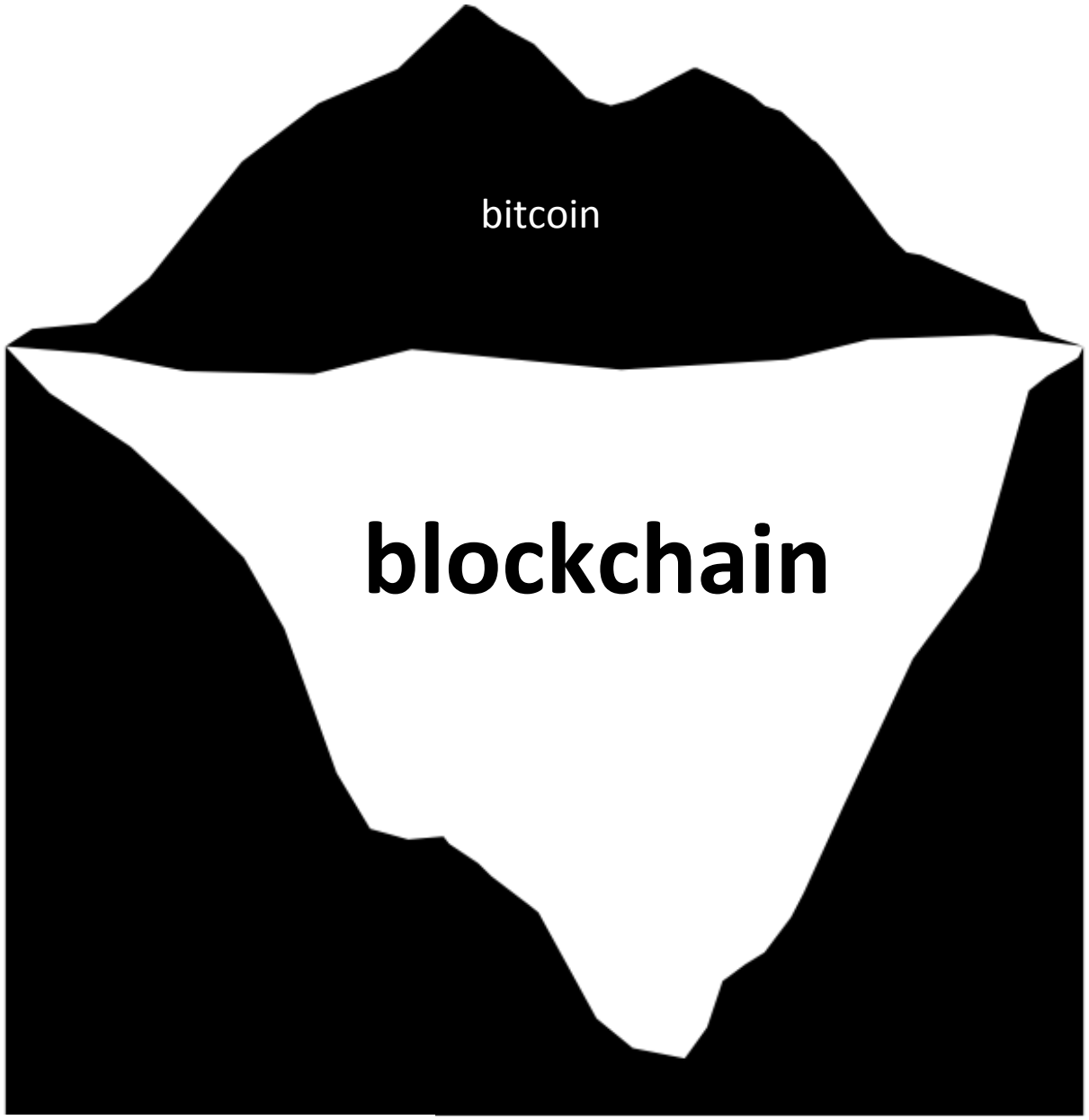
Blockchain:
The Iceberg Beneath Bitcoin

John Callahan, PhD

JHU/APL

WARNING: many simplifications ahead


bitcoin
blockchain

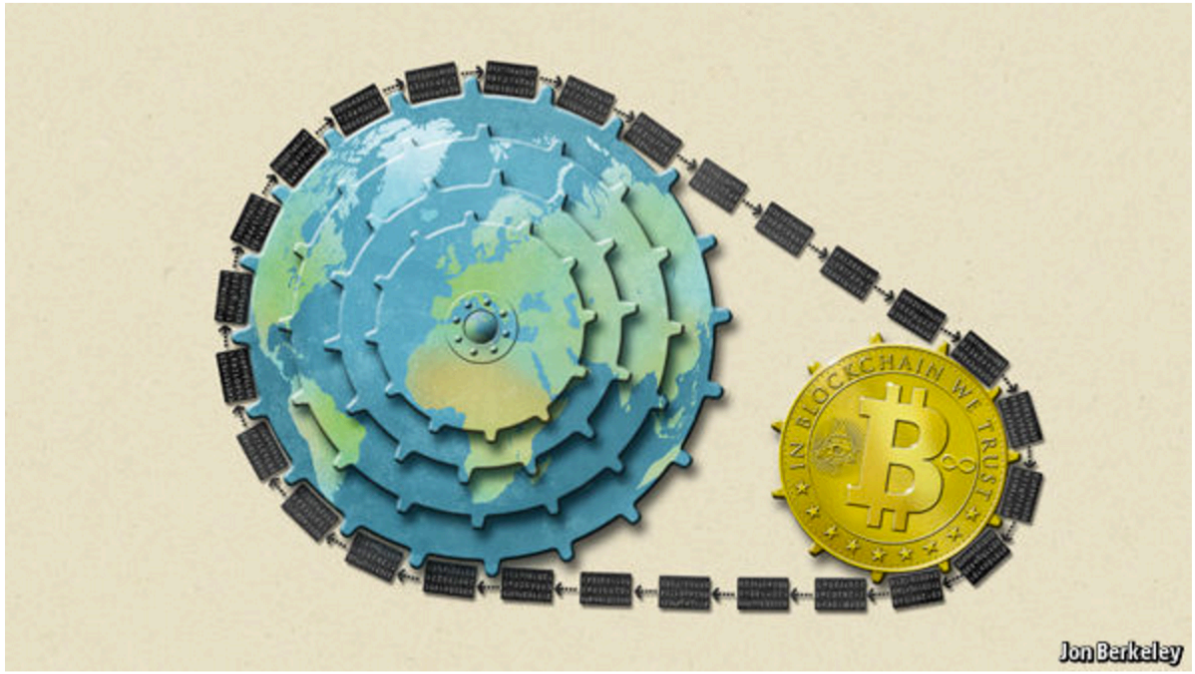
The promise of the blockchain

The trust machine

Comment (108)
E-mail
Print
Timekeeper reading list
Reprints & permissions

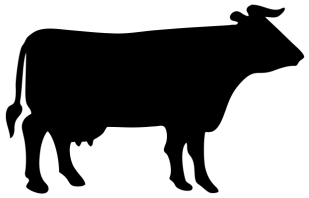
The technology behind bitcoin could transform how the economy works

Oct 31st 2015 | From the print edition



BITCOIN has a bad reputation. The decentralised digital cryptocurrency, powered by a vast computer network, is notorious for the wild fluctuations in its value, the zeal of its supporters and its degenerate uses, such as extortion, buying drugs and hiring hitmen in the online bazaars of the “dark net”.

Barter

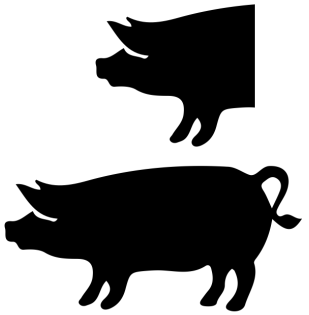


Created by Chris Pyper
from Noun Project

?

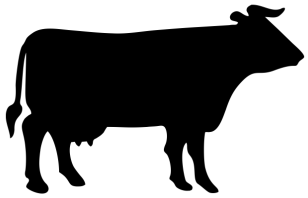
=

Created by Verena Gutentag
from Noun Project



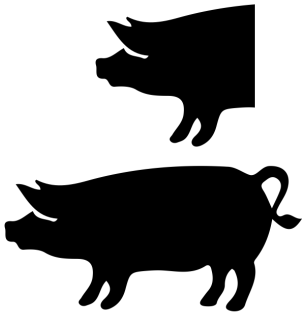
Created by Ealancheliyan s
from Noun Project

