Philanthrop3 Collective

What is Web 3 and Blockchain Technology

What is cryptocurrency?

Cryptocurrency is a new form of digital currency. It was first conceptualised in a whitepaper in 2008 (after the global financial crisis) by an unknown person or group of people using the name Satoshi Nakamoto. The white paper called 'Bitcoin - A Peer to Peer Electronic Cash System' discussed a form of electronic cash that could be sent directly from one party to another without going through a financial institution or trusted third party. This is achieved through forming a public record that cannot be changed called the blockchain (more on that later).

What was the problem it was solving?

1. Reliance on Banks

Until cryptocurrency, transactions on the internet rely almost exclusively on financial institutions serving as a trusted third party to authentic transactions between parties. In person, when a business transacts with a person using physical currency, there is limited risk involved as money is physically exchanged. In electronic payments, merchants need to be wary of their customers and obtain more information on them to ensure that the money will be exchanged. Financial institutions play the role of the trusted third party, to authenticate the consumer and the availability of funds for the merchant, and act as a mediator if dispute arises over payment. This system has worked for most transactions online, however, this trust based model increases transaction costs, limits the ability for small casual transactions and leaves out over 2 billion people who do not have access to a bank account.

Additionally, it places total power over money within the financial system. The 2008 financial crisis demonstrated this system was not without flaws, which was the catalyst for the blockchain concept. Bitcoin, as the first cryptocurrency, was created as another option, aiming to provide a fairer system and placing the power of a transaction back to the individual.

2. Access to Banking

It is estimated 2 billion people do not have access to banking and financial services. In remote places, everything has to be done in cash and even that can be difficult to manage. Despite technological advances, the traditional banking system relies on manual processes and traditional data to conduct identity verification checks. The reliance of traditional application process and traditional identity data, removes large demographics who may not have formal identity documents for creating accounts, applying for loans or mortgages or possibly gaining access to financial opportunities. Of those who have forms of identification, lack of credit records required by financial services leads to providers being unable to conduct due diligence of credit-worthiness.

What was the problem it was solving? (cont.)

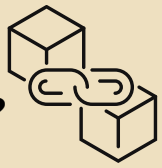
3. International Transactions

Traditionally, sending money internationally involves long lead times and multiple fees. This is due to the fees on the bank or financial entity as well as loss due to foreign exchange margins. Cryptocurrency can be a cheaper and more convenient method for sending money overseas. Cryptocurrency allows faster transactions directly between individuals crypto wallets via the blockchain. International workers that send money to their home country, as well as for charitable donations to Ukraine during the crisis have been two successful use cases of cryptocurrency.

4. Open Source Auditing

The blockchain is a publicly accessible distributed ledger that records all transactions. While the information is anonymised as a cryptographic hash (a series of numbers and letters derived from an algorithm), transactions on the blockchain can be tracked from production to delivery or use by the recipient.

What is the blockchain?



The blockchain is a digital ledger of information, that is distributed across a network of computers using cryptographic technology. Put more simply, it is a type of record keeping technology that records all transactions and other information as a digital ledger - like a fancy spreadsheet. The key difference between a typical database and the blockchain is its structure. The blockchain records a number of transactions together as a group, called a block. Once a block has reached its storage capacity of information, it is timestamped, closed and linked to the previous block. This forms a chain of blocks. Any new information that follows is then compiled into a new block. This forms a chronological record of all transactions on the blockchain. This information is stored publically across many computers across the world, so no single company or central database holds the information and everyone can see it. This is all done through several concepts from cryptography, including digital signatures and hash functions.

The key elements are the blockchain:

- A **digital ledger** of information;
- The data is grouped as **blocks**, chronologically added to a chain;
- It is **publicly available**;
- It is **decentralised** across a network of computers across the world; and
- It is **immutable** (can't be changed).

The blockchain started in 2009 with Bitcoin, today there are at least 1000 blockchains with at least four types of networks.

Is the blockchain secure?

One of the reasons blockchain technology is so popular, is the data structure makes it secure. It is designed to prevent anyone from being able to delete or change it. Each block in the chain is unique and has its own unique code (hash), as well as reference to the previous block hash and a timestamp.

