

Innovation and Cryptoventures

# The Blockchain Identity

Campbell R. Harvey

Duke University, NBER and

Investment Strategy Advisor, Man Group, plc

Revised January 13, 2017

# Imagine ...

## Buying and selling stock with t0 settlement

- Today is t+3 no different than the 1920s
- All stock transactions would reside in a secure ledger devoted to a company's equity



# Imagine ...

## Closing on a house with

- No title insurance
- Minimal legal
- No title search
- Simply consult a secure ledger that establishes the person you are buying the house from actually owns it



Imagine ...

## Instantly transferring funds between accounts

- Transfers are not immediate today – even within your own bank!
- Transfers are secure and inexpensive

## FINANCIAL TIMES

May 24, 2016 7:13 pm

### The growing threat from online bank robbers

[Share](#) [Author alerts](#) [Print](#) [Clip](#) [Gift Article](#) [Comments](#)

A series of heists forces the Swift cross border network to tighten up



Imagine ...

## The end of counterfeiting

- Massive number of counterfeit bills in circulation





Imagine ...

## The end of counterfeiting

- Massive number of counterfeit bills in circulation



Imagine ...

## The end of counterfeiting

- Not just North Korea
- Peru is the world leader



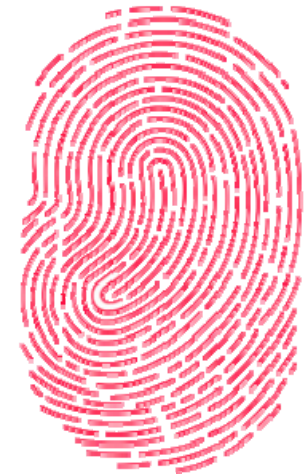
'Counterfeiting is an art': Peruvian gang of master fabricators churns out \$100 bills

Campbell R. Harvey 2017

Imagine ...

## Starting your car with your thumb print

- A secure ledger is checked to verify that you own the car

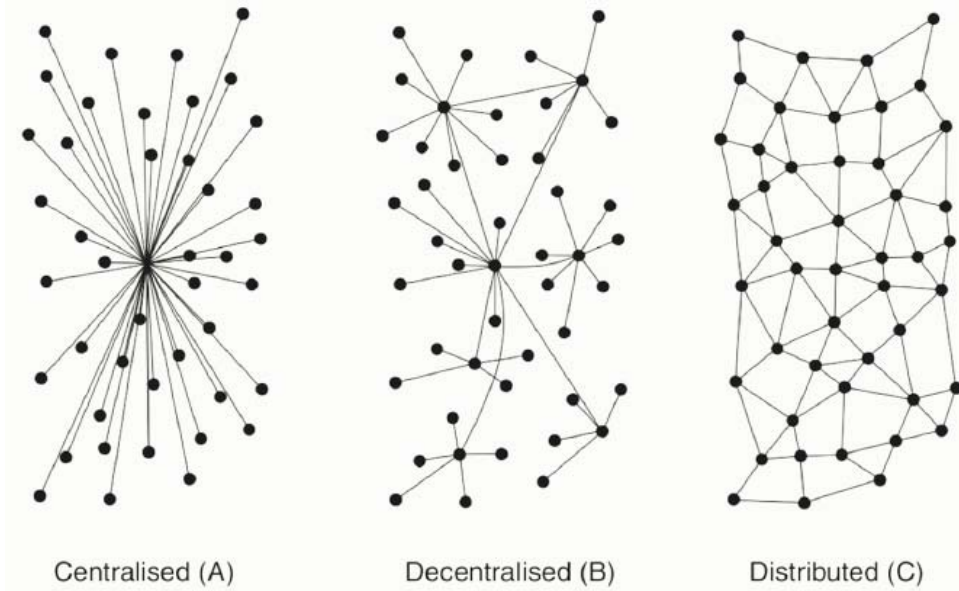




# Overview

## What is it? A blockchain is

- A distributed, secure, transparent ledger that establishes ownership and allows for the efficient exchange of ownership



# Overview

## What is it? A blockchain is

- Transactions are grouped together into blocks. Current transactions are cryptographically linked (chained) to past transactions (and future transactions)
- Blockchains can be private or public

# Overview

## Definitions

- A public blockchain is a blockchain, in which there are no restrictions on reading blockchain data (which still may be encrypted) and submitting transactions for inclusion into the blockchain.
- A private blockchain is a blockchain, in which direct access to blockchain data and submitting transactions is limited to a predefined list of entities.

## In the news....

### R3CEV includes:

- Goldman
- JPMorgan
- Credit Suisse
- ...

September 15, 2015 12:42 pm

## Blockchain initiative backed by 9 large investment banks

Philip Stafford

[Share](#) [Author alerts](#) [Print](#) [Clip](#) [Gift Article](#) [Comments](#)



Nine of the largest investment banks, including [Goldman Sachs](#), [JPMorgan](#) and [Credit Suisse](#), are planning to develop common standards for blockchain technology in an effort to broaden its use across financial services.

The group is looking to channel data, ideas and financial backing to a start-up called [R3CEV](#), a New York-based group of trading and technology executives.

Campbell R. Harvey 2017

# In the news....

R3CEV includes:

- \$600b market cap
- 60% are Global SIFIs





In the news....

Goldman drops out  
Nov 21, 2016

# THE WALL STREET JOURNAL.

## Goldman Sachs Drops Out of R3 Blockchain Group

Founding member leaves as cooperative seeks equity investors



Goldman Sachs Group Inc. let its membership lapse in R3, a high-profile blockchain group founded to spread the technology that is best known for underpinning bitcoin. PHOTO: REUTERS

Campbell R. Harvey 2017

In the news....

May 11, 2015 6:43 pm

## Nasdaq adopts bitcoin backbone for stocks

Richard Waters in San Francisco

[Share](#) [Author alerts](#) [Print](#) [Clip](#) [Gift Article](#) [Comments](#)



[Nasdaq](#) is to start using the technology behind the virtual currency bitcoin to handle transactions on its market, making it what is thought to be the first major financial market to adopt the idea.

