The Blockchain Identity

Campbell R. Harvey

Duke University, NBER and

Investment Strategy Advisor, Man Group, plc

Revised August 17, 2017

Blockchain is a technology

There is no “the” blockchain … blockchain is a technology.

- Concept invented by Haber and Stornetta (1991) in the context of time-stamping digital documents.
- Also, blockchain is not bitcoin. Bitcoin uses a blockchain technology.

J. Cryptology (1991) 3: 99–111

Journal of Cryptology
© 1991 International Association for Cryptologic Research

How To Time-Stamp a Digital Document[1]

Stuart Haber and W. Scott Stornetta
Bellcore, 445 South Street,
Morristown, NJ 07960-1910, U.S.A.
stuart@bellcore.com stornetta@bellcore.com

Blockchain is a ledger

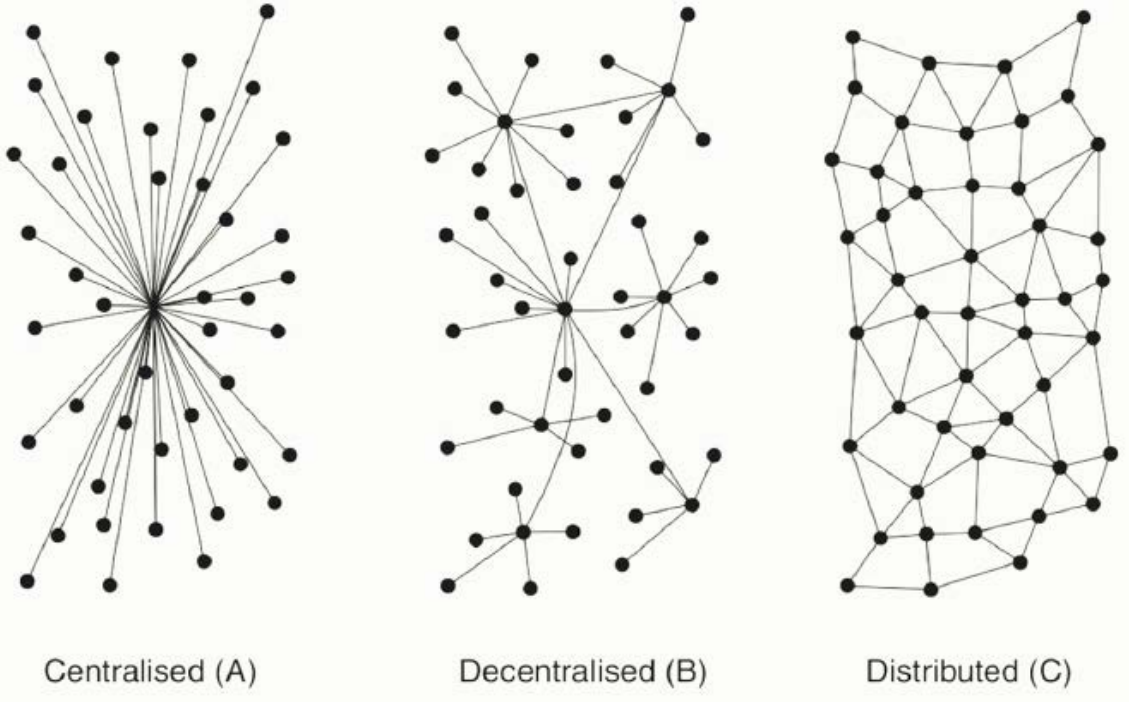
A very special ledger…

- Quickly and easily accessed and shared by many -- distributed

Blockchain is a ledger

A very special ledger…

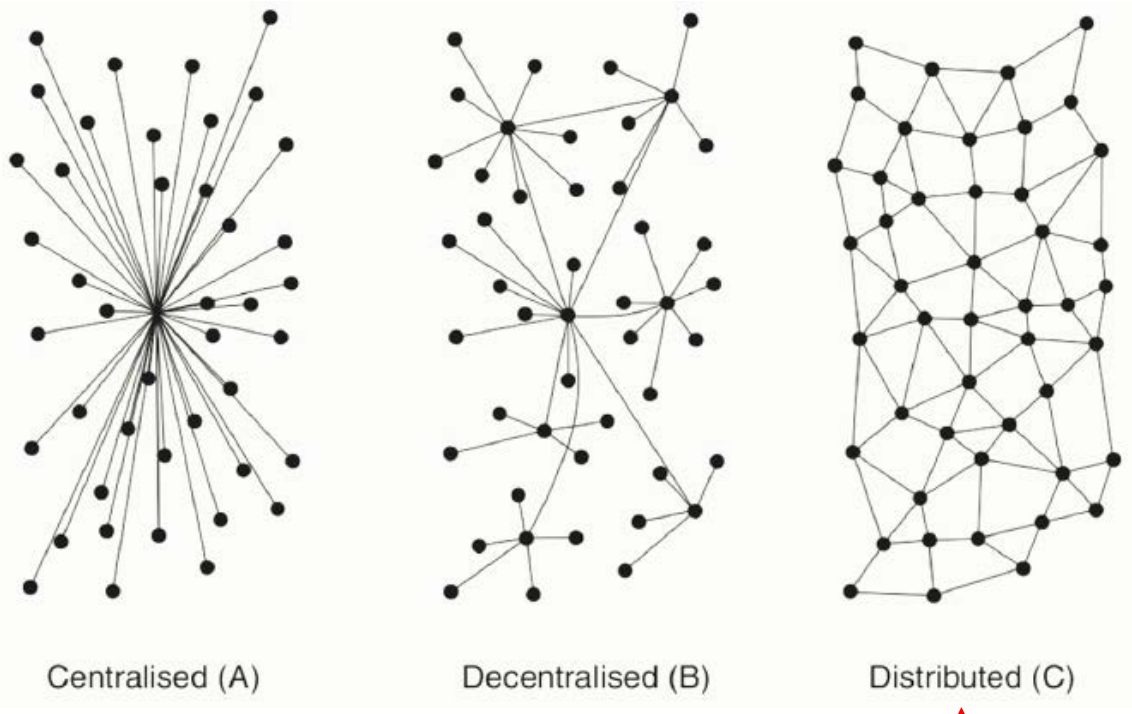
- Quickly and easily accessed and shared by many -- distributed



Blockchain is a ledger

A very special ledger…

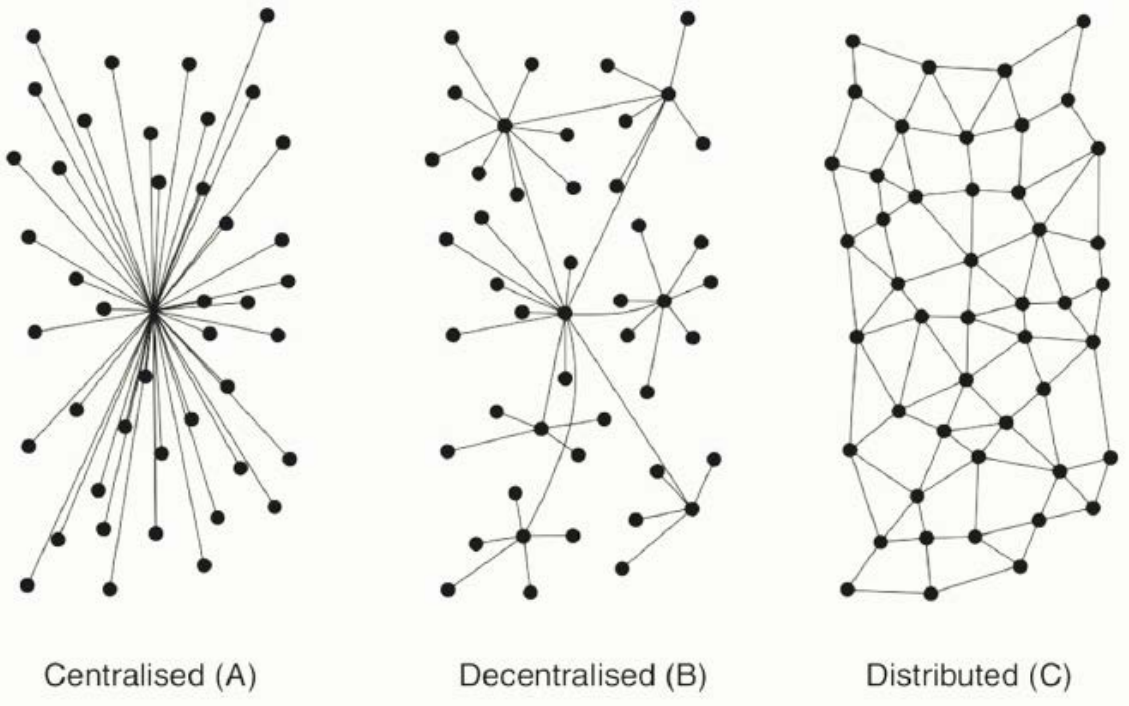
- Quickly and easily accessed and shared by many -- distributed



