RSAConference2018
San Francisco | April 16 – 20 | Moscone Center

SESSION ID: IDY-R14

THE LONG ROAD TO IDENTITY ON THE BLOCKCHAIN

Steve Wilson

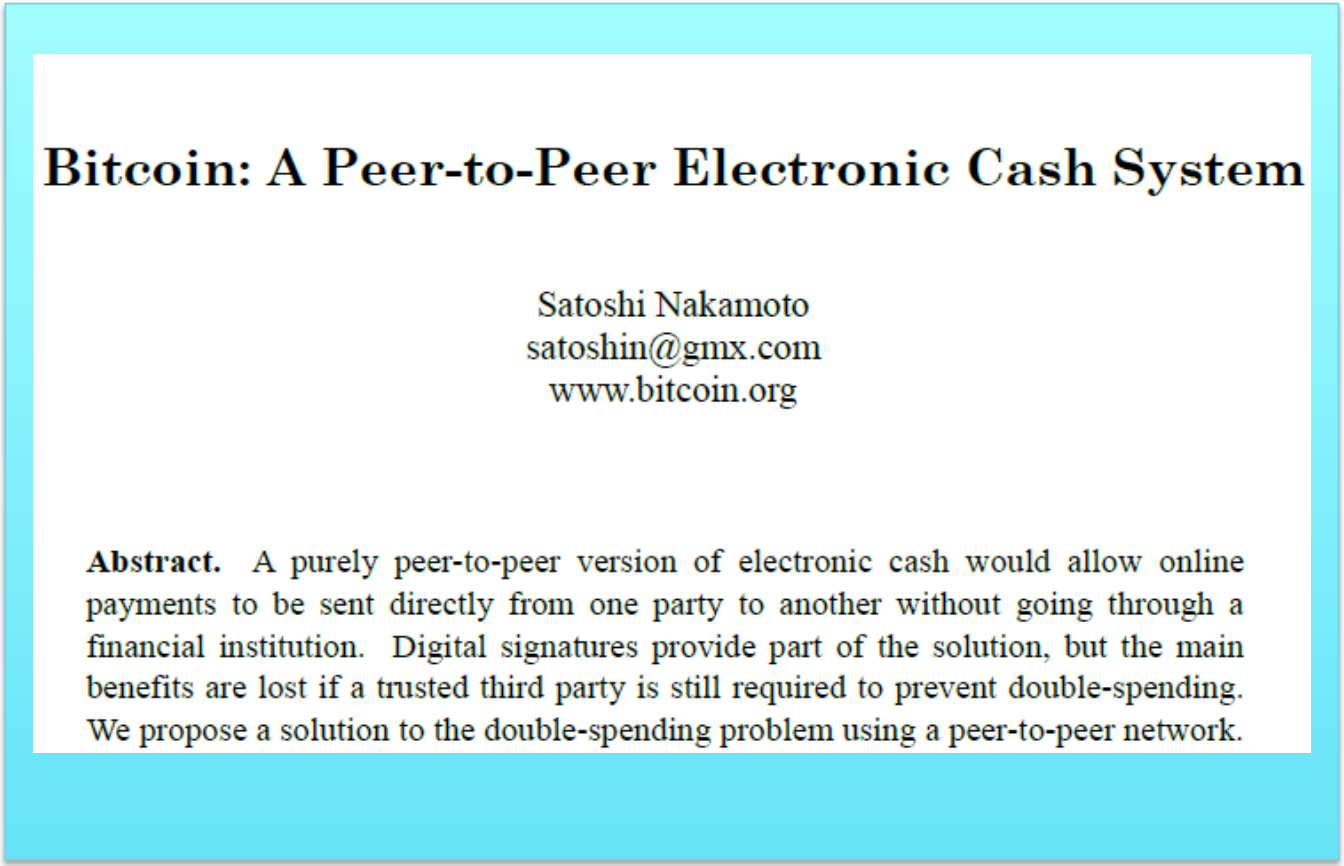
Vice President and Principal Analyst
Constellation Research
@Steve_Lockstep

November 2008

An obscure paper appeared

November 2008

An obscure paper appeared



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.