The blockchain — the backbone on which bitcoin depends — has attracted wide interest in the financial world as a potentially revolutionary way to streamline many different types of transactions, though few alternative applications have yet been tried beyond bitcoin.



Campbell R. Harvey 2017





The New York Times

In the news... DealB%k WITH FOUNDER ANDREW ROSS SORKIN

## Wall Street Clearinghouse to Adopt Bitcoin Technology

By NATHANIEL POPPER JAN. 9, 2017

After months of talk and hype, the world's biggest banks have taken the first steps toward moving a significant piece of financial infrastructure onto a so-called blockchain — the technology introduced to the world by the virtual currency Bitcoin.

The company that serves as the back end for much Wall Street trading — the Depository Trust and Clearing Corporation, or [D.T.C.C.](#) — said on Monday that it would replace one of its central databases, used by the largest banks in the world, with new software inspired by Bitcoin. The organization, based in New York, plays a role in recording and reporting nearly every stock and bond trade in the United States, as well as most valuable derivatives trades.

[IBM](#), which has been making a big push into blockchain technology, will be leading the project for the D.T.C.C. and aims to have it fully functioning by early next year.

Campbell R. Harvey 2017

BANKING • FEATURES • INTERVIEWS • NEWS

## \$11 Trillion Bet: DTCC to Clear Derivatives With Blockchain Tech

Michael del Castillo (@DelRayMan) | Published on January 9, 2017 at 12:59 GMT

FEATURE

# Original blockchain

## Let's start with the bitcoin blockchain:

- A distributed, secure, transparent, public ledger that establishes ownership and allows for the efficient exchange of ownership
- Available to anyone for download on the Internet (decentralized)
- Does not depend on trust (controlled by no one – monitored by everyone)
- Backed by strong cryptography secured by the world's most powerful network of computers
- Miners provide security and are rewarded with new cryptocurrency

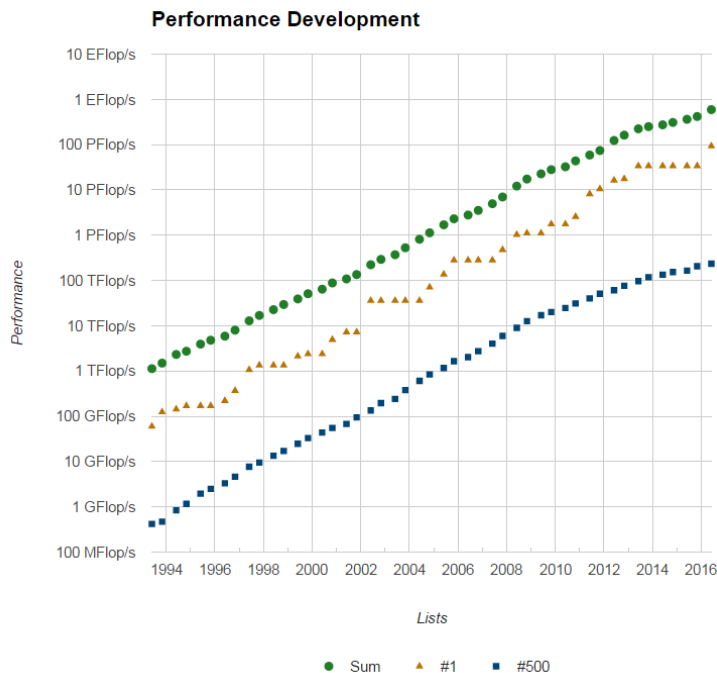


# Original blockchain



## How powerful?

- Currently 30 million petaFLOPS
- #1 supercomputer is **Sunway TaihuLight** at 93 PetaFLOPS
- Sum of top 500 is only 593 petaFLOPS
- Blockchain uses specialized hardware and floating point operations are not needed. Cost of 50% of the network power is about \$1 billion



Campbell R. Harvey 2017

<http://bitcoincharts.com/bitcoin/> <http://www.top500.org/> <https://www.top500.org/statistics/perfdevel/> (20 zettaFLOPS)

# Hashing 101

## A simple hash

Suppose I send an email to Luke. However, he needs to verify that what I sent him is exactly what he received.

- Email contains a single word “hello”.
- Encode the word (a=1, b=2, ..., z=26), so 8 5 12 12 15.
- Multiply the numbers to get 86,400.
- I post the hash on my website. After Luke gets my email, he does the same hash and checks my website.
- If the message was corrupted the hash will not match, for example, “hallo”=  $8 \times 1 \times 12 \times 12 \times 15 = 17,280$  which does not match the original.
- This hash is too simple (e.g. hello=ohell)

# Hashing 101

## SHA-256 (Secure Hashing Algorithm)

<http://www.xorbin.com/tools/sha256-hash-calculator>

Hashing is a one-way function.

For example, passwords are routinely stored on websites in hashed form.

The output of a SHA-256 is 256 bits no matter how big the input

Let's do some examples:

# Hashing 101

## SHA-256 (Secure Hashing Algorithm)

<http://www.xorbin.com/tools/sha256-hash-calculator>

Let's hash the phrase: "Hello, world!" with a special number appended. No spaces. Do it three times for three different strings.

Hello, world!0

Hello, world!1

Hello, world!4250

# Hashing 101

## SHA-256 (Secure Hashing Algorithm)

- King James Bible (4.2mb)  
47f63b8cd8470051acd3a3c0bd5c77c4aa9574d79cf5bfb3e576facabbcb11491
- King James Bible (4.2mb) – with 5 characters deleted  
961c112581bd04e67285f56a354c98ad56cd65244dc768545cfde5bd8ef639c1

## Note: You can hash the hashes

- King James Bible SHA-256 of SHA-256  
0c8b120036a32525e9737fa8ed67b9af337affc7dae557d7244592c286b2cfd8



# Hashing 101

How many combinations in a SHA-256 hash?

