

Blockchains

For
Automation Professionals
and the
IOT
Internet of Things

Peter Chipkin

Meow you
will learn
something.



A 5 Minute Roadmap to Understanding Blockchains

Hi,

This isn't as bad as you may think. They are structurally quite easy to understand. As soon as you grasp the idea of hashing and the idea that there is a consensus protocol as part of the structure then you are well on your way to getting it.

The following short notes are the outline and the key points from our short journey. If I only had 5 minutes this is what I would tell you.

Prime Numbers

Multiplying two large prime numbers together – Easy

Reversing the operation – find the factors – Insanely Hard

This is the basis of public / private key encryption.

Hashes

A mathematical formula. Feed data in. (words, images etc)

Get a number out.

Every chunk of data produces a different number.

Aha – a signature.

Distributed Ledgers

Imagine that someone broke into your bank and destroyed / stole their servers?

Imagine the bank records were stored on thousands of duplicate servers scattered around the world.

You might have a higher level of trust.

Public, Visible

Imagine that every record on every server is visible to anyone in the world.

Imagine the servers are not under the control of one entity.

You would have a high(er) trust of the data if all the servers matched.

Consensus

The only problem is when new data is written to all these distributed ledgers.

How do you know the blocks of new data being added are valid ?

The cheating might occur here.

The ledgers talk to each other in public. Anyone who breaks the rules gets ignored or kicked out (called branching).

Encrypt / Sign the messages so people cant alter them.

Mining

To add a new data record, a calculation must be performed. A very hard calculation to do but easy to verify. One so hard that it takes the average desktop PC about 2.7 million years. It's a race between miners. The 1st one to announce the correct answer wins. The others get nothing. The ledgers all use the 1st correct answer announced and add the block of data.

The winning miner also gets a piece of the blockchain itself. In the case of bitcoins is worth money because the blocks of the bitcoin are bitcoins.

Miners on some chains also charge transaction fees.

Mining is expensive – You need energy to run high power computers.

Trust

Trust comes from working with untrustworthy people, miners and servers.

To cheat, you have to change the majority of the ledgers simultaneously

To change data in the past you have to recalculate all the answers for previous blocks and update all the ledgers before anyone else spots it because its all in public view.

Organized crime uses blockchains do you think they trust each other ?

Quick Summary

Each block in a blockchain contains the hash (signature) of the previous block.

To verify a block calculate its hash – this is easy and fast.

Extract the signature from where it is stored in the next block and compare.


The forward chaining of signatures gives the system a ‘trivial to verify’ ability.

So trivial that bitcoin blockchain does not keep your balance. Rather it calculates by reverifying every single transaction.

The distributed public ledgers

The consensus protocol that ruthlessly ignores cheaters.

The fact that the rules are built into the blockchain itself. The blockchain is not only a ledger of data it is also set of instructions.



Organized crime use
blockchains.
Do you think they trust
each other ?



Bitcoins / ICO's

Bitcoins are a special version (implementation) of a blockchain.

Not all blockchains are equal. Usually the designer has a specific purpose in mind.

In the case of Bitcoins it was financial. In the case of Ethereum it was to make a general purpose blockchain that people could embed programs in.

Bitcoins will always get rarer because it gets harder and harder to make them and people lose them all the time.

Rarity and value do not correlate.

People spin off bitcoins by changing the rules – they get rejected by the old blockchain. And they become a new chain. What is the value of the coin on the new chain. That's what an Initial Coin Offering (ICO) will determine.

Smart Contracts

If data in a blockchain is immutable then how about a program embedded in the chain.

It is immutable too – meaning it is guaranteed to execute under its trigger condition

The program is visible and distributed so it can be verified.

How do you know you can trust the lotto – that their selections are crooked and that they will have the money to pay if you win. If the program and the money is imbedded in the blockchain. You can inspect it any time you want. On any of the distributed ledgers.

A program embedded in a blockchain is called a contract.

The end.

Ongoing

This information is fleshed out in a series of Chipkin publications.

1. Checksums and Hashes - The roots of blockchains
2. Blockchains – Features, Structure, Operation
3. Blockchain Smart Contracts
4. Blockchain Applications
5. Blockchains - Risk, Lies and Hype
6. Hands On – Spend a few dollars and do some basic blockchain things.