Money: fungibility

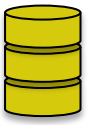


Created by Chris Pyper
from Noun Project

Created by Verena Gutentag
from Noun Project

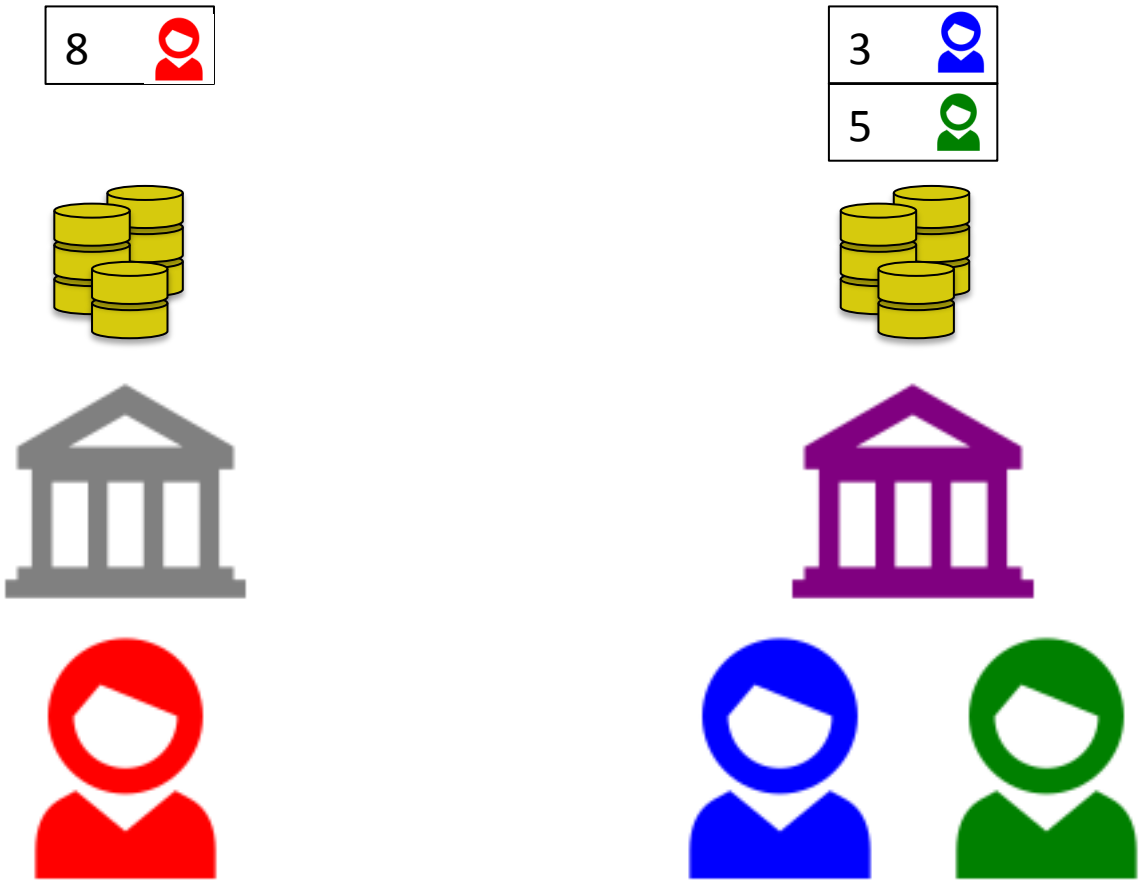


Created by Ealancheliyan s
from Noun Project

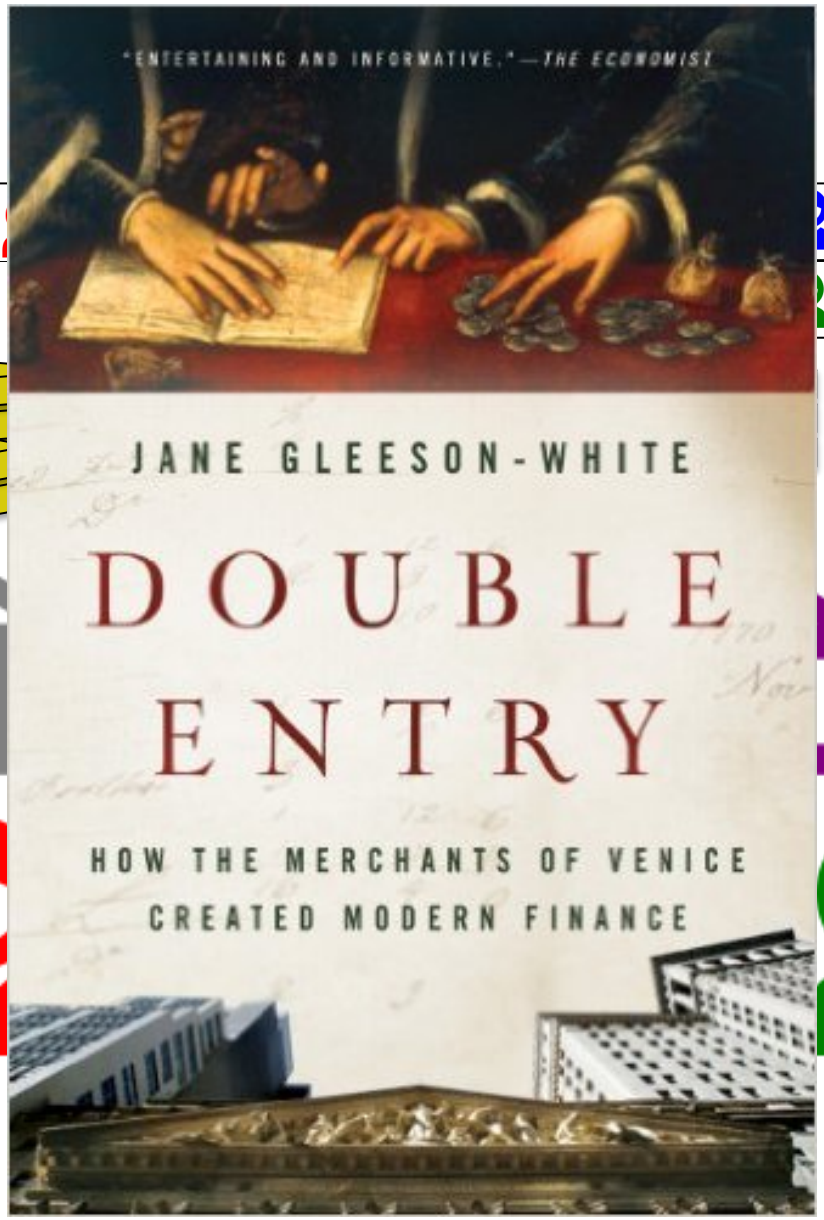


Banking

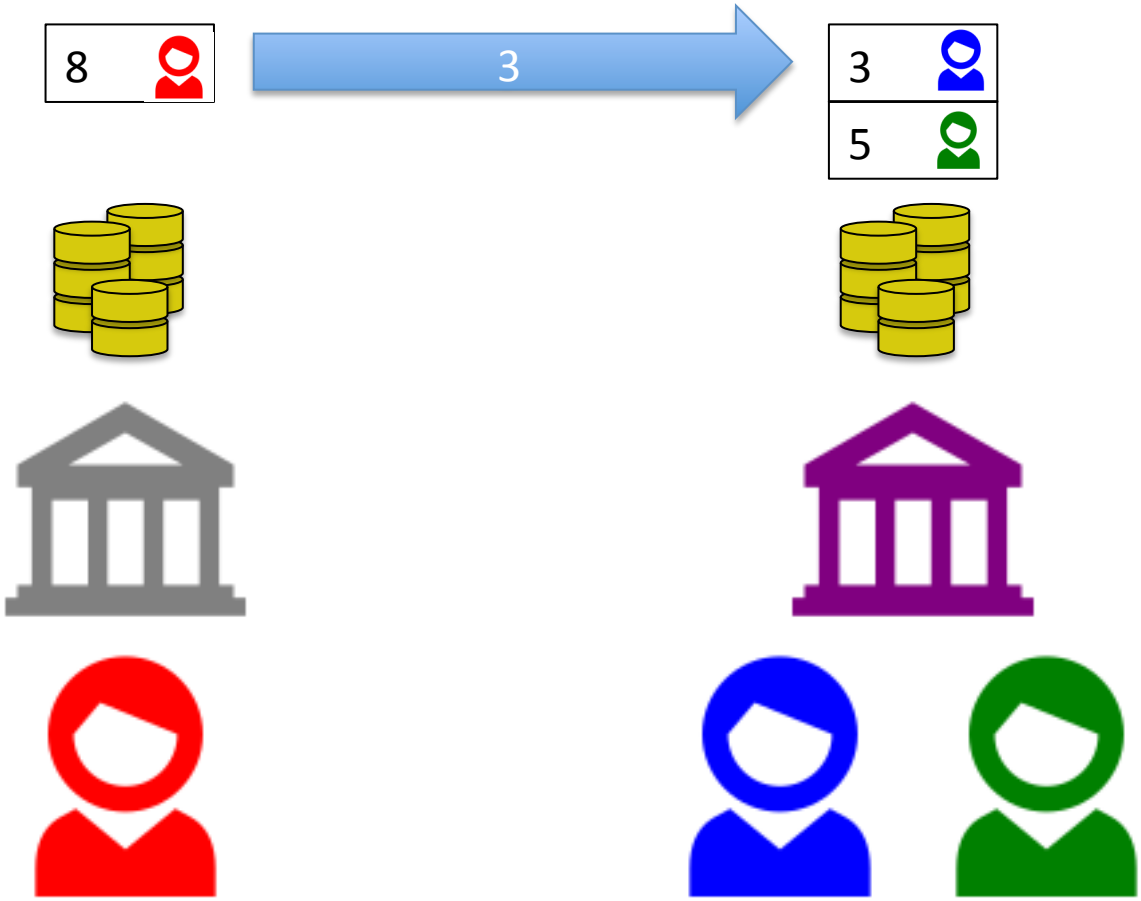
Banking 1.0



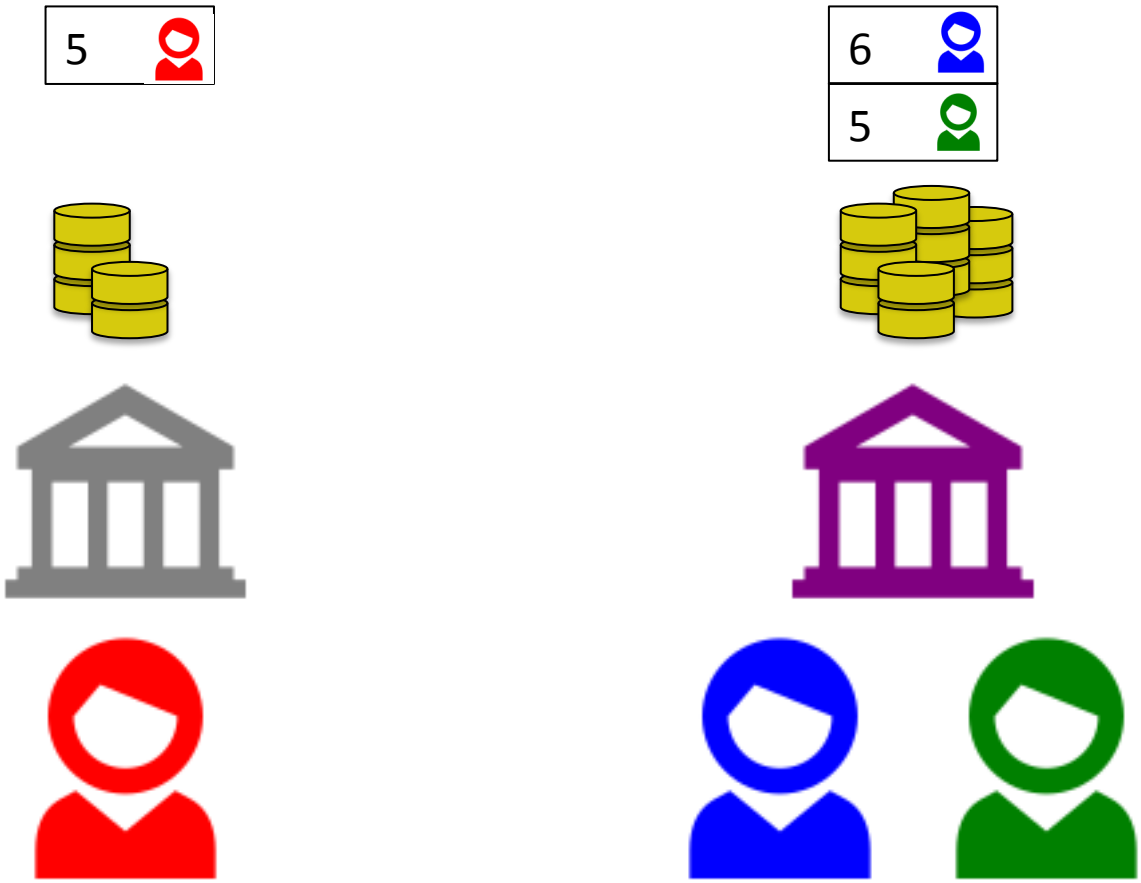
8


"ENTERTAINING AND INFORMATIVE."—THE ECONOMIST
JANE GLEESON-WHITE
DOUBLE ENTRY
HOW THE MERCHANTS OF VENICE CREATED MODERN FINANCE