- Need  $2^{255} = 1.15 \cdot 10^{77}$  guesses
- Which is roughly the number of atoms\* in the known universe!

\*Number of atoms between  $10^{78}$  to  $10^{82}$  <http://www.universetoday.com/36302/atoms-in-the-universe/>  
Campbell R. Harvey 2017

# Hashing 101

## SHA-256 hashes widely used for email and file transfer

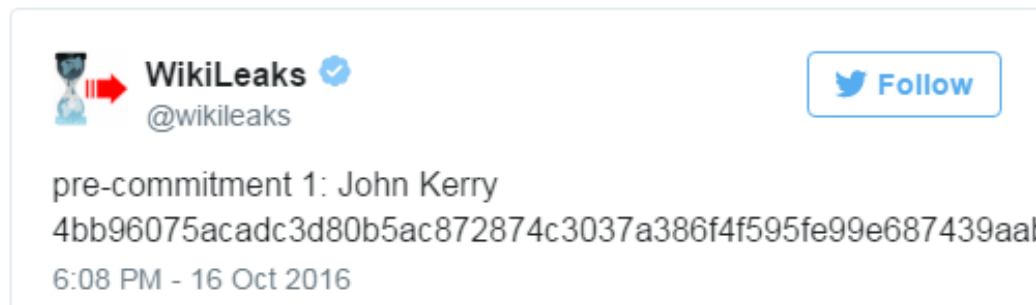
- Returning to the email example, I want to send a file to Louise
- I SHA-256 the file
- I send Louise the original file
- Louise does her own SHA-256 hash of the file
- Louise checks to see if her hash of the file matches the hash that I have on my website
- If there is any difference, the file has been corrupted
- This all happens automatically and is called “checksum”

# Hashing 101

SHA-256 appears in Wall Street Journal

## THE WALL STREET JOURNAL.

On Sunday, one day after Ms. Anderson's visit, WikiLeaks issued a series of three messages over Twitter. Each one began "pre-commitment" and then the number 1, 2, or 3, followed by a short phrase, and then an assortment of 64 letters and numbers.



The image shows a screenshot of a tweet from the account WikiLeaks (@wikileaks). The tweet text is: "pre-commitment 1: John Kerry 4bb96075acadc3d80b5ac872874c3037a386f4f595fe99e687439aab". The tweet was posted at 6:08 PM on October 16, 2016. The account name is "WikiLeaks" with a verified badge and the handle "@wikileaks". There is a "Follow" button next to the account name.

Campbell R. Harvey 2017

# How does the bitcoin blockchain work?

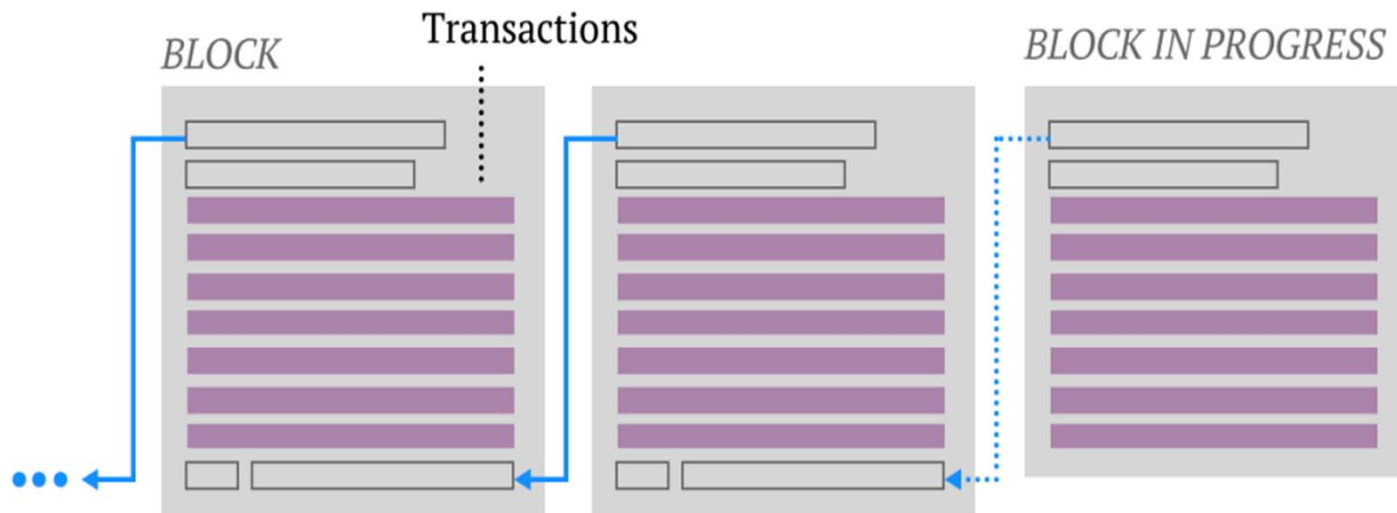
Every transaction ever made on the blockchain is public

- Ledger is append-only and immutable
- Serves as a basis of trust
- Can store (limited) metadata as well as transactions

