Blockchain

Disruptive Service or Just Another Buzz Word?

28th April 2016

@jtdavies

Flow

C24

What is a Blockchain?

The pain in Blockchain's butt —> Bitcoin

Smart Contracts & how do they work

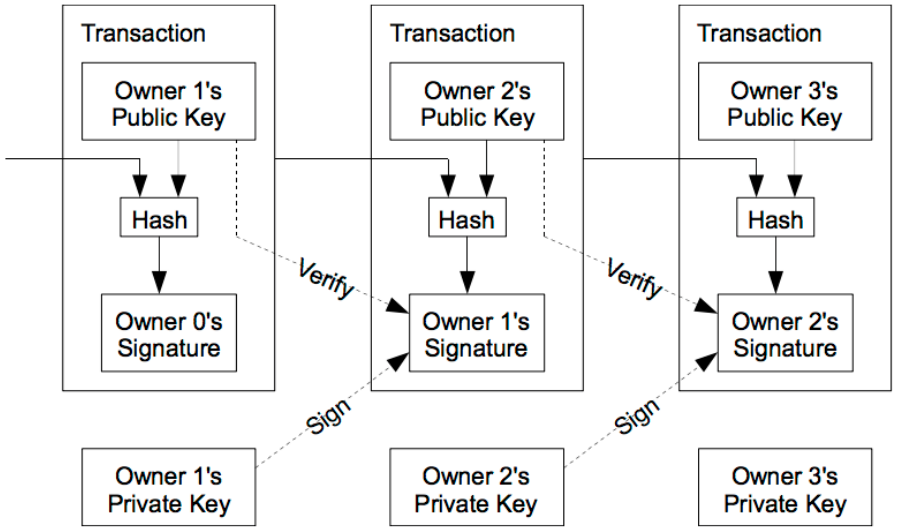
Potential problems and opportunities with Blockchain

Blockchain or Ledger?

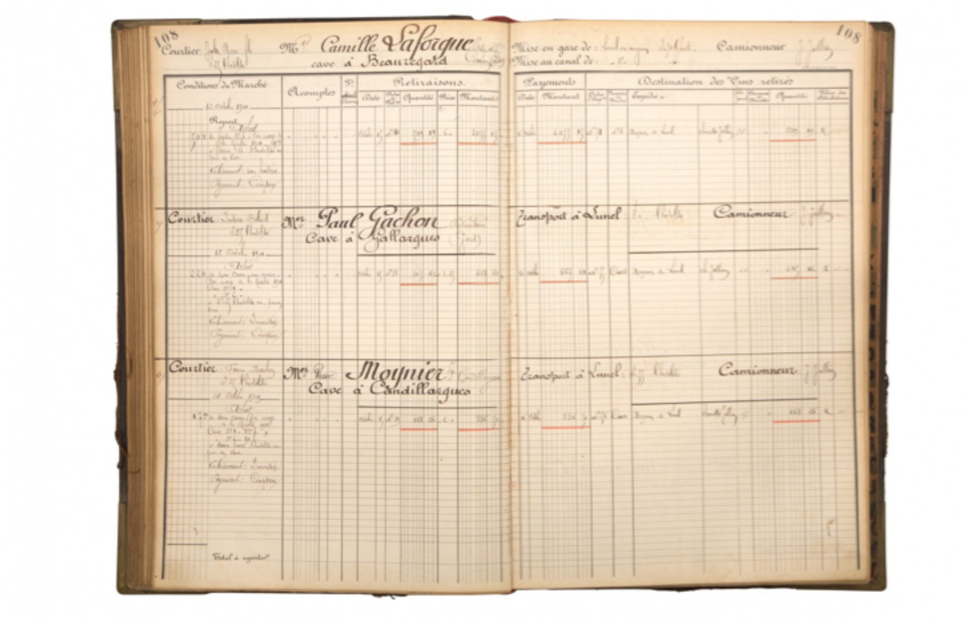
In most cases we can interchange the word blockchain with ledger

- Distributed Ledger, Permissioned Ledger etc. refer to distribute and permission blockchains respectively

Blockchain is the digital form of a ledger (not the only one though)



=



I will generally refer to blockchain today, I could use either

Digital signatures and Hashes

A digital hash or digest is the mathematics behind the blockchain

A hash is a mathematical seal on each record that proves it hasn't been changed in ANY way

It is virtually impossible to create a message to match a given hash

The likelihood of 2 different documents having the same hash value (a collision) is incredibly low

Hash examples

The SHA-256 hash of “C24 Technologies Ltd.” is…

- 0EE19D3551F3CC21D269BB7CBF9808BD2E14149A76C498B56FE8E33DD8C43D24

The SHA-256 hash of “C24 Technologies Ltd” is…

- A0DE2800299C8F5966AE270E6255E8D6EFFD42C761BEED659AC6D4E7EBCE5FB6

Google “482C811DA5D5B4BC6D497FFA98491E38” and you’ll find it’s an MD5 hash for “password123”

- This isn’t reverse-engineers but simply a dictionary previously known hashes

Hashes can be used for almost anything to “represent” large or complex files, document or contracts

On the command-line

You can use “md5” and “shasum” on any linux command line

- If you have Windows then delete it and install Linux

It’s best to use perl to strip the linefeed…

```
perl -e "print qq(C24 Technologies Ltd.)" | shasum -a 256
0ee19d3551f3cc21d269bb7cbf9808bd2e14149a76c498b56fe8e33dd8c43d24  -
```

If you just use “echo” you will get a line-feed (0x0A) included…

```
echo "C24 Technologies Ltd." | shasum -a 256
caa6ffd4a6a3a6a3044c9283c0ceb6e7dece7c80dda36d5894c00d5fcbc1763e  -
```

How to get a Hash in Java

Creating a hash in Java is extremely simple

```java
byte[] input = "C24 Technologies Ltd.".getBytes();
MessageDigest digest = MessageDigest.getInstance("SHA-256");
digest.update(input);
byte[] hash = digest.digest();
```

And you can turn it into Base64 or Hex equally simply…

```java
Base64.Encoder encoder = Base64.getEncoder();
String string = encoder.encodeToString(hash);
System.out.printf("Base64: %s%n", string);
System.out.printf("Hex: %s%n", DatatypeConverter.printHexBinary(hash));
```

How do we add a new contract to the chain?

