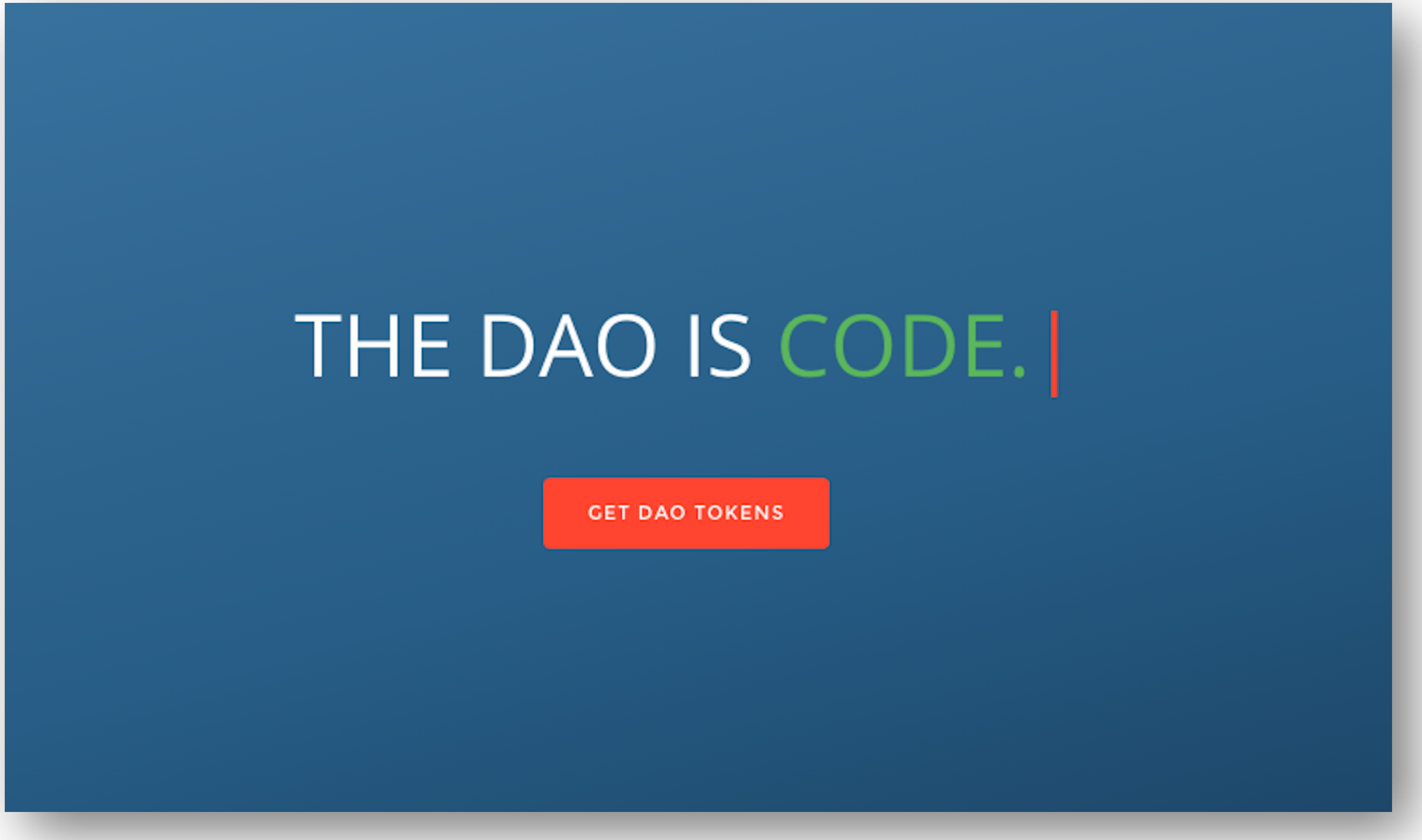
Case study: The DAO

“Do smart contracts remove all form of risk?”