# How does the bitcoin blockchain work?

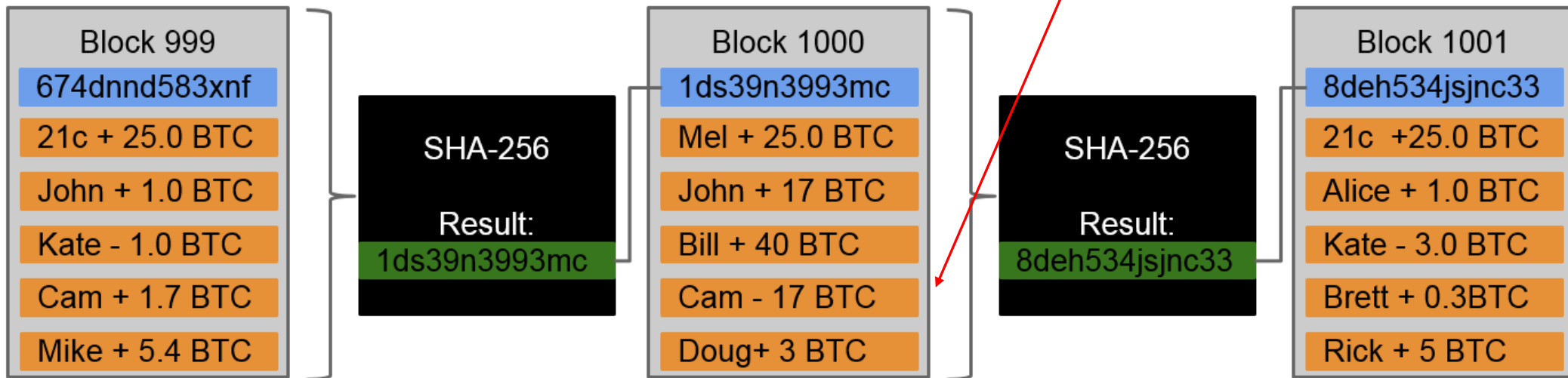
Ledger broken up into 10 minute “blocks”

- Every block contains a hashed reference to the block before it so you can trace every transaction all the way back to 2009



# How does the bitcoin blockchain work?

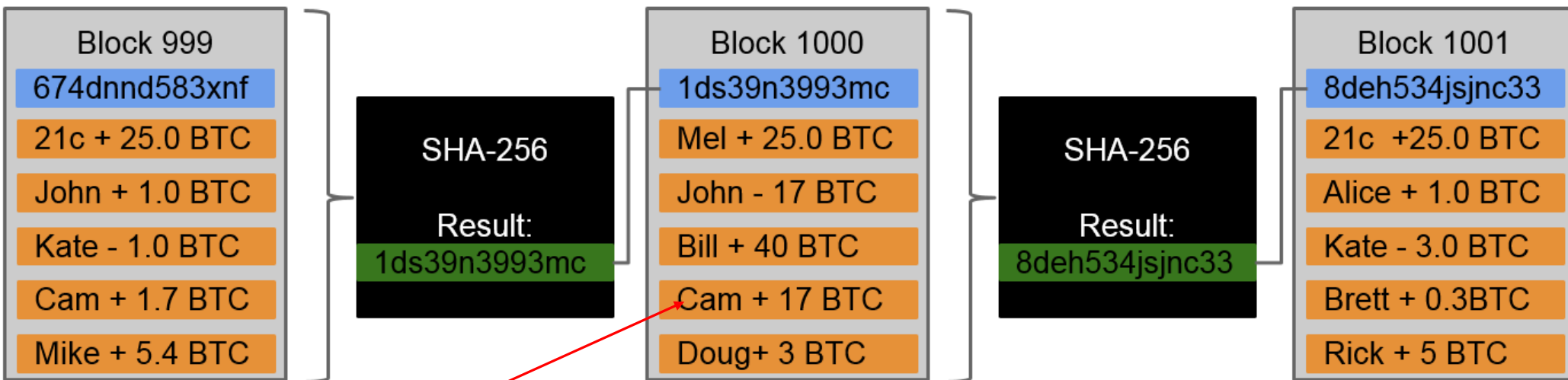
Example. In block 1000, I buy a car (for 17 BTC) from John





# How does the bitcoin blockchain work?

Suppose I edit the block on my computer – to give me 17 BTC!  
I then broadcast to the network