Blockchain is a ledger

A very special ledger…

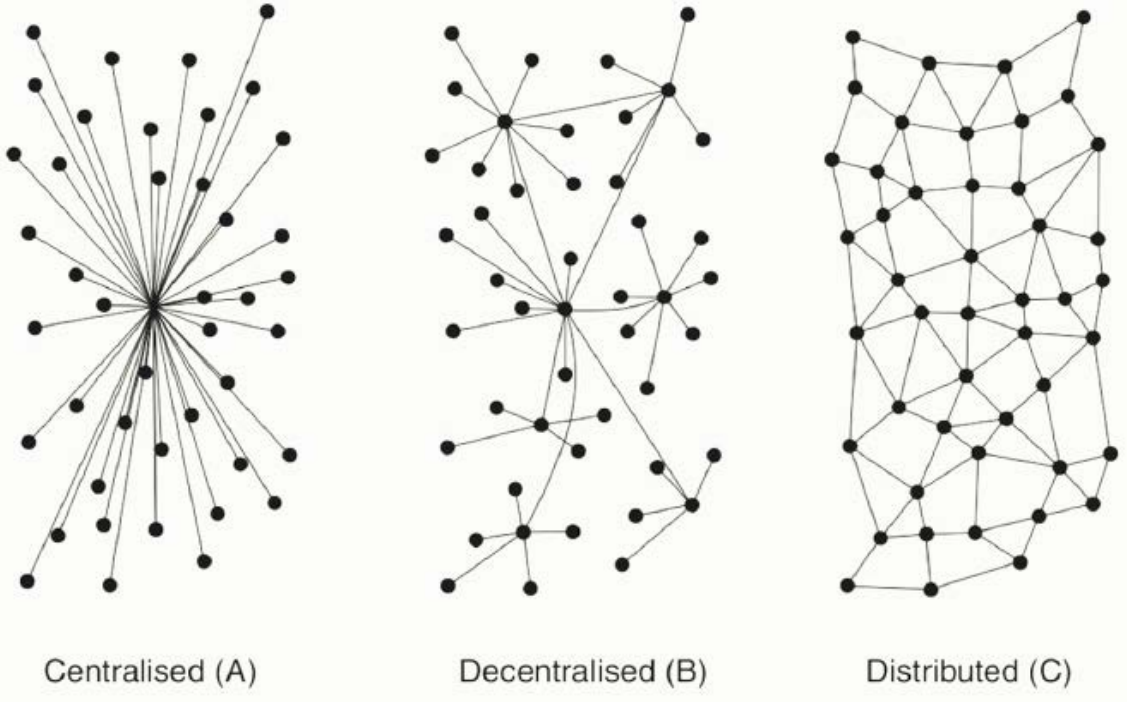
- Quickly and easily accessed and shared by many -- distributed
- Various levels of transparency depending on application
- Immutable (you can only add to it – you cannot alter history)

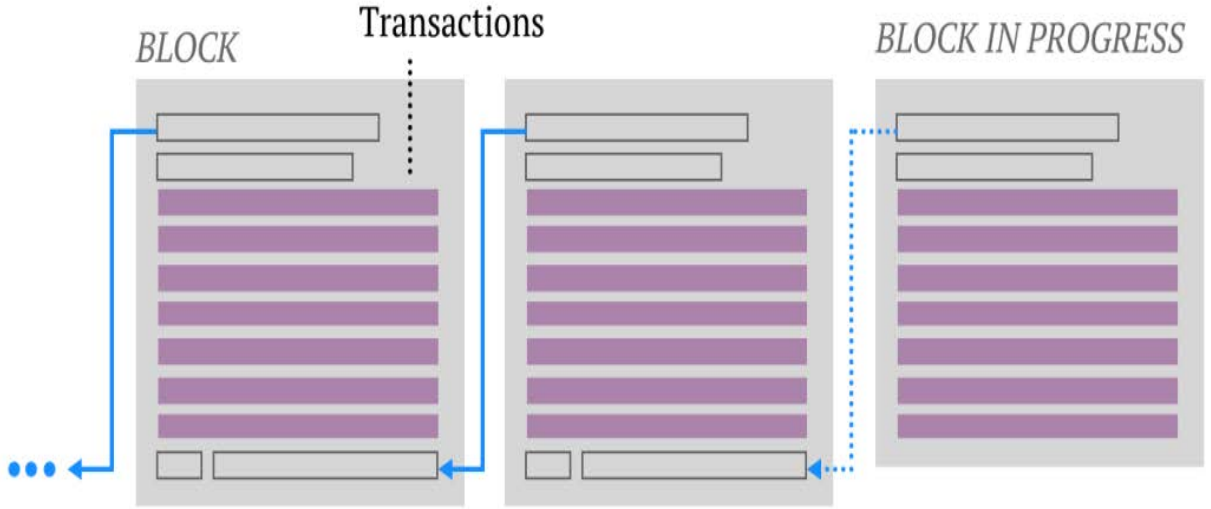


Blockchain is a ledger

A very special ledger…

- Quickly and easily accessed and shared by many -- distributed
- Various levels of transparency depending on application
- Immutable (you can only add to it – you cannot alter history)
- Cryptographically secured

