CHICAGO
INTERNATIONAL
SOFTWARE DEVELOPMENT
CONFERENCE 2016

goto; conference

Blockchain

Disruptive Service or just another buzz word?

John Davies
@jtdavies

follow us @gotochgo

Conference: May 24th-25th / Workshops: May 23rd & 26th

Flow

What is a Blockchain?

What is Bitcoin & how does it work?

Smart Contracts & how do they work

Distributed Ledgers

What problems does this all solve?

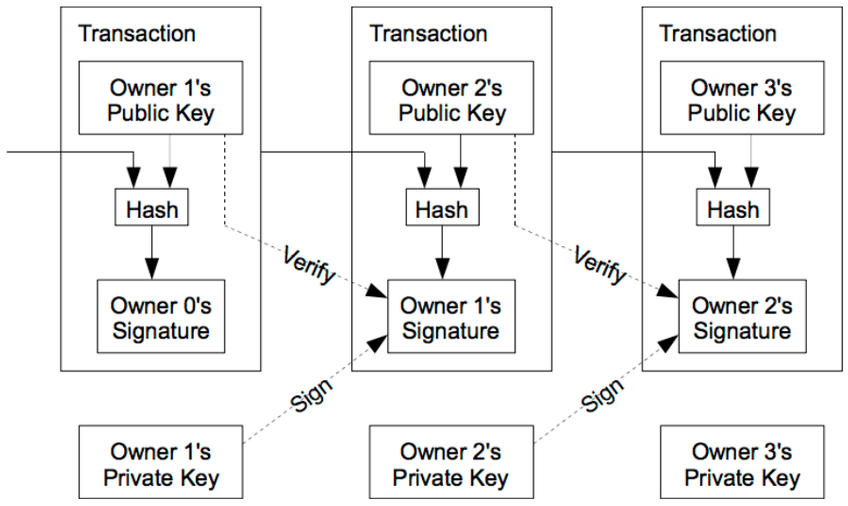
Just another buzz-word?

Blockchain or Ledger?

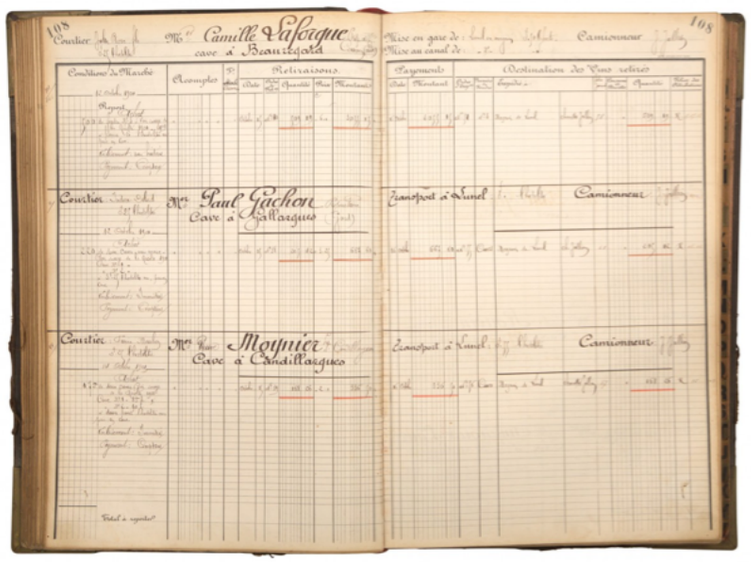
In most cases we can interchange the word blockchain with ledger

- 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)