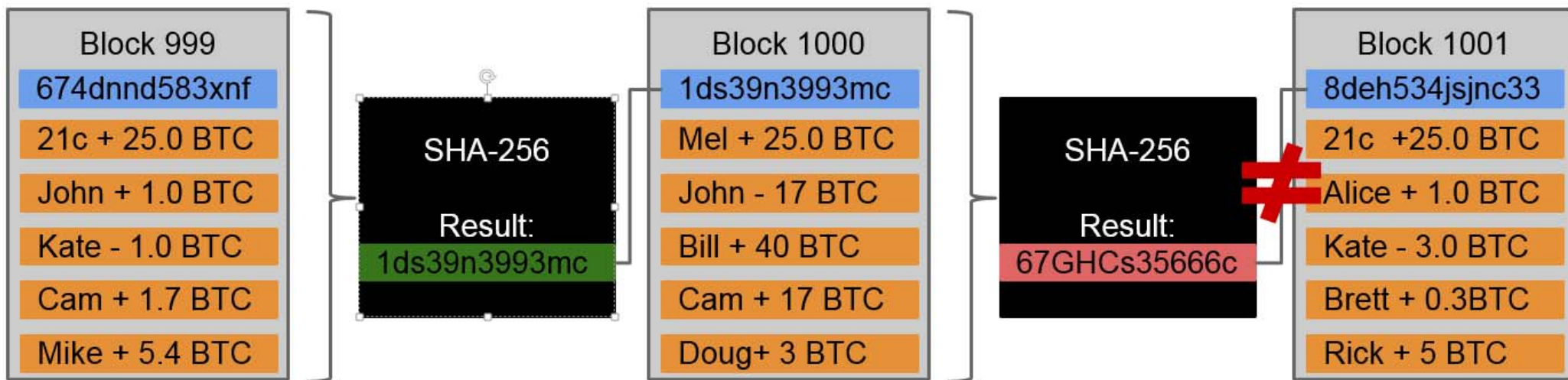


Nefarious action

Campbell R. Harvey 2017

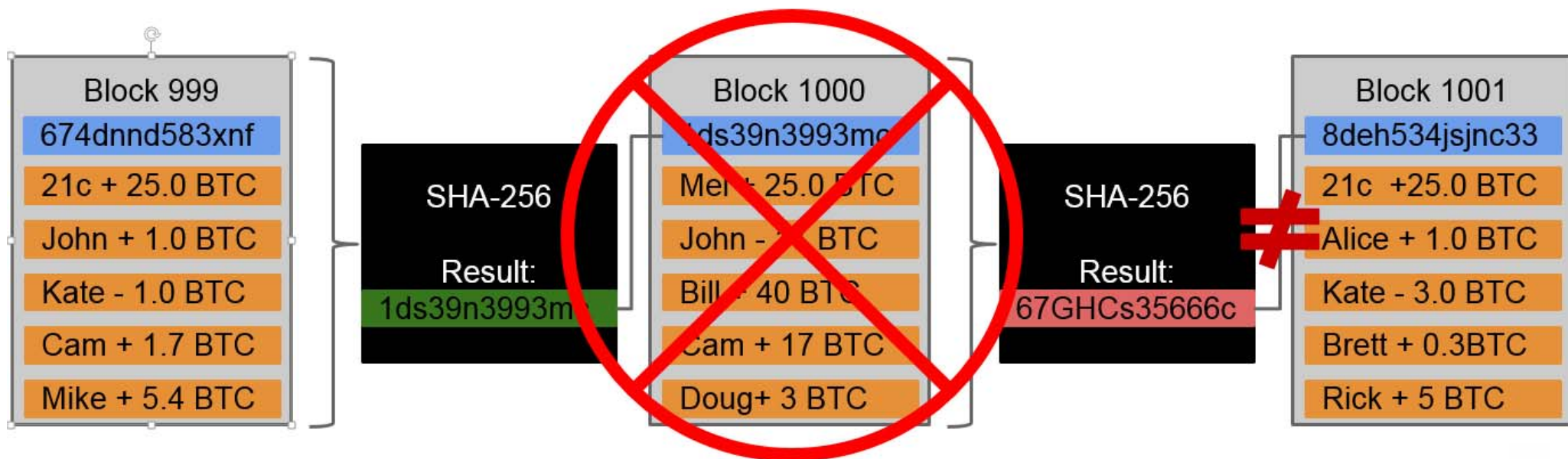
# How does the bitcoin blockchain work?

Even making that small change results in a very different block hash. It no longer matches what is stored in block 1001.



# How does the bitcoin blockchain work?

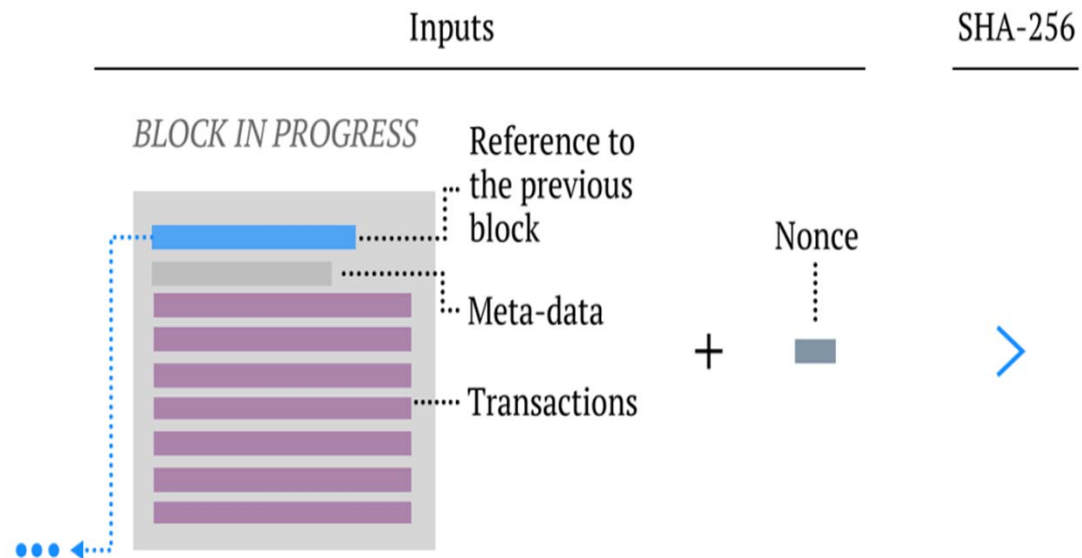
Blockchain clients automatically compute the hash themselves - if no match, they reject the block - Check other peers in the network for correct block



# How does the bitcoin blockchain work?

But there is more to it! Here is where the miners come in.

- Miners group the current transactions together and take a hash of the transactions plus a “magic number” – called a “nonce”.



# How does the bitcoin blockchain work?

But there is more to it! Here is where the miners come in.

- Miners try different nonces to get a special hash that has a certain number of leading zeros
- More leading zeroes means fewer solutions – and more time to solve the problem
- Think of shuffling 5 decks of cards. Your goal is to turn over 5 aces of spades in the first five cards! That will be a lot of shuffling.

# How does the bitcoin blockchain work?

But there is more to it! Here is where the miners come in.

- Current difficulty is 17 leading zeros! Probability =  $(1/16)^{17}$
- Odds of winning two Powerball jackpots\* in a row approx  $(1/16)^{15}$
- Someone finds the winning hash approximately every 10 minutes
- This means 1 billion gigahashes calculated every second
- System is immune to increases in computing speed – the difficulty automatically adjusts if the hash is found in less than 10 minutes

\*One Powerball = 3.4223E-09; two Powerballs in a row = 1.17122E-17; 17 zeroes in winning hash 3.3888E-21; 18 zeros 2.117E-22



# How does the bitcoin blockchain work?

But there is more to it! Here is where the miners come in.

- It is easy to verify the hash is correct
- Anyone can take the hash of the transactions + nonce and get the hash with the 17 leading zeros
- However, any change in any transaction – no matter how trivial – will lead to a completely different hash (and unlikely to have any leading zeros)
- Miners are rewarded with cryptocurrency for finding the winning hash and verifying transactions. There are also small transaction fees.