This type of data structure makes the data irreversible. If a block was altered, the change would be detected as it would no longer align with the rest of the chain. In theory, to maliciously change or delete data, it would require a change to every block in the chain before it. This would take huge computing power that is unavailable today.

But what about inputting false data into an open block?
The way trust is achieved on the blockchain is through consensus across the network. When a block is formed, the majority of the network then has to agree that the block is valid before it is added to the chain. Once a block is added to the chain, everyone in the network gets an updated copy of the chain. Therefore to be able to bypass this security, a malicious actor has to control more than 51% of the active network.

What can the blockchain be used for?

Currency:

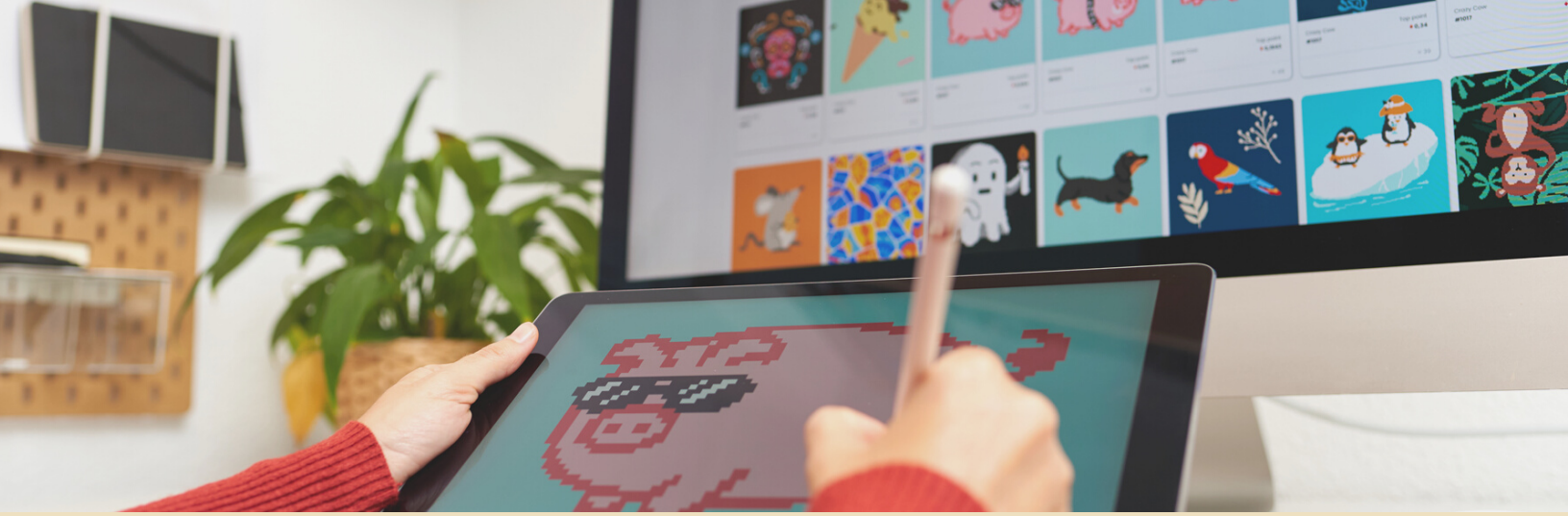
The blockchain technology was originally conceived for supporting currency, Bitcoin specifically. Cryptocurrency or 'crypto' is any form of digital money that uses cryptography to secure the transaction. Crypto exists purely as a digital entry on an online database. Rather than using banks, crypto uses a peer-to-peer system that records transactions on a public ledger. If you own crypto, you won't have anything tangible, rather you have a cryptographic key that allows you to move currency from one person to another.

Cryptocurrency, like fiat money (AUD, USD etc) can be used to buy items, such as NFTs, but are also legal tender in a small number of countries (e.g. El Salvador and Ukraine). It can also be exchanged for fiat money, at rates determined on exchanges. Crypto is most commonly used as a speculative, long term investment.

