Blockchain & Cryptocurrencies

# What does it do?

To understand what it is that can be achieved by blockchain and cryptocurrencies, it must be first realised that the two are very different things.

Blockchain as it is known, is but the underlying technology adopted by many cryptocurrencies (namely, Bitcoin). Rudimentarily, a block is just an organised data structure that can contain whatever it is one wishes to store. In the application of cryptocurrencies, a block is generally comprised of metadata about the block, commonly known as the block header, followed by a list of digital transactions. Hence a blockchain is a chain of blocks, with each block cryptographically linked to the previous block. As each block is timestamped, the contents of each block can be proven mathematically that it existed at the specified time. Blockchain was originally conceived as a solution to digital media being easily edited (Haber & Stornetta, 1991), but was not notably implemented until its application in Bitcoin.

Cryptocurrency on the other hand, is an implementation of several technologies (often incorporating a blockchain) resulting in a transferable asset, be it money, digital contract, utility token (akin to a movie ticket) or a company security. Digital signatures (cryptography) provide part of the solution (Nakamoto, 2008) when transferring the asset from one party to another, hence the name “crypto” currency.

As each cryptocurrency has an exchange price, it can be assumed that those which represent the “state of the art” are those considered most valuable by the market. Taking the top 5 cryptocurrencies by market cap, we will investigate Bitcoin, Ethereum, XRP, Bitcoin Cash and EOS (CoinMarketCap.com, 2019). Of these 5, Bitcoin and Bitcoin Cash are both shooting for a decentralised store of value and medium of exchange, Ethereum and EOS are decentralised computer systems that execute highly programmable smart contracts and XRP is intended to be an international inter-banking platform like SWIFT. All but XRP utilise blockchain technology, as XRP implements a proprietary ledger.

Considering the application variance amongst the top 5 cryptocurrencies, we will focus on the use of cryptocurrency as a cryptographically secure digital currency. This leaves us with Bitcoin and Bitcoin Cash. Having both share the same fundamental structure and the same ledger up until the split on the 1st of August, development for each has now diverged. The split came about from a community-wide disagreement on how to scale to worldwide usage.

Bitcoin aims to limit the size of block to 1MB, to ensure the entire history of the blockchain is never too cumbersome for anyone to download at home, whilst scaling will come in the form of an “off-chain” technology known as the Lightning Network. The Lightning Network is a network of bi-directional payment channels that enable millisecond secure transactions between two parties. These channels can be “chained” from channel to channel, allowing Alice to pay to Carol through Bob, in which the funds can not be seized by Bob. The Lightning Network was been in development since 2016, and although there is a released version on the Bitcoin network it is not expected to enable worldwide usage anywhere from 3 years to 10 years.

Bitcoin Cash aims to allow the network to determine the acceptable size of a block, letting the size of the blockchain grow proportionally to its usage. Ideally this means that the network supply will always be greater than what the network demands. Currently supporting a throughput of roughly 100 transactions per second, there are still many obstacles faced by developers to enable a throughput that will enable worldwide usage.

# What is the Likely Impact

A decentralised cryptocurrency enables for the first time in human history, a sound form of money that is not controlled by any one party, that is resistant to inflation, that is accessible worldwide, that is not subject to government spending or printing, is easily transferable from peer to peer.

The immediate impact of the adoption of cryptocurrency as a peer-to-peer electronic cash will likely be that of a societal flip on how money is viewed and accessed around the world. A common mantra of Bitcoin and cryptocurrency is that it enables every individual on the planet to be their own bank, to bank the unbanked whilst un-banking the banked.

As of 2017, roughly one third of the world’s population did “not have a bank account or access to a financial institution via a mobile phone or any other device” (Hodgson, 2017). The effect of this situation is that a large portion of the population is not engaging in economic activity with the rest of the world, leaving those without access to a financial institution behind the rest of the world’s economic growth.

If we did see worldwide adoption of this technology, it would disrupt many current financial industries, namely banks and national reserve banking. At first it may be believed that upon the establishment of this technology that banks would no longer be necessary however, it is likely there will still be financial institutions responsible for custodianship and lending of the cryptocurrency in question. As for national reserve banking, there would be little to no reason for governments to continue issuance of a national currency if everyone globally were using the same cryptocurrency.

# How will this affect you?

The adoption and realisation of this technology would have a great affect on me and my daily life. As a prospective programmer, there would be many new job opportunities for those who have vested interest and skills in learning the workings of the technology behind cryptocurrencies.

As an individual on earth, cryptocurrency would enable open trade between me and anyone else around the planet without the hassle of currency exchange rates or international transfer fees. Without the necessity for a trusted 3rd party to safely and surely execute the transfer of funds, the transaction can be done on our own terms, as we see fit.

The affect this may have on friends and family members is very much the same of the affect it would have on me, however if the technology was implemented with the broader population in mind (those who may not care for many of the additional features a programmable money might provide) there should be no noticeable difference in their current use. For to ensure worldwide adoption can be achieved, it must be accessible and understandable by everyone, not just a select few technologists in the space who understand all the ins and outs.

The main take-away from how cryptocurrency will affect everyone across the globe, is that there is now an option to forego the need of a 3rd party when it comes to transacting on a peer-to-peer basis.

# References

* HABER, S. & STORNETTA, W. S. 1991. How to time-stamp a digital document. *Journal of Cryptology,* 3**,** 99-111.
* Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. 1st ed. [pdf] Available at: https://bitcoin.org/bitcoin.pdf [Accessed 12 Apr. 2019].
* CoinMarketCap.com (2019). [website] Available at: https://bitcoin.org/bitcoin.pdf [Accessed 12 Apr. 2019].
* Hodgson, C. (2017). *The world's 2 billion unbanked, in 6 charts*. [online] Business Insider. Available at: https://www.businessinsider.com/the-worlds-unbanked-population-in-6-charts-2017-8/ [Accessed 13 Apr. 2019].

# Appendix

* Bitcoin Whitepaper - https://bitcoin.org/bitcoin.pdf
* Etheruem Whitepaper - https://github.com/ethereum/wiki/wiki/White-Paper
* XRP (Ripple) Whitepaper - https://ripple.com/files/ripple\_consensus\_whitepaper.pdf
  + Updated - https://arxiv.org/pdf/1802.07242.pdf
* Bitcoin Cash – https://bitcoincash.org (same paper as bitcoin)
* EOS Whitepaper - https://github.com/EOSIO/Documentation/blob/master/TechnicalWhitePaper.md
* “How does a blockchain work?” - https://www.youtube.com/watch?v=SSo\_EIwHSd4
* “Bitcoin, Dogecoin and Other Cryptocurrencies as Fast As Possible” - https://www.youtube.com/watch?v=u4j\_\_TKnCt4
* “Ever wonder how Bitcoin (and other cryptocurrencies) actually work?” - https://www.youtube.com/watch?v=bBC-nXj3Ng4