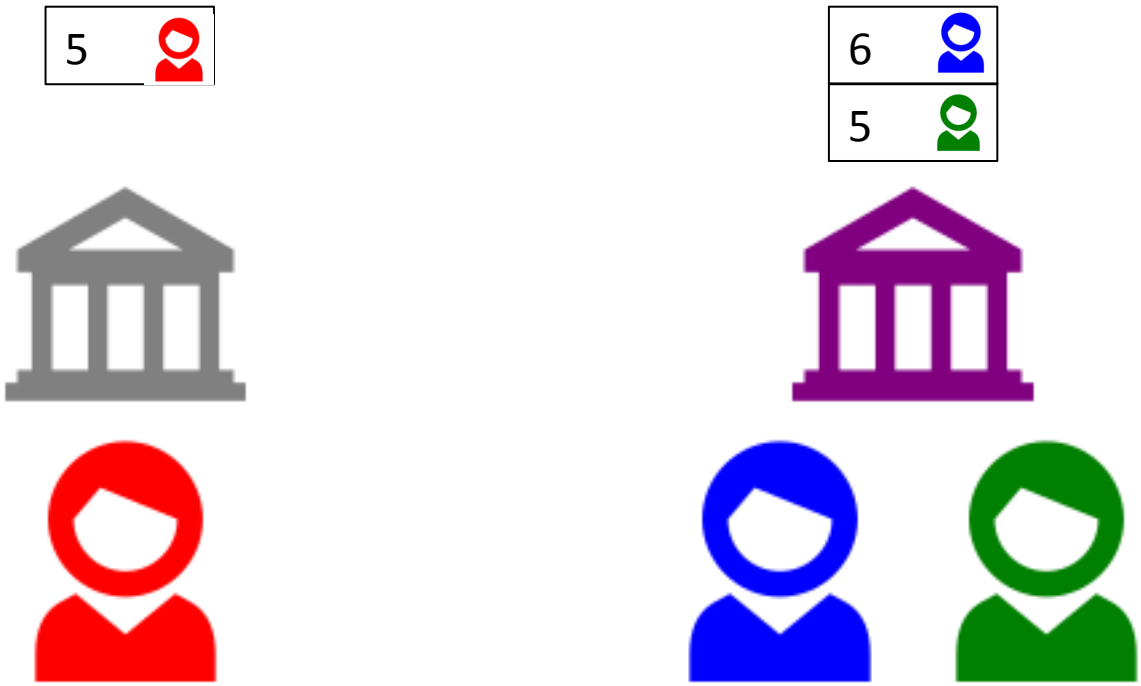
Banking 1.0



Banking 1.0

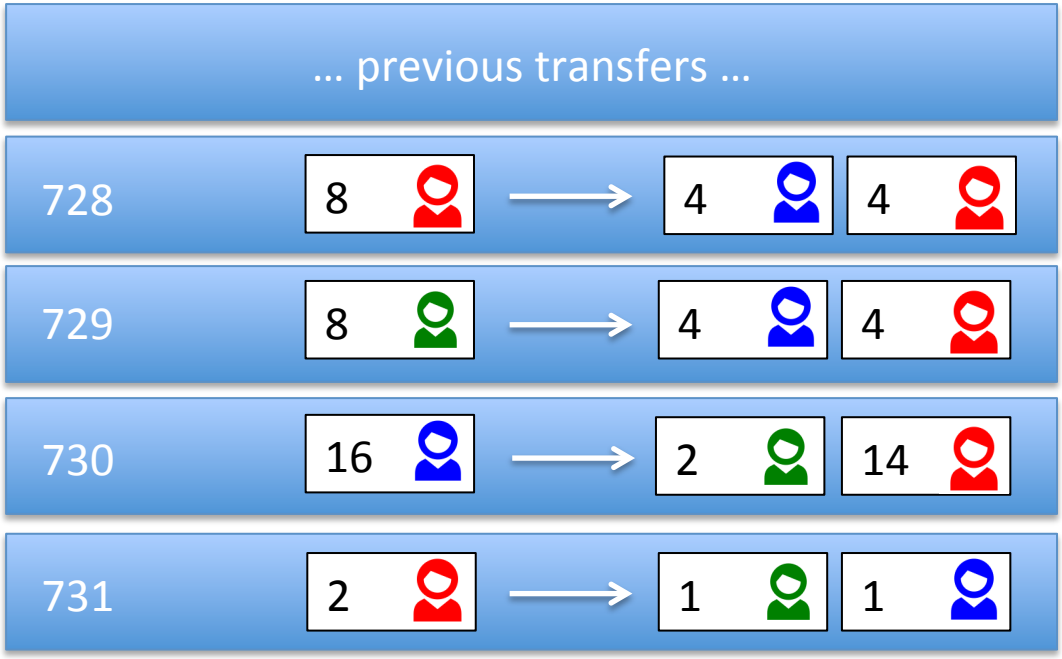


Banking 2.0



Bitcoin: *a ledger of financial transfers?*

Assume all previous transfers leave a balance of 8 for each person

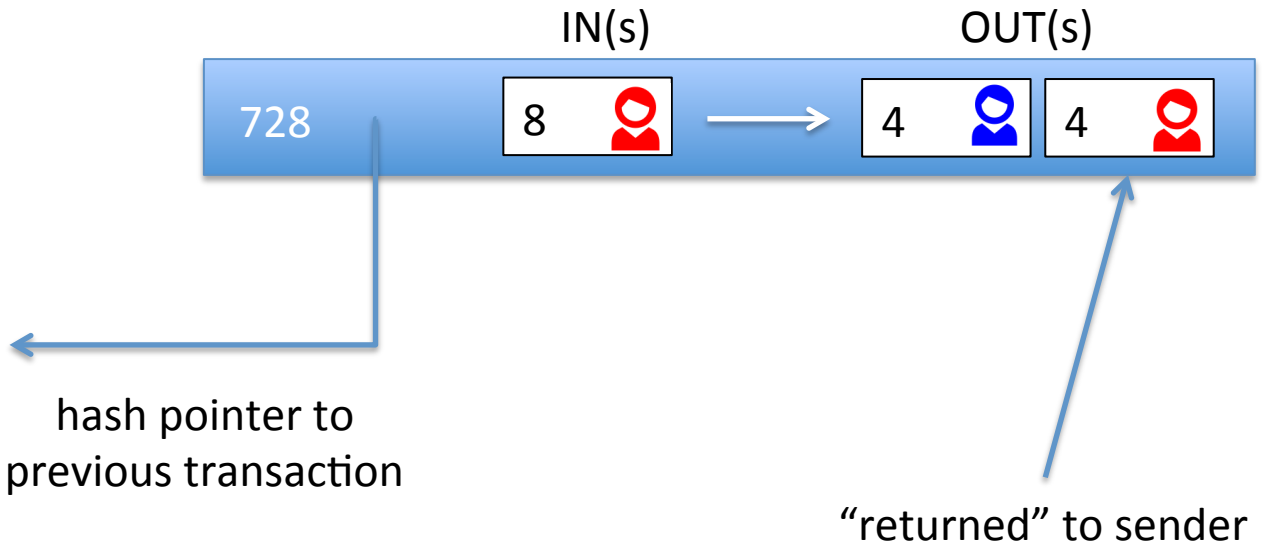


transaction	amounts	RED
		8
728	-8+4	4
729	+4	8
730	+14	22
731	-2	20

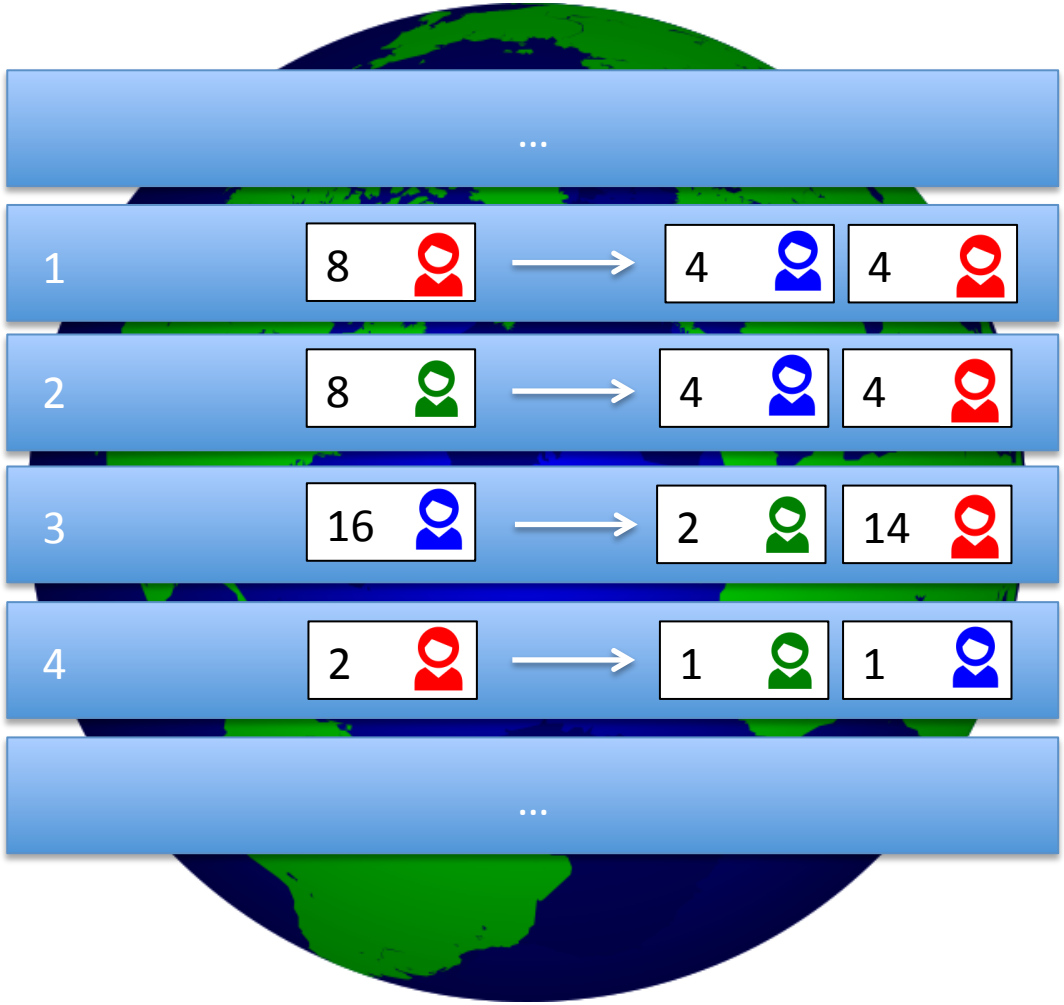
transaction	amounts	BLUE
		8
728	+4	12
729	+4	16
730	-16	0
731	+1	1

