Blockchain Reality Check

Blockchain & Healthcare Workshop

NIST Headquarters, Gaithersburg, Maryland.

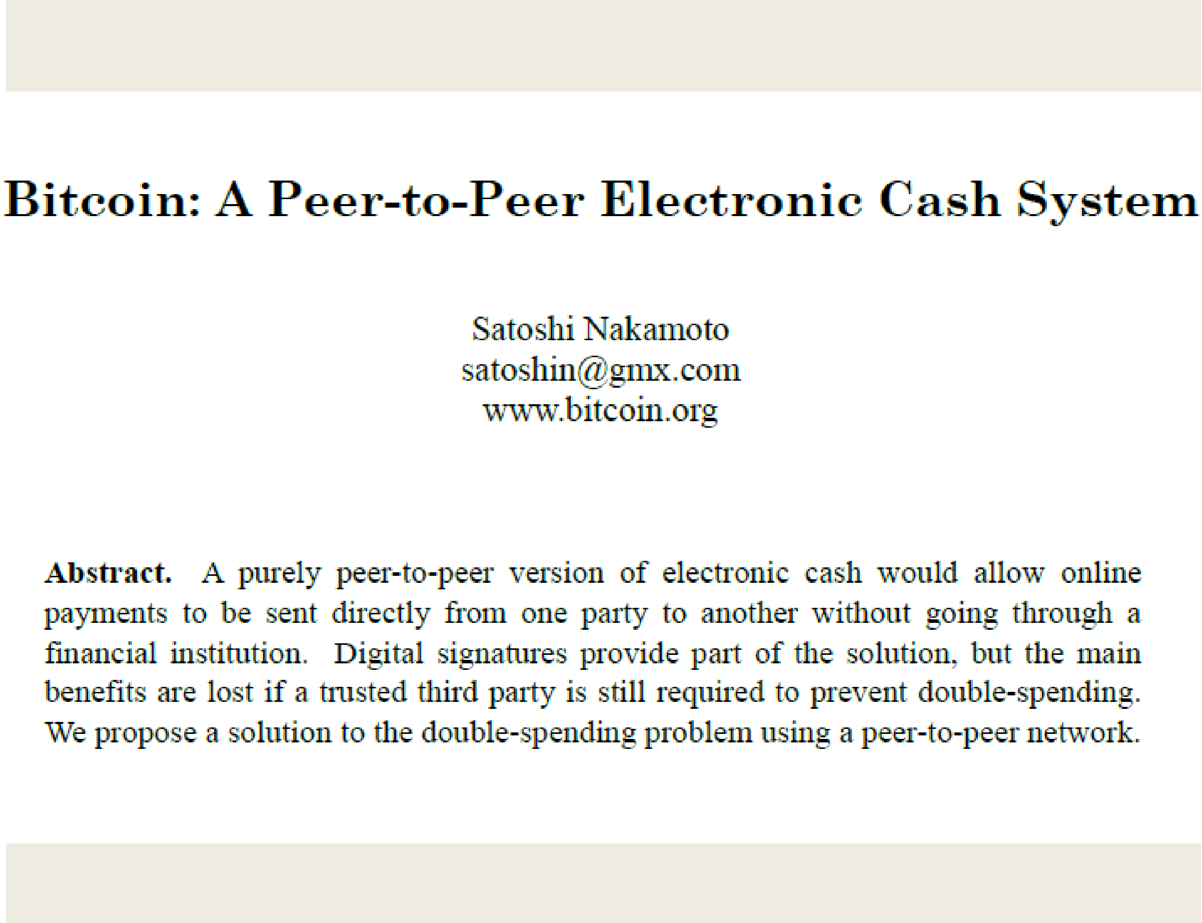
SEPTEMBER 26-27, 2016

STEVE WILSON

VICE PRESIDENT AND PRINCIPAL ANALYST

constellation™ RESEARCH

November 2008: an obscure paper appeared



Bitcoin: A Peer-to-Peer Electronic Cash System

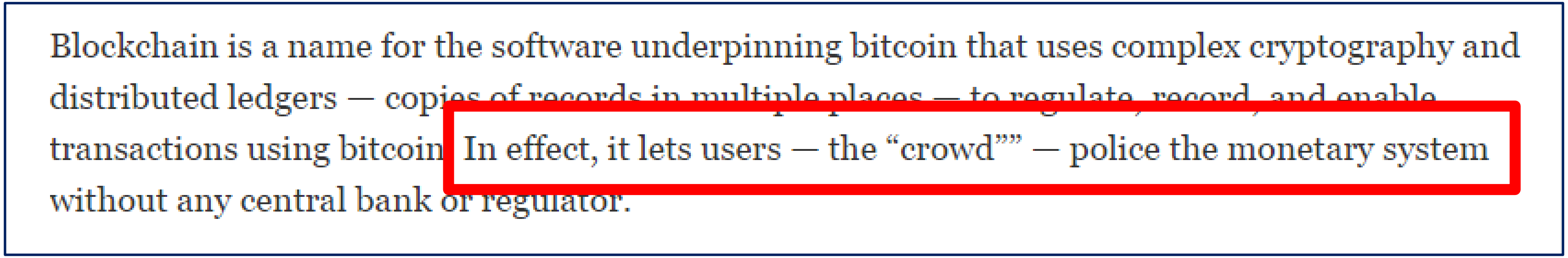
Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

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.

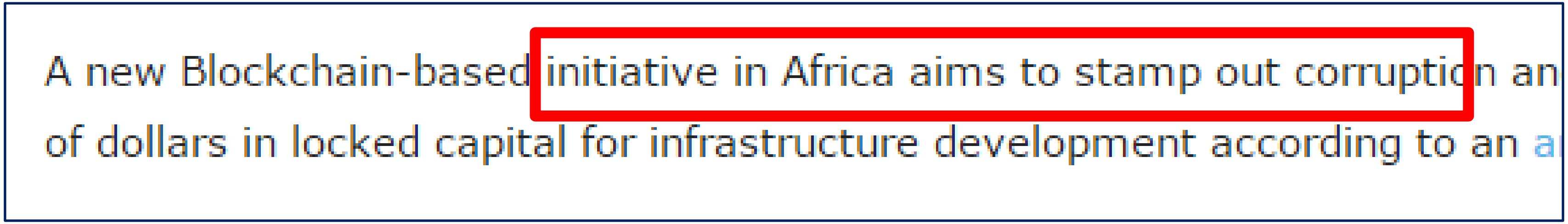
BLOCKCHAIN REVOLUTION
HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD
DON TAPSCOTT
BESTSELLING AUTHOR OF WIKINOMICS
and ALEX TAPSCOTT
INSIDE: A 12-PAGE SPECIAL REPORT ON COLOMBIA
The Economist
