**What is it?**

Blockchain is a cryptographic technology; it began with Bitcoin (BTC) in 2008 when Satoshi Nakamoto released its whitepaper.

Blockchain uses a decentralised, immutable ledger which keeps track of all transactions in the network. Miners compete to solve a cryptographic hash; the miner that solves it then adds the next block to the chain, gaining a set amount of Bitcoin as well as the fees from the transactions.

After Bitcoin's adoption, new cryptocurrencies which were based on it entered the market, such as Ethereum (ETH), which was the first programmable blockchain. These new coins are called Altcoins, short for "Alternative Coins".

Later, new currencies emerged that were based on Ethereum which are called tokens, as well as new designs altogether. Tokens use another blockchain such as Ethereum rather than having their own unique blockchain.

Ethereum was the first blockchain to introduce DApps which are apps which run on the network. It also introduced SmartContracts.

Besides coins which are designed for payments, there are a variety of different types of cryptocurrencies:

* Privacy coins such as Monero focus on making payments in a way which cannot be tracked back to the consumer.
* Gambling tokens which are used by online crypto casinos to play games on the blockchain.
* Voting tokens which enable consumers to voted digitally in a reliable manner.
* Energy coins which enable consumers to buy and sell electricity peer-to-peer.
* Supply chain tokens which track information about a product in the supply chain.
* Stable coins such as Tether are pegged to fiat in order to reduce volatility.
* Exchanges commonly offer a token for use on their platform, which provides some perks such as reduced trading fees.
* Ad tokens such as BAT which pay you for watching ads and allow you to tip content creators on the web. (This token is integrated in the Brave browser.)
* Decentralised Finance coins allow users to take out loans.

(Types of cryptocurrencies: explaining the major types of cryptos, 2019)

China is working on a cryptocurrency of their own which is backed by gold. (Bloomberg)

This is a form of Government-endorsed digital currency which may be common in the future.

It is rumoured that PayPal and Venmo may be planning on allowing buying, selling and storing of cryptocurrencies. (Allison, 2020)

If this turns out to be accurate, this will significantly increase adoption and simplify the process for a consumer to get into the crypto space.

Another crypto called Lolli is partnering with a number of retailers online to provide cashback in the form of Bitcoin in order to increase adoption and get more consumers into the space. (Techcrunch)

**Wallets**

Typically, a consumer's wallet consists of two important addresses: a public address (akin to an account and BSB number in a bank), which others use to send funds to him; and, a private key (or address) which is like a bank account's username and password. Whomever owns the private key has access to the wallet, and can transfer the funds inside. Transactions are irreversible.

Wallets can be created via websites, smartphone apps, or even hardware devices. The concern with digital wallets is you are potentially vulnerable to viruses, malware and hacking. Physical hardware wallets offer much more security in comparison but are not free.

**What does blockchain aim to do?**

Blockchain aims to remove the middleman: when we send payments online, we use our bank, or services such as PayPal to act as a middleman. The focus of blockchain is on decentralised processing and validation; essentially, removing that middle man from the equation, but still ensuring that both parties get what they agreed upon.

Using Bitcoin as an example, when someone sends a transaction, it is validated first by the network and then it is included in what is called a block. Miners compete to add the next block to the chain by solving a cryptographic hash, and they are rewarded both with the fees of then transactions added to the block, and with a set amount of Bitcoin.

There are various types of validation found in blockchain projects:

**Proof of Work (PoW)**

This type of validation is used by Bitcoin and many other coins. Transactions are gathered into blocks; these blocks are then linked together.

Miners try to solve a cryptographic hash which gives them the right to add the next block to the chain; it is this mechanism that keeps the network safe. One potential issue with this form of validation is if one entity owns 51% of the mining network; this allows for that entity to decide whether transactions are legitimate or not.

Miners join "pools" which are large networks of miners who work together to crack the hash; rewards are divvied out proportionally based on a miner's contribution.

**Proof of Stake (PoS)**

Coin holders lock their coins in the system; the system then decides which of the holders will validate the next block. The more coins that are staked, the higher the odds of being chosen.

**Delegated Proof of Stake (DPoS)**

Coin holders lock their coins in the system, providing them with a proportional amount of voting power; holders vote for a delegate who manages the blockchain, ensuring security and consensus. (What Is Staking? | Binance Academy, n.d.)

**What could blockchain do over the next few years?**

**Supply chain authentication**

Various cryptocurrencies focus on supply chain authentication. The goal is to prove the authenticity of products and provide information about their journey along the supply chain, as well as additional potentially relevant information such as: when it was packed, where it was packed, and by whom was it packed.

According to CoinCodex the top 5 cryptocurrencies in this field include: WaltonChain (WTC); Modum (MOD); VeChain (VET); Ambrosus (AMB); Tael (WABI).

In the coming years, we may see these cryptocurrencies begin to gain traction in consumer markets and provide consumers with the confidence that their product is indeed what is advertised.

Supply chain authentication is a big deal in China due to the large number of counterfeit products that are sold across a range of categories such as food, beverages, footwear, apparel, technology and many more.