With the contract…

- Take the hash from the previous record
- Add the details of the contract

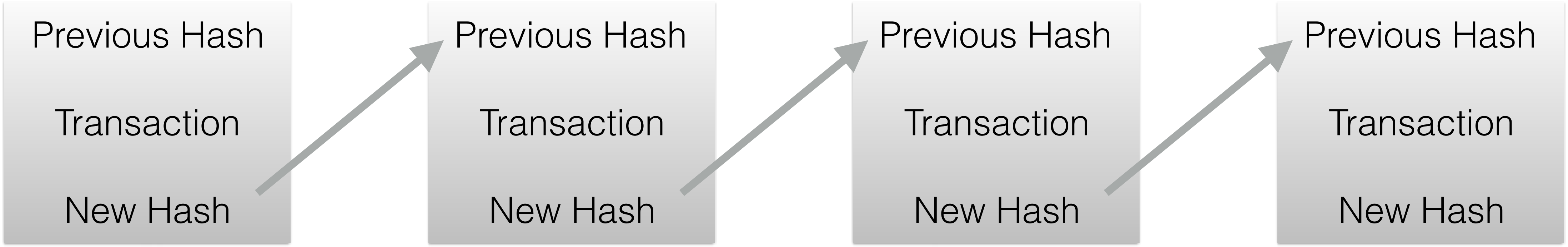
Hash everything to create a new hash

- Contract details, access permissions etc.

We can now either replicate the block or just distribute the hash

- Or both

We have a blockchain (pretty much)… A chain of blocks!



Previous Hash

Transaction

New Hash

Previous Hash

Transaction

New Hash

Previous Hash

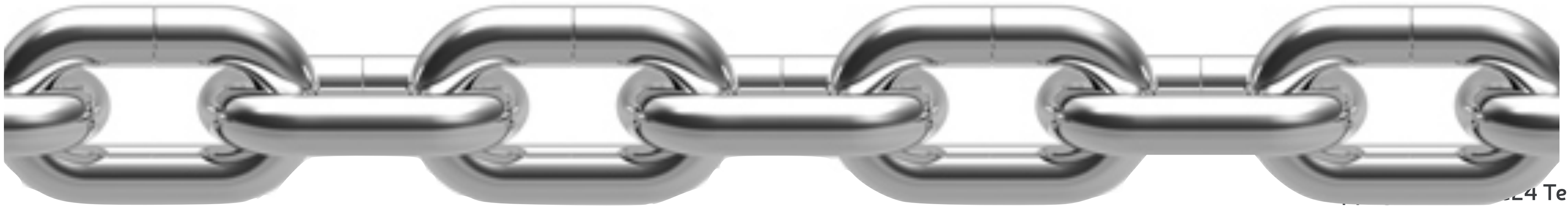
Transaction

New Hash

Previous Hash

Transaction

New Hash



Blockchain Distribution

We can keep the blockchain and distribute the hashes (centralised)

We can distribute the blockchain to trusted parties (de-centralised)

Or everyone can have a copy of the blockchain (distributed)