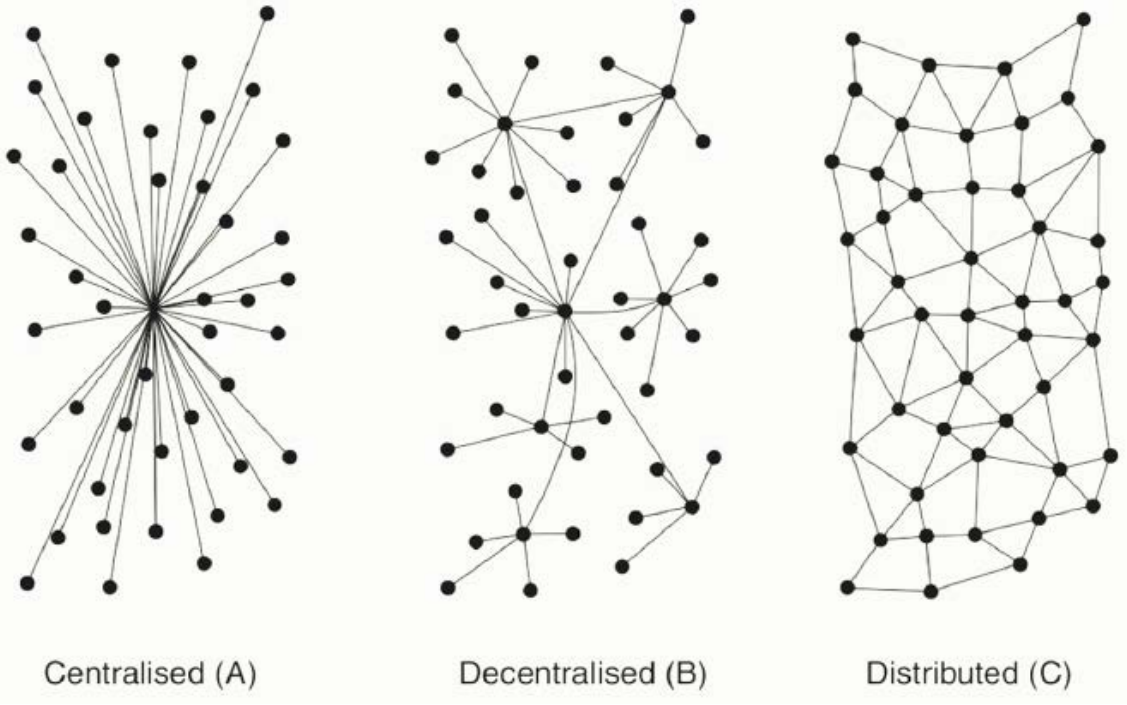


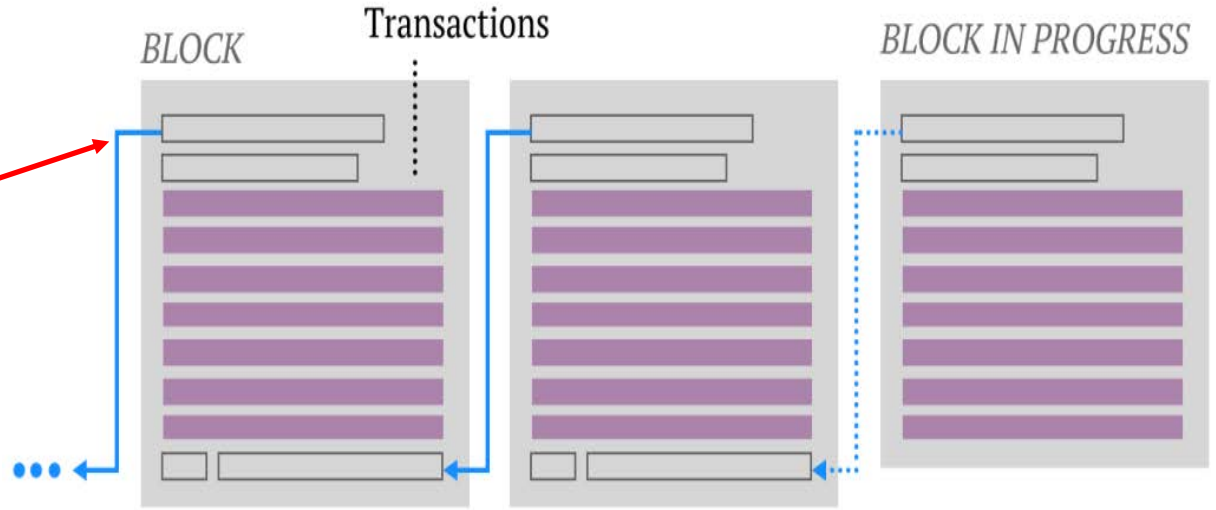


Blockchain is a ledger

A very special ledger…

- Quickly and easily accessed and shared by many -- distributed
- Various levels of transparency depending on application
- Immutable (you can only add to it – you cannot alter history)
- Cryptographically secured





What can blockchain technology do?

Solves many problems

- Verification of ownership (quickly check the immutable history recorded on a blockchain to see if someone owns something)
- Efficient exchange of ownership (direct transactions without middle person, everybody treated the same whether customer, retailer or banker).

Imagine …

Buying and selling stock with t0 settlement

- Today is t+3 not much different than the 1920s
- All stock transactions would reside in a secure ledger devoted to a company's equity

Imagine …

Closing on a property 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 <u>secure</u> 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 …

Starting your car with your thumb print

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

Prime targets of disruption

Any situation with a thick layer of middle people

- Blockchain is fundamentally a P2P technology.

Types of blockchains

Public blockchains

- Trustless. Original example bitcoin blockchain. Open source code.
- Ethereum blockchain allows for contracting and is the main choice for most corporate applications. Contracts can be conditional, if then statements. Bitcoin blockchain cannot do this.
- Variety of mechanisms to ensure security (Proof of Work, Proof of Stake, Proof of Authority, Zero Knowledge Proof, etc.)

Types of blockchains

Private blockchains

- Trust required.
- Need to determine if the cost of trustlessness is worth it. Most applications today involve trust. Combining blockchain technology with trust allows for much more efficient transactions (think of payments)

In the news….

We should understand the cover stories in *The Economist*

In the news….

The New York Times

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.

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

In the news….

Spotify aiming to solve its unpaid royalties problem with acquisition of Mediachain startup

Chance Miller - Apr. 26th 2017 4:47 pm PT @ChanceHMiller

SPOTIFY

Spotify buys blockchain startup, April 26, 2017

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 84,521,630 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

http://bitcoincharts.com/bitcoin/ http://www.top500.org/ https://www.top500.org/statistics/perfdevel/

Hashing 101

A simple hash

Suppose I send an email to Marie. However, she needs to verify that what I sent her 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 Marie gets my email, she does the same hash and checks my website.
- If the message was corrupted the hash will not match, for example, “hallo”= 8x1x12x12x15=17,280 which does not match the original.
- This hash is too simple (e.g. hello=ohell) and causes a “**collision**”

Hashing 101

SHA-256 (Secure Hashing Algorithm)

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

Hashing is a one-way function.

Hashing is not "encryption" because you can't decrypt.

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)
  47f63b8cd8470051acd3a3c0bd5c77c4aa9574d79cf5bfb3e576facabbc11491

- 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 $2^{255} = 1.15*10^{77}$ 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/

Hashing 101

SHA-256 hashes widely used for email and file transfer

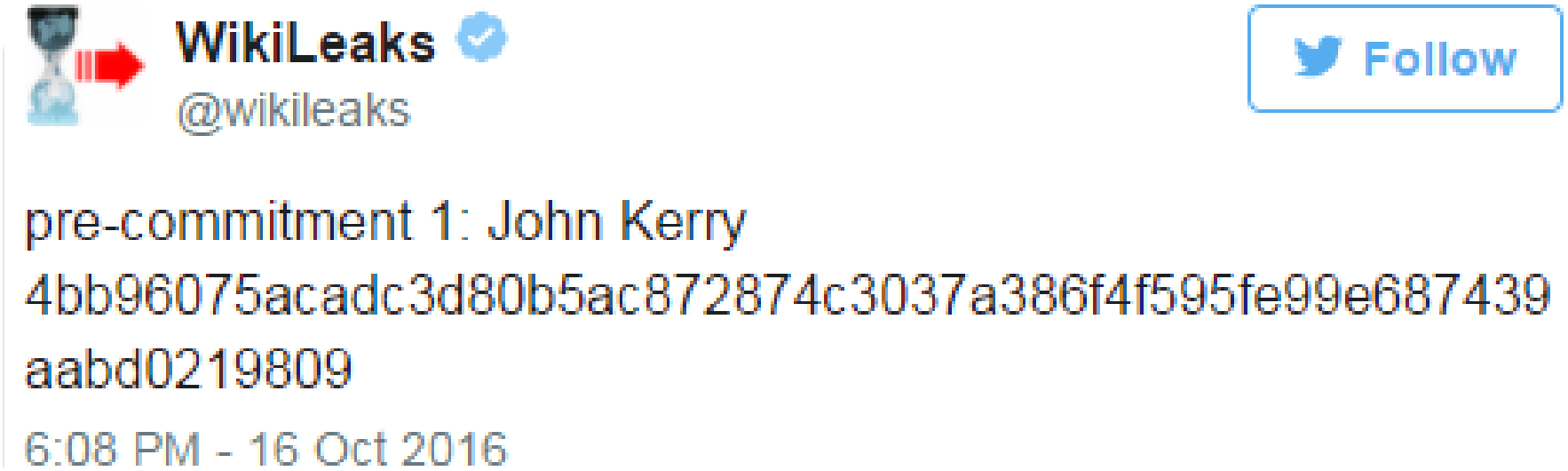
- Returning to the email example, I want to send a file to Marie
- I SHA-256 the file
- I send Marie the original file
- Marie does her own SHA-256 hash of the file
- Marie checks to see if her hash of the file matches the hash that I have on my website
- If there is any difference, the file has been 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.