007 and the spectre of Britain's past
Turkey votes to the sound of bombs
Those 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 TO REINVENT MONEY
The Science of the Blockchain
O'RE
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
Government Office for Science
Distributed Ledger Technology: beyond block chain
A report by the UK Government Chief Scientific Adviser
THE QUEST FOR IDENTITY AND AUTONOMY IN A DIGITAL SOCIETY
FROM BITCOIN TO BURNING MAN AND BEYOND
EDITED BY JOHN H. CLIPPINGER AND DAVID BOLLIER

Within a few years blockchain became a publication phenomenon.

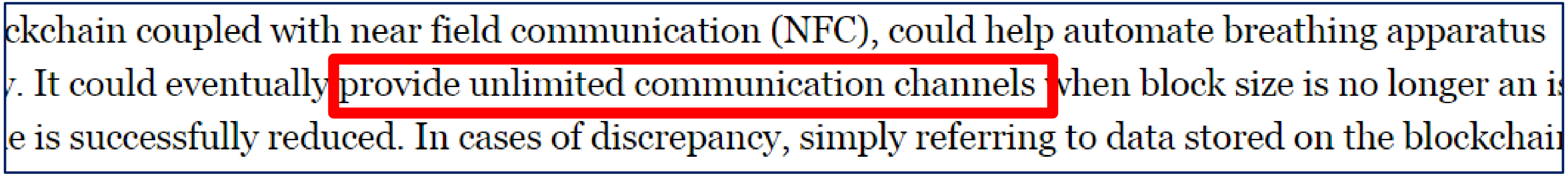
Far beyond payments, a vast array of use cases for blockchain have been proposed, many of them frankly preposterous.



