Blockchain

What the heck is a Blockchain any way?

In a few words, a blockchain is a digital ever-growing list of data records. Such a list is comprised of many blocks of data, which are organized in chronological order and are linked and secured by cryptographic proofs.

Wait a minute these was not few words!

My bad think of it like boxes tied together with a rope that never ends

i. e. Simply Blockchain is a collection of block of data where each block is connected to it's previous and next block through a secure cryptographic proofs.

Rope === secure cryptographic proofs. (Hash data)

Block Chain

Some fancy terms

- Consensus mechanism

  - Proof-of-Work (PoW)

  - Proof-of-Stack (PoS)

Block Chain

Proof-of-Work (PoW)

- Dated back to 1993 the PoW concept was developed to prevent Denial-of-Service (DoS) attack or other attacks like spam on the network by requiring some work from the service user.
- Meaning processing time by a computer.
- In 2009 Bitcoin introduced a way to use PoW as a consensus algorithm to validate transaction and broadcast new block to the blockchain.

PoW

How Does It Work

- Miner on a network will compete against each other to solve complex mathematical puzzles, once the miner able to get the solution they will be able to broadcast the block to the network, then other miners will verify the solution is correct

Miners will try to guess pseudo-random number aka (nonce), when this number combined with data provided in the block and passed through a hash function (e.g. SHA-265) must produce a result that matches a given condition.

For example a hash that matches the previous hash block.

when this happen the other node or miners will verify the validity of the outcome and the miner node will be rewarded with block reward.

PoW

A successful attack

- Will require a lot of computational power and a lot of time to do the calculation as a result the the incurred cost will be much higher than the potential reward for attacking the network

One issue on PoW algorithm

- Mining require expensive hardware which consumes a large amount of power

Joke Time

Some fancy jokes

Algorithm *(noun.)*

Word used by programmers when...
they do not want to explain what they did.

Joke Time

Some fancy jokes

Q: What is a programmer's favourite hangout place?

A: Foo Bar

Joke Time

Some fancy jokes

How do you tell HTML from HTML5?

- Try it out in Internet Explorer.
- Did it work?
- No?
- It's HTML5.

Joke Time

Bear with me let me tell you the last fancy joke
I have today

3 Database SQL walked into
a NoSQL bar.

A little while later...
they walked out

Because they **couldn’t find a table.**

PoS

Back to the boring staff

Proof-of-Stack (PoS)

It uses a pseudo-random method of election to select a node that will be the validator of the next block based on the following combination of factors.

- Stacking age
- Randomization
- Nodes wealth (amount of stack they have)

Ethereum

What is ethereum?

Simply ethereum is a decentralized global software platform powered by blockchain technology

It is

- Decentralized
- Open-source blockchain and
- With smart contract functionality

It uses Ether as it’s native cryptocurrency, and solidity as its programming language!

Developed for developers by developers

Ethereum

Some fancy terms!

- Smart contract
- Gas (Execution fee)

Smart contract :- are a peace of code (script) that stored on a blockchain that run when predetermined conditions are met.

They simply follow the “if/when…then…” statements.

> In a none programmer sound I would say they are simple app that live on the blockchain nest

More on later how you can write a smart contract on ethereum blockchain :) sound fancy eee