=



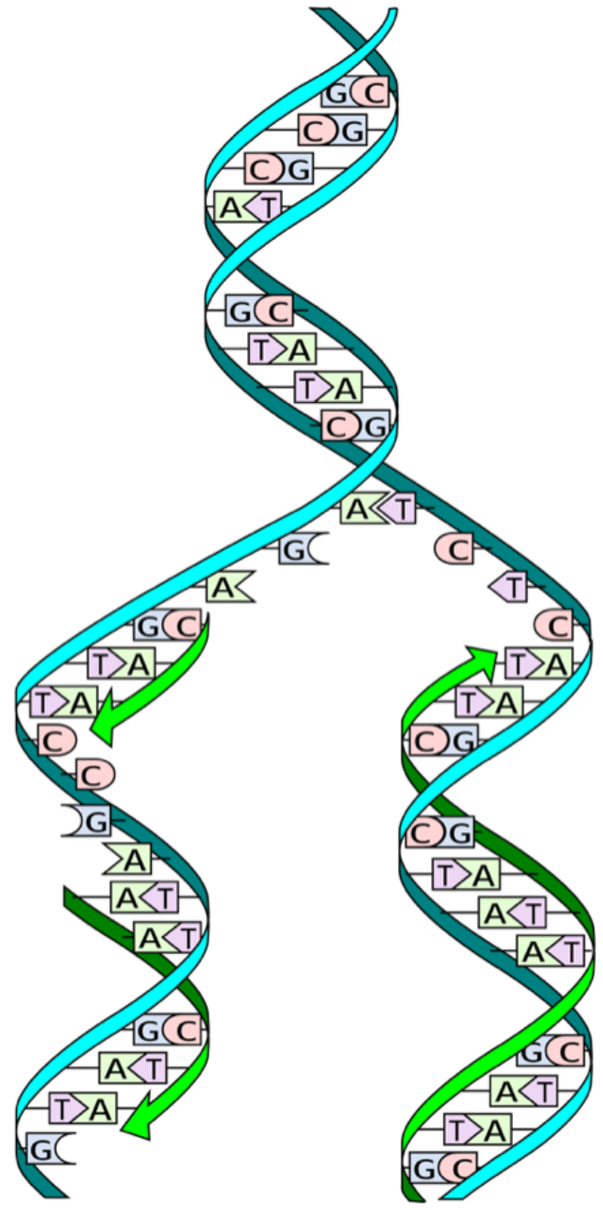
I will generally refer to blockchain today, I could use either

What is Blockchain?

A blockchain is like a simple database - Records are linked in a chain, the chain forms a block. We can also refer to is as a ledger

In some ways a blockchains are like genes running through a generation

- Once the genes are mixed at conception there's no going back



The key asset of a blockchain is, like your own DNA, each record is uniquely linked to its parent(s)

Once written and accepted it can not be changed

- Your parent's and your grandparents DNA is locked in you

Why can't a blockchain be modified?

You can modify it but you'd leave a huge trail, you'd break the chain

To erase the trail you will need to re-write history since the entry

Mathematically the blockchain is incredibly secure

This is the USP of the blockchain, it records history (records, contracts, transactions etc.) in a way that cannot be disputed

Example use-case

Nasty insurance company EvilCorp insures Elliot's car and informs him the policy is active immediately

Elliot crashes his car the next morning and makes a claim

EvilCorp claims Elliot's policy wasn't received before the accident so refuses to pay

- A long dispute leaves Elliot the likely loser, EvilCorp records record profits that year

If only the contract was on a blockchain!

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 “John Davies” is…

- `12c9091df458d8791744a1dc385cc7e0ac31b0e9231c5506fd6c1d4624e53ded`

The SHA-256 hash of “John Davies.” is…

- `9c82ec2a789f6acc61d86acfaad9b1c1b4bbaf2ca7db2d8650d7bf83adf25e36`

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(John Davies)" | shasum –a 256
12c9091df458d8791744a1dc385cc7e0ac31b0e9231c5506fd6c1d4624e53ded  –
```

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

```
echo "John Davies" | shasum –a 256
30d2ad9f9c76abb17f1b5c4fb8a619c566315724d886a3d2530de0e3cd0e4927  –
```

How to get a Hash in Java

Creating a hash in Java is extremely simple

```
byte[] input = "John Davies".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...

```
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));
```

```
Base64: EskJHfRY2HkXRKHcOFzH4KwxsOkjHFUG/WwdRiTlPe0=
Hex: 12C9091DF458D8791744A1DC385CC7E0AC31B0E9231C5506FD6C1D4624E53DED
```

How do we add a new contract to the chain?