How does the bitcoin blockchain work?

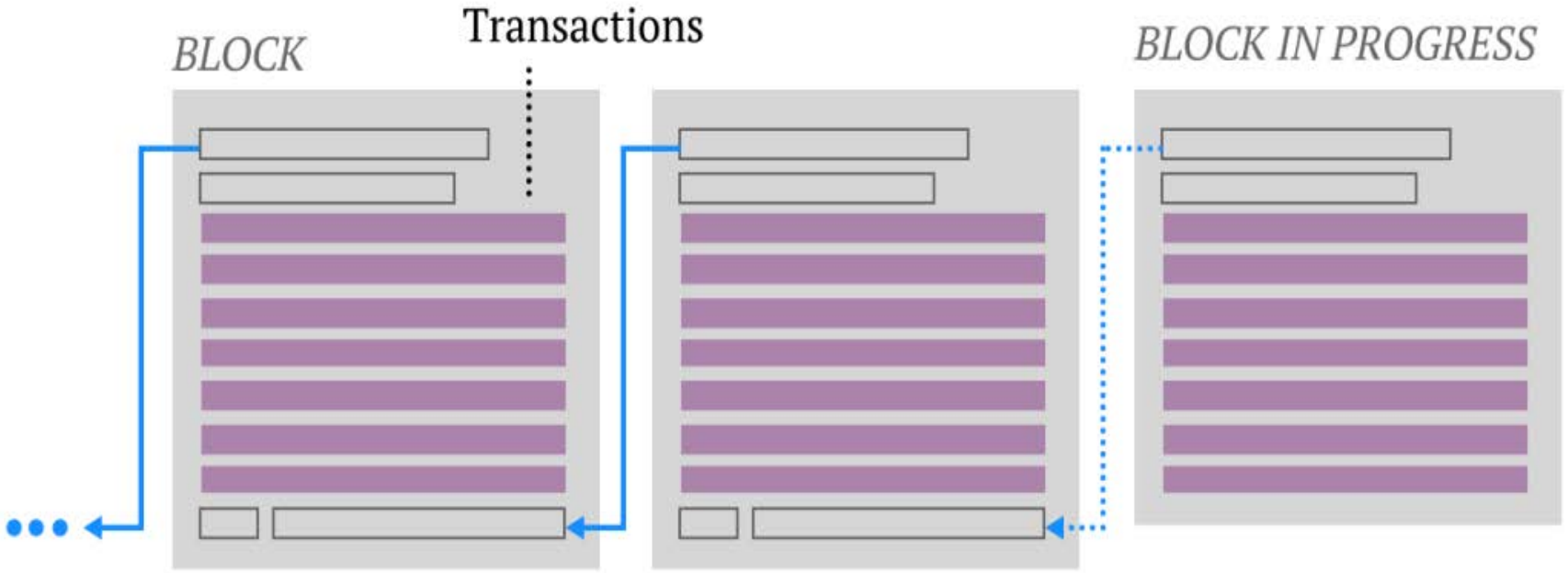
Every transaction ever made on this blockchain is public

- 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?

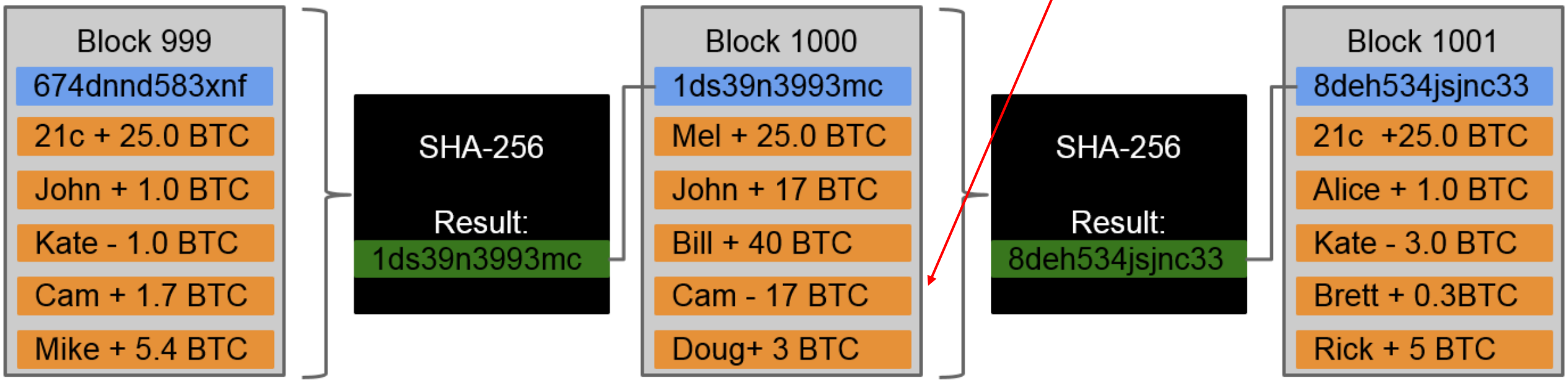
Ledger broken up into 10 minute “blocks”

- 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?

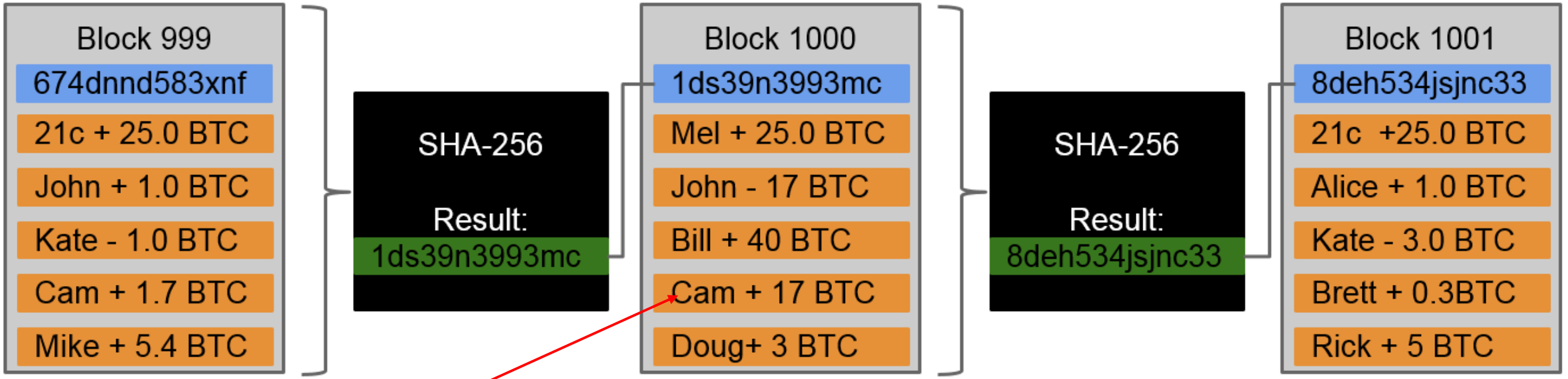
Example. In block 1000, I buy a car (for 17 BTC) from John



How does the bitcoin blockchain work?