Blockchain is a name for the software underpinning bitcoin that uses complex cryptography and distributed ledgers — copies of records in multiple places — to regulate, record, and enable transactions using bitcoin In effect, it lets users — the “crowd”” — police the monetary system without any central bank or regulator.

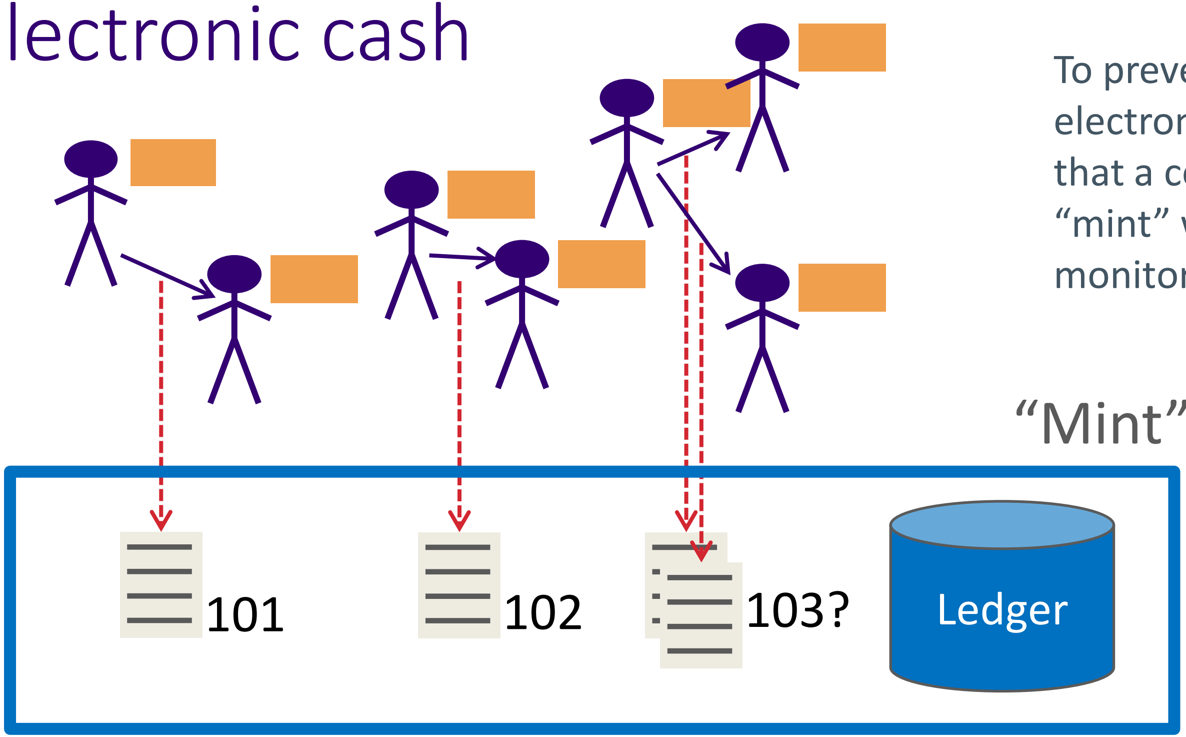


A new Blockchain-based initiative in Africa aims to stamp out corruption an
of dollars in locked capital for infrastructure development according to an a