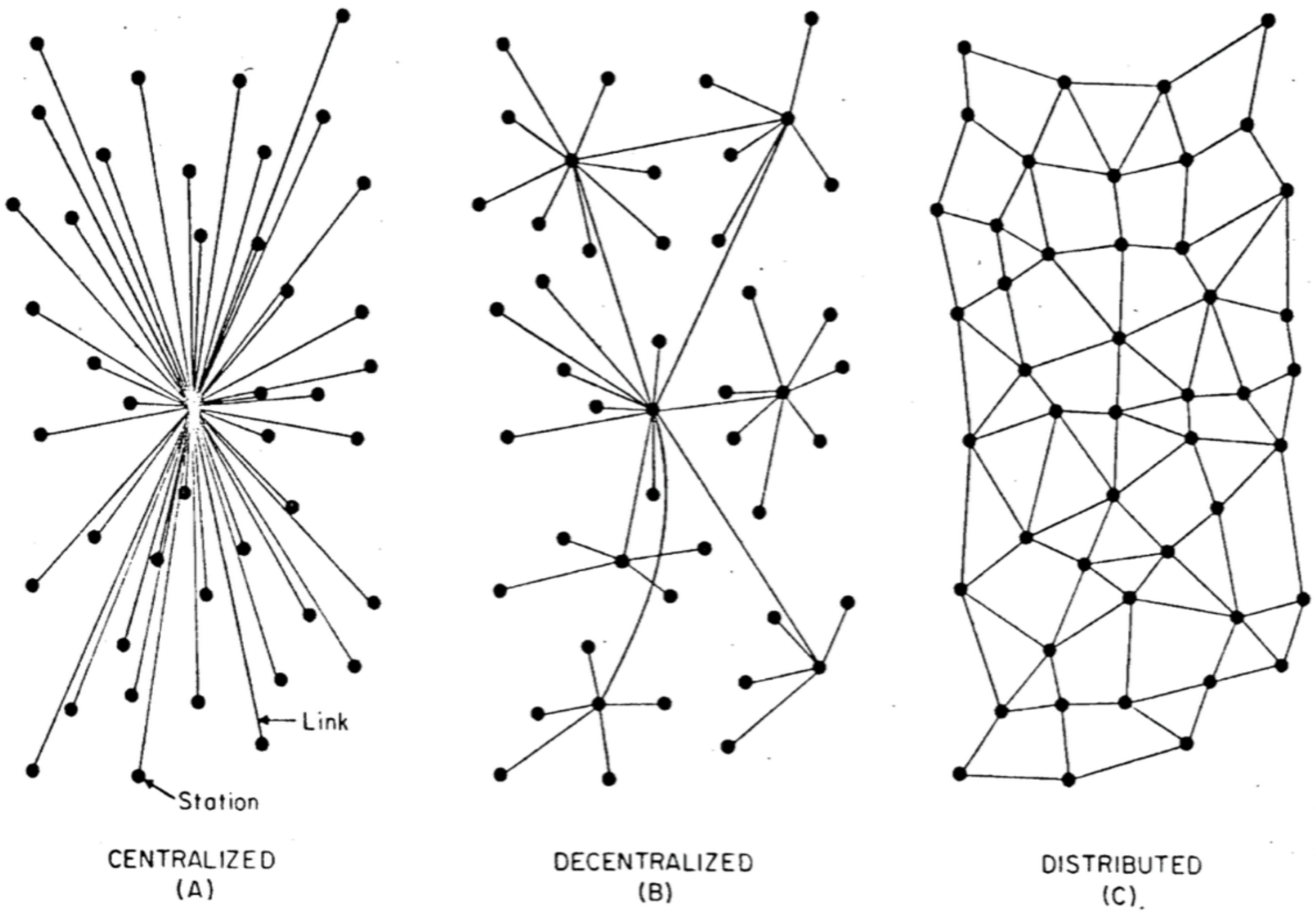


FIG. I — Centralized, Decentralized and Distributed Networks

Source: On Distributed Communications Networks - Paul Baran 1962

Permissioned or Unpermissioned

Unpermissioned

Since a distributed blockchain has no owner there can be no access controls, everyone must have access and identical copies

- This is the case for Bitcoin
- Consensus is slow and requires an anti-hacking mechanism

Permissioned

This is the more common model, additions to the blockchain must be checked by the owner(s) of the blockchain

A permissioned ledger has better integrity and is faster than an unpermissioned one

Blockchain in Bitcoin

BitCoin is a specific implementation of blockchain

- Sometimes called Blockchain 1.0
- It is **distributed** and **unpermissioned**

A bank or banks could have hosted BitCoin but avoiding “nasty” banks was the main ‘*raison d’être*’

BitCoin transactions are anonymous, this is achieved with another mathematical feature called Public Key Infrastructure (PKI)

Effectively the owner of the private key is owner of the bitcoins

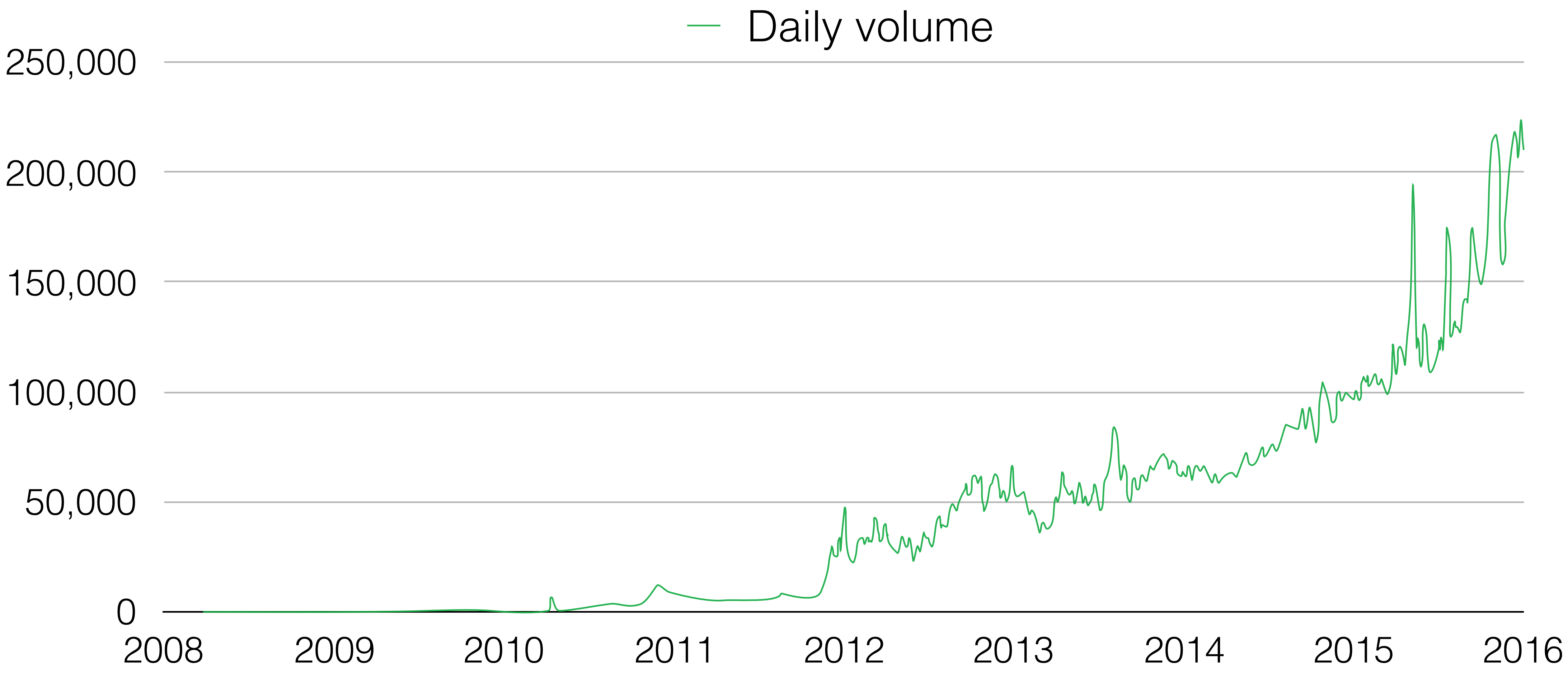
Anarchy?