With our contract…

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

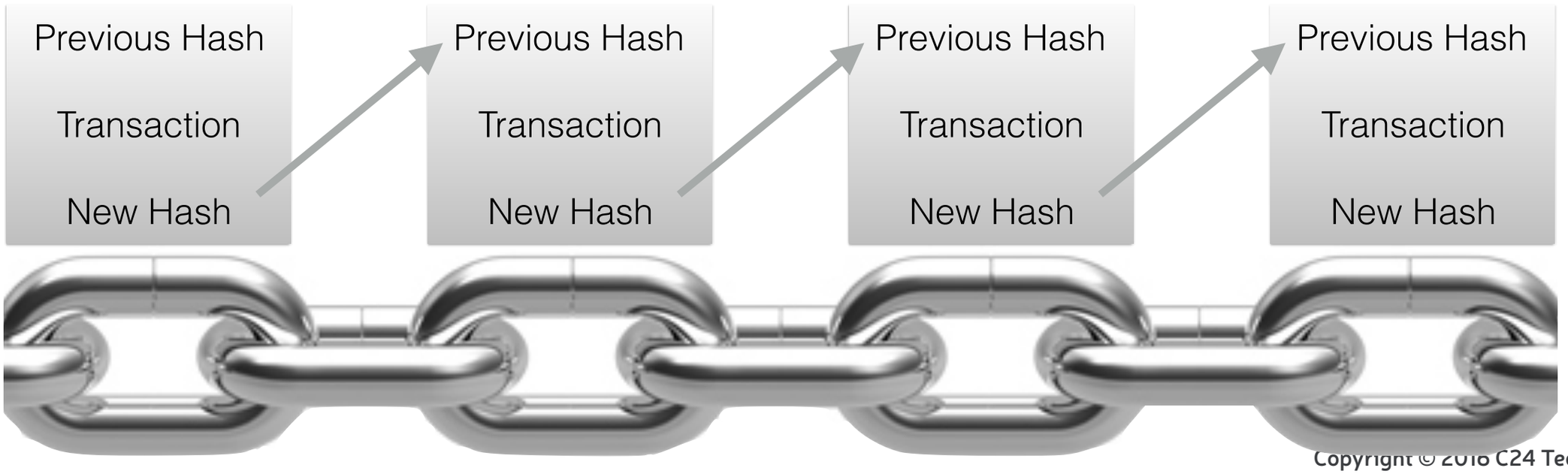
Hash everything to create a new hash

- 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)…



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)