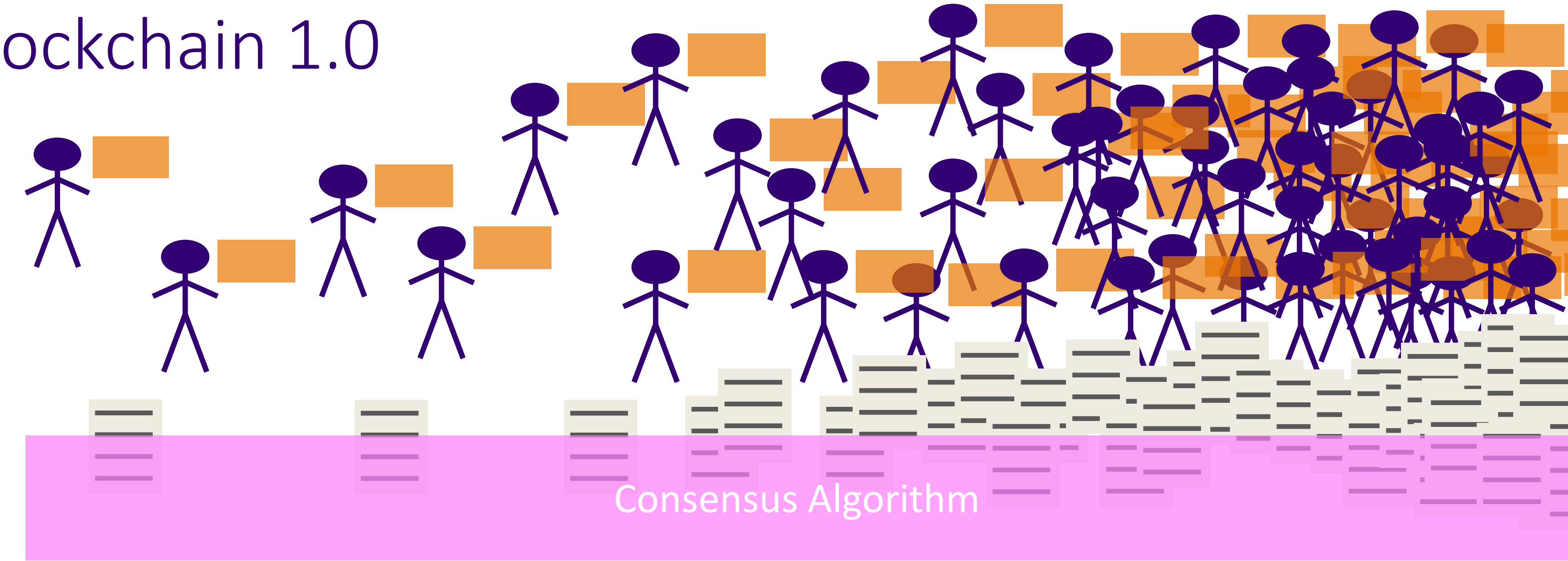
ckchain coupled with near field communication (NFC), could help automate breathing apparatus
y. It could eventually provide unlimited communication channels when block size is no longer an is
e is successfully reduced. In cases of discrepancy, simply referring to data stored on the blockchai