# Distributed public ledger

## Bitcoin blockchain:

- Anyone can write to ledger and anyone can mine, i.e. no “censorship”
- Network determines “settlement”
- Having extreme “difficulty” is expensive (power consumption) but reduces or eliminates the possibility of any single person (or miners) from doing anything nefarious.

# Permissioned blockchains

## What not just operate on consensus?

- Consensus may be problematic if the blockchain is open because someone could take over millions of computers and impose their will (Sybil attack)
- However, significant advances have been made by firms like Ethereum to refine the consensus method and eliminate the Sybil attack risk



The image shows a screenshot of a DealB%k article on The New York Times website. The article title is "Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's". The author is Nathaniel Popper, and the date is March 27, 2016. The article is part of a series of news items on the site, with other headlines visible in the background: "The Race Is On to Control Artificial Intelligence, and Tech's Future", "In Yahoo, Another Example of the Buyback Mirage", "Challenge to Yahoo's Board Makes a Sale More Certain", and "Law (Her S)". The DealB%k logo is prominently displayed above the article title, with the text "WITH FOUNDER ANDREW ROSS SORKIN" below it. Social media sharing icons for Facebook, Twitter, and Email are located at the bottom right of the article.

HOME SEARCH

The New York Times

Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's

The Race Is On to Control Artificial Intelligence, and Tech's Future

FAIR GAME In Yahoo, Another Example of the Buyback Mirage

DEAL PROFESSOR Challenge to Yahoo's Board Makes a Sale More Certain

Law (Her S)

**DealB%k** WITH FOUNDER ANDREW ROSS SORKIN

*Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's*

By NATHANIEL POPPER MARCH 27, 2016

f t e

# Private blockchains

This is where permissioned blockchains enter

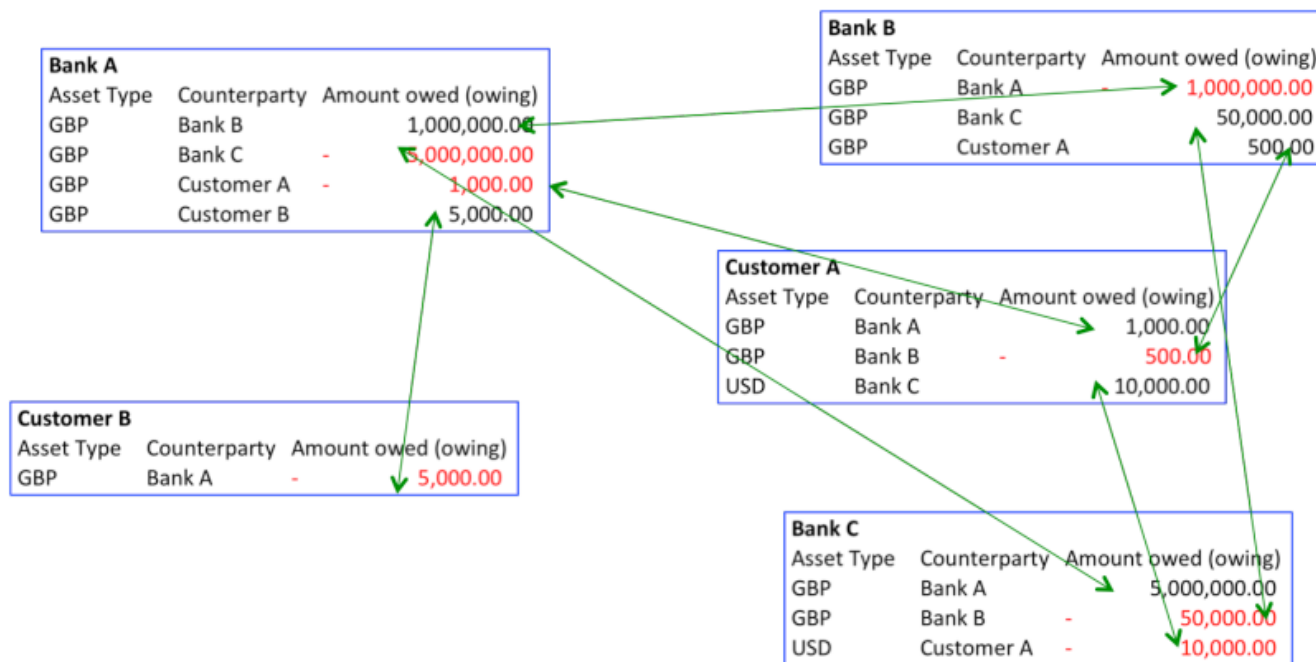
- All major banks are now in this space (e.g. R3CEV and DAH-Hyperledger)
- Currently, bank accounting systems are inefficient where each bank has its own independent ledger
- Having a unified but distributed ledger is very attractive: obvious cost savings on technology, instant transactions across banks, reduced need for branches, heightened security
  - Global bank IT spending in 2015 estimated at \$196 billion (Celente)\*
  - Distributed ledger could save \$15-\$20 billion per year (Santander)\*\*

\* <http://www.finextra.com/news/fullstory.aspx?newsitemid=26979>

\*\* <http://www.finextra.com/finextra-downloads/newsdocs/The%20Fintech%202%200%20Paper.PDF>

# Private blockchains

## Example: 3 banks, 2 customers



Campbell R. Harvey 2017

<http://gandal.me/2015/04/27/how-to-explain-the-value-of-replicated-shared-ledgers-from-first-principles/>

# Private blockchains

Example: 3 banks, 2 customers + 1 blockchain

Bank A		
Asset Type	Counterparty	Amount owed (owing)
GBP	Bank B	1,000,000.00
GBP	Bank C	- 5,000,000.00
GBP	Customer A	- 1,000.00
GBP	Customer B	5,000.00

Bank B		
Asset Type	Counterparty	Amount owed (owing)
GBP	Bank A	- 1,000,000.00
GBP	Bank C	50,000.00
GBP	Customer A	500.00