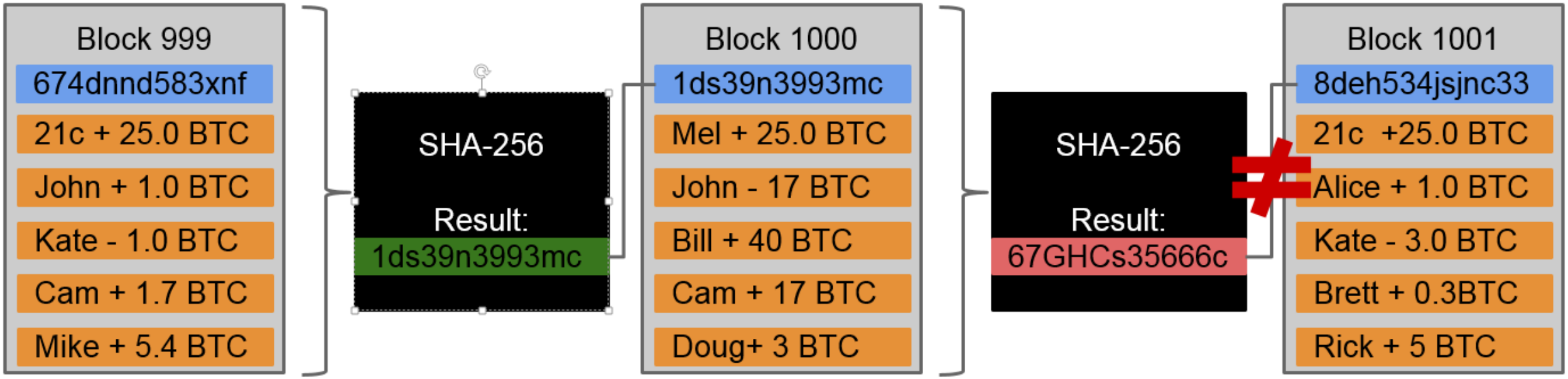
Suppose I edit the block on my computer – to give me 17 BTC!

I then broadcast to the network



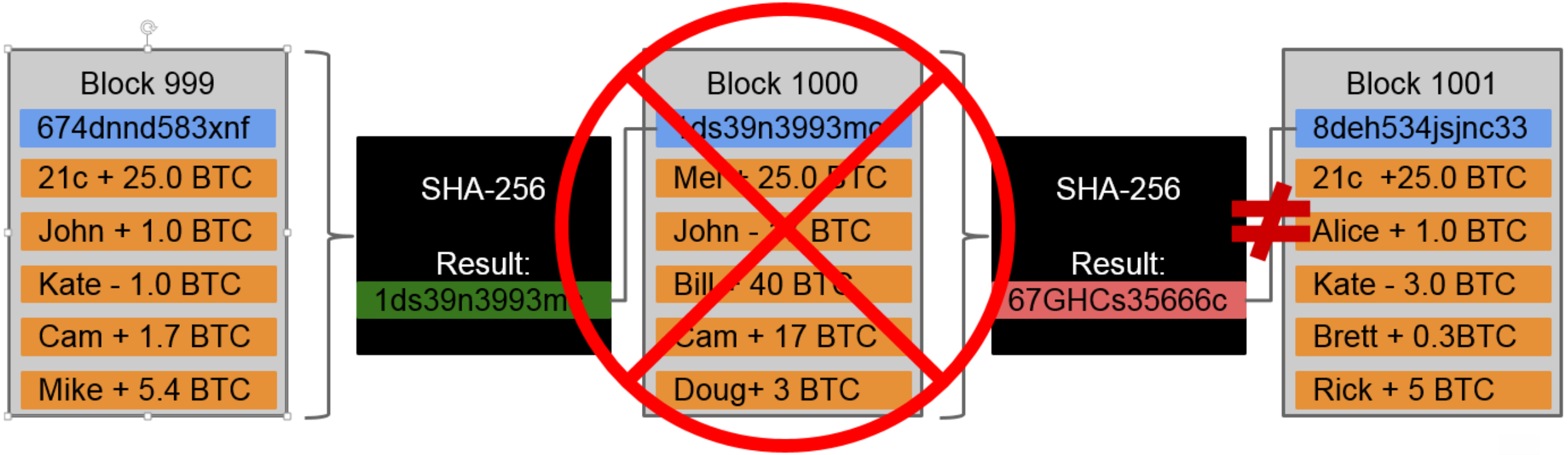
How does the bitcoin blockchain work?

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?

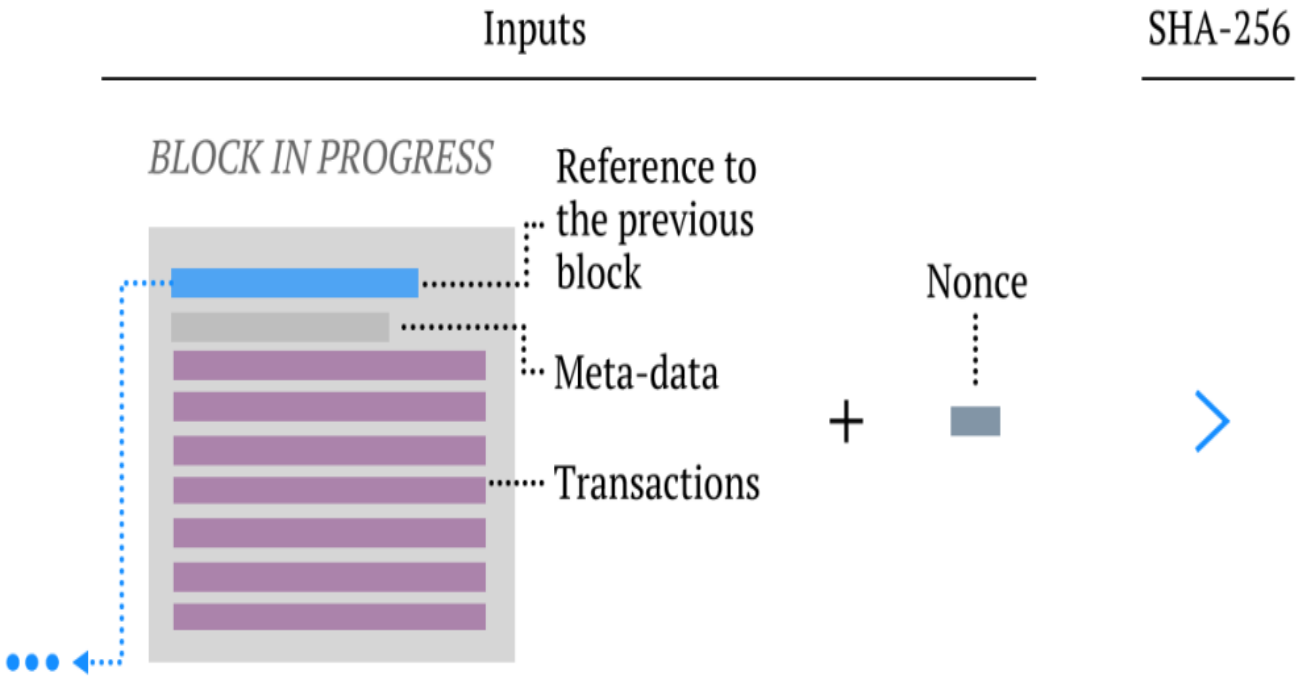
Blockchain clients automatically compute the hash themselves - if no match, they reject the block - Check other peers in the network for correct block



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. You 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 18 leading zeros! Probability = $(1/16)^{18}$
- Odds of winning two Powerball jackpots* in a row approx $(1/16)^{15}$
- Someone finds the winning hash approximately every 10 minutes
- This means 3.4 billion gigahashs 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; 18 zeroes in winning hash 2.117E-22

** https://blockchain.info/charts/hash-rate Note 1 gigahash=1 billion hashes

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 18 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