C24

Bitcoin started after the financial crisis of 2007/8

Volumes have increased but it’s not exponential - watch this space!

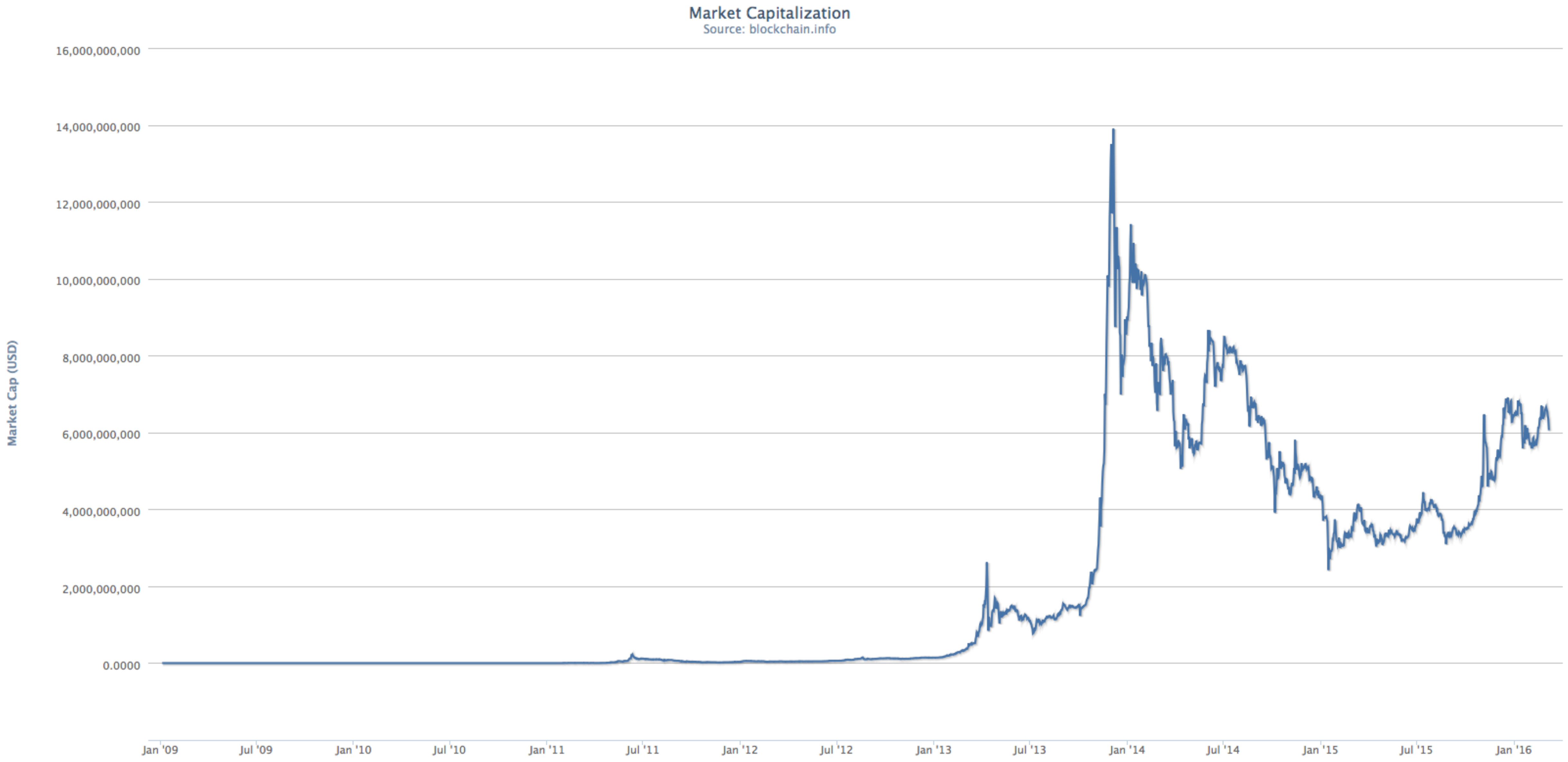
- Also worth noting is the tendency towards gold rather than Bitcoin in the recent (early 2016) market jitters