November 2008

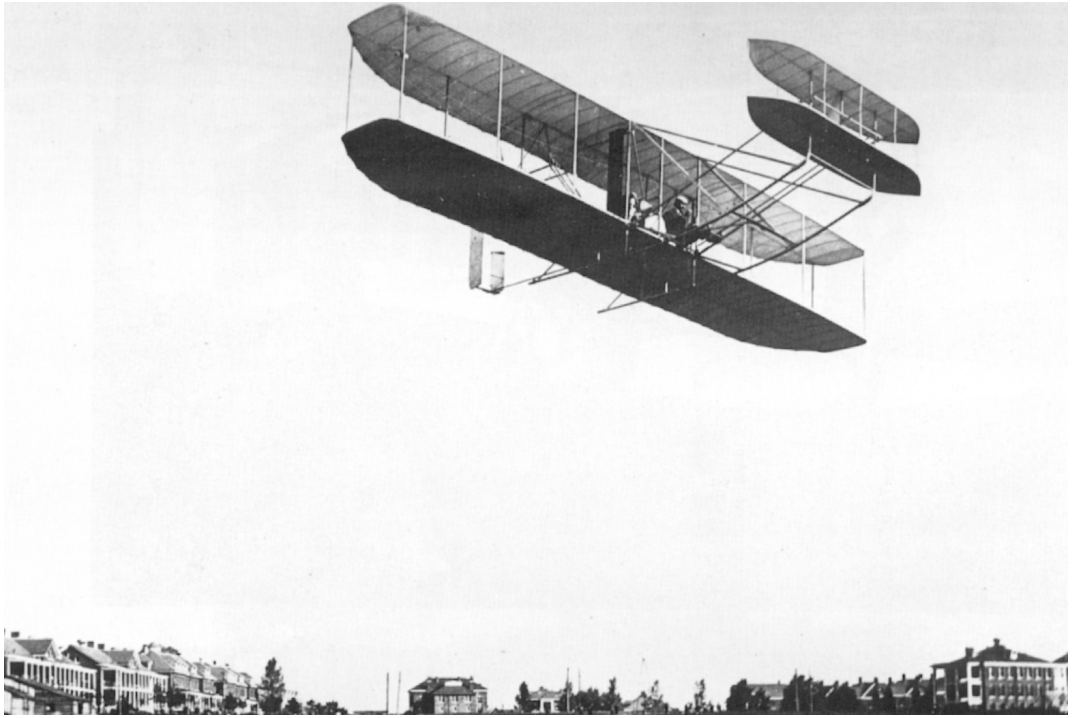
An obscure paper appeared

Bitcoin: A Peer-to-Peer Electronic Cash System

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

We propose a solution to the double-spending problem using a peer-to-peer network.

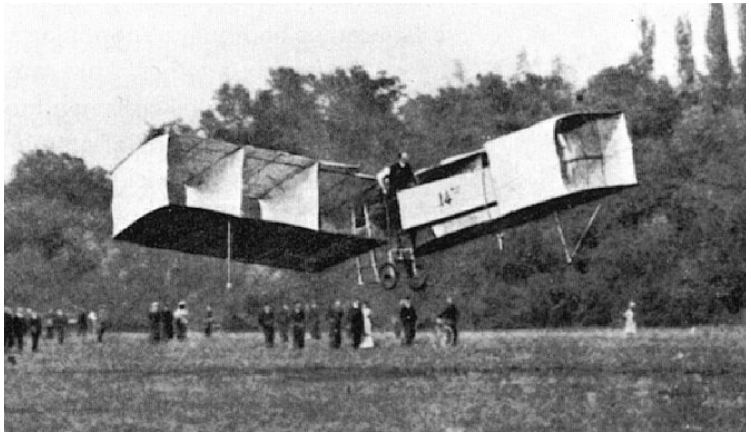
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

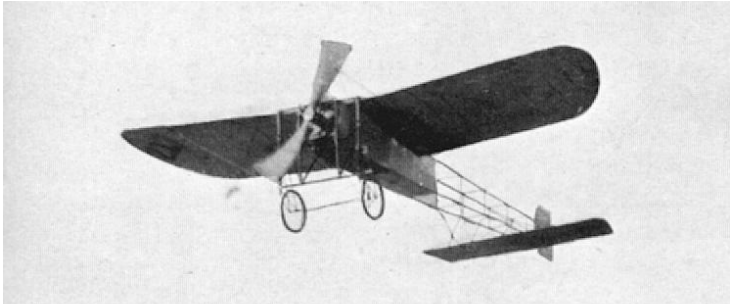


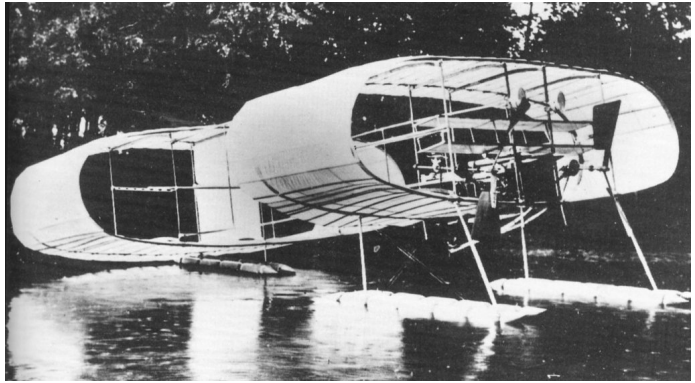
1903

1903-13

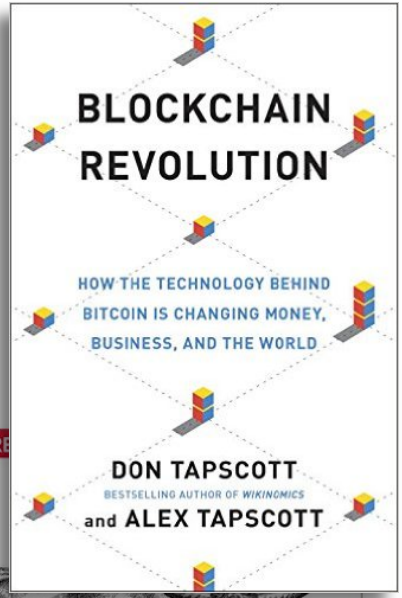
Second mover advantage?