In 2013, the global trade for counterfeit products reached half a trillion dollars, with most of the counterfeit being produced in China or Hong Kong. (OECD)

It has recently been announced that Chase Shiel will be using VeChain to confirm the authenticity of its Nike shoes. According to the article, knockoff shoes are a big issue for footwear makers. (Toshendra Sharma, 2020)

**Gambling**

Another aspect which blockchain aims to improve is gambling. Blockchain removes the element of trust from the equation. Is the house cheating? Is a player cheating? Everything is recorded on the blockchain, which means everything can be verified. (Blockchain and gambling)

FunFair is a coin which can be used in an online casino made by the same company, allowing users to gamble on their platform.

**Voting**

An important issue which involves much trust is voting. Some concerns with the existing system are that it is expensive to run a vote and that it is unreliable. Moving voting to the blockchain means all votes are verifiable and the costs are far, far cheaper.

Two companies that focus on this field include Horizon State and FollowMyVote.

**Payments**

Cryptocurrencies are competing with each other to become the most popular for payments and to outperform credit card systems.

One of the most significant benefits of blockchain in the field of payments is the ability to pay someone anywhere in the world without a middle man. However, at this stage, transaction speeds are not fast enough -- ranging from hours to minutes.

In the future, we will see transactions that can be processed in a matter of seconds, securely between two parties.

**Private payments**

Because the blockchain is public, meaning anyone can view it and follow a trail of transactions, that means there is a need for privacy. Privacy coins such as Monero do this by obfuscating the buyer's public address. (A low-level explanation of the mechanics of Monero vs Bitcoin in plain English, n.d.)

The overall impact of the blockchain will vary depending on the particular field in which it is being employed. In supply chain management, counterfeit products will be purchased less as consumers can verify the authenticity of genuine goods; this will help consumers stay away from potentially dangerous, counterfeit products. Over time, the massive market for counterfeit products will decrease.

In payments, as improvements to the technology occur, consumers will be able to complete high-speed transactions across the globe for minute fees.

In terms of voting, there are many benefits, including:

* Voting from any device in your own home
* Secure voting that anyone can audit
* Ability to change your vote easily
* Reduced costs for vote-holders, making votes more practical and economical

In 2017 the Australian government a postal survey to ask citizens whether or not gay marriage should be legal. The survey cost 122 million dollars which is an enormous figure. (Australia: ‘Yes’ Vote to Marriage Equality | Human Rights Watch, 2017)

With a substantial reduction in cost, more votes can be held to allow a country's citizens to weigh in on important issues; whereas, right now it is not fiscally viable to do so.

**How will this affect society?**

There is much value to be gained by using blockchain in the supply chain field. The ability to scan a QR code to check the authenticity of a product is game-changing. This technology is something that will be able to be utilised day-to-day, even though counterfeit products are not as common in Australia as other countries.

Blockchain is gaining more and more adoption, and in turn, companies are hiring more and more developers; this creates many job opportunities in an emerging market.

The use of blockchain in banking, and a full move to digital currency, may make bankers and tellers are a thing of the past.

**References**

Monero.how. n.d. *A Low-Level Explanation Of The Mechanics Of Monero Vs Bitcoin In Plain English*. [online] Available at: <https://www.monero.how/how-does-monero-work-details-in-plain-english> [Accessed 29 June 2020].

Allison, I., 2020. *Paypal, Venmo To Roll Out Crypto Buying And Selling: Sources - Coindesk*. [online] CoinDesk. Available at: <https://www.coindesk.com/paypal-venmo-to-roll-out-crypto-buying-and-selling> [Accessed 29 June 2020].

Human Rights Watch. 2017. *Australia: ‘Yes’ Vote To Marriage Equality | Human Rights Watch*. [online] Available at: <https://www.hrw.org/news/2017/11/15/australia-yes-vote-marriage-equality> [Accessed 29 June 2020].

Capital.com. 2019. *Types Of Cryptocurrencies: Explaining The Major Types Of Cryptos*. [online] Available at: <https://capital.com/types-of-cryptocurrencies> [Accessed 29 June 2020].

Crichton, D., 2018. *Techcrunch - Lolli Launches To Give You Free Bitcoin While You Shop*. [online] Techcrunch.com. Available at: <https://techcrunch.com/2018/08/22/lolli-launches-to-give-you-free-bitcoin-while-you-shop/> [Accessed 5 July 2020].

sofi. n.d. *Understanding The Different Types Of Cryptocurrency*. [online] Available at: <https://www.sofi.com/learn/content/understanding-the-different-types-of-cryptocurrency/> [Accessed 29 June 2020].

Peili, R., 2019. *Top 5 Supply Chain Management Cryptocurrencies | Coincodex*. [online] Coincodex.com. Available at: <https://coincodex.com/article/4925/top-5-supply-chain-management-cryptocurrencies/> [Accessed 5 July 2020].

Bloomberg.com. 2020. *Bloomberg - China’S Digital Currency Could Challenge Bitcoin And Even The Dollar*. [online] Available at: <https://www.bloomberg.com/news/articles/2020-06-01/china-is-making-cryptocurrency-to-challenge-bitcoin-and-dollar> [Accessed 5 July 2020].

Binance Academy. n.d. *What Is Staking? | Binance Academy*. [online] Available at: <https://academy.binance.com/blockchain/what-is-staking> [Accessed 29 June 2020].