transaction	amounts	GREEN
		8
728	0	8
729	-8	0
730	+2	2
731	+1	3

Each transaction: IN = OUT



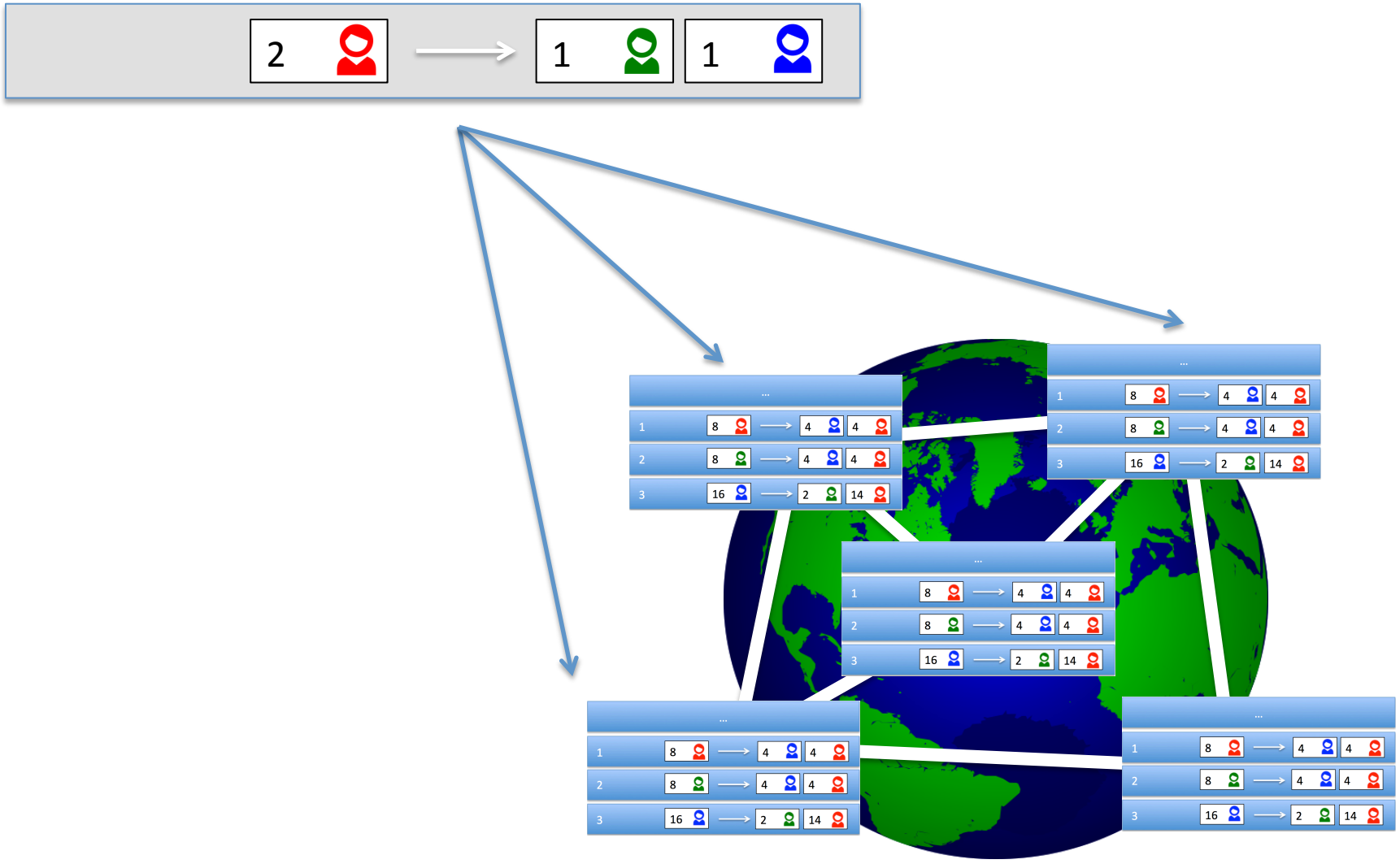
Bitcoin: a *public* ledger of financial *transactions*?



Bitcoin: a decentralized*, public ledger of transactions

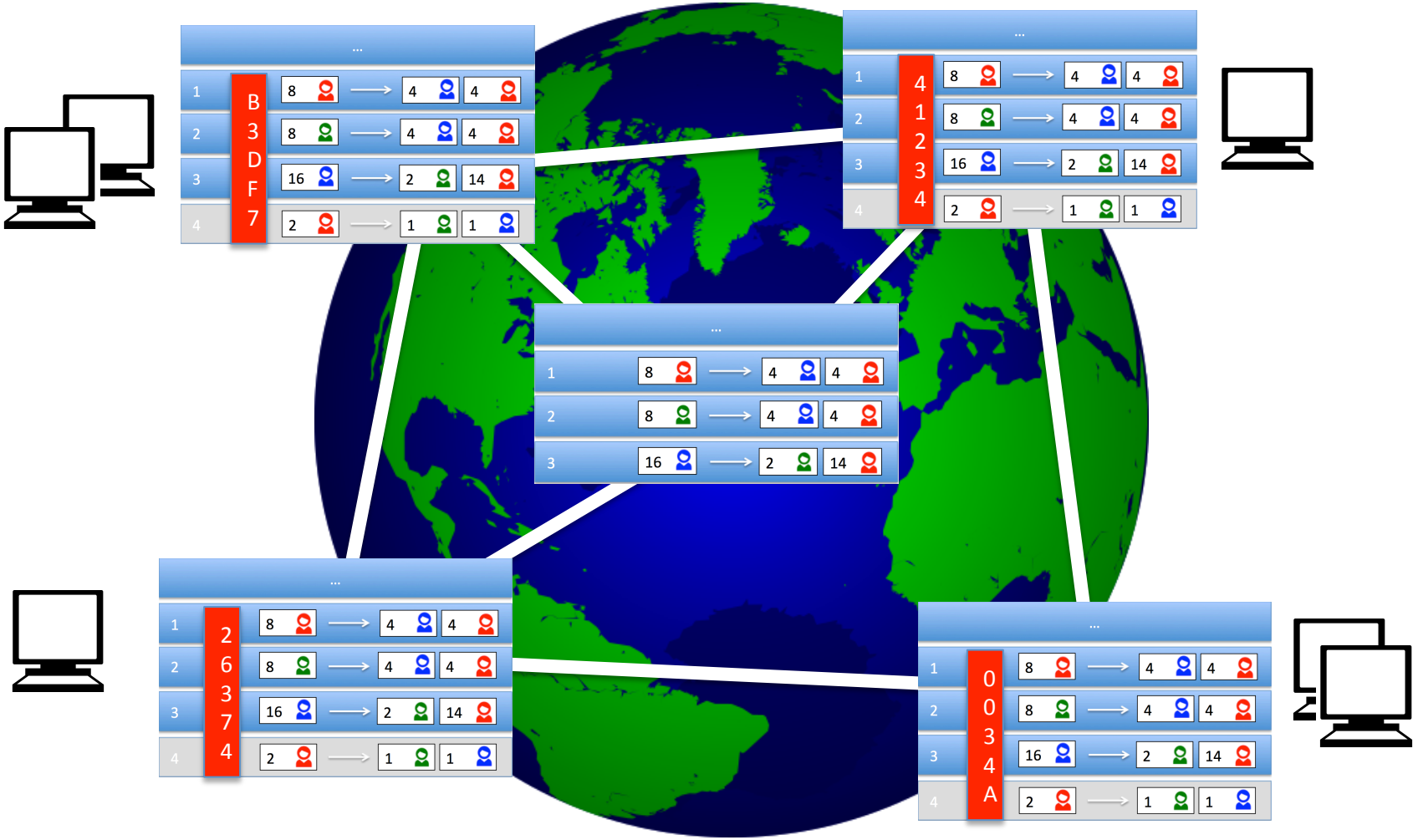
* on a peer-to-peer (p2p) virtual network

Step 1: “broadcast” new transaction to peers



Step 2: append new transaction to next “block”