Electronic cash



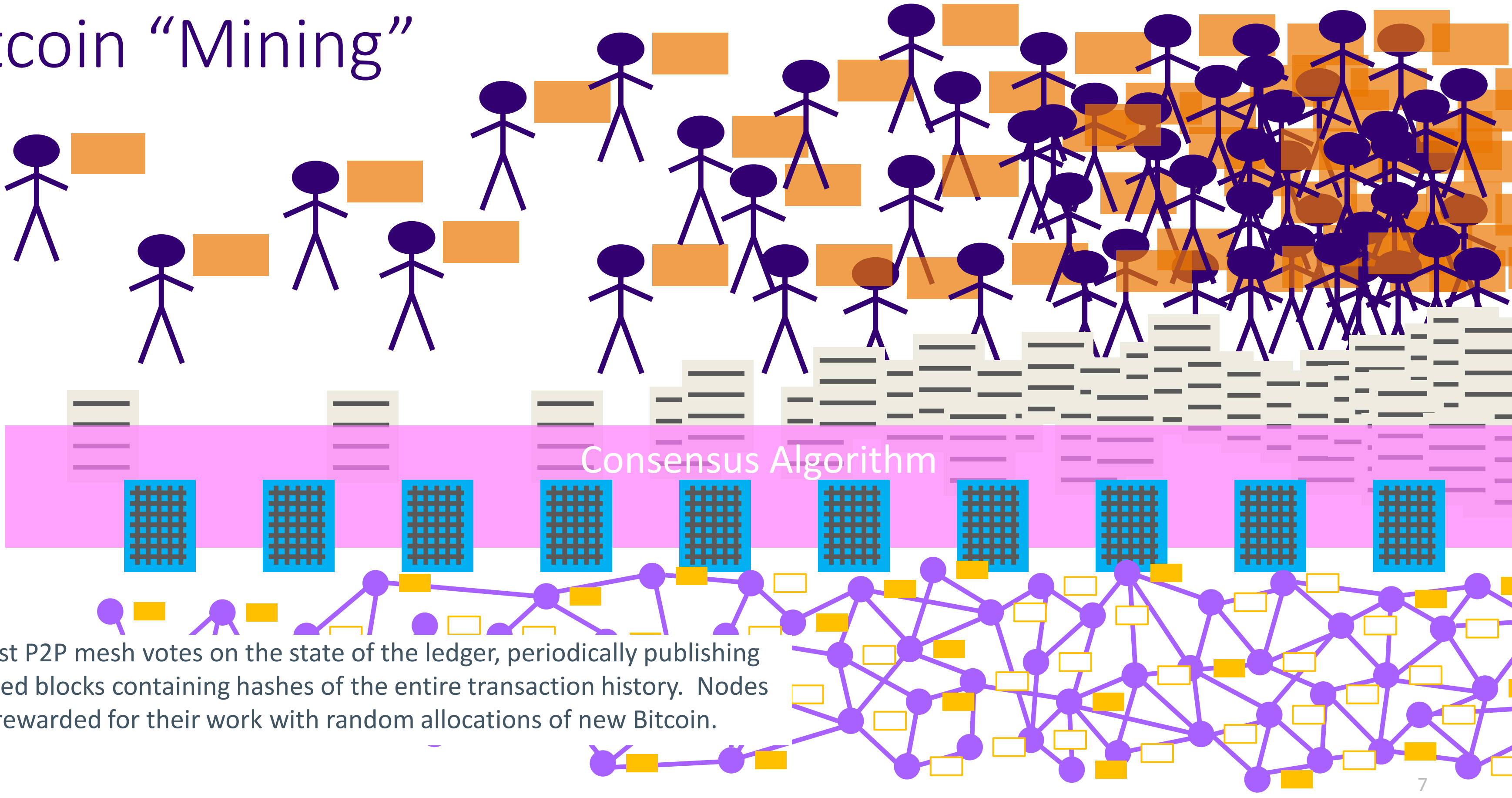
To prevent double spend of electronic cash it was long thought that a central digital reserve bank or "mint" would be required, to monitor all transactions.

Blockchain 1.0



Nakamoto got rid of the central umpire by crowd-sourcing the monitoring of all transactions, to reach consensus on their order.

Bitcoin “Mining”



A vast P2P mesh votes on the state of the ledger, periodically publishing agreed blocks containing hashes of the entire transaction history. Nodes are rewarded for their work with random allocations of new Bitcoin.