Market Capitalisation

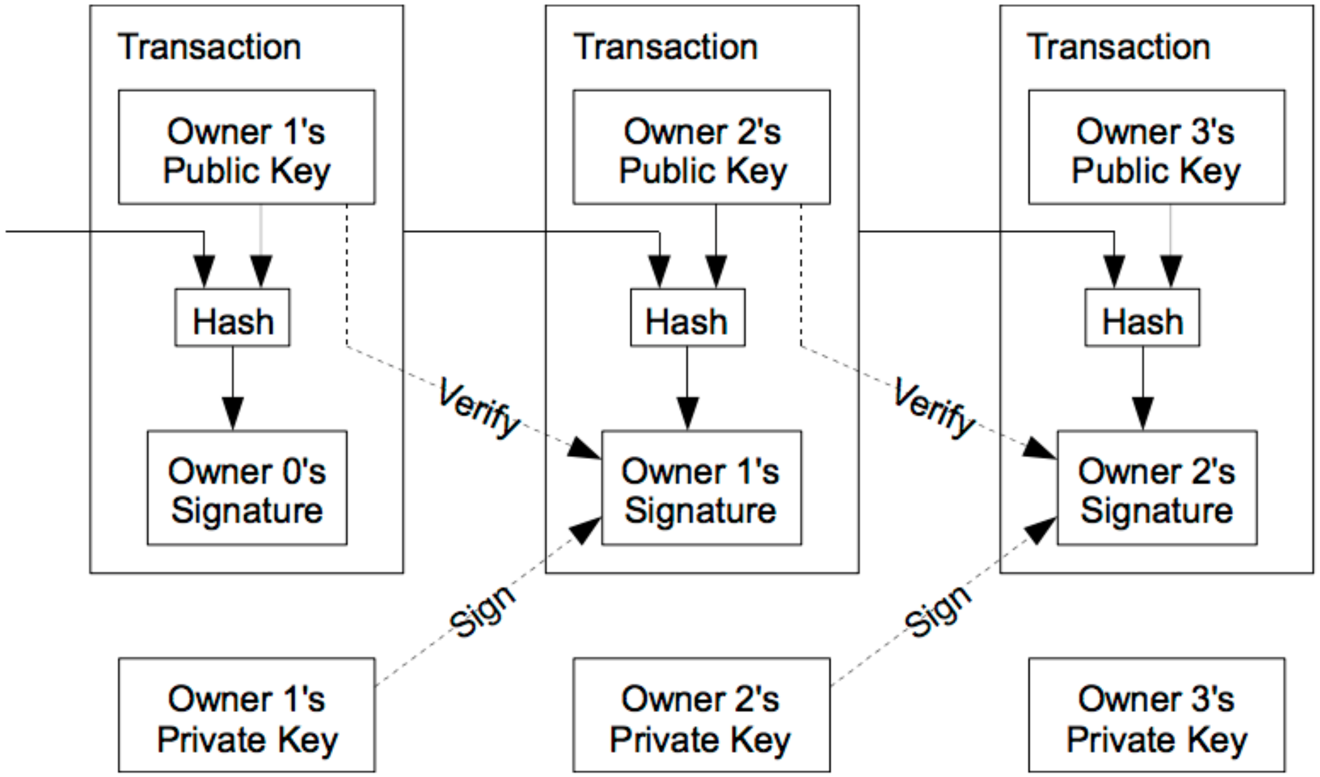
C24

Again it's not exactly revolutionary…



How does it work?

Only the owner of the private key (part of PKI) can unlock the coins in the public key account (BitCoin address)



Every BitCoin transaction is public, the sender, recipient, amount and date/time

- But the parties are anonymous (by choice)

With the sender initiating the transaction this is the opposite to traditional eCommerce

- The PSP starts by debiting of the card member (buyer)'s account first

Who holds the blockchain for Bitcoin?

Every record in the Bitcoin blockchain has a “proof of work”

The “work” is a seriously huge amount of computation

- Basically computers generate hashes with as many leading 0s as possible
- Given that the generated hash is “random” the chances of one leading 0 is 1:58, the chances of two are 1:58^2 and so on

10 leading 0s has a 1:430,804,206,899,405,824 chance

Each hash can be verified so “proof of work” is verifiable

- This is similar to SETI and requires huge computing resources

This is called Bitcoin “mining” and the effort is rewarded by bitcoins

- The reward must always be more than the potential gain from hacking bitcoin
- Almost any computer can mine but some are now designed with a specific purpose of BitCoin mining

Now you understand most of it

Blockchain at its most basic is a linked list of hashed records where the hashes become the proof

Bitcoin is a decentralised blockchain using PKI to secure ownership of coins

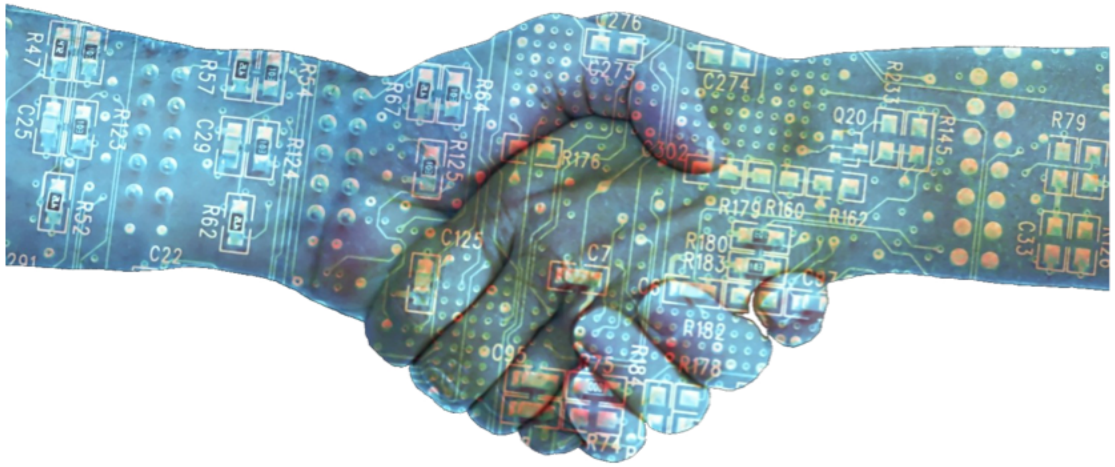
- There are a few other things like Merkle trees, difficulty level, nonces etc. but you have the basics
- New additions and alternatives like SideChains, LiteCoin, DogeCoin, NameCoin, Colored Coins, MetaCoins etc.

So why is everyone so excited about blockchain?