Step 3: attempt to solve the block nonce puzzle

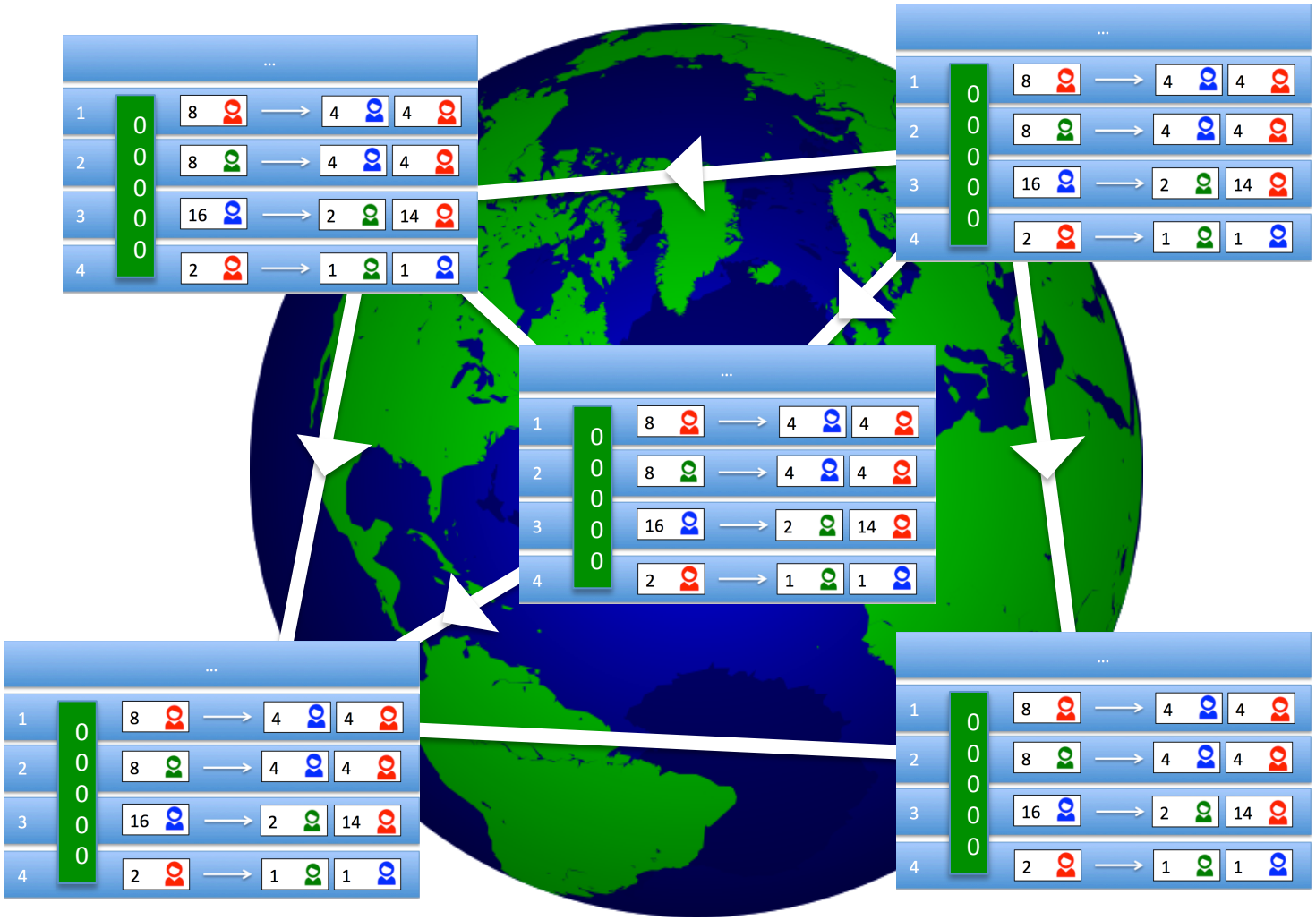


Note: no single entity should own >= 51% of computing cycles

Step 4: solve the block nonce puzzle*

* … and collect a small transaction fee

Step 5: “broadcast” the valid nonce

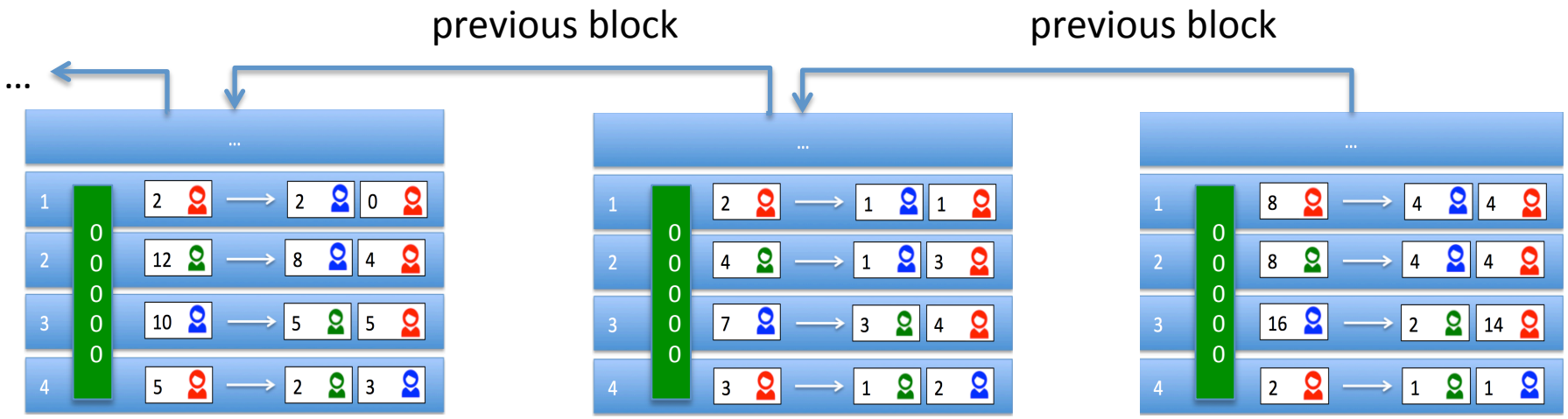


Note: … here be race conditions (and vulnerabilities)

Summary

1. YOU 
   - "Broadcast" new transaction to peers
2. The Bitcoin Network
   - Append new transaction to the next block
   - Attempt to solve the block nonce puzzle
   - Solve the block nonce puzzle
   - "Broadcast" the valid nonce
3. PROFIT! :-)

Blockchain:
latest valid block appended to end of the “chain”

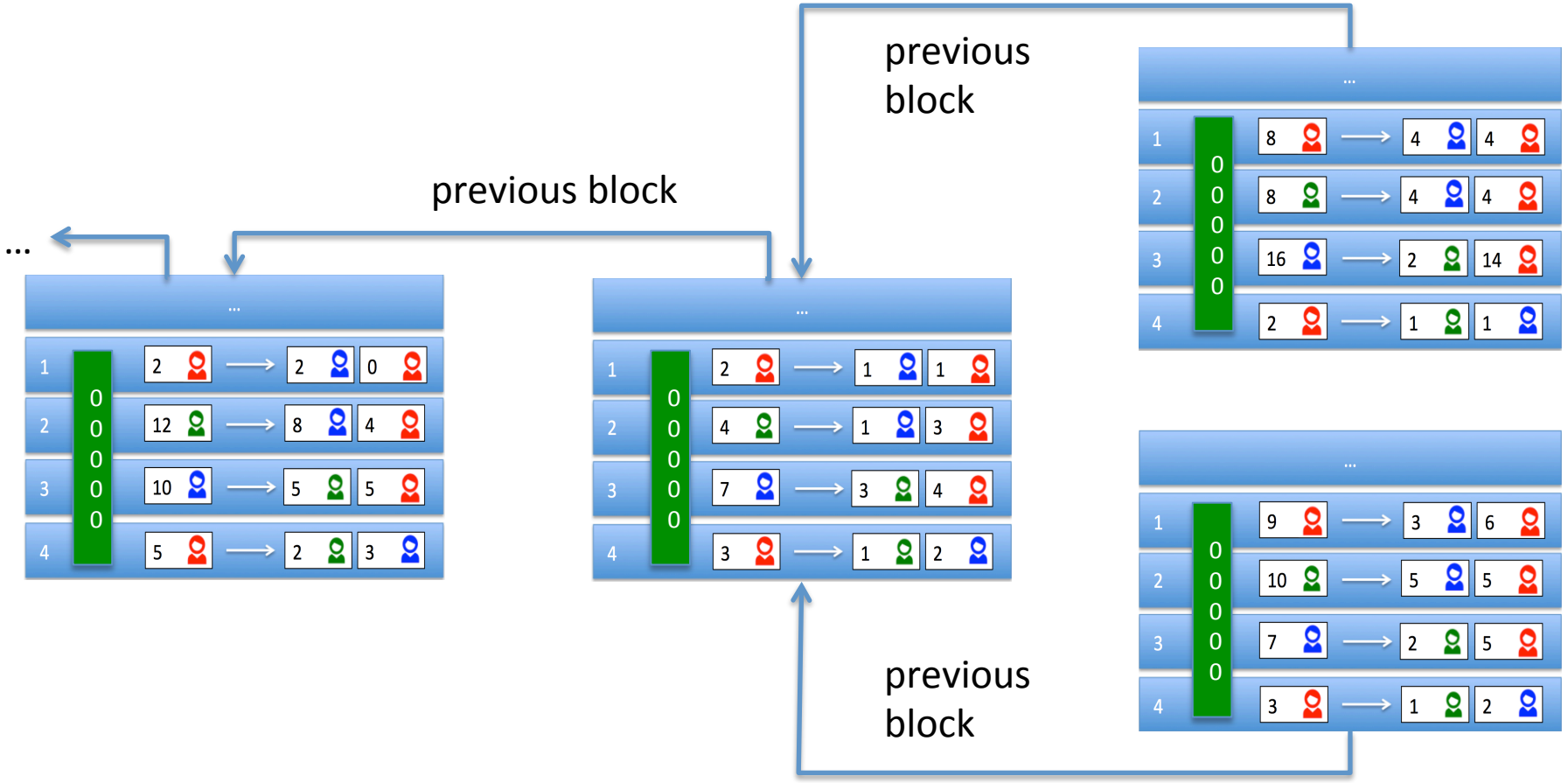


Note: this is a solution for achieving distributed consensus,
but is still vulnerable to various attacks*

* Details of attacks and counter-measures NOT covered in this talk

Blockchain:

latest valid block appended to end of the *longest* “chain”



Blockchain: a generic protocol for transactions

private key: [illegible]
public key: **1CE74**

private key: [illegible]
public key: **EB451**

private key: [illegible]
public key: **88AE7**

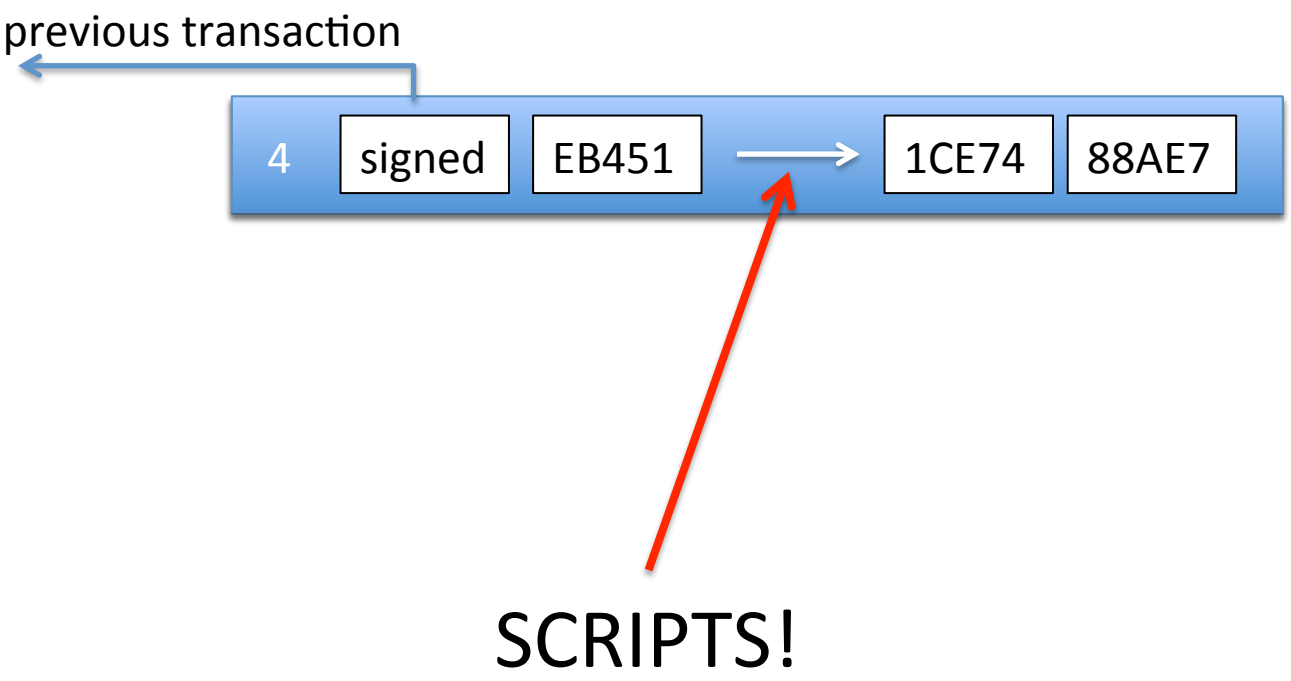
Blockchain: a generic protocol for transactions dependent on public key encryption