Like other currencies, crypto is valued based on the scale of community involvement and its restricted supply vs. demand. Unlike fiat money, cryptocurrency is not backed by a government authority, and it is decentralised from a system of banks. As of 2022, over 300 million people in the world use cryptocurrency with a total market cap over $2 trillion.

Smart Contracts:

One of the ways blockchain technology has moved beyond currency is through the use of Smart Contracts. These are agreements made between people in the form of computer code. As they are on the blockchain, they are public and cannot be changed. They are also coded to run automatically (self-executing) when a predetermined condition is met. *Note: Putting an agreement into code does not automatically make it a contract in the legal sense.*



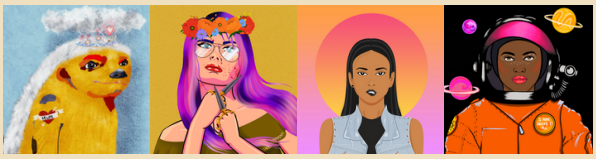
What can the blockchain be used for? (cont.)

Non-Fungible Tokens (NFTs):

Non-Fungible means that something is unique and cannot be replaced or traded like-for-like. A $1 coin for example is the same value, regardless of the coin (except for collectables), therefore it is fungible. A trading sports card, however, is unique and if traded for another card, would be something entirely different (non-fungible).

NFTs are supported across multiple blockchains, and can be anything digital (art, music, tv shows). The blockchain allows these items to be registered on the blockchain, giving it unique and non-interchangeable data within the item. This can be used to establish proof of ownership.

Unlike money, each NFT is non-fungible and cannot be traded like-for-like as the file is storing additional information that includes when it was put on the blockchain, who it was created by and who has owned it.



Decentralised Finance (DeFi):

DeFi is an umbrella term for financial services on the blockchain. Blockchain technology can mirror many functions of traditional financial systems including money transfers, lending and insurance. These are enabled by smart contracts, which automatically execute contract terms between parties. Typically they are peer-to-peer rather than routing through a centralised system. The goal of DeFi is to make finance more accessible and get rid of third party involvement in transactions.

Gaming:

The gaming industry has begun leveraging blockchain technology to change the way games are made, managed, played and paid for. Players can vote on the game's development direction and can create profiles and buy items in games that move between different games.

Real Estate:

At the time of writing, three properties worldwide have been sold and transferred via the blockchain. The latest was a condo in Miami in April 2022. Using blockchain technology to verify and transfer property ownership (including deeds and titles) is an emerging area and use of this technology.

What can the blockchain be used for? (cont.)

Decentralised Organisation (DAO):

A DAO is a new form of organisational structure built on blockchain technology. DAOs are member-owned communities from across that globe that are formed for a common purpose. DAOs operate online and require people to buy into the DAO, in the form of an NFT or crypto token, that the DAO is run by.

The primary aim of a DAO is to organise autonomously without traditional leadership and hierarchy of previous forms of organisations. DAOs are governed by democratic or highly participatory processes or algorithms. DAOs are backed by smart contracts and the blockchain to record what goes on in the group to achieve common goals.

DAOs radically challenge the traditional hierarchical structure of a company, focusing on participation and open entry for participants as well as operational transparency. At the time of writing over $10.9 billion in assets are managed by DAOs according to DeepDao.

Possible future applications:

As the blockchain is an electronic verifiable and immutable database, there are many future applications of the technology.

- Governments could use the blockchain as a database of births, deaths, marriages, vehicle registration, medical records and insurance, education records, property ownership and title transfers.
- Voting could also take place on the blockchain, and the administration of government benefits could be distributed via the blockchain.
- Tickets to games, concerts and events could be sold via the blockchain.
- Businesses may use the blockchain for payroll and tax records.

This is just scratching the surface. In the future, most products and services could run on some form of blockchain technology. From finance to healthcare, art and education, the use cases are endless. This is one of the reasons that learning the basics of this technology is important now.

To learn more about DAOs check out Honey Badges NFT

A philanthropic DAO funding global change-makers and revolutionising the charity world

BLOCKCHAINS

As a recap, a blockchain is a chronological list of electronic records in blocks that are linked together as a chain using cryptography. Each block contains transaction data, a cryptographic hash of the previous block and a timestamp.