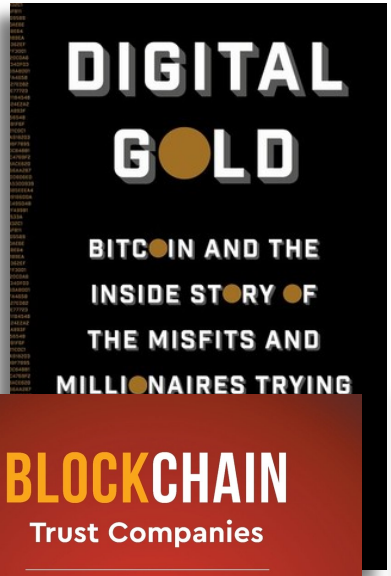


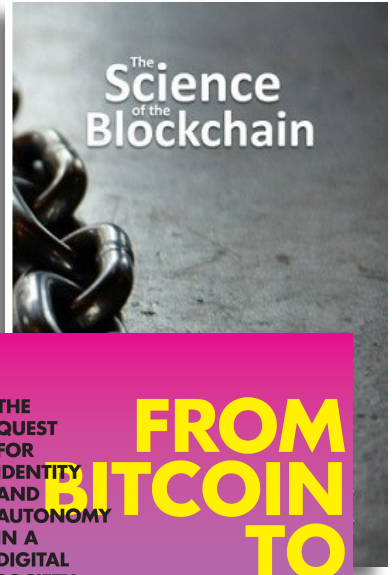


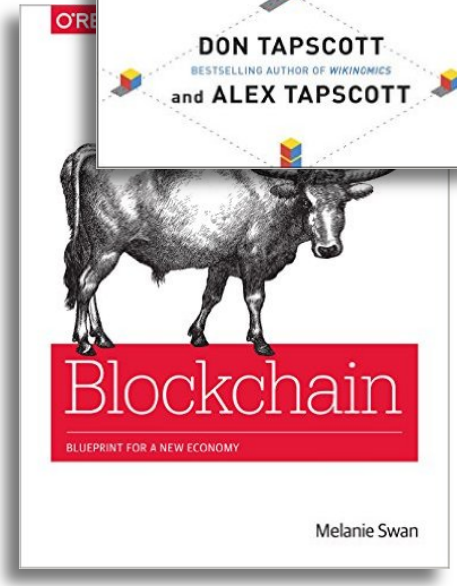
Ref: “Landing without crashing”, http://www.wright-brothers.org

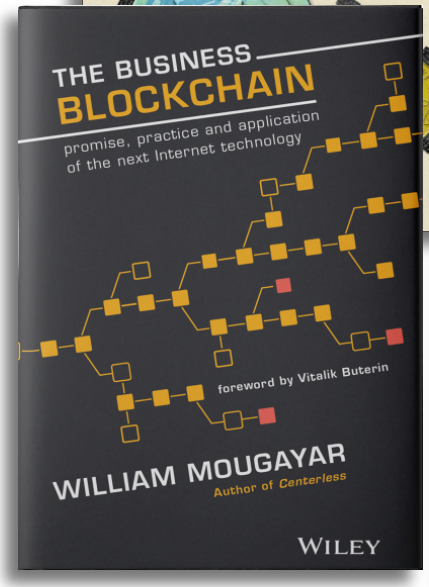

BLOCKCHAIN
REVOLUTION
HOW THE TECHNOLOGY BEHIND
BITCOIN IS CHANGING MONEY,
BUSINESS, AND THE WORLD
DON TAPSCOTT
BESTSELLING AUTHOR OF WIKINOMICS
and ALEX TAPSCOTT

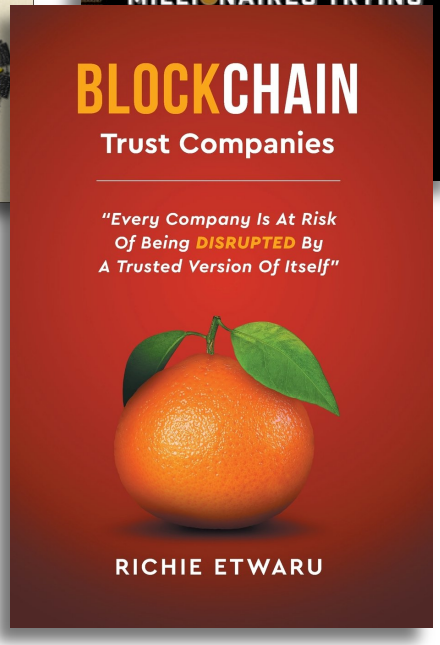

INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA
The Economist
007 and the spectre of Britain's past
Turkey votes to the sound of bombs
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
The trust machine
How the technology behind bitcoin
could change the world