Case study: The DAO

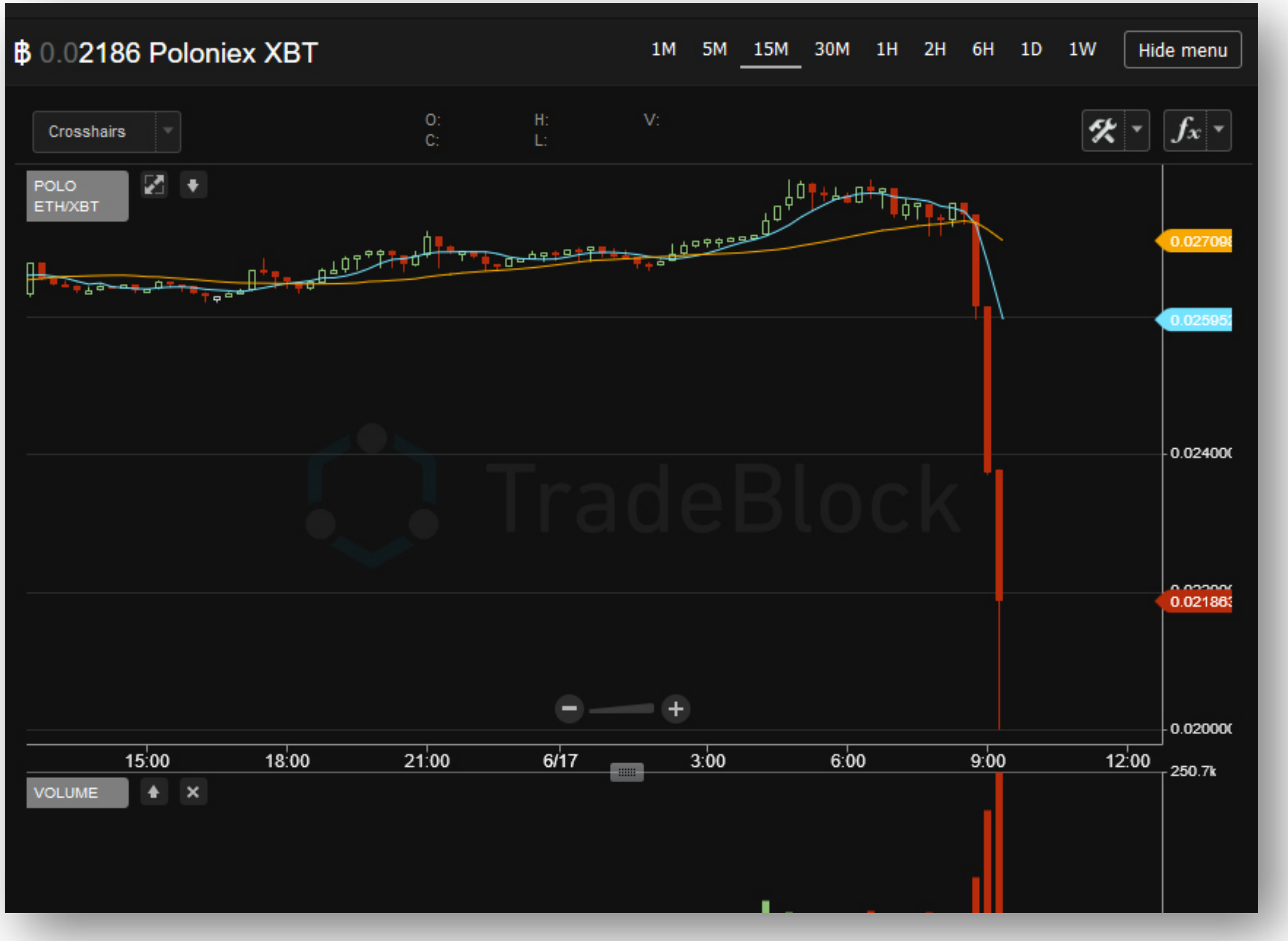


Case study: The DAO



THE DAO IS CODE.

Case study: The DAO



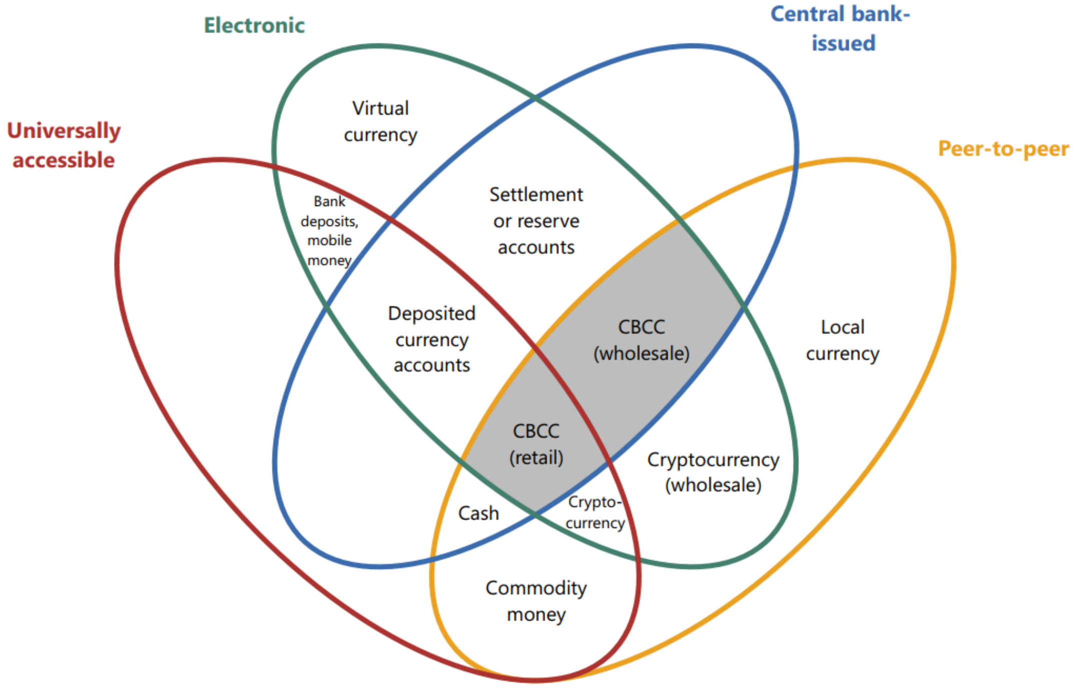
Discussion

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

- The challenge of storing cryptocurrencies
- What about central-bank-issued digital currencies?

The money flower: a taxonomy of money

Graph 3


Electronic
Central bank-issued
Universally accessible
Peer-to-peer
Virtual currency
Settlement or reserve accounts
Bank deposits, mobile money
Deposited currency accounts
CBCC (wholesale)
Local currency
CBCC (retail)
Cryptocurrency (wholesale)
Cash
Crypto-currency
Commodity money