private key: [illegible]
public key: **1CE74**

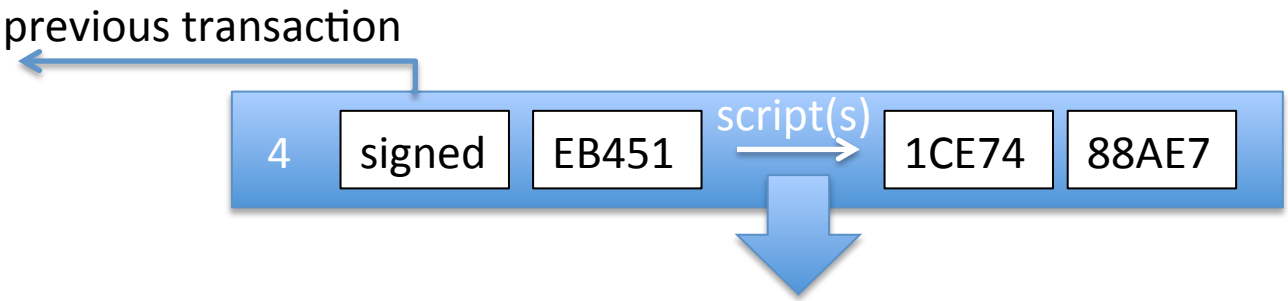
private key: [illegible]
public key: **EB451**

private key: [illegible]
public key: **88AE7**

Note: Here be simplifications…



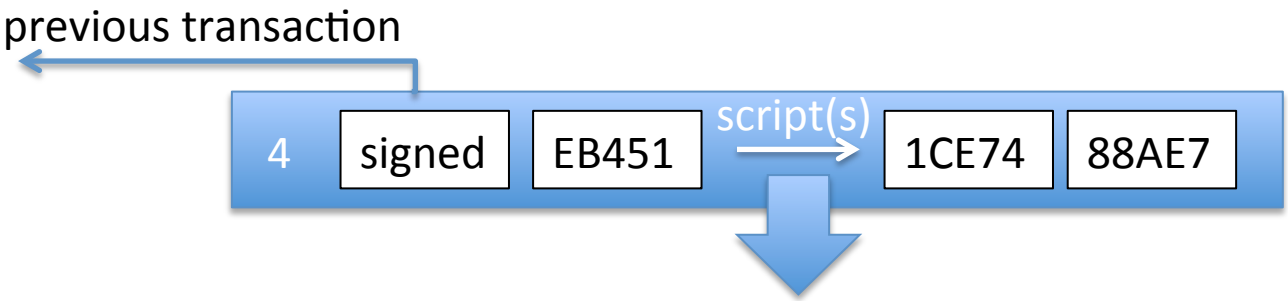
Some standard transaction scripts



Type	Script
Pay to Public Key Hash (P2PKH)	`OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
Pay to Script Hash (P2SH)	`OP_HASH160 <Hash160(redeemScript)> OP_EQUAL`
Multisig	`<m> <A pubkey> [B pubkey] [C pubkey] <n> OP_CHECKMULTISIG`
Null Data	`OP_RETURN <0 to 40 bytes of data>`

BY DESIGN,
the scripting language is **stack-based** and **NOT Turing-complete**
(source: https://bitcoin.org/en/developer-guide)