Smart Contracts

The Smart Contract

A Smart Contract is a block with more than just who pays what to whom for what by when



A Smart Contract can respond to messages and requests, you could call these actions

- In the object oriented programming world these are “methods” and the Smart Contract is an object

A novation on a CDS would be an excellent example of how a smart contract might be used

- `CDS.novate( contractID, securityCredentials, destinationLEI)`
- Method to access fields in the contract are also permissioned

Blockchain and Smart Contracts

Insurance - as I've attempted to demonstrate

Land and property registry

- Land often gets divided and sold in parts with leases

Software contracts

- How many CPUs, cores, users, duration, MIPS etc.

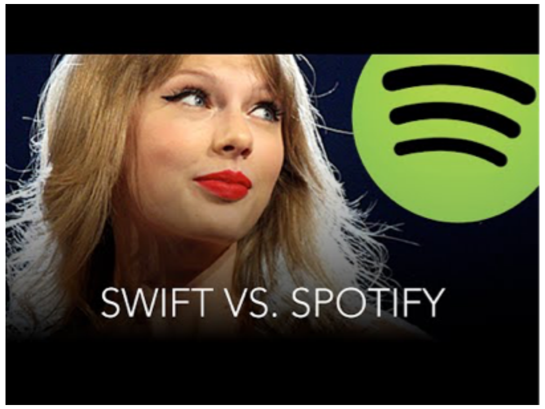
ORACLE

IBM

Peer to peer lending - Crowd funding

- Many to many relationships and money changing hands

Music rights



- How many times was that played and how much do Google own me?

Medical and pharmaceutical

- IDs, treatment, medical history, who operated on who etc.
- Medicare - Bundled payments

There are several players in this space

ripple

- Codius - Ripple
- Ethereum
- Many many others

The Digital 5

Five nations (Estonia, UK, Israel, New Zealand and South Korea) are looking at blockchain to reduce their administrative burden

Estonia is trialling Keyless Signature Infrastructure (KSI), it allows citizens to verify the integrity of their records on government databases

Citizens can be assured that data is held securely and accurately

The Estonian government was able launch digital services such as e-Business Register and e-Tax

Ethereum, Ripple & R3

Ethereum - Crowd funded, alternative to Bitcoin with blockchain platform and relatively mature thinking around smart contracts

- A good white paper: https://github.com/ethereum/wiki/wiki/White-Paper

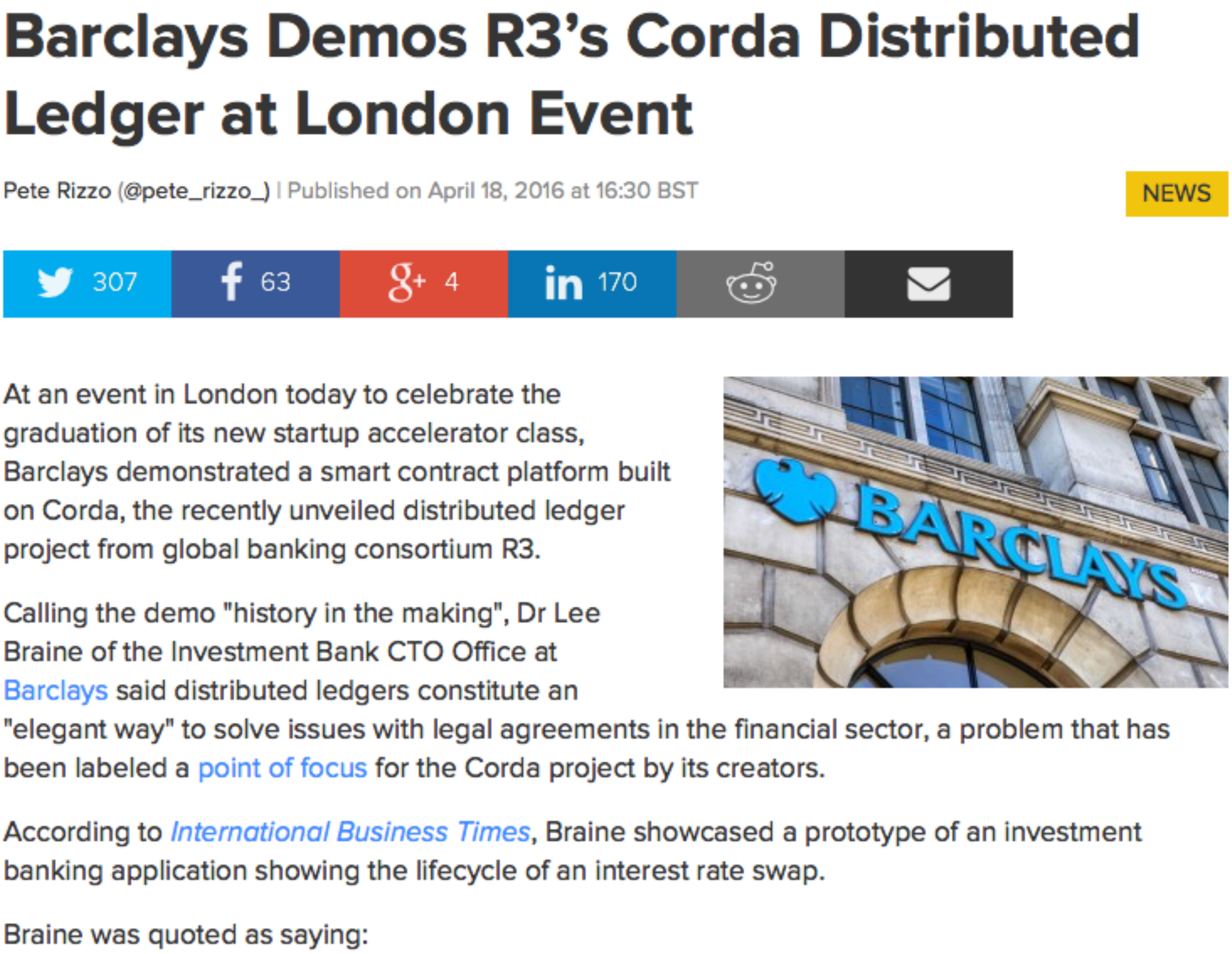
Ripple - Aims to provide a platform for banks to transact without needing central counterparts or correspondents

- Probably the closest to what the investment banks are looking for today

R3 - Originally a consortium of 9 banks (Sept 2015), now 42 banks - Product is called "Cordia"

- Plenty of opportunities for startups to extract the bank's money

Last week…



Barclays Demos R3's Corda Distributed Ledger at London Event

Pete Rizzo (@pete_rizzo_) | Published on April 18, 2016 at 16:30 BST

At an event in London today to celebrate the graduation of its new startup accelerator class, Barclays demonstrated a smart contract platform built on Corda, the recently unveiled distributed ledger project from global banking consortium R3.