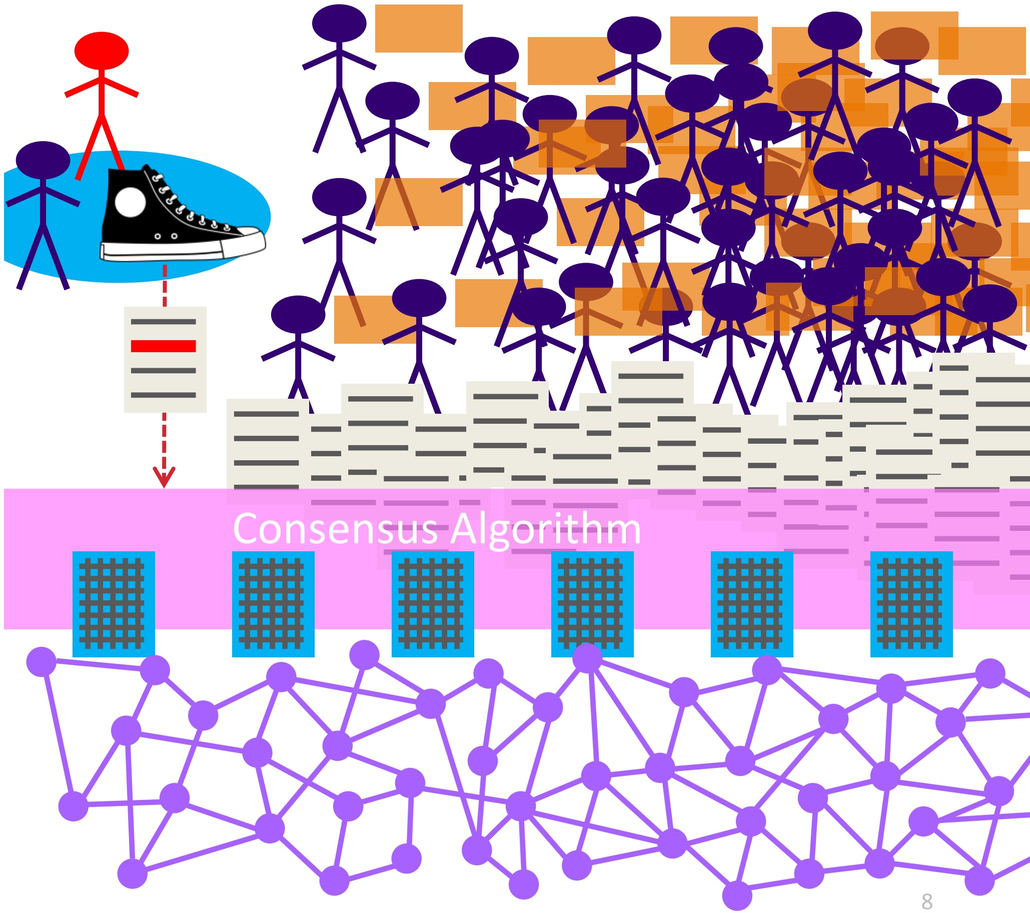
Other Applications

Bitcoin APIs allow other data

- Land Titles
- Diamonds
- Marriages
- Sneakers
- Identities
- Health Records

But Blockchain was designed for digital only.

- BTC account holders self register
- Physical assets need registering *off-chain*
- No *native* “Internet of Value”.