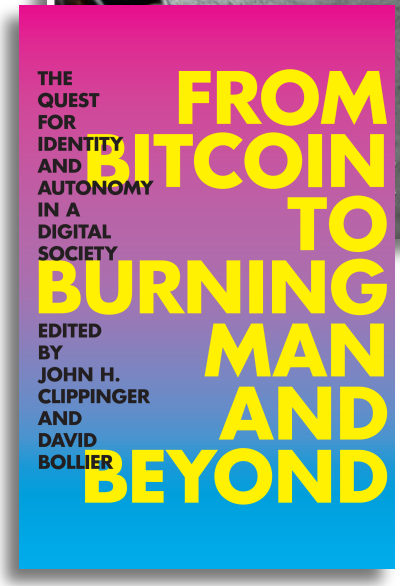

DIGITAL
GOLD
BITCOIN AND THE
INSIDE STORY OF
THE MISFITS AND
MILLIONAIRES TRYING


The Science of the Blockchain


Blockchain
BLUEPRINT FOR A NEW ECONOMY
Melanie Swan


THE BUSINESS
BLOCKCHAIN
promise, practice and application
of the next Internet technology
foreword by Vitalik Buterin
WILLIAM MOUGAYAR
Author of Centerless
WILEY


BLOCKCHAIN
Trust Companies
"Every Company Is At Risk
Of Being DISRUPTED By
A Trusted Version Of Itself"
RICHIE ETWARU


THE
QUEST
FOR
IDENTITY
AND
AUTONOMY
IN A
DIGITAL
SOCIETY
EDITED
BY
JOHN H.
CLIPPINGER
AND
DAVID
BOLLIER
FROM
BITCOIN
TO
BURNING
MAN
AND
BEYOND

November 2008

An obscure paper appeared

Bitcoin: A Peer-to-Peer Electronic Cash System

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

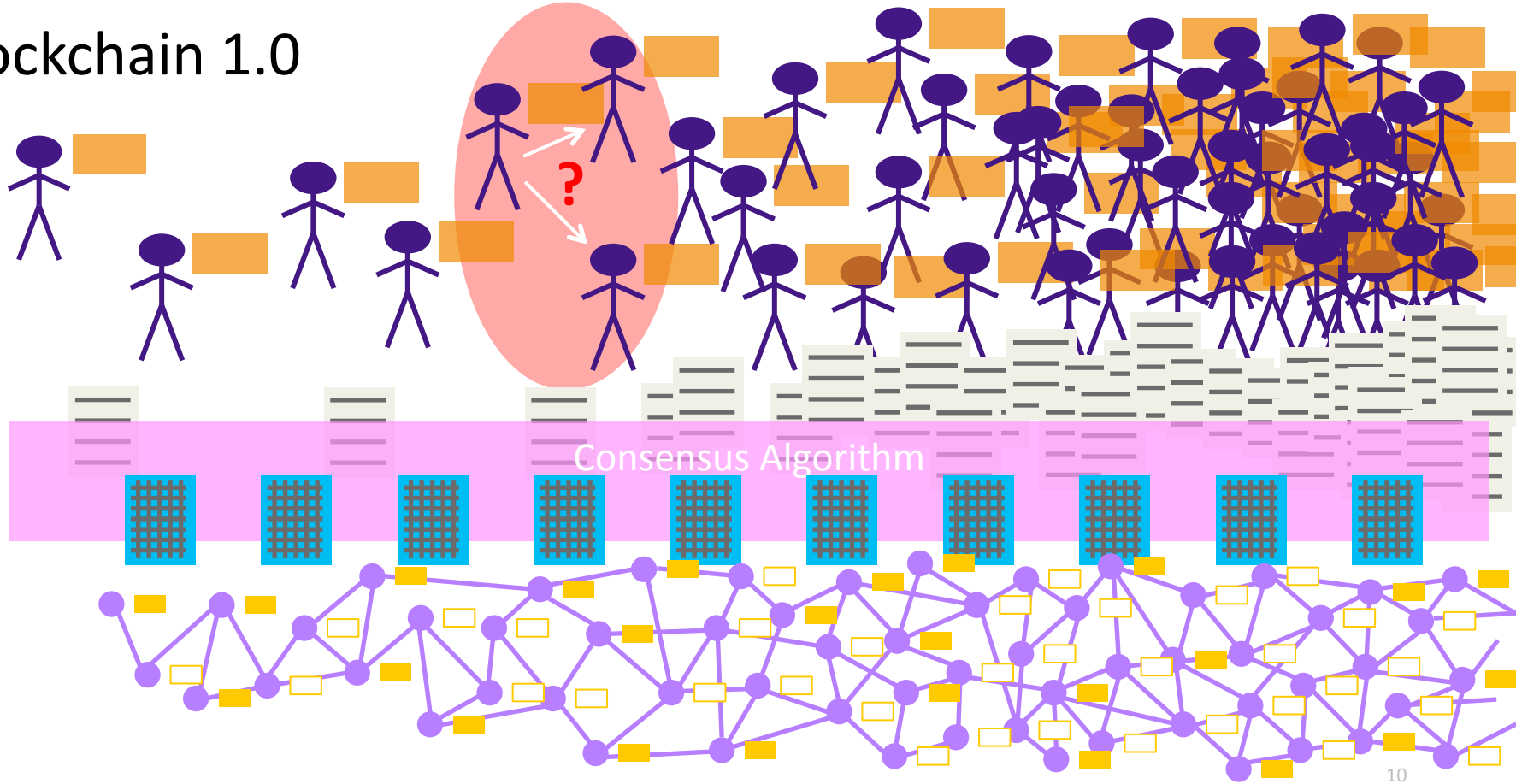
benefits are lost if a trusted third party is still required

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.

