**BLOCKCHAIN AND CRYPTOCURRENCIES**

A blockchain is a type of database, a collection of data which is stored and then structured in a format that allows for easier searching, processing and filtering. What sets apart a blockchain from your everyday database is that rather than simply storing the data in a table the blockchain collects information in groups and forms it into a *block* which can be thought of as a set that holds data. Due to storage limitations when enough data has been grouped to form a block that block will then become ‘locked’ and a new block will begin production to form a chain. *Blockchain.* When implemented in a decentralised manner this makes each completed block not only immutable, but completely transparent. Each block is timestamped and the chain itself functions as a sort of timeline.

Blockchain is the technology behind Bitcoin, the most popular cryptocurrency or *coin*. For many people blockchain and bitcoin are synonymous, usually referring to any cryptocurrency as bitcoin or internet money. With blockchains key qualities of immutability and transparency, this has led to the main use case of this technology as a ledger, a collection of financial transactions. Unlike a typical database, centralised, a blockchain isn’t generally affected by DoS attacks, environmental catastrophes, machine failures, or even a legislative ban from an entire country. If a standard database will use a large amount of computers in a centralised location, a blockchain will typically store the database across many locations and many computers, hundreds of thousands even. This decentralised approach can translate each computer and network location as a *node*.

In a blockchain, each and every node has a full copy of the blockchain, and each node works to validate the previous blocks and ensure continuous block production. If one user tries to alter the existing blockchain the rest of the nodes will work through the data and invalidate altered blocks and stop or *fork* the chain. In order to change the blockchain a majority of the decentralised nodes will need to agree with the changed data, then the chain can continue. If a user forks the chain with altered data it basically renders it useless, as no one else will be contributing to that chain and there’ll be no value within. However hard forks have occured before, see Ethereum VS Ethereum Classic, a case where the minority of miners or nodes stayed with the altered chain and kept enough momentum to continue production, albeit as another blockchain altogether.

Due to the decentralised nature of Bitcoin, or most blockchain projects, anyone can view the transactions that were made on the chain. They can see what address it came from, when it was made and the fiat and crypto nominal value. This implementation also creates greater security than a conventional centralised approach, blocks are always added chronologically and its very difficult to alter past blocks, doing so would generally result in the other nodes cross checking and discarding your nodes chain as illegitimate. In fact if any minute piece of data is changed at all then the *hash code* (a sort of signature of the block) will change as well, flagging it for illegitimacy. Say someone wants to alter the blockchain and give themselves a bunch of the native currency, other nodes will cross check this and the alteration will have been fruitless, this ensures that someone can’t steal someone elses holdings by just editing the chain. In a truly decentralised blockchain the only way to really attack the network is with whats called a *51% attack.*

Succeeding with a hack like a 51% attack would require immense wealth and computing power. The hacker would need to effectively hijack 51% of the nodes and alter the chain so that consensus can be reached and the nodes accept the new chain. Due to the treatment of crypto as an extremely volatile investment vehicle, the more fiat value the chain acquires the more expensive it is to overtake the majority of nodes, as more miners flock to contribute to nodes more processing power will also be needed to control the increase in nodes. Keep in mind, even if the hacker can successfully alter the chain due to the transparent nature everyone would notice and value and trust would quickly be lost in the project. Many blockchain projects have collapsed under the weight of a 51% attack, as miners move their resources to a different project after noticing the hack, or existing nodes forking to another version of the chain and not keeping momentum with resources or development.

Still we must ask ourselves, *where is the inherent value in the blockchain and its native cryptocurrencies?* Is it simply a digital ledger? What use cases exist that can create value in the real world? Companies like Pfizer, Walmart and Unilever use blockchain technology to trace product routes and verify product authenticity, but projects like VET (VeThorChain trading at $0.16) which are built and utilised for this specific purpose aren’t as big in market cap as Bitcoin or Etheruem, $65k and $4k respectively as of October 2021.

Perhaps the industry which stands to be the most impacted by this technology is the financial sector, what crypto enthusiasts are beginning to refer to as tradfi (traditional finance) due to the emergence of DeFi (decentralised finance). DeFi has allowed for a much more appealing alternative to banks, the money you can keep in your savings account might net you 0.5% interest a year at best, while *staking -* contributing to coin governance, security and block production - functions the same as a savings account but can safely net you anywhere from 4% - 10% interest per annum. Today you can even take loans out against your crypto as collateral.

Blockchains have inbuilt currencies referred to as coins, these coins are distributed as a reward for the node that completes a block, the coins are then given a fiat value as dictated by normal market mechanics. Nodes can be made up of one owner running several machines to try complete blocks or nowadays by individuals who will pool their resources together to a node and then split the reward. The appeal in this is that the value of your currency isn’t at the whims of a central authority and not subject to the same inflation or deflation mechanics. Coins can be inflationary or deflationary, but as a core design choice of the protocol rather than the musings of governments. Without the need for a central authority, transactions can be processed whenever rather than on banking days and hours, this does however result in transaction fees being imposed on the user. This is generally acceptable by users and the only real negative impact of cryptocurrencies is the environmental effect mining (using an enormous amount of computing power) can have, this is being quickly negated however as chains turn to proof of stake rather than proof of work, with many chains aiming to be carbon neutral or negative.

Holding your funds in a blockchain can prove to be significantly more lucrative than a traditional savings account, and the chain will never tell you where you can spend your money or control your deposits/withdrawals. This creates a terrifying worst case scenario for banks who are at the risk of becoming obsolete, however big banks generally aren’t stupid and have been accumulating mass amounts of cryptocurrency in order to hedge themselves as well as control large sectors of big blockchain projects, this helps them centralise and consolidate their power as well as create significant influence on governance which is becoming a more common feature amongst blockchains.

Huge innovations have been made since the beginning of bitcoin and blockchains, some of the recent more substantial improvements have been non fungible tokens, smart contracts and proof of stake.

What impacts your daily life is the effect cryptocurrency can have on the greater market, as at 10th October 2021 the entire crypto market is valued at 3.2 trillion AUD, almost 3 times the value of Australia’s entire GDP. With institutions beginning to pile in, significant crashes can start to affect more than just overleveraged individual investors. The main reason mass adoption hasn’t occurred yet in my opinion is the barrier of access to cryptocurrencies, it’s not exactly as easy to use as cash or a bank card, storing and being in complete control of your funds also keeps the onus for security on the owner and investors have been subject to many rugpulls, hacks and scams over the years.

Interestingly enough, in september 2021 the President of El Salvador has declared Bitcoin legal tender and has spent much of the countries money on acquiring the asset. The law has resulted in the requirement that businesses must accept Bitcoin if offered and many citizens downloading the governments *Chivo wallet* in order to hold and spend bitcoin. To incentivise adoption, the government of El Salvador even offered its citizens who downloaded the Chivo wallet $30USD in Bitcoin. El Salvador, like its cousin Venezuela is another country which is subject to the US Dollar, its centralised bank and severe inflation. As this is a recent development and first step toward mass adoption, time will tell what this event will do the country citizens and financial health.

Roy A 2021 ‘In El Salvador, More People Have Bitcoin Wallets Than Traditional Bank Accounts’ *Forbes* Oct 7 2021, viewed Oct 10 2021

<<https://www.forbes.com/sites/theapothecary/2021/10/07/in-el-salvador-more-people-have-bitcoin-wallets-than-traditional-bank-accounts/?sh=83c64bb20b57>>

Conway L 2021, *Blockchain Explained,* InvestOPedia, viewed Oct 10 2021

<<https://www.investopedia.com/terms/b/blockchain.asp>>