Blockchain & Cryptocurrencies

What does it do?

**Blockchain**

In simple terms a blockchain is a data structure that acts as a ledger for transactions with each “block” containing digital pieces of information about a transaction. These include the date, time and amount of a transaction along with the participants who are identified only by a digital signature. Each block can contain a single transaction or many thousands of them. Each block stores its own unique identifying code called a “hash” that makes the block uniquely distinguishable from every other block in the chain. Only once all transactions in the block have been verified through a consensus process can a hash be added. When a new block is made it contains the hash code of the most recent block before it. This creates a link between the blocks and is the “chain” in blockchain.

What makes a decentralised blockchain unique compared with traditional financial transactions is that it does the transactions without the use of a single trusted third party. The blockchain network instead runs on thousands of independent public computers called “miners” which all have the exact same copy of the blockchain and process transactions which update as a new block is added to the chain. This is what makes a blockchain arguably more secure than that of a centralised system such as a bank. If a malicious person attempts to manipulate a transaction this would change the hash of the block which would fail to match the hash generated by other mining computers processing the same transaction, thereby failing the consensus verification, resulting in the rogue block being discarded.

These features are only secure if the blockchain is public with the ledger of all transactions viewable to anyone who wishes to access it. If a blockchain is stored entirely on a centralised private company’s server this creates the same vulnerability to that of a traditional banking system, meaning there is a lack of transparency and the administrators of that central server have full access to manipulate transactions and alter the ledger.

**Cryptocurrencies**

Cryptocurrencies are a form of digital currency and use blockchain technology as the backbone for tracking and managing transactions and account balances. Just as a safe or vault is used to protect government-issued cash currency (referred to herein as ‘fiat’ currency), cryptocurrencies use a form of encryption called cryptography to secure people’s accounts from hacking and theft, this is what gives the “crypto” in cryptocurrency. Using cryptography to secure transactions means cryptocurrencies are nearly impossible to counterfeit.

Most cryptocurrencies work on a decentralised platform, meaning they are not controlled by a single individual, group, entity or government but operate on a public peer-to-peer basis. This concept means they can operate without the interference or influence of governments. This is partly the attraction of cryptocurrencies among people that desire independence from government control.

The first decentralised cryptocurrency created was Bitcoin in 2009 by a pseudonymous developer or group under the name Satoshi Nakamoto. This was in response to the GFC where people became sceptical about the stability of fiat currency and manipulation by governments and central banks. Bitcoin is still the largest and most widely known cryptocurrency in the world, with a current market capitalisation of US$130 Billion and dominance of around 65% relative to the combined total of all other cryptocurrencies. Other cryptocurrencies are referred to as “Altcoins”. There are now thousands of such altcoins being traded globally. The largest of the altcoins include Ethereum and Litecoin, with market capitalisation of US$20 Billion and US$3Billion respectively.

Bitcoin, Ethereum and Litecoin are referred to as “Utility” coins and can be considered as virtual currency or cryptocurrency platforms. On the other hand altcoins are more often considered as ‘Security Tokens’ and are sold to the public through initial offerings similar to traditional IPO’s, where a particular company is capital raising for a particular project or vision. Both utility coins and security tokens are similarly traded on public cryptocurrency exchanges, where people gather online to trade different cryptocurrencies at market determined exchange rates.

Another type of cryptocurrency worthy of note is Stablecoins . Stablecoins were created to provide a cryptocurrency that does not have the high volatility of other cryptocurrencies. Stablecoins are aligned to an asset or group of stable assets, such as US Dollar or gold, and allow users to buy and sell them when they predict the value of cryptocurrencies will fluctuate. This is more desirable than frequently switching to and from fiat currencies, which normally attract higher commissions by exchanges, and often taxable events in many countries . The largest Stablecoin is Tether, which is backed at one-to-one ratio by USD, it has a current market capitalisation of US$6.34 Billion.

Cryptocurrencies allow users to make transactions with a degree of anonymity as only their digital signature or a pseudo username is logged in the blockchain. There is some traceability where a cryptocurrency is traded through a regulated exchange which complies with a country’s ‘know your customer’ regulations, however there are many other means of transacting that are anonymous. While Bitcoin, Ethereum and many other cryptocurrencies make signatures transparent in the blockchain, some other altcoins known as “privacy” coins, keep this detail hidden. Coins such as Monero, Dash and Zcash are favoured for private activity, tax evasion, and underworld activity and near impossible to trace back to an individual.

Cryptocurrencies are stored in a virtual wallet which contain both public and private keys which are linked. When a person sends cryptocurrency to another person, they will send it to their public key. The private key (similar to a password used for any account) is then used to access the wallet which had the cryptocurrency sent to it. When cryptocurrency is sent to another person’s public key, ownership of that cryptocurrency is transferred and the transaction forever recorded in the blockchain. It similarly relates to the function of handing over physical cash to another person to put in their physical wallet, with the only difference being there is an indisputable transaction record stored of the event.

Every transaction is confirmed in the blockchain by miners and a small pre-determined fee is paid to miners for the use of their computers and energy. When making a transaction a user has the option to pay a higher fee for a faster transaction. The time of each transaction depends on the computational power and efficiency of the blockchain that the cryptocurrency is operating on; this ranges from a few seconds to a few hours. Bitcoin’s blockchain operates over millions of computers with large mining facilities located around the world usually where electricity is low cost as cryptography is energy intensive. This concept is contrastingly different to that of traditional financial institutions who can often charge significant fees on transactions, particularly international, place limitations on customers, take several days to transfer funds, and can be logistically difficult for the receiving party to obtain.

