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 thousands of them. Each block stores its own unique identifying code called a “hash” that makes this block distinguishable from every other block in the chain. Only once all transactions in the block have been verified 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 opposed more traditional ways of financial transactions as that it does the transactions without the use of a trusted third party. The blockchain network instead runs on thousands of different computers which all have the exact same copy of the blockchain which updates as a new block is added the to the chain. This is what makes a blockchain arguably more secure than that of a centralised system such as a bank. If a person wanted to alter your transaction this would change the hash of the block meaning that the individual would have to change the hash of subsequent blocks to hide their tracks.

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 one company’s server this creates the same vulnerability to that of a traditional banking system, meaning that if a person gained access to the server they would have access to 100% of the network and could alter transactions.

**Cryptocurrencies**

Cryptocurrencies are a form of digital currency which use digital files instead of notes and coins as their money. Just like a safe or vault is used to protect cash currency cryptocurrencies use cryptography to secure and hide their information, this is what gives the “crypto” in cryptocurrency. Using cryptography to secure its transactions means the cryptocurrencies are nearly impossible to counterfeit.

Cryptocurrencies work on a decentralised platform, mainly a blockchain, meaning that they are not controlled by a single group or government and operate on a peer to peer basis. This concept means they can operate largely without influence or alteration by governments.

The first decentralised cryptocurrency created was Bitcoin in 2009 by a pseudonymous developer named Satoshi Nakamoto. Bitcoin is still the largest and most widely known cryptocurrency in the world. Other cryptocurrencies are referred to as “Altcoins”. There are now thousands of cryptocurrencies being traded globally. The largest of the Altcoins include Ethereum and Litecoin. These are all mining-based cryptocurrencies. Altcoins can include alternatives to mining-based cryptocurrencies such as Stablecoins. Stablecoins were created to provide a cryptocurrency that didn’t have such high volatility in the marketplace like many mining-based cryptocurrencies do. Stablecoins are aligned to an asset or group of assets. The largest Stablecoin is Tether, which as of April 2020 has a market cap of 6.34 Billion USD.

Cryptocurrencies allow users to make transactions with a degree anonymity as only their digital signature or username is logged in their place in the blockchain. Each transaction made is confirmed in the blockchain by “miners” and a small pre-determined fee is paid to said miners for the use of their computers. 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 of the blockchain that the cryptocurrency is operating on. Bitcoin’s blockchain operates over millions of computers with large mining facilities located around the world usually where electricity is cheap and verify every transaction that occurs. This concept is contrastingly different to that of traditional financial institutions who charge large fees on domestic and international transactions because of the monopoly they hold over the conventional currency system.

Cryptocurrencies are stored in a virtual wallet which contain both public and private keys which are linked. When a person wants to send you cryptocurrency they will send it to the public key, you then use your private key (similar to a password you use for any account) to prove you own the public key which has had the cryptocurrency sent to it. Once this is done your wallet will now show a new value. When you send cryptocurrency to a person’s public key you are essentially giving away ownership of that cryptocurrency and the transaction will be forever recorded in the blockchain. It all relates to the function of handing over physical cash to another person to put in their physical wallet the only difference being there is an indisputable transaction record kept of the event.

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 of a currency that is not controlled and manipulated by a government to suit there needs but of a collective goal by users across the world. The downside to this is with no government to back the coin its value can increase and decrease rapidly with no real control.

If each country was 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 no doubt use it to monitor its citizens.

A worldwide centralised cryptocurrency seems hard to conceive as so many factors go into what makes a fiat currency operate. Just as 1 AUD can buy a loaf of bread in one country it can’t in another. The same goes for 1 unit of a cryptocurrency relative to whatever goods or service and individual wants to purchase. Too many variants exist in the make up of a country to suggest 1 currency could suit all these include GDP, social policies, security and more.

Its hard to say if changing the financial system of a fiat currency to that of all 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 maintenance and infrastructure development of a new blockchain and cryptocurrency.

How will this affect you?

Cryptocurrencies are incredibly volatile in terms of rapidly changing values which makes clear and accurate forecasting models hard to create. The emergence of thousands of Altcoins in the tradable marketplace that have a low market cap are at risk of “pump and dump” attacks which creates distrust in the system. A pump and dump scheme will operate similarly to a pyramid scheme. A group of traders will identify an Altcoin and drum up support for it online to potential buyers who are unaware of the scheme. Trading of the Altcoin will then increase at a massive amount and create an incredibly sharp rise in the coin to the point where the group will sell off causing a massive downfall in value and leaving many with large losses. These sorts of things are why a lot of the public are apprehensive about cryptocurrencies becoming the normal way of paying for items. Individuals want to know then when they go to sleep at night that the amount of money, they have in their wallet will be worth the same when they wake up in the morning.

The true affect of this on an individual will most likely come down to a trade off of privacy by using a government backed blockchain and cryptocurrency where they have complete oversight but will not be subject to such volatile markets and fluctuations and where a person’s funds will be more secure whilst be transferred and stored.

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>