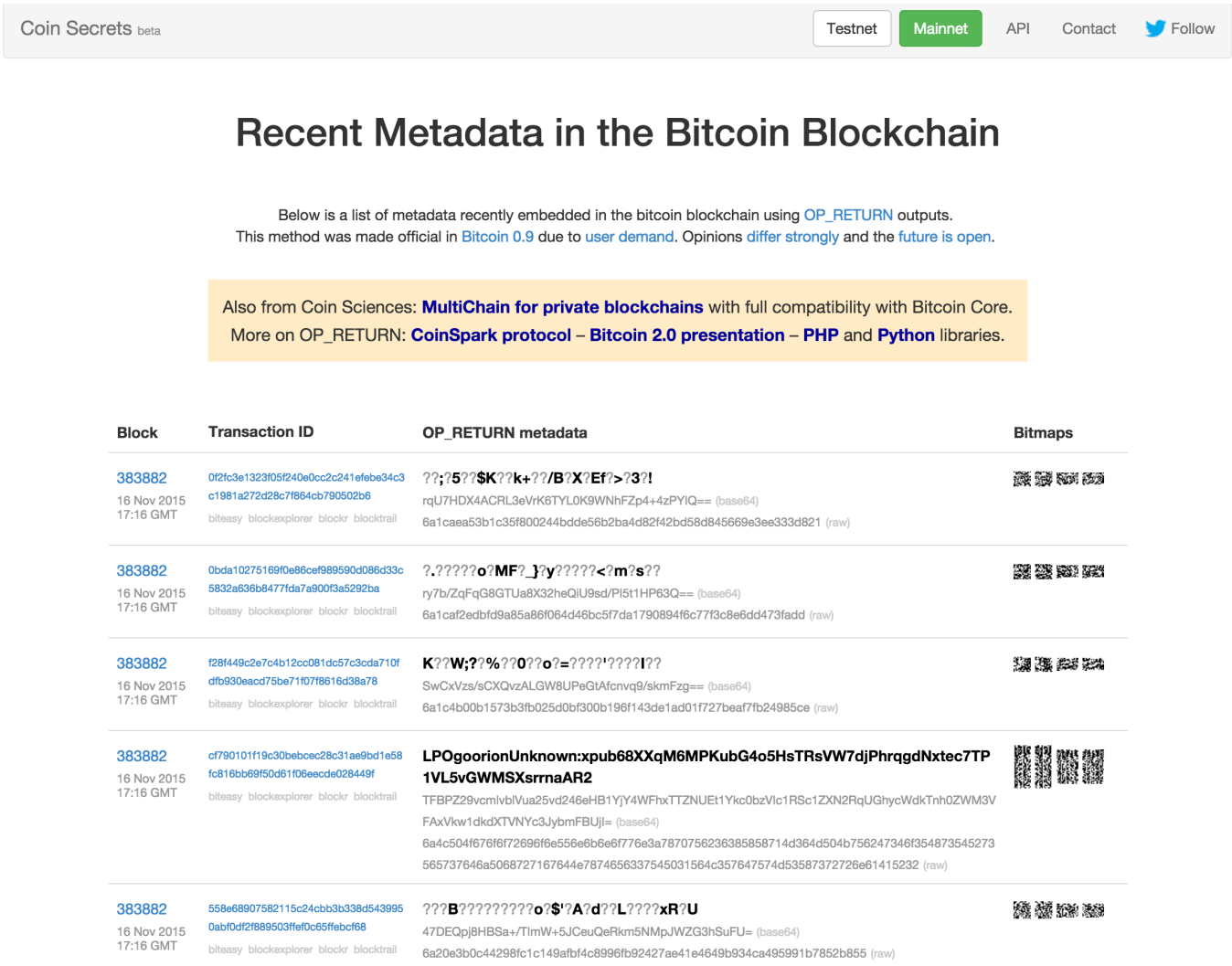
Some standard transaction scripts

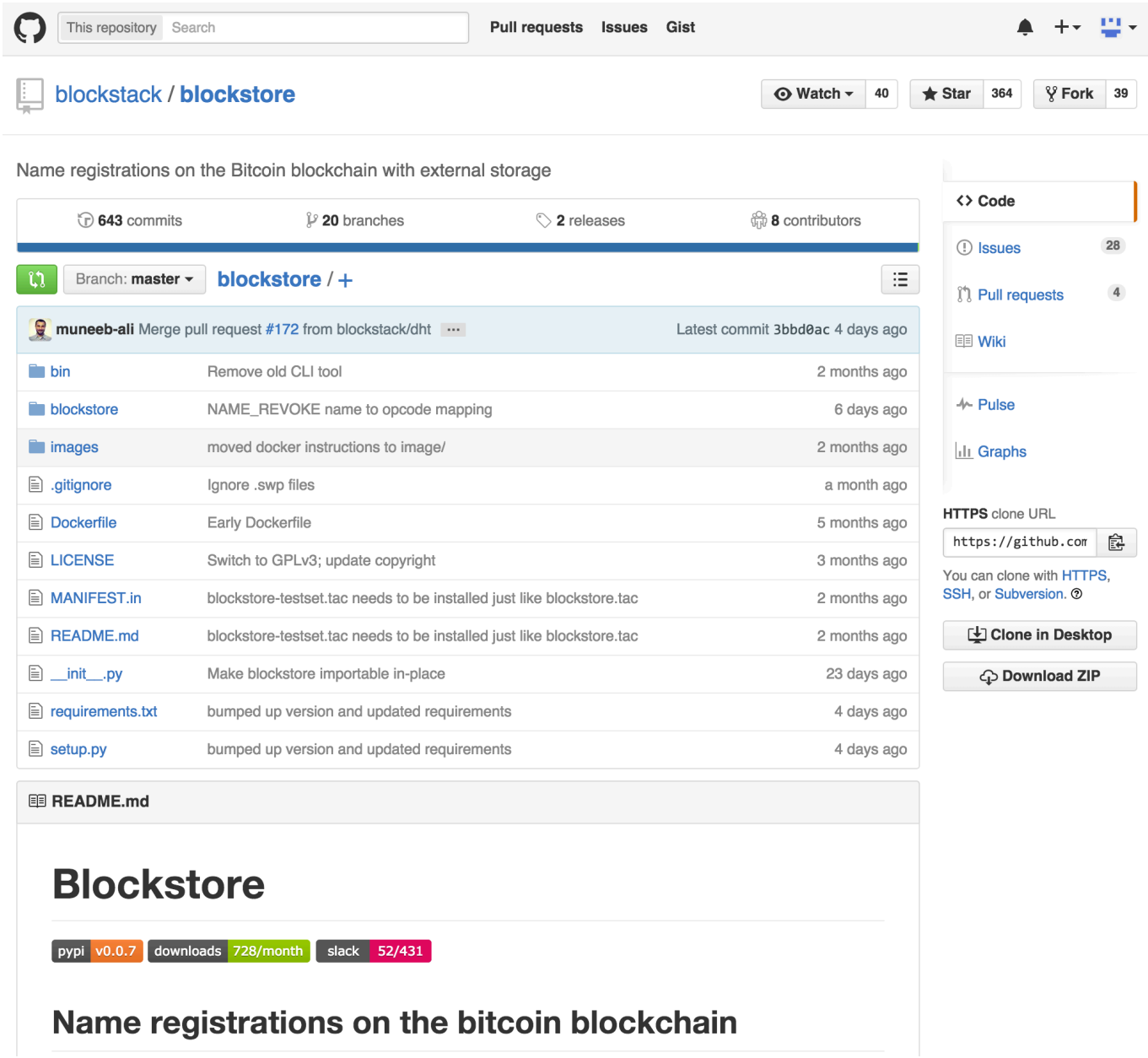


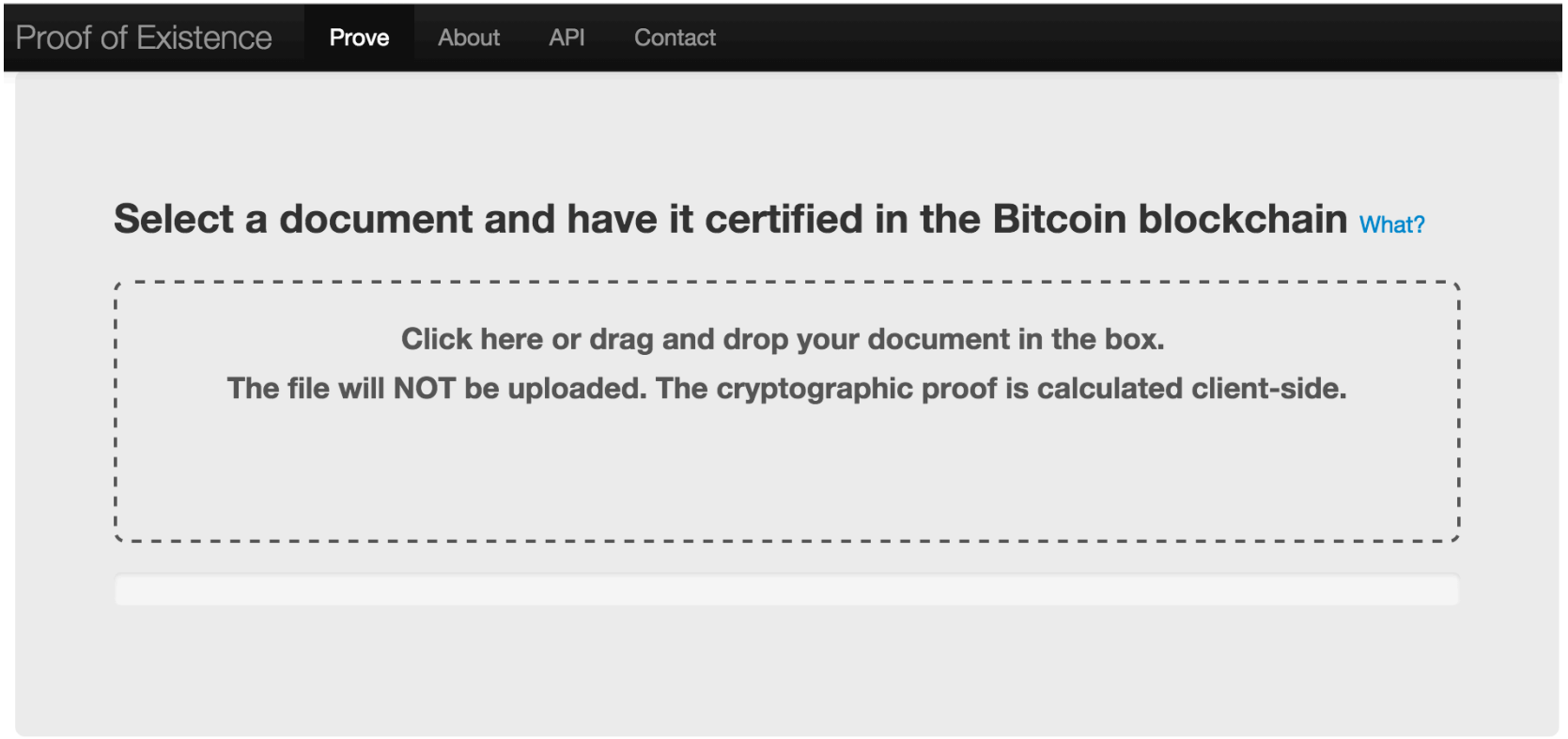
Type	Script
Pay to Public Key Hash (P2PKH)	`OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG`
Pay to Script Hash (P2SH)	`OP_HASH160 <Hash160(redeemScript)> OP_EQUAL`
Multisig	`<m> <A pubkey> [B pubkey] [C pubkey] <n> OP_CHECKMULTISIG`
Null Data	`OP_RETURN <0 to 40 bytes of data>`

BY DESIGN,
the scripting language is **stack-based** and **NOT Turing-complete**
(source: https://bitcoin.org/en/developer-guide)

OP_RETURN:
A decentralized, trusted means to “send” data

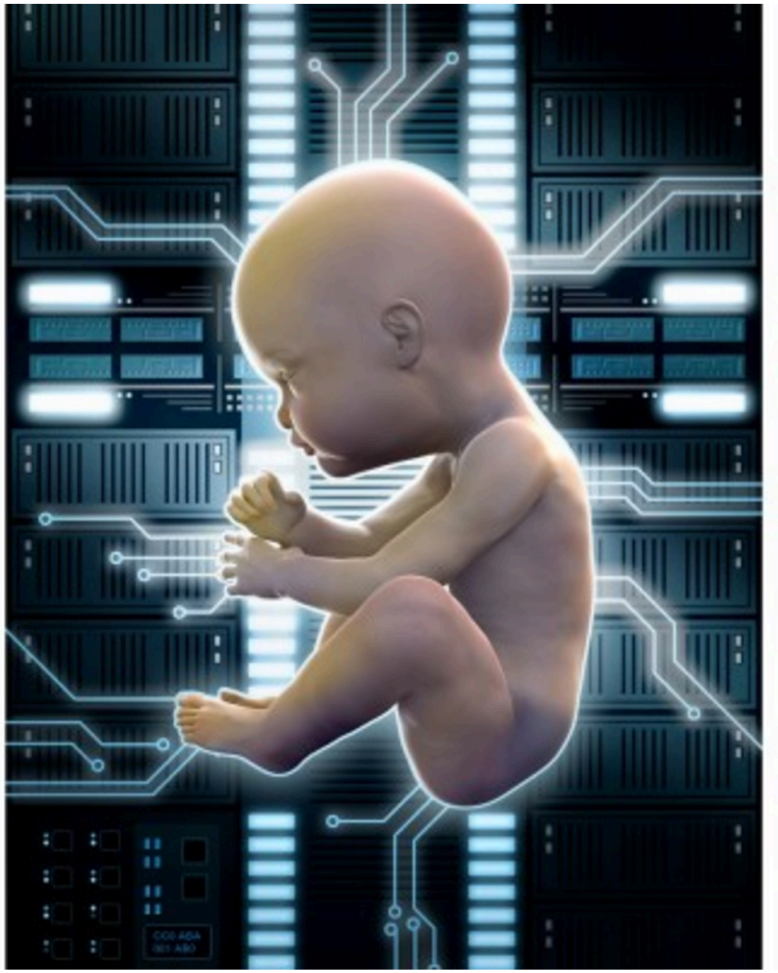



This repository Search
Pull requests Issues Gist
blockstack / blockstore
Watch 40 Star 364 Fork 39
Name registrations on the Bitcoin blockchain with external storage
643 commits 20 branches 2 releases 8 contributors
Branch: master blockstore / +
muneeb-ali Merge pull request #172 from blockstack/dht ··· Latest commit 3bbd0ac 4 days ago
bin Remove old CLI tool 2 months ago
blockstore NAME_REVOKE name to opcode mapping 6 days ago
images moved docker instructions to image/ 2 months ago
.gitignore Ignore .swp files a month ago
Dockerfile Early Dockerfile 5 months ago
LICENSE Switch to GPLv3; update copyright 3 months ago
MANIFEST.in blockstore-testset.tac needs to be installed just like blockstore.tac 2 months ago
README.md blockstore-testset.tac needs to be installed just like blockstore.tac 2 months ago
__init__.py Make blockstore importable in-place 23 days ago
requirements.txt bumped up version and updated requirements 4 days ago
setup.py bumped up version and updated requirements 4 days ago
README.md
Blockstore
pypi v0.0.7 downloads 728/month slack 52/431
Name registrations on the bitcoin blockchain
Code
Issues 28
Pull requests 4
Wiki
Pulse
Graphs
HTTPS clone URL
https://github.com
You can clone with HTTPS, SSH, or Subversion.
Clone in Desktop
Download ZIP



Last documents registered:

Document Digest	Timestamp
c8f1ccebe28241c3a0e746e47ced975a8d1c230cad2e8f4095b88d3cf8a8a61e	2015-11-16 17:21:32
ab80c7bbbaf379557c4684f6cbf9cd4e79f5bd49c3da56ca9fefe4732f43fe71	2015-11-16 17:20:35
ec9e5dc0a93e91ab5ed0679406064c8cbdf52c50b5d74763fe570e9bcb160362	2015-11-16 14:08:33
c2d623cc7ea0094d7b07f1ef7da5ab95189e45ac92b0842aaea9a048d4e84a53	2015-11-16 13:39:44
315f5bdb76d078c43b8ac0064e4a0164612b1fce77c869345bfc94c75894edd3	2015-11-16 13:16:10