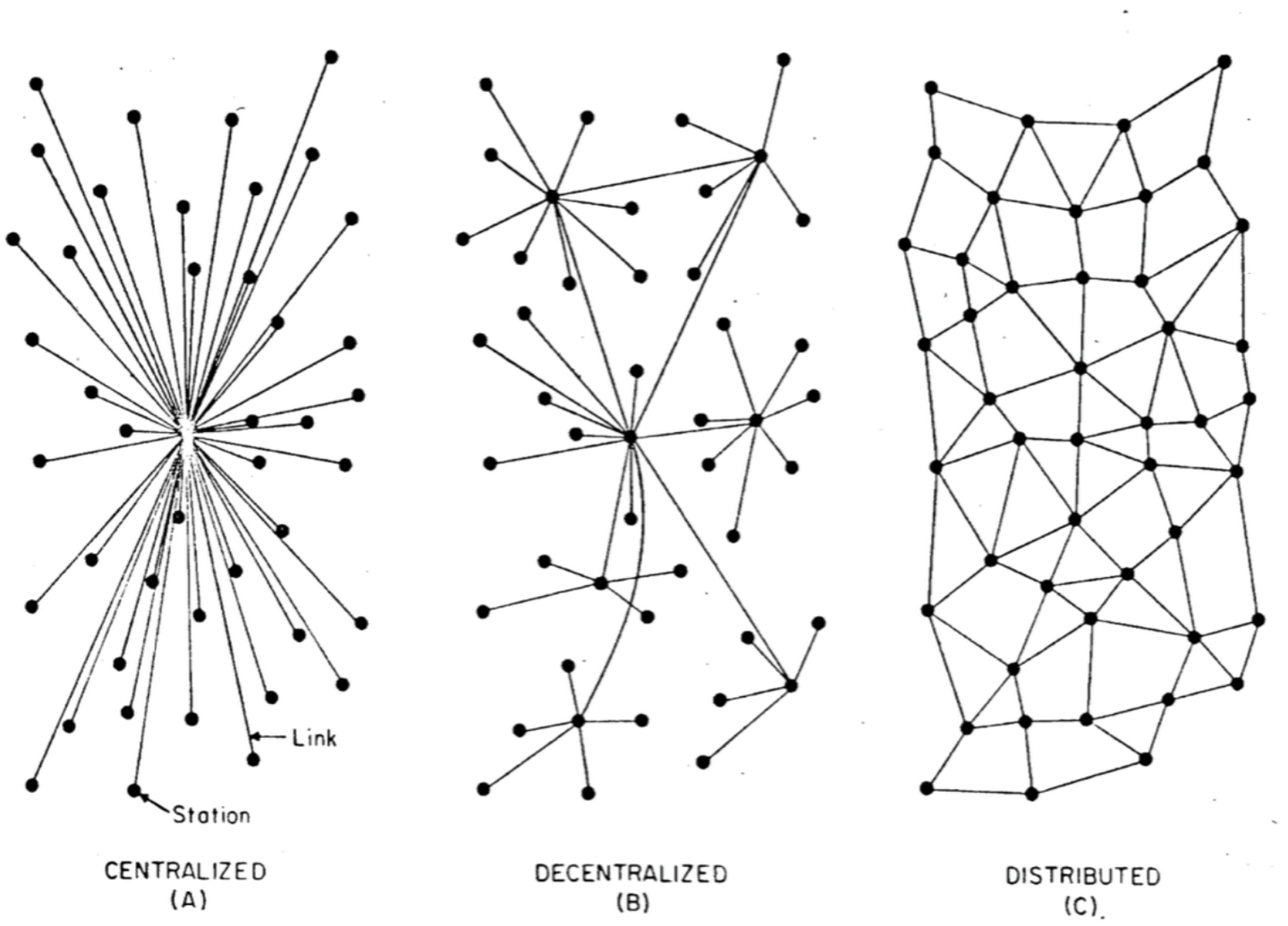


FIG. 1 — Centralized, Decentralized and Distributed Networks

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

The Digital 5 - Centralised & Permissioned

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

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)

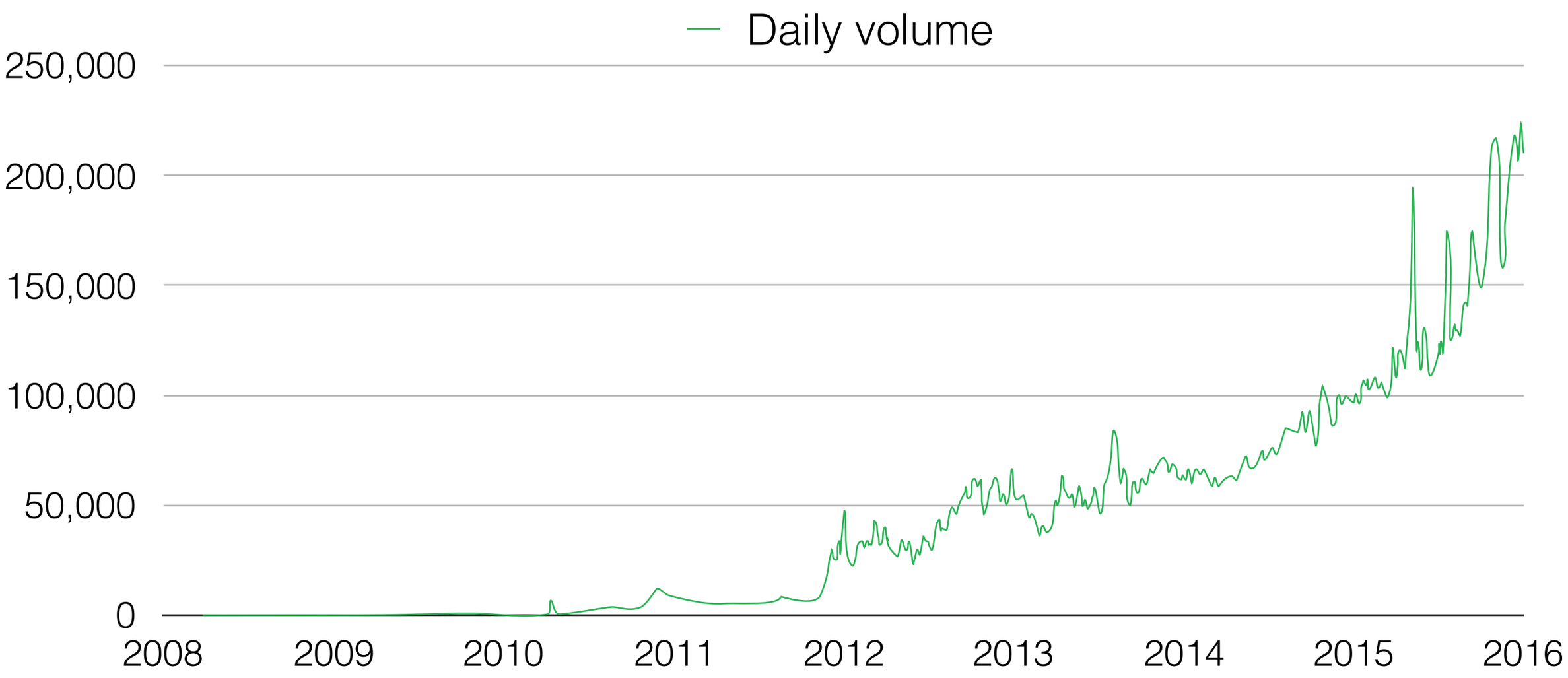
Effectively the owner of the private key is owner of the bitcoins