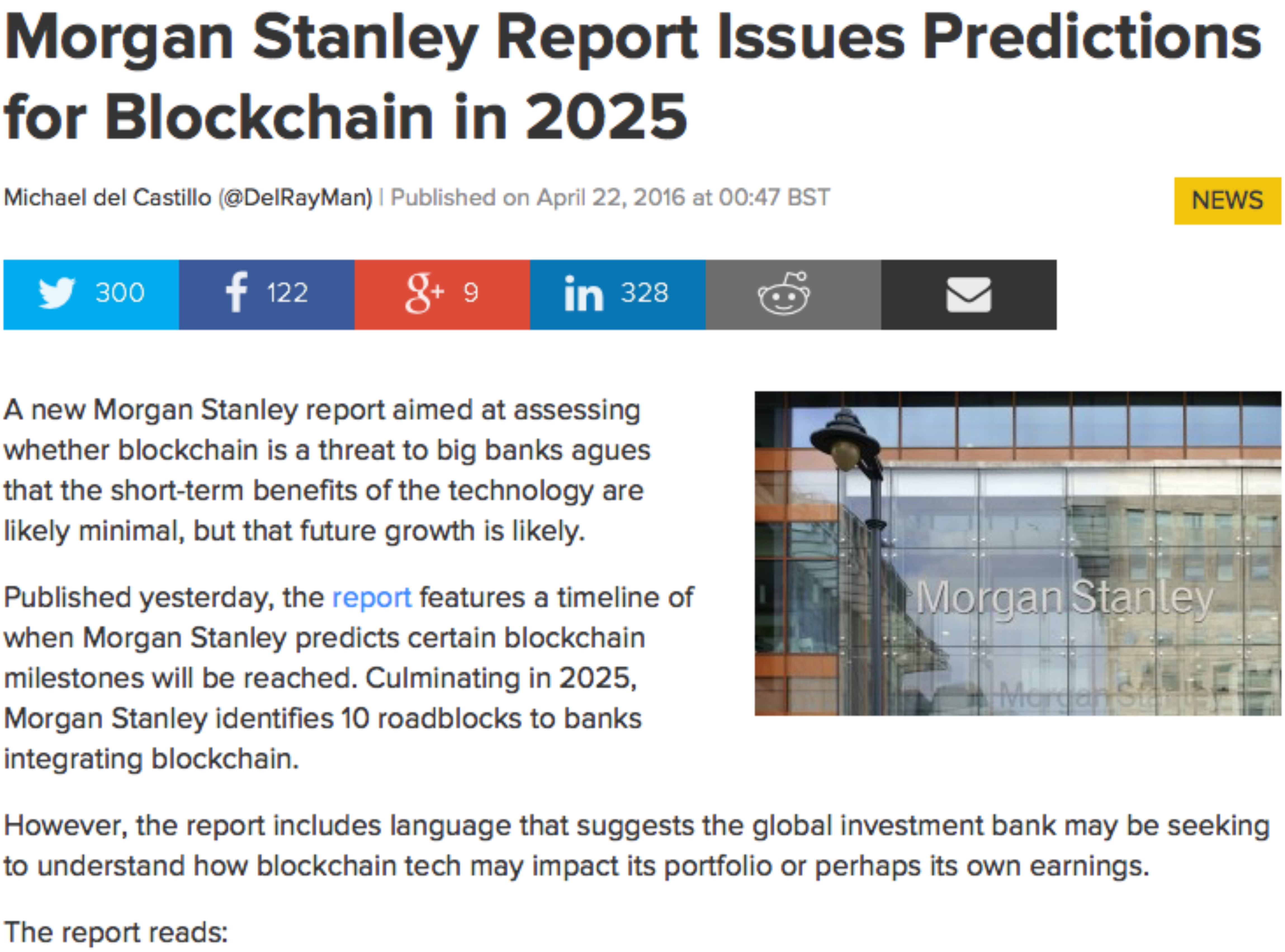
Calling the demo "history in the making", Dr Lee Braine of the Investment Bank CTO Office at Barclays said distributed ledgers constitute an "elegant way" to solve issues with legal agreements in the financial sector, a problem that has been labeled a point of focus for the Corda project by its creators.

According to *International Business Times*, Braine showcased a prototype of an investment banking application showing the lifecycle of an interest rate swap.

Braine was quoted as saying:

Again last week…

C24



Morgan Stanley Report Issues Predictions for Blockchain in 2025

Michael del Castillo (@DelRayMan) | Published on April 22, 2016 at 00:47 BST

NEWS

A new Morgan Stanley report aimed at assessing whether blockchain is a threat to big banks agues that the short-term benefits of the technology are likely minimal, but that future growth is likely.

Published yesterday, the report features a timeline of when Morgan Stanley predicts certain blockchain milestones will be reached. Culminating in 2025, Morgan Stanley identifies 10 roadblocks to banks integrating blockchain.