Bank C		
Asset Type	Counterparty	Amount owed (owing)
GBP	Bank A	5,000,000.00
GBP	Bank B	- 50,000.00
USD	Customer A	- 10,000.00

Customer A		
Asset Type	Counterparty	Amount owed (owing)
GBP	Bank A	1,000.00
GBP	Bank B	- 500.00
USD	Bank C	10,000.00

Customer B		
Asset Type	Counterparty	Amount owed (owing)
GBP	Bank A	- 5,000.00

Issuer	Holder	Asset	Amount
Bank A	Bank C	GBP	5,000,000.00
Bank A	Customer A	GBP	1,000.00
Bank B	Bank A	GBP	1,000,000.00
Bank C	Bank B	GBP	50,000.00
Bank C	Customer A	USD	10,000.00
Customer A	Bank B	GBP	500.00
Customer B	Bank A	GBP	5,000.00

Campbell R. Harvey 2017

<http://gendal.me/2015/04/27/how-to-explain-the-value-of-replicated-shared-ledgers-from-first-principles/>



# Private blockchains

## Private blockchains restrict who can verify

- For example, only banks are allowed to verify transactions and only banks are allowed to write to their blockchain
- Their contribution to the computing capacity is by contract
- This system imposes “censorship” – but, importantly, there is no obvious need for censorship-resistance
- In this case, there is not even a need for a cryptocurrency

# Permissioned blockchains

## Private blockchains advantages

- No need for cryptocurrency to pay miners
- Less (or no) mining necessary and lower power consumption
- Common accounting system benefit for banks
- Clear governance
- No limit on the number of transactions (currently the bitcoin blockchain can only handle 7 transactions a second – and scalability is an issue)
- Faster blocks (could be every few seconds not 10 minutes)
- Specialized ledgers (multiple blockchains) for other types of contracts
- Blockchain greatly eases the job of the regulator who has the ability to see all transactions – and the identities of the transactors

# Permissioned blockchains

## Private blockchains disadvantages

- Are they as secure as bitcoin blockchain? Potential issues with banks holding private keys and verifying their own transactions.
- Centralized rather than decentralized (you need to rely on the banks and banks will do what is in their best interests)
- Reliant on central bank currencies (which is not a big deal in the U.S., but is in many other countries)
- Blockchain vs. database debate: All blockchains are distributed ledgers but not all distributed ledgers are blockchains.

# Private blockchains

Can the different types of chains be connected?

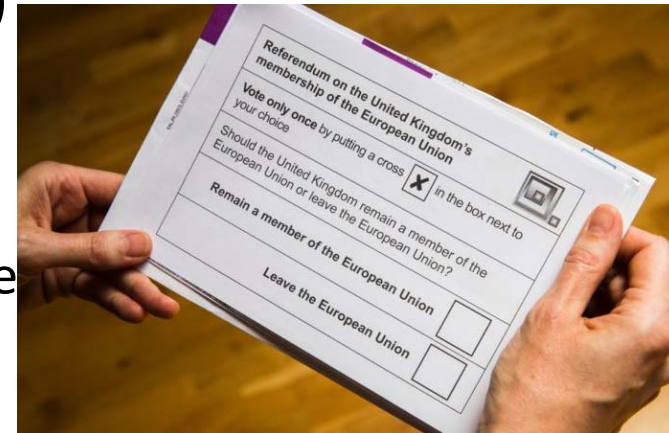
- Yes.
- A [sidechain](#) is a “blockchain that validates data from other blockchains”
- It is possible to run a permissioned sidechain that is “pegged” to the bitcoin blockchain. This is the idea of Blockstream’s [Liquid](#).\*

\*<https://blockstream.com/2015/11/02/liquid-recap-and-faq/> and <https://blockstream.com/sidechains.pdf>

# Blockchain applications

## Voting

- Each citizen registered to vote is issued a voting token
- The token cannot be sold and it can be used only once
- It expires after the election
- Voter needs to provide proof of identity (thumb print) to vote
- Blockchain is checked to see if that voter has the token to “spend”
- Your vote can be anonymous even though you provide proof of identity with “zero knowledge proof”



Campbell R. Harvey 2017

# Blockchain applications

## Internet of Things

- Only you can control your thermostat
- Provide proof of identity (blockchain is checked) and IoT device works for you
- Strong protection against hacking because the hacker would have to rewrite the entire blockchain and take over the majority of computing



# Blockchain applications

## Internet of Things

- Only you can control your car
- Provide proof of identity (blockchain is checked) and IoT device works for you
- Driverless cars are a “no go” unless they are hack proof.

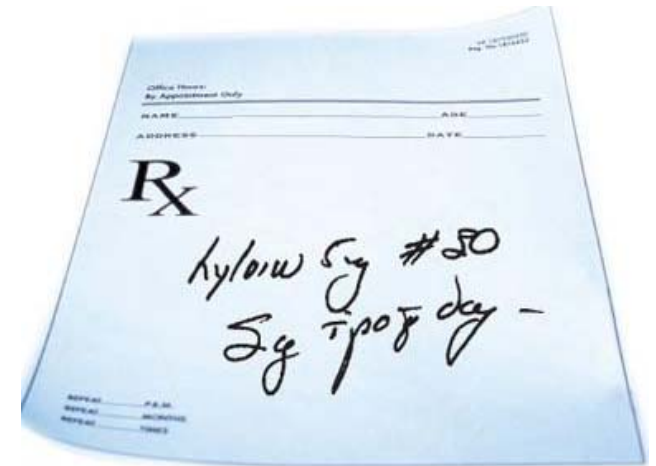


# Blockchain applications

## Prescriptions

- Widespread fraud
- Blank scripts are stolen from doctors' offices or forged
- Some doctors abuse the system
- Token issued to patient: it cannot be resold and has an expiration
- Patient presents token to pharmacist and blockchain is checked to make sure patient owns the token (and has not already spent it)