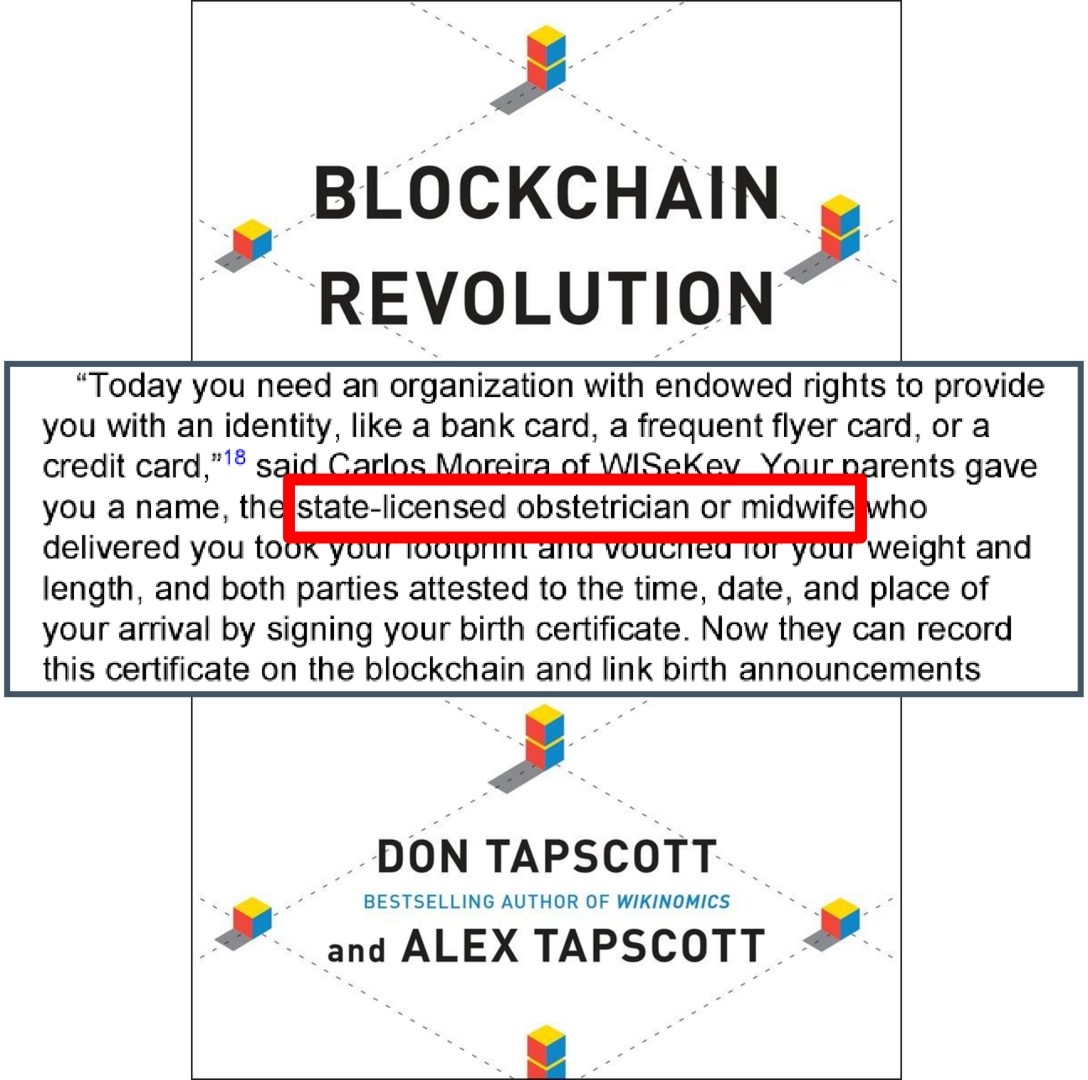


Healthcare

Availability
Important for health but is global decentralization going too far?

Confidentiality
Leads to permissioned or private chains, with smaller pools and weaker security. And key management is huge challenge.

Authority
Blockchain is trust-less, but healthcare is inherently hierarchical.



"Today you need an organization with endowed rights to provide you with an identity, like a bank card, a frequent flyer card, or a credit card,"[18] said Carlos Moreira of WISeKey. Your parents gave you a name, the state-licensed obstetrician or midwife who delivered you took your footprint and vouched for your weight and length, and both parties attested to the time, date, and place of your arrival by signing your birth certificate. Now they can record this certificate on the blockchain and link birth announcements