Any sufficiently advanced technology is indistinguishable from magic.

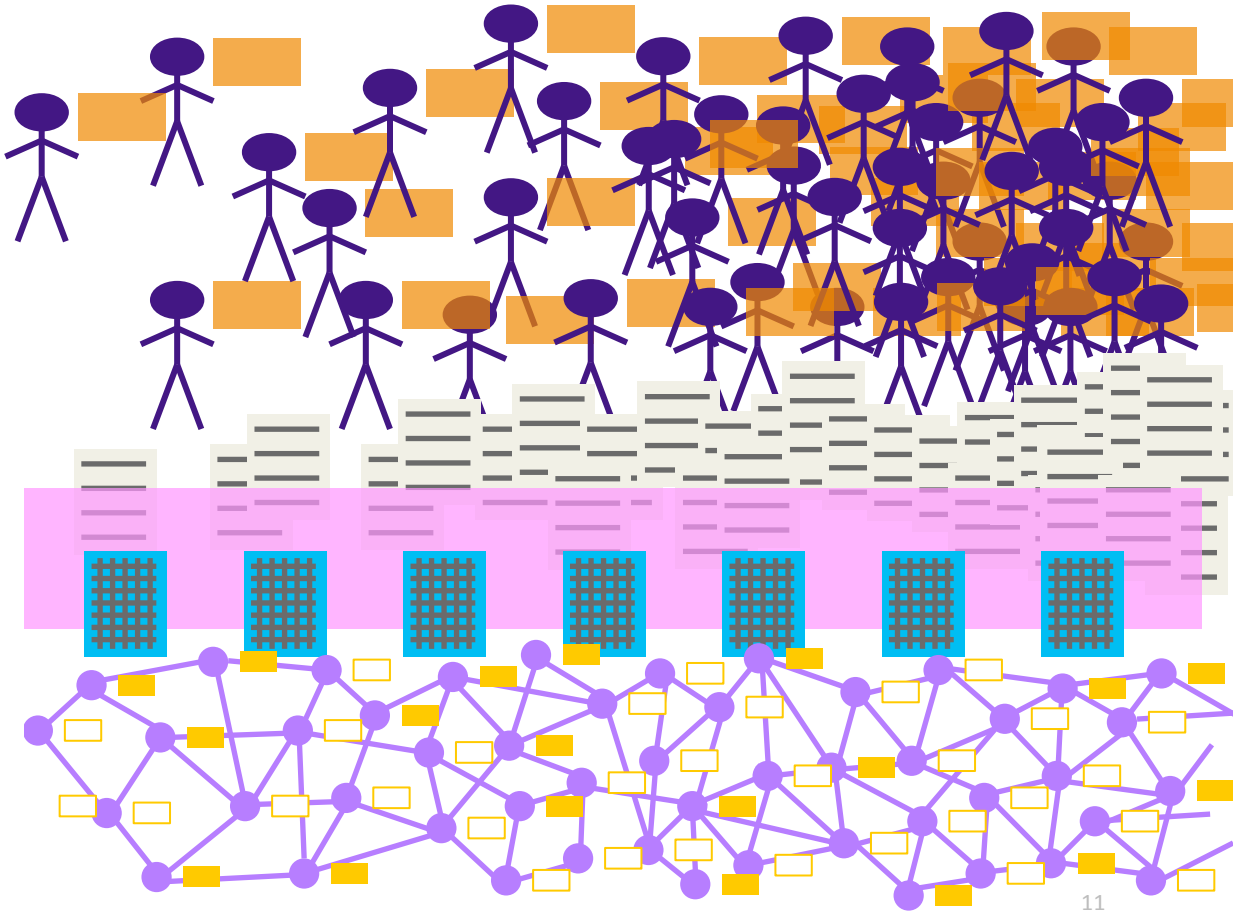
Arthur C. Clarke

Blockchain 1.0



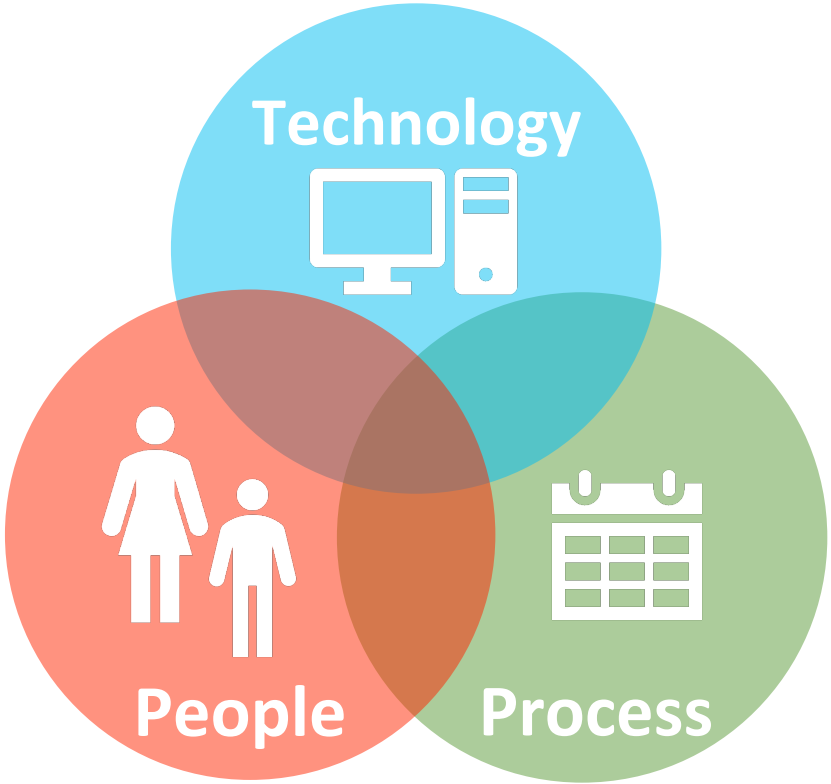
Blockchain 1.0

- Permissionless
- “Anonymous”
- Transparent
- Decentralized
- “Trustless”.




The Economist
007 and the spectre of Britain's past
Turkey votes to the sound of bombs
Those ever-creative accountants
America takes the fight to IS
Coywolves: the new superpredator
OCTOBER 31ST-NOVEMBER 6TH 2015
Economist.com
The trust machine
How the technology behind bitcoin could change the world
IN BLOCKCHAIN WE TRUST

"Trustless"?