Anarchy?

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

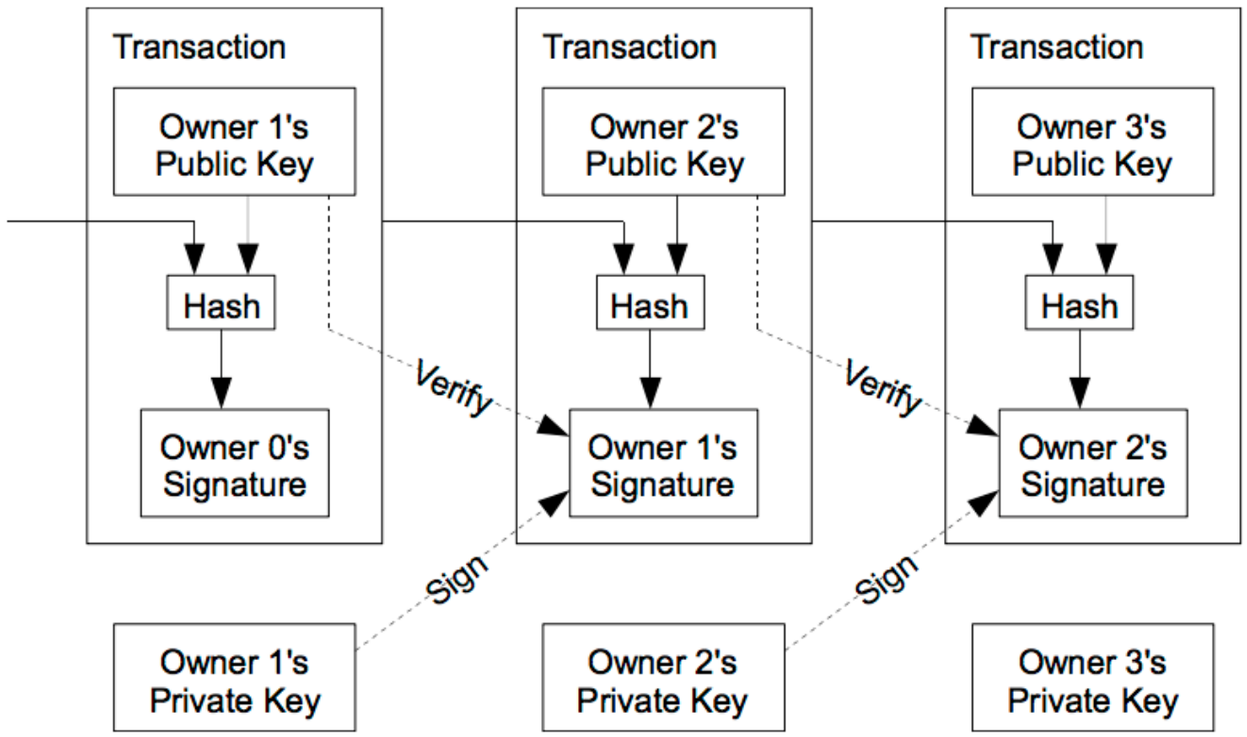


Market Capitalisation

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

Generating Keys in Java

```
public static final String ALGORITHM = "RSA";
private static String clearText = "This is a message in clear text";

public static void main(String[] args) throws Exception {
    Base64.Encoder encoder = Base64.getEncoder();

    KeyPairGenerator keyPairGenerator = KeyPairGenerator.getInstance(ALGORITHM);
    keyPairGenerator.initialize(2048, SecureRandom.getInstanceStrong());
    KeyPair keypair = keyPairGenerator.generateKeyPair();

    PrivateKey priv = keypair.getPrivate();
    PublicKey pub = keypair.getPublic();

   System.out.printf("Message: %s%n", clearText);
    byte[] encrypt = encrypt(clearText.getBytes(), pub);

    System.out.printf("Encrypted (in Base64): %s%n”,
        encoder.encodeToString(encrypt));

    System.out.printf("Decrypted: %s%n", decrypt(encrypt, priv));
}

// And the output…

// Message: This is a message in clear text
// Encrypted (in Base64): cDy1a6cysQ7BKdkugmNi9Me3zhLWJzYyCeVmasit…
// Decrypted: This is a message in clear text
```