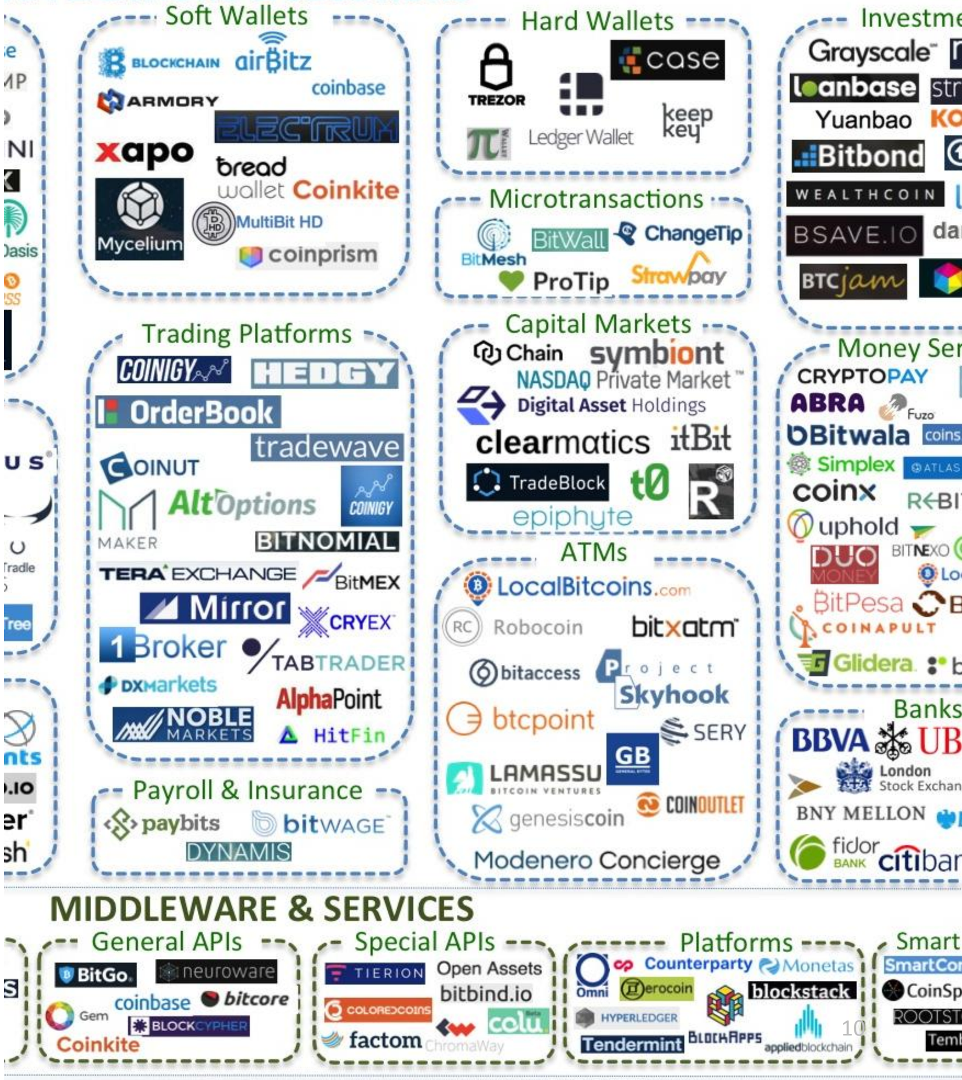
Inspiration

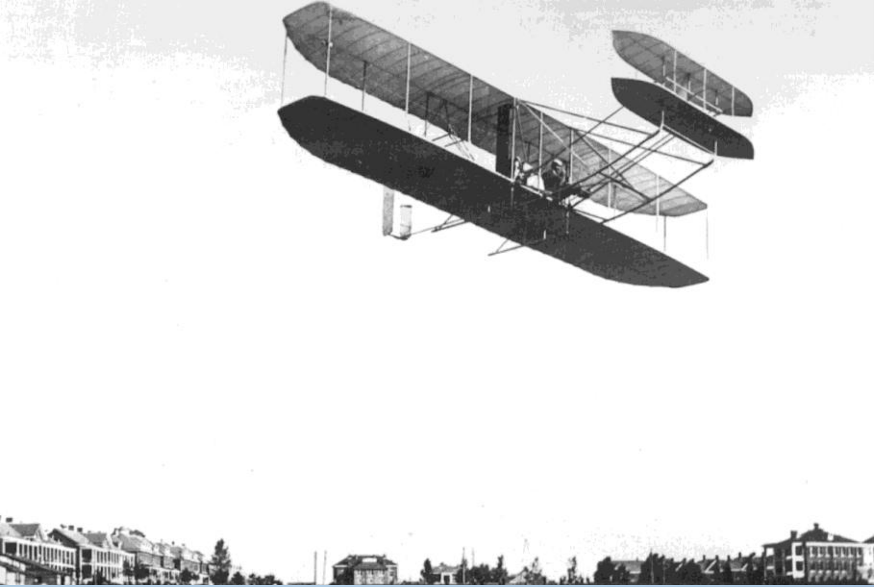
The *Merkle's Puzzles* or the *Wright Bros Flyer* of crypto currency (Merkle's Puzzles was a thought experiment that inspired public key cryptography).

It legitimizes decentralised architectures, one of the holy grails of computing.

BTC does address many needs of the unbanked; seems to have some potential to destabilize banking.

But only disruptive for disruption's sake?





Only the beginning

The Blockchan is no “Internet of Value”.

But decentralised consensus is important.
Expect much R&D into consensus algorithms.

What problems are we trying to solve?
How are we trying to solve them?

Follow the big joint ventures & consortia:

- R3
- Hyperledger
- Microsoft Ethereum BaaS.

Solid R&D on consensus in identity

- Ping Identity / Swirlds

Thank you.

Steve Wilson

☎ +61 414 488 851

✉ Steve@ConstellationR.com

@steve_lockstep

www.constellationr.com/users/swilson

⌂ www.ConstellationR.com

constellation™ RESEARCH