Technology
People
Process

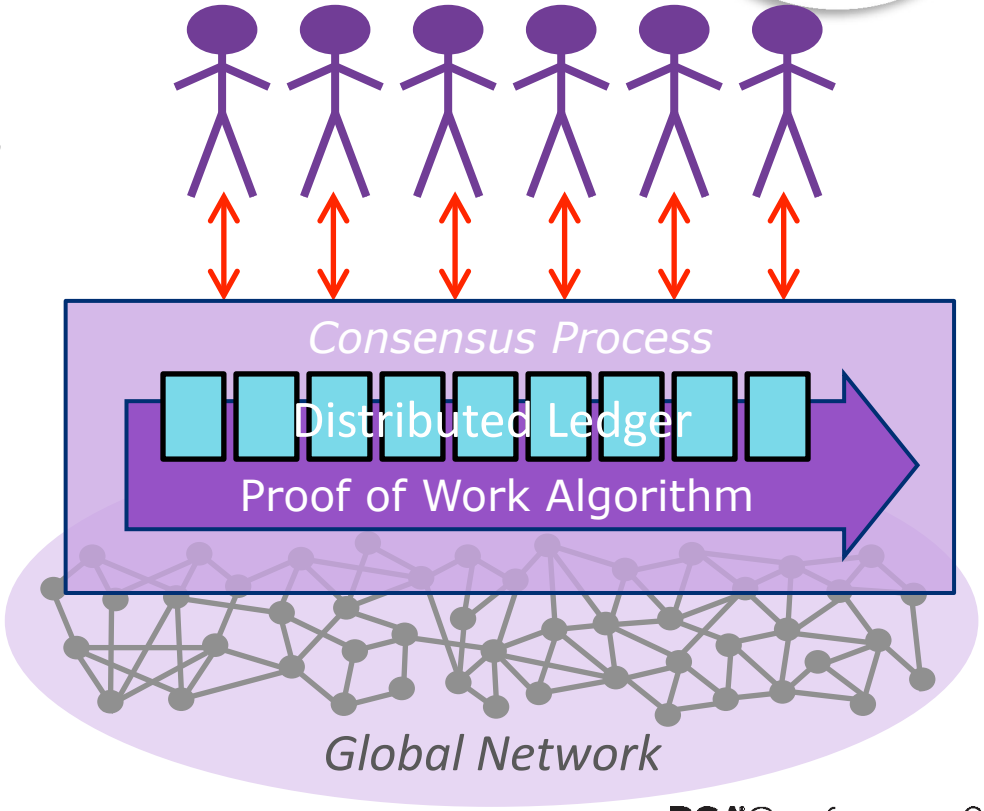
Trustless

People

Process

Blockchain 1.0 vs Reality

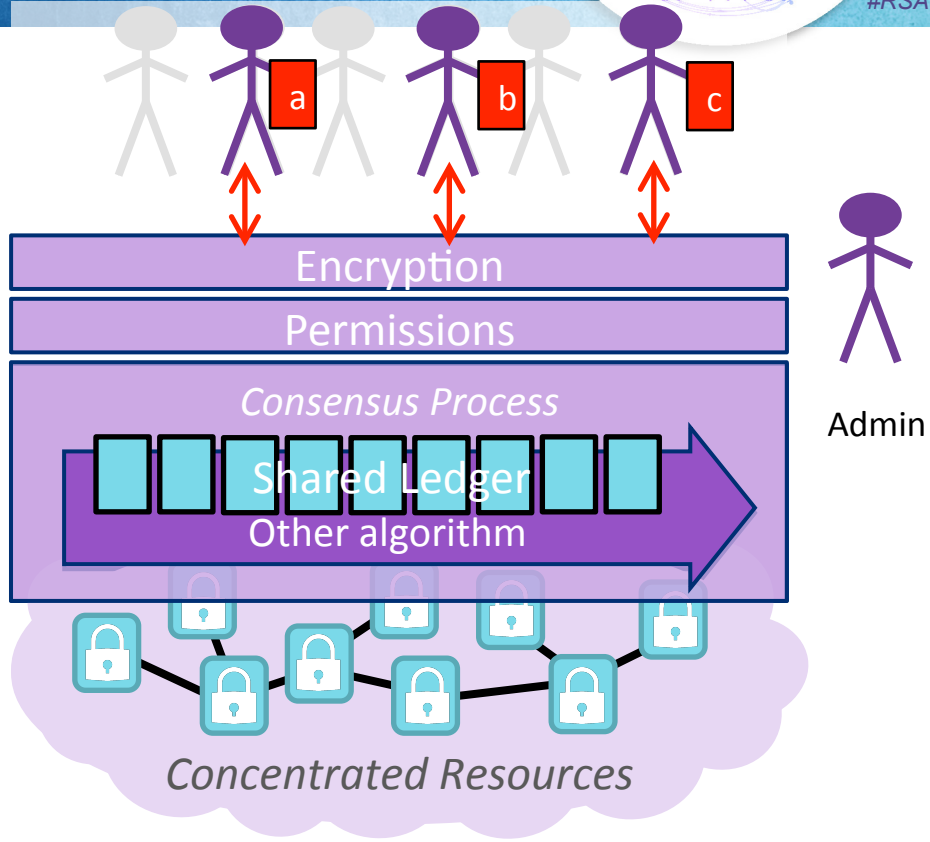
- Consensus – *but as to what?*
- Confidentiality
- A very special use case
- Anti-establishment.



“Proof of concept”?

Evolution to 3rd Gen *Synchronous Ledger Tech*

- People & Process are inherent
- Administered