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

Private blockchains

This is where permissioned blockchains enter

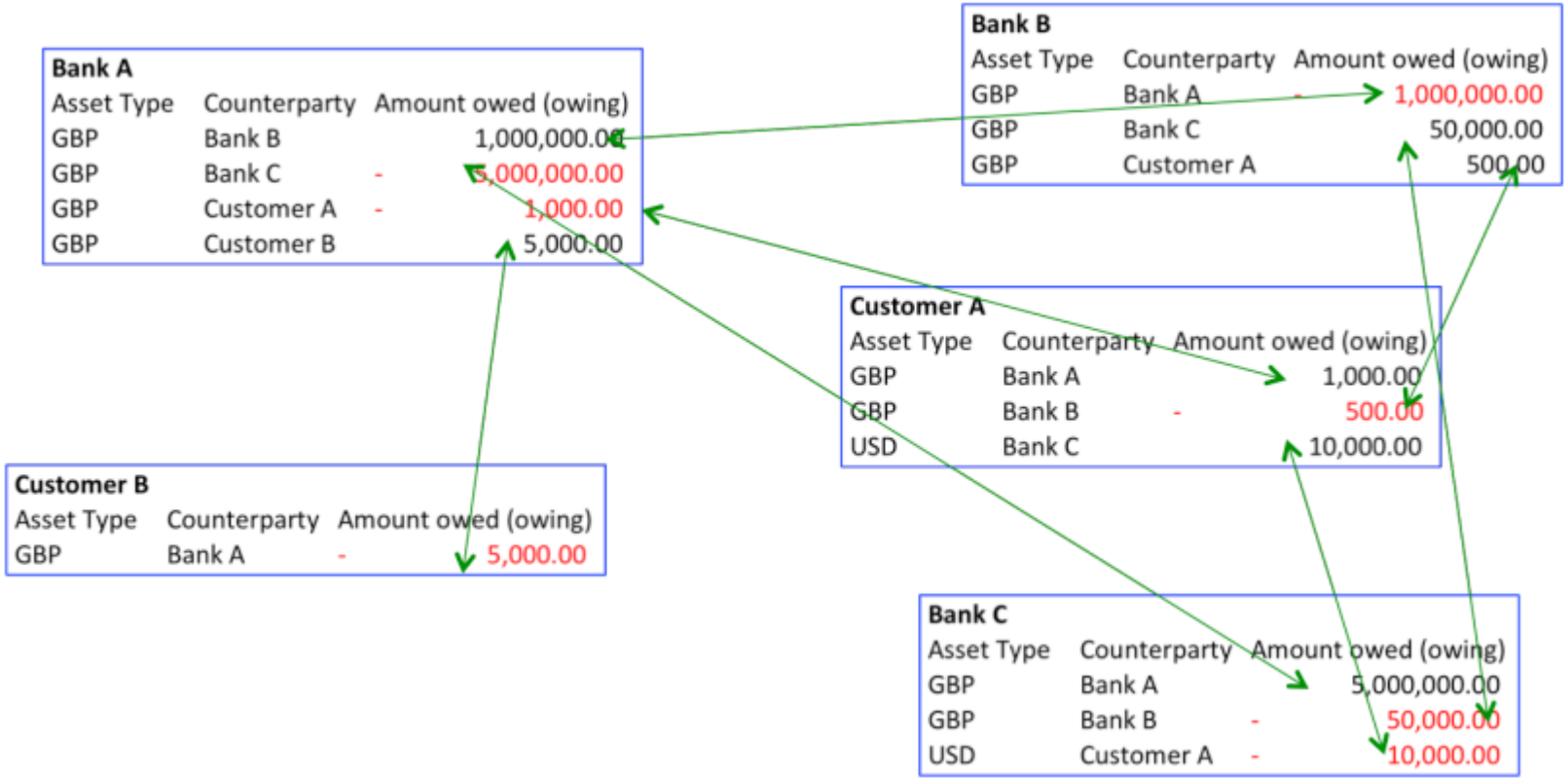
- Most major banks are now in this space (plus consortia R3 and DAH-Hyperledger)
- Currently, bank accounting systems are inefficient where each bank has its own independent ledger
- Having a unified but distributed ledger is very attractive: obvious cost savings on technology, instant transactions across 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



http://gendal.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

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

Private blockchains: Example

JP Morgan's Quorum

- Ethereum based private chain
- Blockchain includes encrypted versions of all contracts
- For a specific contract, only the parties to the contract have the ability to decrypt the contract
- So their blockchain includes all history, is immutable, but you can only see the transactions you are a party to
- Disrupts back office functions – large cost savings

Machine to Machine Payments

Three stages of the Internet

- Initially, a way to gather information (via search or just visiting a website).
- Next, social media where new communities were enabled by the Internet.
- Over the next few years, the third wave will be machine to machine payments enabled by the Internet.

Machine to Machine Payments

Current payments on the Internet

- Today, it is possible to pay for things on the Internet. However, the technology is clunky. APIs allow you to enter credit card or bank information.
- Current payments are only feasible if they are of sufficient size.
- Merchants face a 3% credit card fee.
- You need to have a credit card or bank account to play in this space.

Machine to Machine Payments

With today's technology, there are severe constraints

- Consumers pay for things but they cannot be paid.
- It is infeasible to think about forcing customers to pay, say 5 cents to visit your webpage and it is equally infeasible to think about paying someone to visit your website or advertisement.

Machine to Machine Payments

It is generally not known that machine to machine payments are possible in HTTP – they just aren't used.

- Look up HTTP 402 code (you all know the frequent 404 error – website not found).

402 Payment Required
Reserved for future use. The original intention was that this code might be used as part of some form of digital cash or micropayment scheme, but that has not happened, and this code is not usually used.

https://en.wikipedia.org/wiki/List_of_HTTP_status_codes

Machine to Machine Payments

It is generally not known that machine to machine payments are possible in HTTP – they just aren't used.

- It is feasible to exchange funds (instantly, seamlessly, and securely) in a secure way using a digital cryptocurrency in the background using current blockchain technology.
- 21.co is the leading company in this space and they are well funded by one of the most highly-respected venture capital firms in the world, A16Z

Machine to Machine Payments

Tasks and demographic information

- Amazon Turk has essentially farmed out tasks. However, they operate in only two countries (U.S. and India) and payments for the tasks are made once a month.
- Using HTTP combined with a cryptocurrency wallet, the payments are instant. Further, you do not need a traditional bank account.
- Think of getting into an Uber and completing a few surveys during your ride. For each survey, you get $2.50. Enough to pay for the Uber.
- Some of these tasks are explicitly learning about your preferences. That is, you are offering up your demographic profile.

Machine to Machine Payments

A new way to think about email

- At the top of your inbox are emails from your work, friends and family.
- However, companies pay you to accept email from them.
- The highest paying company will have the highest placement in your inbox.
- If you open the email, you are also paid. If you click on a link in the email, you may be paid more.

Machine to Machine Payments

Email is no longer free

- Everybody pays to send an email.
- If I am sending to a friend, the fee is very low, say 1/10th of a cent.
- Companies will pay far more if my demographic profile is attractive to the company.
- As a side benefit, spam is eliminated. Over half of all Internet email traffic is spam today.
- In terms of the economics, it is never efficient to price something at zero.

Machine to Machine Payments

The web is no longer free

- In this world, almost every site you visit you pay a small fee.
- The fee is so small that it does not deter even the poorest user in Africa.
- While small, this fee puts the entities that engage in DDoS attacks out of business – freeing up about one third of the current bandwidth.

M2M will disrupt …

Google and Facebook account for 80% of online advertising

Models like Google AdWords are <u>not sustainable</u> in the M2M world

- Google has $90b in advertising revenue in 2016.

Micropayments will disrupt:

- Cellular service, audio/video/ pay-for-view, computing, storage, share economy, etc.