However, the report includes language that suggests the global investment bank may be seeking to understand how blockchain tech may impact its portfolio or perhaps its own earnings.

The report reads:

Blockchain Distribution

There is one advantage in a blockchain and that's that is only the end that changes

- But existing issues remain -> **CAP theorem** -> Consistency, Availability & Partition tolerance, roughly you can have any two but not all three

Even so you need to be able to provide consistence and availability on a global level

- Who gets the lock to write the next block?
- How do all parties agree they're ready?
- Are we back to 2-phase commits?

If the blocks are complex smart contracts (e.g. derivatives, corporate actions) then they're going to be large and slow to distribute

- This will limit performance and increase latency

Block size and Querying

You are probably aware of the controversy in BitCoin about the block size

- BitCoin was a thought experiment someone took seriously
- But the implementation is not enterprise-ready, they already need to change it

The reason the block is a fixed size if to facilitate searching, how will a “real” blockchain manage with varying data sizes?

It’s very unlikely that you’ll be able to get your contracts into fixed sized blocks so how are you going to search the chain?

- FpML, ISO-20022, even SWIFT MTs with their fixed 10k size

Potential social resistance

While technically a blockchain is the perfect ledger it raises some issues that need some serious consideration

Identity theft

- Once someone has stolen your ID and destroyed your credit the history can not be erased
- Today you can work with your bank to “correct” your history, while this is already difficult today, it will be impossible with a blockchain

History “correction”

- Anything from witness relocation, wrongful arrest/conviction, cyber bullying, personal changes, with a blockchain you cannot “correct” history
- Many people have fought of the right to have their history “corrected” or deleted on Google for example, this would not be possible in a blockchain

Loss of private key or payment to wrong account

- Lose your key and your money is gone forever end of story, there’s no going to the bank to prove your identity
- Pay into the wrong account or an account without an owner and it’s gone forever…

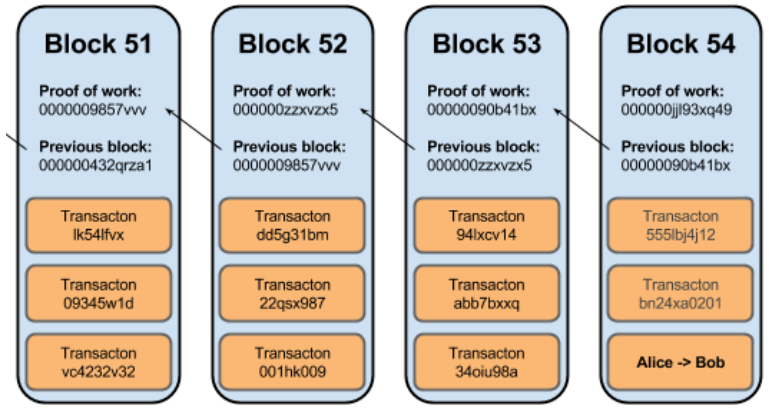
In conclusion

Bitcoin is not going to change the world

- It's still largely for the dark web

Blockchain itself not exactly new

- But it's still interesting
- We will find use-cases for it but it's not exactly a new revolution



Block 51
Proof of work:
0000009857vvv
Previous block:
000000432qrza1
Transacton
lk54lfvx
Transacton
09345w1d
Transacton
vc4232v32

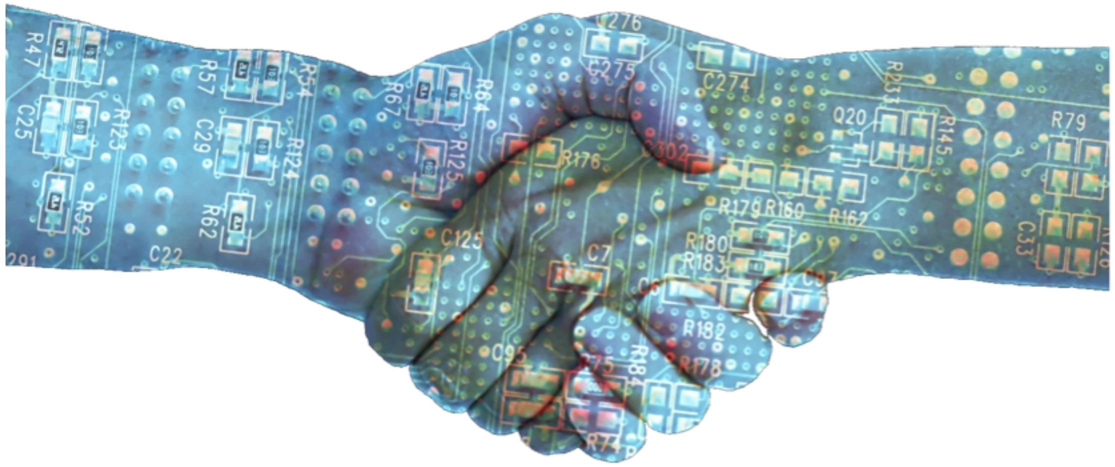
Block 52
Proof of work:
000000zzxvzx5
Previous block:
0000009857vvv
Transacton
dd5g31bm
Transacton
22qsx987
Transacton
001hk009

Block 53
Proof of work:
00000090b41bx
Previous block:
000000zzxvzx5
Transacton
94lxcv14
Transacton
abb7bxxq
Transacton
34oiu98a

Block 54
Proof of work:
000000jjl93xq49
Previous block:
00000090b41bx
Transacton
555lbj4j12
Transacton
bn24xa0201
Alice -> Bob

Smart Contracts are where innovation will take place

- Now these are cool, but they're not defined or accepted yet
- It will be a long time before we see these being used between companies
- There are already several good internal use-cases being developed now



Hopefully you have a better understanding of these technologies and how they might be used in the coming years

Thank you!

@jtdavies