- Configurable
- Distributed but concentrated
- Focus on permissions
- Focus on key management
- Shift to managed services
- Needs traditional infosec.



The hard work

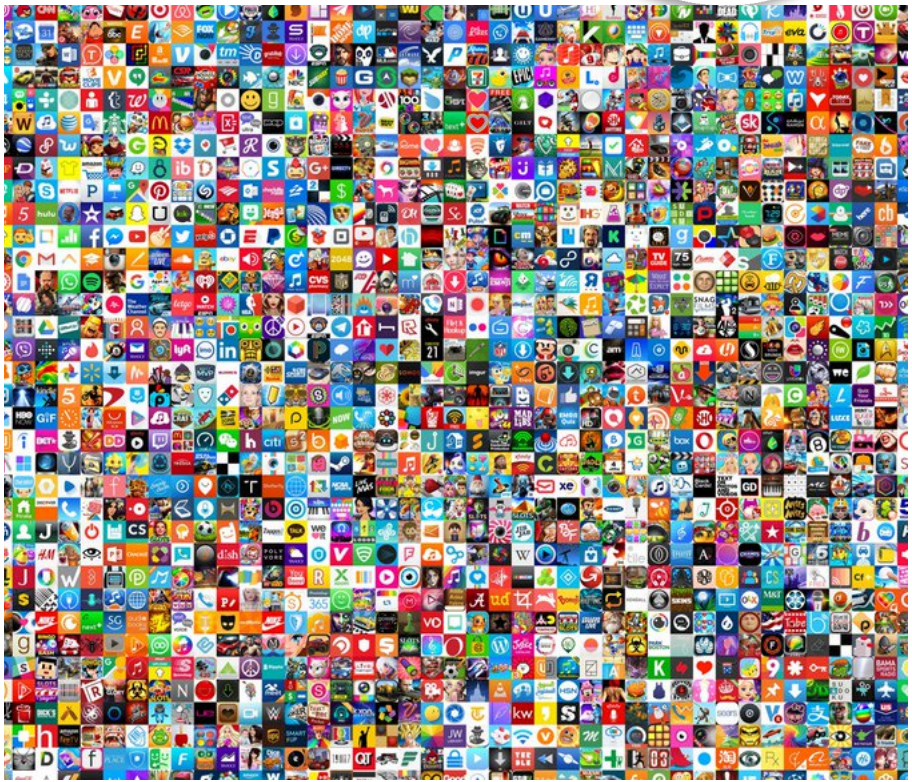
- R3
- Swirlds Hashgraph
- Sovrin Plenum
- Hyperledger Fabric
- Hyperledger Sawtooth, Indy …
- Ethereum Enterprise Alliance
- IBM BaaS
- Microsoft BaaS, Coco.