Encrypting data in Java

```
public static byte[] encrypt(byte[] data, PublicKey key) {
    byte[] cipherText = null;
    try {
        final Cipher cipher = Cipher.getInstance(ALGORITHM);
        cipher.init(Cipher.ENCRYPT_MODE, key);
        cipherText = cipher.doFinal(data);
    } catch (Exception e) {
        e.printStackTrace();
    }
    return cipherText;
}
```

```
public static String decrypt(byte[] crypt, PrivateKey key) {
    byte[] dectyptedText = null;
    try {
        final Cipher cipher = Cipher.getInstance(ALGORITHM);
        cipher.init(Cipher.DECRYPT_MODE, key);
        dectyptedText = cipher.doFinal(crypt);
    } catch (Exception ex) {
        ex.printStackTrace();
    }
    return new String(dectyptedText);
}
```

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

Want to send me some money?

All donations welcome...

1JdGZgtQQ4JjCVCnsiwACt47dpTcQiYSN

Problems with Blockchain

Distributing the blockchain brings us back to the existing issues of throughput, latency and bandwidth

- The blockchain could present the additional issue of having large proportion of data with hashes and keys - these don't compress at all

A blockchain is mathematically solid but not (yet) legally solid

Most of the complexity of contracts are the contracts themselves, blockchain is just a technology not a silver bullet

If someone ever "solves" primary key factoring or quantum computers are able to brute-force crack keys & hashes it's all useless

- That being said we'll have bigger problems to worry about
- Perhaps the NSA or GCHQ already can crack RSA, they're unlikely to let us know

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

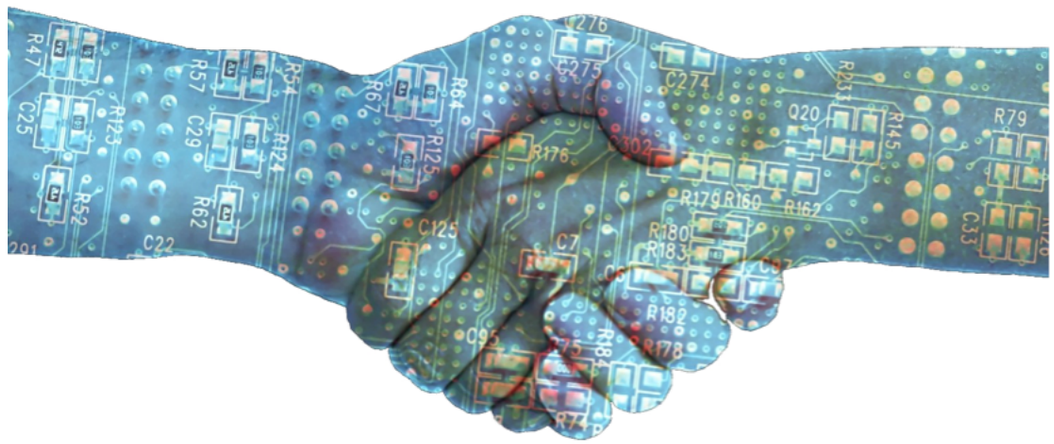
- There are a few other things like Merkle trees, difficulty level, nonces etc. but you have the basics
- New additions and alternatives like SideChains, LiteCoin, DogeCoin, NameCoin, Colored Coins, MetaCoins etc.

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 (Credit Default Swap) 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

ORACLE®

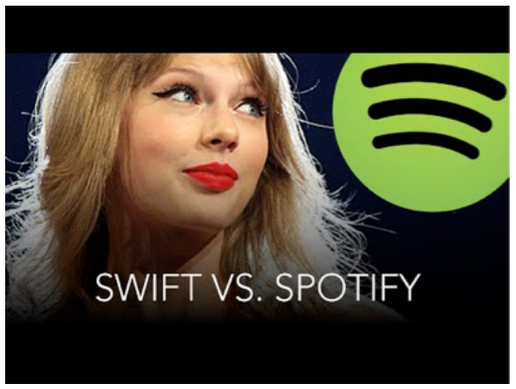
IBM®

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

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

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

If you want to play...