Bitcoin was the first blockchain in 2009. Now, there are over 1000. Some of the biggest (by market cap) are Bitcoin, Ethereum, Tether, Solana and XRP.

Blockchain 'mining' is the term used to describe the computer work that goes into creating a new block in the chain. There is no physical mining occurring. Simply, these computer nodes around the world are auditing the electronic transactions that have occurred and agreeing to their validity, before they are added to the chain. This takes the place of a central authority, like a bank, that does this work in traditional electronic transactions. These computer nodes are rewarded for their work in tokens of the chain i.e Bitcoin. This work, however, takes a large amount of computer power.

Energy Consumption

But isn't crypto bad for the environment?

The amount of energy consumed by the blockchain network depends on how the network achieves consensus on the validity of a new block. How this work is done also affects the scalability of the network. The two main types are called 'Proof of Work' and 'Proof of Stake'.

Proof of Work

Proof of Work was the first consensus method and is used by major blockchains including Bitcoin and Ethereum. In this method, 'miners' validate the transactions on the network by solving cryptographic puzzles. This method was the cause of the energy debate in 2021 surrounding the amount of energy the networks were using. The University of Cambridge estimated that Bitcoin mining consumes around 0.5% of all electricity consumption globally or 117 terawatt-hours of electricity per year. Additionally, miners need to consistently upgrade to the latest mining chips to stay competitive, generating significant electronic waste. Bitcoin and other blockchain networks have been shifting towards more sustainable energy sources and have promoted green energy usage, but it has not had widespread adoption. The advantages of this method is that it is a proven way of maintaining a secure network, because of the processing power involved, and the number of miners involved, an individual or group would not be able to interfere with the blockchain.

Proof of Stake

Newer blockchains have moved to more energy-efficient methods of consensus including Proof of Stake. In this method, miners get randomly selected to add the latest block to the chain. To be a miner, however, you have to stake or contribute their own crypto for a chance to validate the newest block and get rewarded with crypto. The more crypto and time invested into the blockchain, the higher the reward for validating a block. Therefore it is how much crypto and time a miner has contributed, rather than the amount of computer processing power, that gives the ability to mine. The result is a faster and more energy efficient blockchain. Blockchains such as Solana and Cardano use this method. Additionally, Ethereum is upgrading to Ethereum 2.0 to employ this method, however this has not been finished at the time of writing. It is estimated that the Ethereum switch to Proof of Stake will reduce energy consumption by over 99%.

BLOCKCHAINS (cont.)

Scalability

Another issue for blockchains as they are adopted more widely is scalability. Bitcoin can handle around seven transactions per second, while Ethereum can handle about 20. This is significantly less than traditional payment networks like Visa or applications like Facebook (Meta) that can process millions of requests per second. This means that users on blockchains may wait minutes for a transaction to be confirmed on the blockchain, or large transaction fees called gas. These gas fees increase in periods of heavy congestion. Scalability solutions are currently being developed.

Cryptocurrencies

Top cryptocurrencies (by market cap) - current as of April 2022

1. ***Bitcoin* (BTC)** - *Proof of Work* - Can be used as a digital currency for peer-to-peer electronic transactions
2. ***Ethereum* (Eth)** - *Proof of Work (currently)* - Ethereum is a decentralised software platform that enables Smart Contracts and Distributed Applications to be built and run on the Ethereum blockchain.
3. ***Tether* (USDT)** - Tether or USDT is a cryptocurrency stable coin that is pegged to the USD. Tether acts as a medium for traders to move between cryptocurrencies without converting back to fiat money like USD.
4. ***Binance Coin* (BNB)** - This cryptocurrency was issued by a cryptocurrency exchange called Binance.
5. ***USD Coin* (USDC)** - Like Tether (#3), USDC is a stablecoin pegged to the USD.
6. ***Solana* (SOL)** - *Proof of Stake* - Solana is a competitor to Ethereum, but uses Proof of Stake verification rather than Proof of Work.