Advanced use cases

- Complex financial instruments
- Trade documentation
- Pharmaceutical serialization
- Database synchronization

Still unproven:

- IoT
- Healthcare
- Identity.



The state of identity

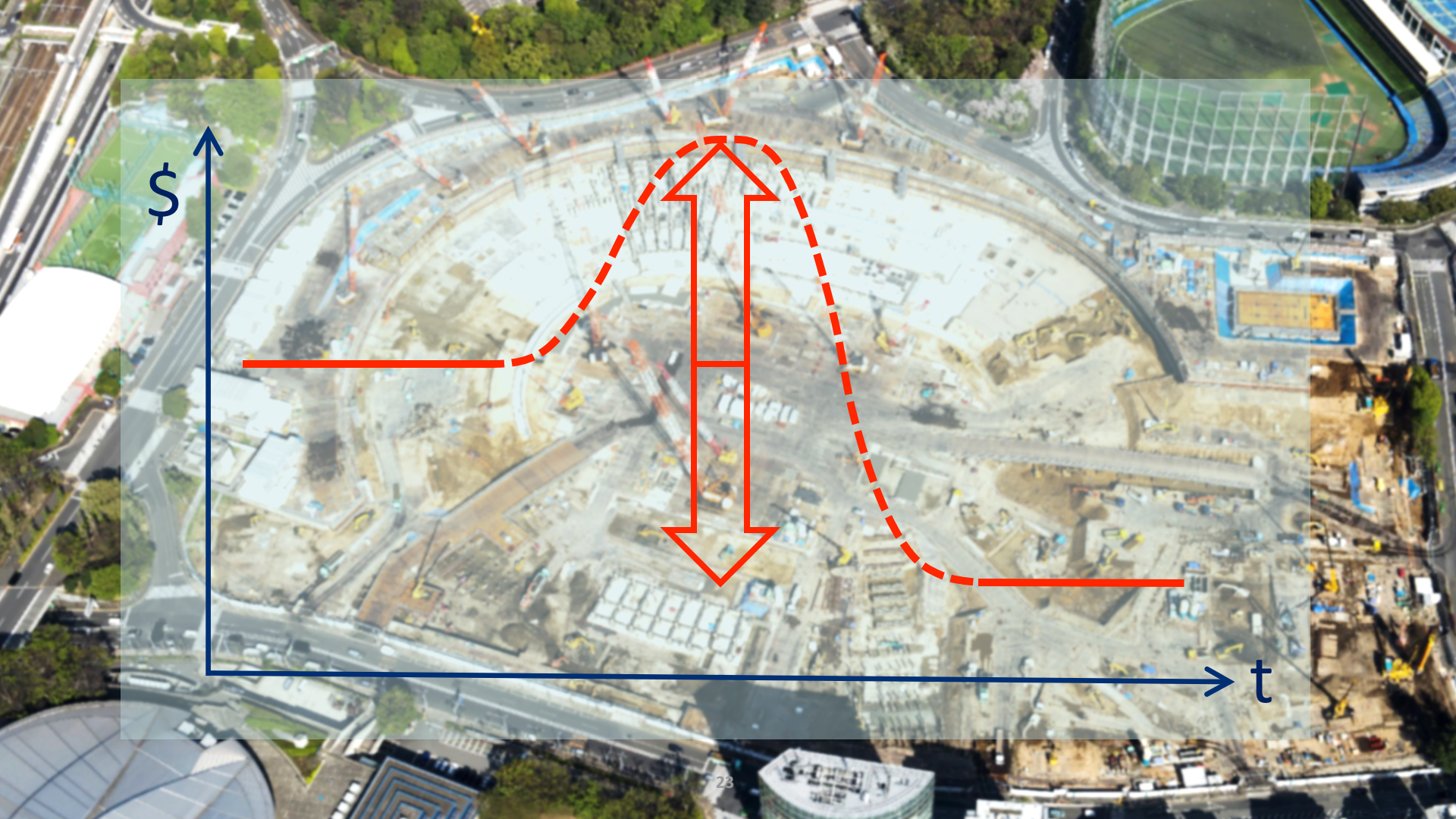
- Focus on Attributes
- Shift From *Who* to *What*
- “Self Sovereign Identity”
- Hardware security
- PKI redux

Case study: Plenum

- Evernym's original R&D
- "Self Sovereign Identity"
- *Verified Claims*
- *Web of Trust Rebooted*
- Sovrin Foundation
- Governance
- Hyperledger Indy.

Apply: Evaluating blockchain proposals

- Ask *why* five times …
- What problem do they purport to solve?
- What does a Proof of Concept *prove*?
- Are BPR and Legal fully engaged?
- Does end user key lifecycle management come first?
- What is distributed consenus *about*?


$
t

Identity fit

- It's not who you know but
- *What* do you know?
- *How* do you know?

- Contest of ideas
- Data supply chains
- Is Blockchain an answer?

THANK YOU

steve@constellationr.com

Discussion