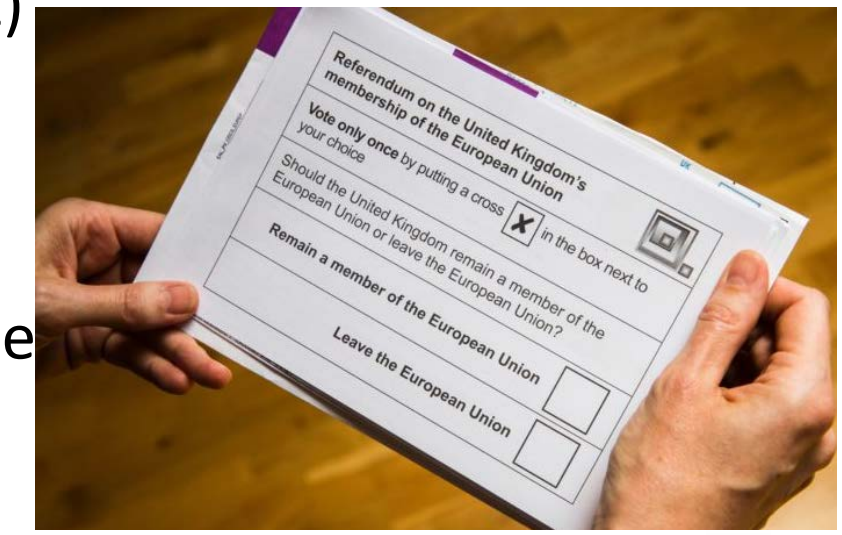
Campbell R. Harvey 2017

https://searchenginewatch.com/2016/05/31/the-most-expensive-100-google-adwords-keywords-in-the-us/

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”



https://crypto.stanford.edu/pbc/notes/crypto/voting.html

Blockchain applications

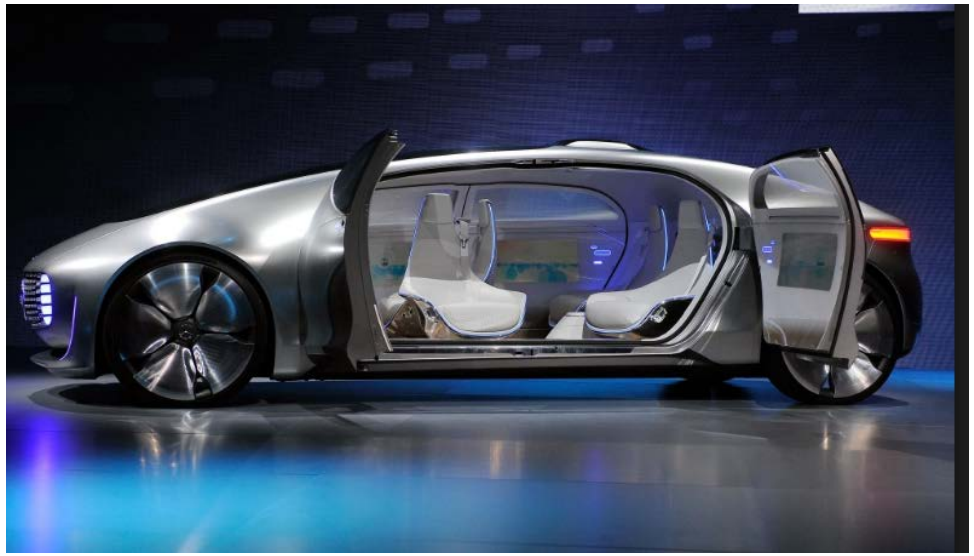
Internet of Things

- 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

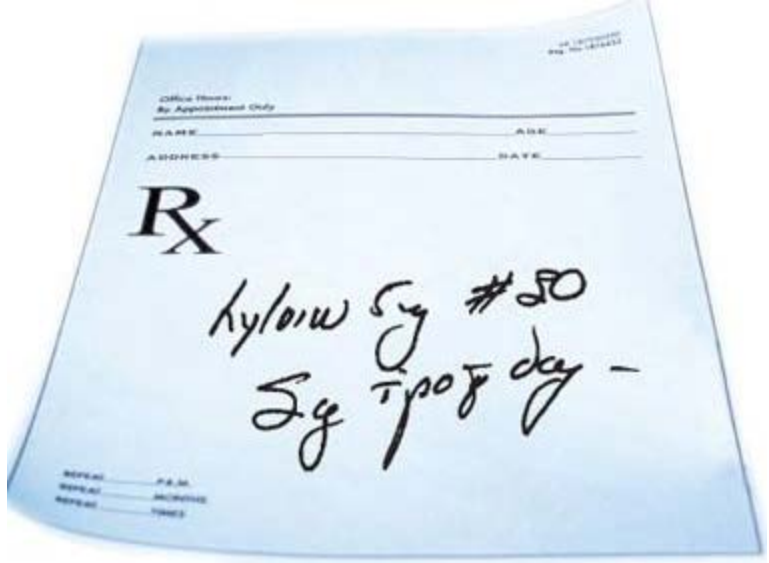
Blockchain applications

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

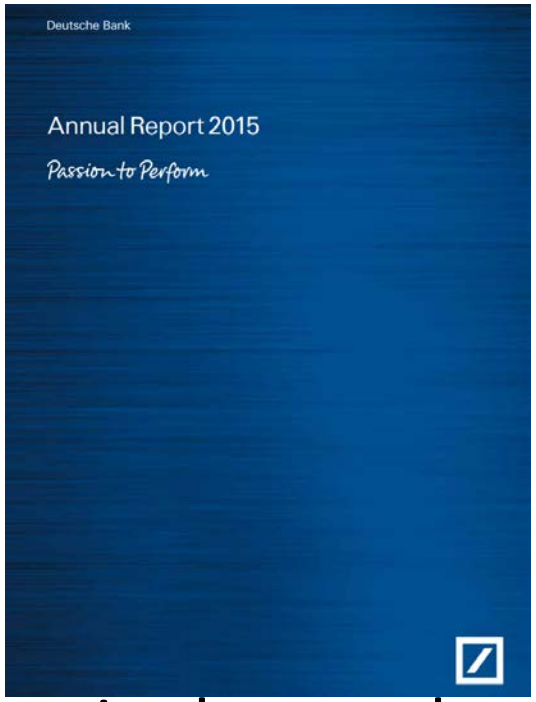
- Widespread fraud
- Blank scripts are stolen from doctors' offices or forged
- Some doctors abuse the system
- Token issued to patient: it cannot be resold and has an expiration
- Patient presents token to pharamacist and blockchain is checked to make sure patient owns the token (and has not already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