Campbell R. Harvey 2017





# Blockchain applications

## Medical records

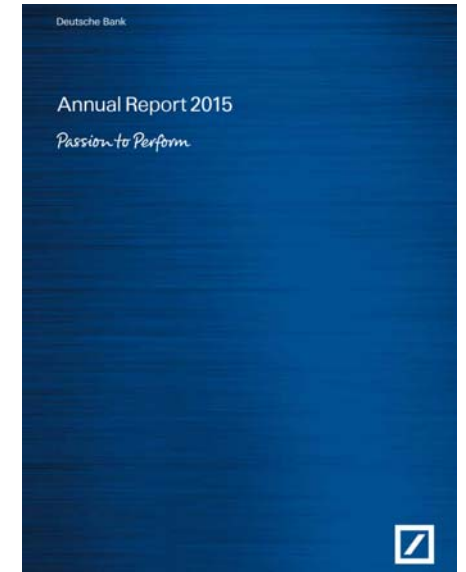
- You enter a health facility (not your home facility)
- You provide proof of identity verified with a blockchain
- Your “private key” unlocks encrypted data related only your health records
- Also provides a much stronger privacy protection
  - Instead of a medical database being encrypted with one key (which might be lost or discovered), each patient’s record has its own key. Hence, to compromise the database you would need to guess potentially millions of keys



# Blockchain applications

## Real time financial statements

- New role for Deloitte, E&Y, PwC, etc. in validating company ledger transactions in real time
- API would allow selected transparency (same categories as in the usual financial statements) in real time
- The end of quarterly reporting – and potentially some of the incentives that are created to engage in short-termism



# Blockchain applications

## Property



velox.RE is an open source blockchain platform for real estate transactions.

*Blockchain will enable every property, everywhere, to have a corresponding digital address that contains occupancy, finance, legal, building performance, and physical attributes that conveys perpetually and maintains all historical transactions. Additionally, the data will be immediately available online and correlatable across all properties. The speed to transact will be shortened from days/weeks/months to minutes or seconds.*— Jason Ray, Nov 2, 2015.  
<https://www.linkedin.com/pulse/blockchain-cre-its-all-speed-transact-jason-ray>

Campbell R. Harvey 2017

## Chicago's Cook County to Test Bitcoin Blockchain-Based Property Title Transfer

Oct 06, 2016 03:47 PM by Kyle Torpey



Through an exclusive partnership with real estate tech startup [Velox.re](#), Chicago's Cook County will test the use of the Bitcoin blockchain for transferring and tracking property titles and other public records. The Cook

# Blockchain applications

## Fedcoin

- 78% of the value of US currency is in \$100 bills
- Large denomination bills method of choice for criminal activity

# Blockchain applications

## Fedcoin

- 78% of the value of US currency is in \$100 bills
- Large denomination bills method of choice for criminal activity
- Fedcoin is a digital USD currency where the complete history of all transactions is visible to the Fed via a Fed blockchain
- Instant monetary policy, see Rogoff (2016)



El Chapo's cash stash



# Blockchain applications

## Central banks

The Telegraph

HOME | NEWS | SPORT

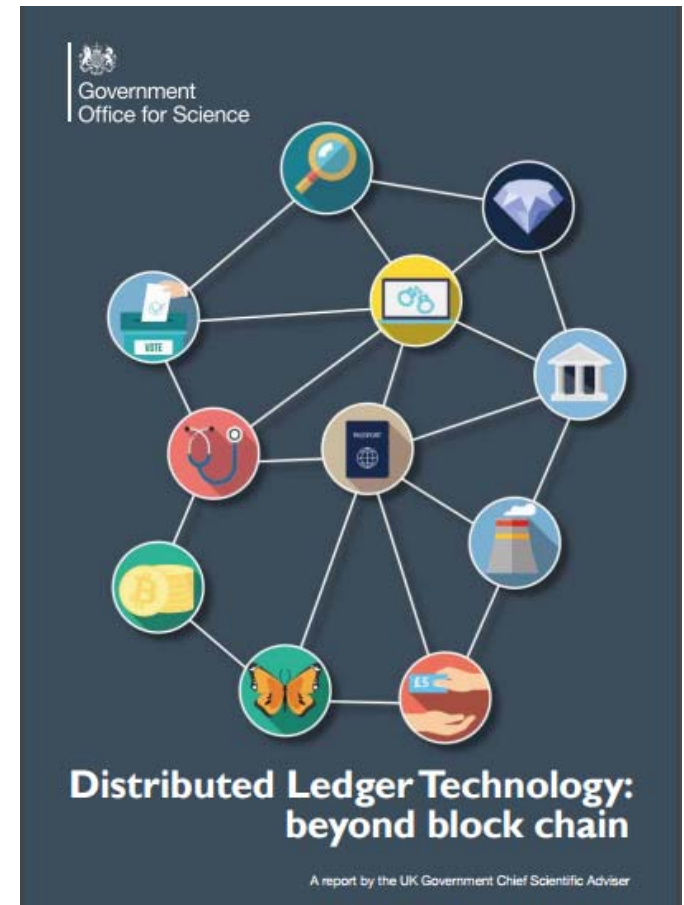
## Business

Economy | Companies | Opinion | Markets | A-Z | Alex | Telegraph Connect | Events

🏠 > Business

## Central banks beat Bitcoin at own game with rival supercurrency

Campbell R. Harvey 2017



# Conclusions

## Blockchain will first disrupt financial services

- Still early going but change will happen quickly
- Low hanging fruit in financial applications
- Next applications based on other types of property like real estate, digital media,...
- Blockchain may be crucial to IoT applications that are at risk from hacking In the short-term, I see the growth of a diverse set of blockchain types
- Bitcoin blockchain is the strongest – but many applications do not require censorship resistance; sidechains offer interesting opportunities
- Alternative blockchains such as the one proposed by Ethereum allow for simple contracts to be embedded in the blockchain and offer great promise
- Blockchain not going away