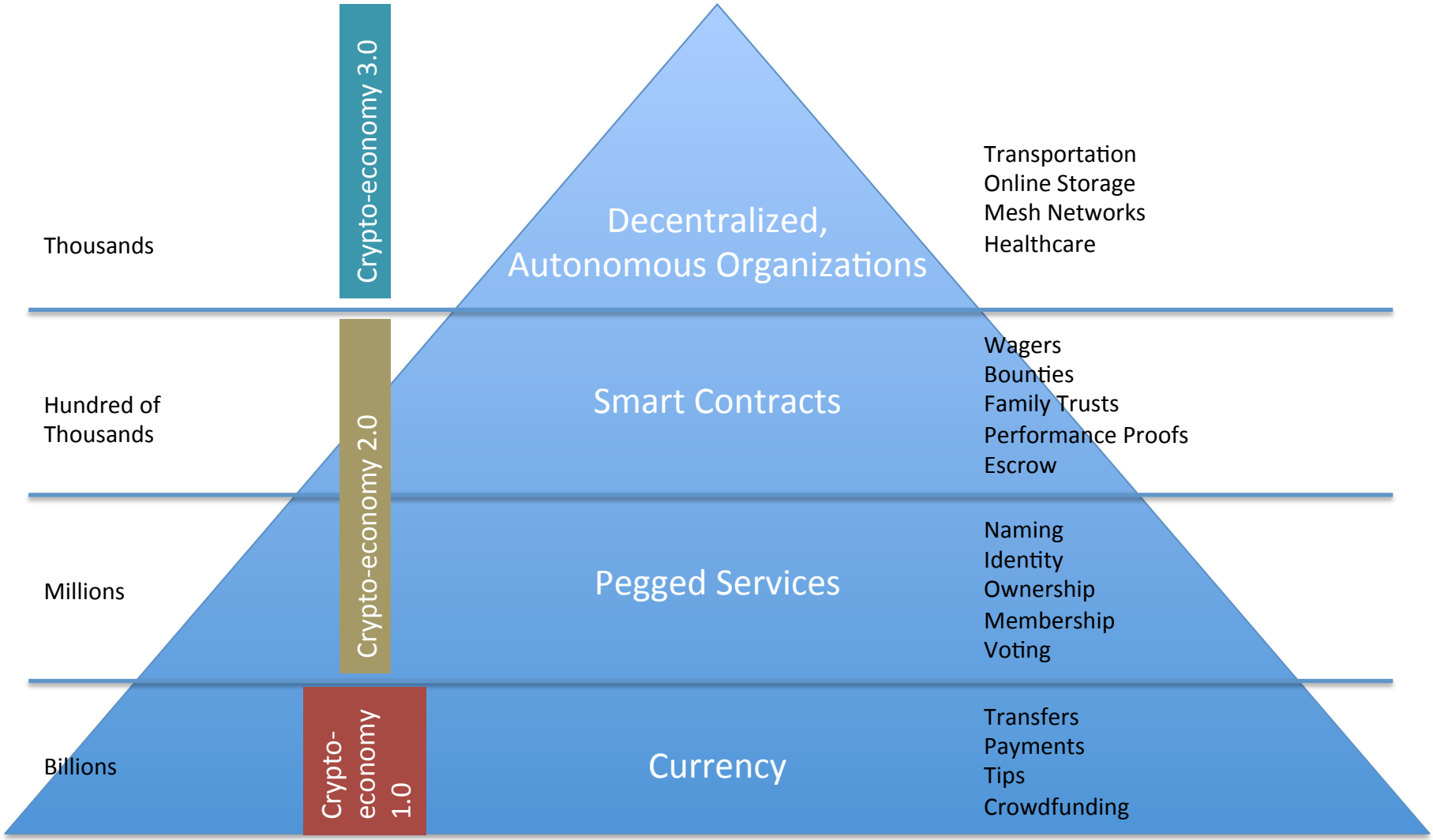


Bitcoin Entrepreneur Registers Birth of Child on the Blockchain

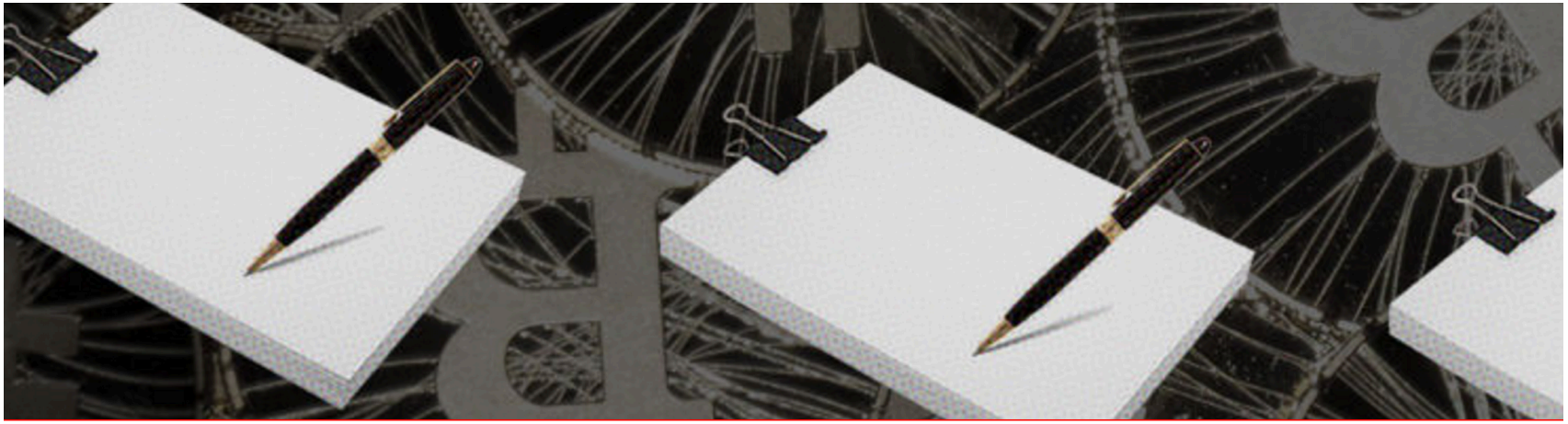
November 14, 2015 | No Comments | 1,567 Views | News | Traderman

Santiago Siri, an entrepreneur and developer based in San Francisco welcomed the birth of his first child named Roma with a proof-of-birth registration on bitcoin's blockchain. Siri used a blockchain verification

Crypto-Currency to Crypto-Economics



Source: Mougayar 2014



2014-09-17
APP ECONOMY

What Are Smart Contracts? Cryptocurrency's Killer App

By giving computers control over contracts, we can make business more efficient and make the legal system more equitable.

By Jay Cassano

9 Notes / 383 Tweet / 356 Like

This article contains interviews with Phil Raporport, drector of markets and trading at Ripple Labs, Stefan Thomas, CTO at Ripple Labs, and Chris Ellis, a cofounder of Feathercoin and show host with World Crypto Network.

What if you could cut your mortgage rate, make it easier to update your will, and ensure that your buddy was never able to weasel out of paying up on a bet? That and much more is the promise of smart contracts, a technology that is getting closer and closer to reality thanks to cryptocurrency.

Smart contracts are computer programs that can automatically execute the terms of a contract. Someday, these programs may replace lawyers and banks for handling certain common financial transactions.

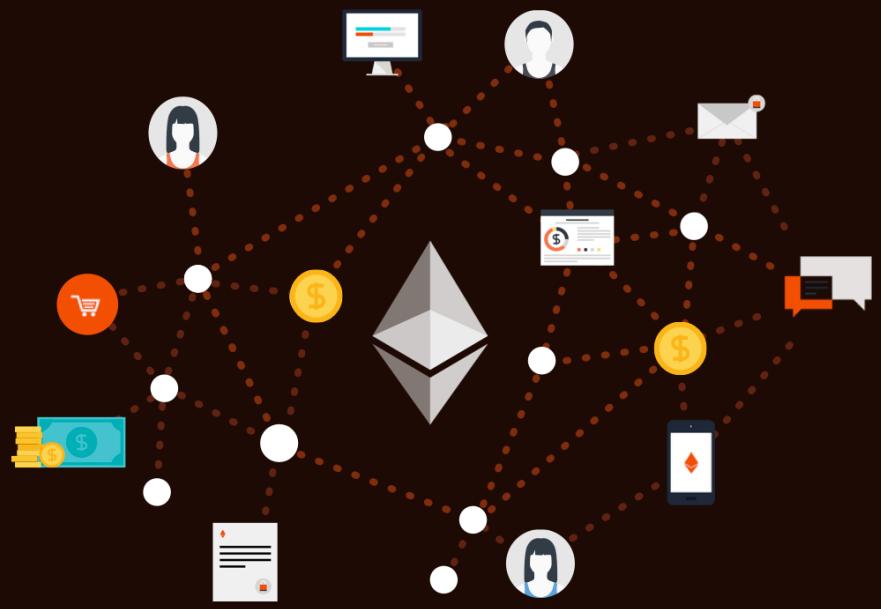
And the potential for smart contracts goes way beyond simple transfers of funds. The door of a car or a house could be unlocked by connecting smart contracts to the Internet of everything. But as always with this cutting edge of financial technology, major

WHAT IS ETHEREUM?

Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference.

Ethereum is how the Internet was supposed to work.

Ethereum was crowdfunded during August 2014 by fans all around the world. It is developed by ETHDEV with contributions from great minds across the globe.



Console: Geth

```
> listProposal(42)
Proposal #42 Send 100 ether to “Bob” for “Website Design”. 4 votes
for, 2 against, 6 hours remaining.
> MyVote = Against
> MyOwnDemocracy.vote.sendTransaction(42, MyVote, {from: me}) |
```

WHAT IS THE FRONTIER RELEASE?

Frontier is the first release of the Ethereum project, tailored specifically for developers. It’s a command line only interface with a Javascript environment that allows building, testing, deploying and using decentralized applications on the Ethereum blockchain.

Exploring the Frontier presents vast opportunities, but also many dangers, and is not for everyone.

Smart Property in Action

by Andrew Wagner

4:48 PM EDT
August 14th, 2014

Smart property is to deeds as Bitcoin is to money. In the same way that Bitcoin revolutionized the concept of currency, smart property revolutionizes the concept of ownership, removing the need for a central authority to say who owns what. Our system of ownership is just one in a growing line of things to be decentralized, but will inevitably be among the most important. The question is, how can we enforce such a system without the firepower backing modern courts?

For those of you still trying to grasp this idea, it's helpful to remember that bitcoins are not actually things: Bitcoin is a decentralized system for deciding who

The Latest


Bitcoin Researcher Has Bitcoins Stolen From Private Key on Shirt

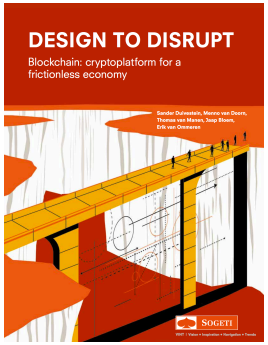

Three Startups Trying to Transform the Music Industry Using the Blockchain


How Prediction Markets Could Guide Bitcoin's Future


Microsoft Launches

Pros and Cons

Source:



Pro	Con
Freedom of payment	Limited adoption
Extremely low fees	High value volatility
Micropayments are going without a hitch	Still a bit shaky and unfinished
Transparent and neutral	Facilitates illegal and dubious practices
Banking the unbanked	No recourse to authority
Protection and control	Coins can be stolen
Lower risk for sellers	A new and unfamiliar form of supervision


"Bitcoin...Stay away from it. It's a mirage, basically..." Warren Buffet
"It will be everywhere and the world will have to readjust", John McAfee
"I'm a big fan of Bitcoin ... Regulation of money supply needs to be depoliticized." Al Gore
"You need to be really rich, really idealistic, or really crazy to invest in Bitcoin", Andrew Couts
"I want Bitcoin to die in a fire", Charlie Stross
"Bitcoin is a technological tour de force." Bill Gates
"Bitcoin is the beginning of something great: a currency without a government, something necessary and imperative." Nassim Nicholas Taleb
"Bitcoin Is Evil", Paul Krugman

Final notes: bumps in the road ahead

- Told to Richard Feynman by a Buddhist monk:

  "*To every man is given the key to the gates of heaven; the same key opens the gates of hell*"

- Existing and Undiscovered Vulnerabilities
  - 51% rule
  - Zero-day attacks?
  - Wallet security problems
- Slow Performance
  - Slow: minutes-to-hours per transaction
  - When to assume a transaction is "valid"?
    - Rule of thumb: after 6 blocks
- The future
  - Lots of Fear-Uncertainty & Doubt (FUD)
  - … but one thing is for certain: Blockchain is here to stay

Nasdaq says to develop blockchain services in Estonia

NEW YORK | BY JOHN MCCRANK

A Bitcoin logo is displayed at the Bitcoin Center New York City in New York's financial district July 28, 2015.
REUTERS/BRENDAN MCDERMID

Exchange and clearing house operator Nasdaq Inc plans to develop several applications for blockchain, the technology underpinning the digital currency bitcoin, using its Estonian settling and clearing business, a senior Nasdaq executive said on Friday.

Credits

- Noun Project icons
  - Iceberg by Florent from the Noun Project
  - Cow by Chris Pyper from the Noun Project
  - Chicken by Verena Gutentag from the Noun Project
  - Pig by Ealancheliyan from the Noun Project
- Bitcoin quotes image from “Block Chain 2.0: The Renaissance of Money”, Wired, January 2015
- Duivestein, Sander, et al., “Design to Disrupt… Blockchain: cryptoplatform for a frictionless economy”, Sogeti, 2015
- NASDAQ to develop blockchain services in Estonia, Reuters (Brendan McDermid)