Bitcoin and other altcoins are an asset class of their own, however have been likened to assets such as gold, where there is a controlled and finite amount determined by the software code which can only be altered with the consensus of the public mining community, who have a vested interest in preserving the asset’s value. Cryptocurrency valuations can however fluctuate heavily as a result of them being unregulated and in the hands of the public, accurate forecasting and models are difficult to create as there are no fundamentals based on earnings, or other meaningful metrics. Traditional ‘pump and dump’ schemes, insider trading, and cartels are rampant in the market. Furthermore, unlike stock markets, where a sharp fall resulting from heavy sell off will trigger a trading halt, cryptocurrencies have no such mechanisms and are valued based on momentary supply and demand.

What is the likely impact?

It is foreseeable in the future that the current format of blockchain based cryptocurrencies or a derivative of it will make its way into the mainstream. The main question is whether it takes the form of decentralised or centralised. A decentralised platform allows users the freedom to send and receive payments internationally that is not traceable or controlled by governments or other private entities.

If each country’s government were to make their own cryptocurrency and blockchain with no physical currency they would have complete oversight of every transaction made by every individual or business meaning that “cash economy” (tax-free) would cease to exist. It also raises the questions of privacy as government would use it for surveillance of its citizens.

A worldwide centralised cryptocurrency seems hard to conceive as many factors go into what makes a fiat currency operate and too many variants exist in the makeup of a country to suggest one currency could suit all, including GDP, social policies, security, politics, and so on.

It’s difficult to predict if changing the financial system of a government currency to that of digital would change the level of employment in the system. As jobs would become redundant, mainly in the supply chain and protection of physical currency, new jobs would be created in the infrastructure, maintenance and development of new blockchain and cryptocurrency. Certainly people in jobs earning non-declared income, who may otherwise be unemployable due to regulations, would be impacted. This may in some cases lead to increased crime, mental health and wellbeing issues, and dependency on social welfare as those people struggle to survive. Tax revenue may increase as evasion becomes more difficult, which would then cover the increased government social assistance, however the social wellbeing impacts may become of greater concern than economic.

How will this affect you?

While it is unlikely that any of the currently known cryptocurrencies will become mainstream and replace government currencies, central banks and governments have expressed concerns that high uptake of some emerging cryptocurrencies from prominent organisations, such as Facebook’s Libra currently under development, could destabilise established financial and banking systems. *(*[*https://www.washingtonpost.com/business/2019/07/12/why-governments-around-world-are-afraid-libra-facebooks-cryptocurrency/*](https://www.washingtonpost.com/business/2019/07/12/why-governments-around-world-are-afraid-libra-facebooks-cryptocurrency/)*)* Many countries therefore initially attempted banning the trading and ownership of cryptocurrency, however most have since relaxed policy attempting instead to regulate and force public declaration for taxation purposes.

In some countries such as Venezuela with political and financial instability, cryptocurrencies have been a saving grace for some citizens, where they have exchanged their devaluing fiat currency for Bitcoin and other altcoins. Some people escaping war ravaged countries have also successfully taken their finances out of the country by exchanging into cryptocurrency, then back to fiat currency after arriving at their destination. *(*[*https://www.bbc.com/news/business-47553048*](https://www.bbc.com/news/business-47553048)*)*

Decentralisised cryptocurrencies and their use cases will therefore likely continue to evolve and develop, particularly in user interface, and will always have their place in society. As we have seen in recent years with futures trading of Bitcoin, more and more people and institutions will start to invest in them which in-turn will generate greater interest and investment over time. Awareness and education would be paramount otherwise many investors may lose significant proportions of their life earnings through innovative cyber crime or simply the volatility associated with decentralised and unregulated currency. These sorts of reasons are why the general public are currently apprehensive about cryptocurrencies becoming the normal way of paying for items. Individuals need the security of knowing then when they go to sleep at night that the amount of money in their wallet will still be worth the same when they wake up in the morning.

Discussion of cashless society has also recently emerged with the novel coronavirus pandemic possibly being spread through handling of cash, and we may see this argument leveraged by governments in the near future as an opportunity to progress cashless society with introduction of government digital currency.

While the prospect of cashless society is attractive for governments in making underworld crime and corruption more difficult, moving to digital currency could impact a significant proportion of the population that rely on cash. Sectors such as hospitality/restaurant workers that rely on tips, personal services that rely on privacy, charities and homeless who ask for money on the street, the elderly and intellectually impaired that struggle with technology would all be affected. Also small retailers that currently operate on cash to avoid electronic payment processing fees would face increased overheads. (<https://www.vox.com/2017/7/24/16021630/cash-payments-cashless-mobile-inequity-square-apple-pay-venmo-amazon>)

Other affects may be positive such as new jobs as governments and private sector look for opportunities to capitalise on the technology, new uses cases appear such as digital finance and investments. For example, in future we may see contract settlements handled with cryptocurrency ‘smart’ contracts, decentralising control and removing any party’s ability to renege.

The true affect of all this on an individual in the future will most likely come down to deciding how much of their wealth and finances to store where, which will be a trade off of privacy using a government backed blockchain, and cryptocurrency where people have independent control and oversight, while subject to volatile markets and fluctuation.

Bibliography

J. Frankenfield, November 3 2019 "Cryptocurrency", *Investopedia*, 2019. [Online]. Available: <https://www.investopedia.com/terms/c/cryptocurrency.asp>

D. Biczok, *The Future of Bitcoin and The Blockchain Technology*, 1st ed. Luxembourg, 2018, pp. 15, 16, 18, 23, 24, 25. Available: <http://investas.lu/CMS/images/PDFs/Biczok_Master_Thesis.pdf>

N. Reiff, "Blockchain Explained", *Investopedia*, 2020. [Online]. Available: <https://www.investopedia.com/terms/b/blockchain.asp>