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

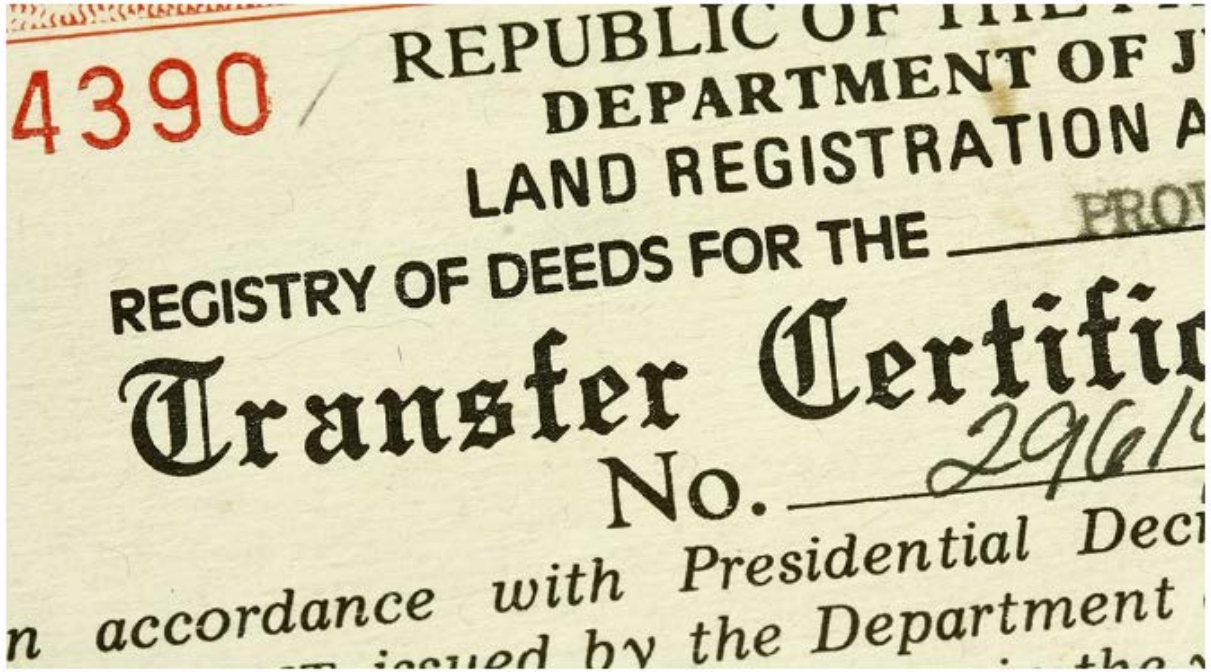
Property

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

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

Digital Twins

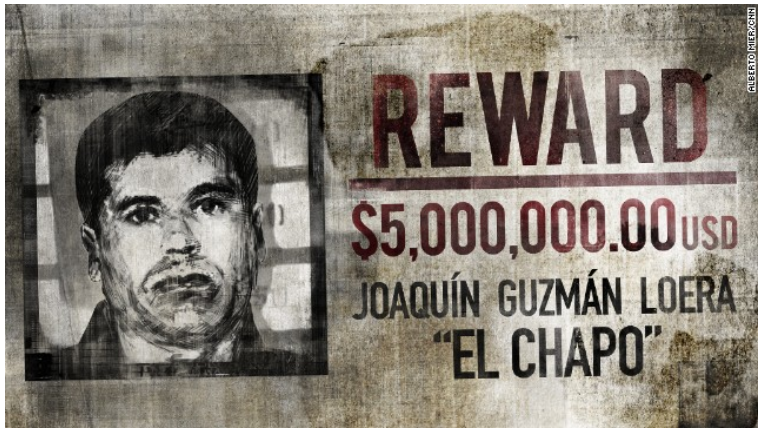
- Example: Jet engine
- Every part, every replacement part, every electronic sensor reading for the complete life of engine in a blockchain-based construct
- Easily monitored and easily transferred if the plane is sold

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

https://www.federalreserve.gov/paymentsystems/coin_currcircvalue.htm

Blockchain applications

Central banks

The Telegraph

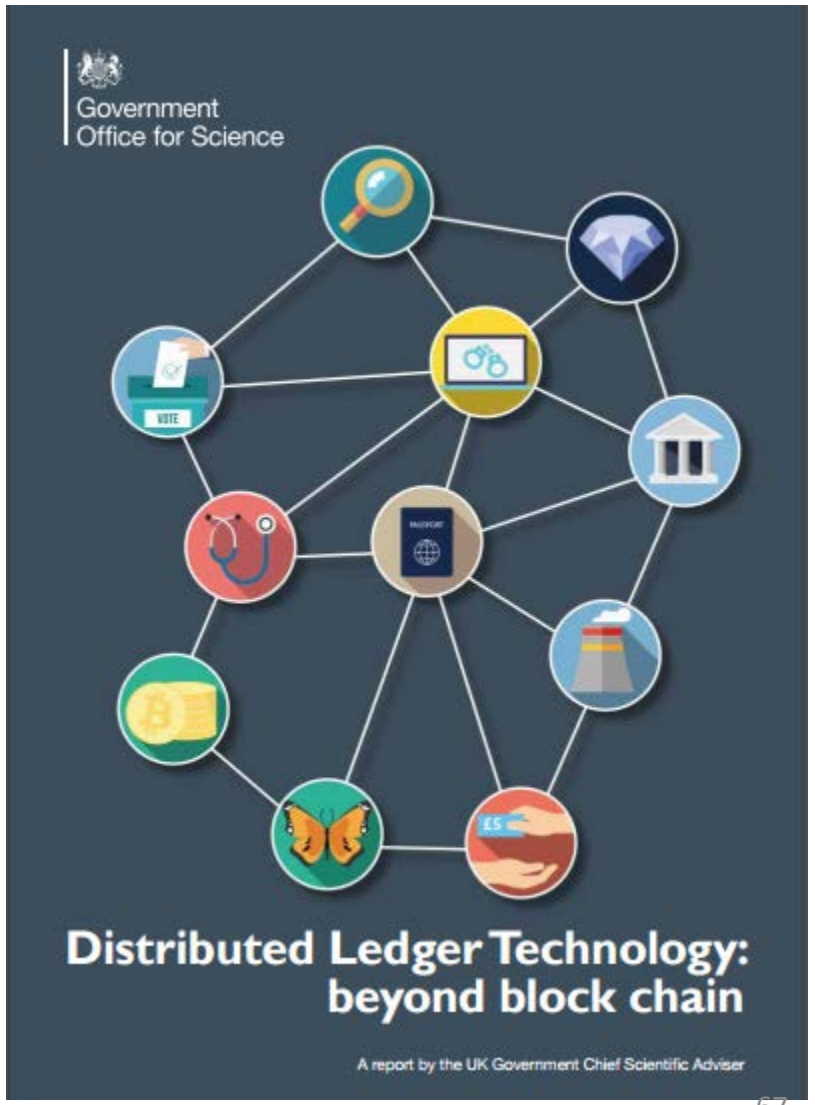
HOME | NEWS | SPORT

Business

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

Business

Central banks beat Bitcoin at own game with rival supercurrency



Blockchain applications

2017 Duke's Innovation and Cryptoventures course:

- Smart guns
- Entertainment and sports ticketing
- Government benefit programs
- Humanitarian aid
- Identity
- Single password for all accounts
- Educational and test score records
- Agricultural supply chain in India
- Aircraft leasing
- Digital twins for large medical devices like CT and MRI

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

More information

Innovation and Cryptoventures syllabus (includes links to background articles and videos)
https://faculty.fuqua.duke.edu/~charvey/Teaching/898_2017/syl898.htm

Innovation and Cryptoventures links to course materials
https://faculty.fuqua.duke.edu/~charvey/Teaching/898_2017/syl898_Topics.htm

Duke Blockchain Lab
https://DukeBlockchainLab.com

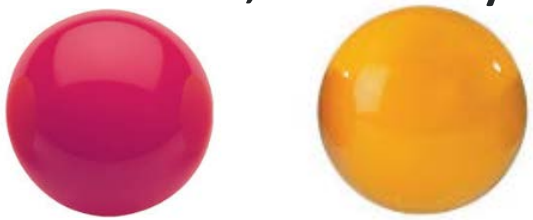
Appendix: Zero Knowledge Proof

How is a voting blockchain feasible if the government can see how everyone votes?

- The answer is a zero knowledge proof
- This means that you provide cryptographic proof that you are a valid owner of a voting token – yet you do not have to reveal who you are.

Appendix: Zero Knowledge Proof

- Imagine your friend is color-blind.
- You have two billiard balls; one is red, one is yellow, but they are otherwise identical.



- To your friend, they seem completely identical, and he is skeptical that they are actually different. You want to prove to him that they are differently colored. On the other hand, you do not want him to learn which is red and which is yellow.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Appendix: Zero Knowledge Proof

Proof system:

- You give the two balls to your friend so that he is holding one in each hand.
- You can see the balls at this point, but you don't tell him which is which.
- Your friend then puts both hands behind his back. Next, he either switches the balls between his hands, or leaves them as they are.
- Finally, he brings them out from behind his back. You now have to "guess" whether or not he switched the balls.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Appendix: Zero Knowledge Proof

Proof system:

- By looking at their colors, you can with certainty whether or not he switched them. If they were the same color and hence indistinguishable, there is no way you could guess correctly with probability higher than 1/2.
- If you and your friend repeat this "proof" T times (for large T), your friend should become convinced that the balls are indeed differently colored; otherwise, the probability that you would have succeeded at identifying all the switch/non-switches is at most $(1/2)^T$
- Furthermore, the proof is "zero-knowledge" because your friend never learns which ball is yellow and which is red; indeed, he gains no knowledge about how to distinguish the balls.

http://mathoverflow.net/questions/22624/example-of-a-good-zero-knowledge-proof

Appendix: 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

Appendix: Permissioned blockchains

Private blockchains disadvantages

- Are they as secure as bitcoin blockchain? Potential issues with banks holding private keys and veryifying 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.

Appendix: Sidechains

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