Amazon Web Services is Now Working With Blockchain Startups

Stan Higgins | Published on May 2, 2016 at 17:30 BST

NEWS

412 463 10 431

Amazon Web Services (AWS), the cloud computing business operated by Web commerce giant Amazon, is partnering with investment firm Digital Currency Group (DCG) to offer a blockchain experimentation environment for enterprises.

In collaboration with the startups in the DCG portfolio, AWS will provide dedicated cloud infrastructure and technical support for those projects. The startups, along with DCG, will collaborate with enterprise businesses looking to explore and test different blockchain applications.

Last month...

Barclays Demos R3's Corda Distributed Ledger at London Event

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

NEWS

307 63 4 170

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 month...

Morgan Stanley Report Issues Predictions for Blockchain in 2025

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

NEWS

300 122 9 328

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

Problems with Smart Contracts

There is no standard, there is not even a proposed standard

There is no legal precedent yet

- Today they are just a curiosity and that will take a long time to change
- Ethereum is the largest implementation but it's proprietary

Imagine the complexity of a derivative contract

- FpML has over 11,000 elements - How long will that take to implement in a useful way?
- It's easy to imagine the advantages of having the workflow automated in the Smart Contract but it could be done in other ways too

At the end of the day the Smart Contract is code, someone needs to write it, test it, debug it and run it

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…

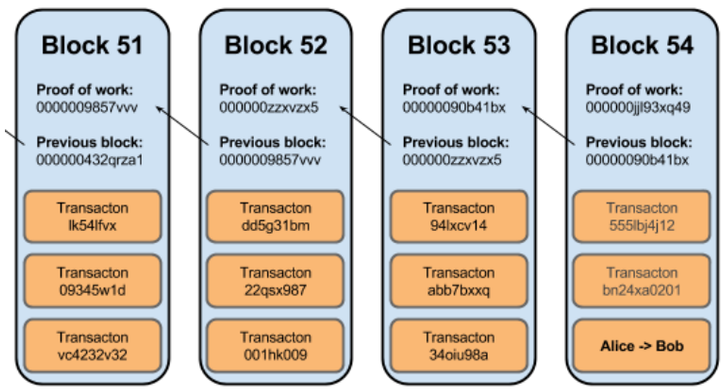
In conclusion

Bitcoin is not going to change the world

- It's still largely for the dark web

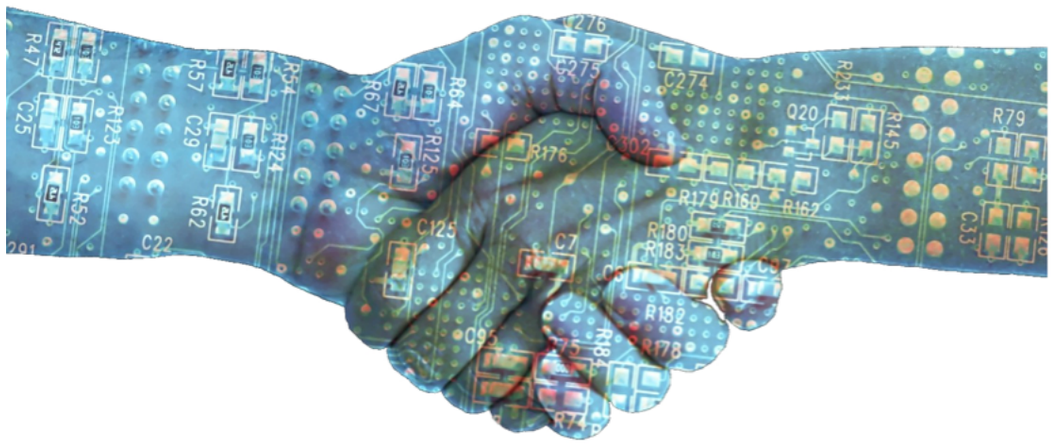
Blockchain is a cool technology

- But it's not new and it's very simple
- We will find use-cases for it but it's not exactly a new revolution



Smart Contracts are cool

- 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

goto; conference

Please

Remember to rate this session

Thank you!

@jtdavies

follow us @gotochgo