AJBell Investcentre

ADVISER GUIDE

Cryptocurrencies – friend or foe

In this guide:

The information in this article is based on our current understanding of the environment, regulations and ecosystem around cryptocurrencies and is subject to change.

Introduction

The interest and debate around cryptocurrencies has raged for the last few years, with two distinct camps emerging around the asset class: those who back the nascent technology and the potential it could bring to a host of industries, as well as the potential for returns in the investment space; and those who see it as nothing more than a collection of Ponzi schemes writ large, with no intrinsic value and a near certainty for the values to fall to zero. Like most things that attract such attention and strong opinion, however, the truth probably sits somewhere in the grey in between. Whilst the vocal classes have both made up their minds on the space, the vast majority of people are likely to be only vaguely aware of some elements of it and, even if they are a little more curious on the space than average, they may not have decided on where they sit on the 'friend-or-foe' spectrum.

This article attempts to give some details around the basics of the ecosystem and the main points proposed by both believers and non-believers, to try and give a baseline understanding for readers and encourage them to explore and research further.

Cryptocurrency – what's in a name?

Firstly, the 'crypto-' part of the word 'cryptocurrency' refers to the fact that these types of assets are signed cryptographically, i.e. they use elements from the field of cryptography as a fundamental part of their construction. Cryptography isn't new, with humans studying encryption and coding to ensure information is only seen or read by those it's created for almost since the dawn of civilization. However, the modern age of cryptography expands beyond just encryption/decryption of a simple message, to include other elements such as digital signatures, data integrity checking, etc., and these types of applications are what are used within the cryptocurrency space.

The 'currency' part of the name, however, could be said to be a bit of a misnomer. For something to qualify as a currency, it should, essentially, fulfil three functions:

1. it should act as a medium of exchange – it can be swapped in exchange for goods and services;
2. it should act as a unit of account – it is measurable and divisible and can be used to price and maintain records; and
3. it should be a store of value – it should preserve its value and not 'waste' or degrade with the passage of time.

In the case of the first and most widely known cryptocurrency, bitcoin, we could at best probably say only two of these criteria are met, with the 'store of value' criteria somewhat lacking, due to the volatile nature of the price, which has seen large swings up and down since it was introduced to the world via a whitepaper, by the pseudonymous Satoshi Nakamoto, in 2008.

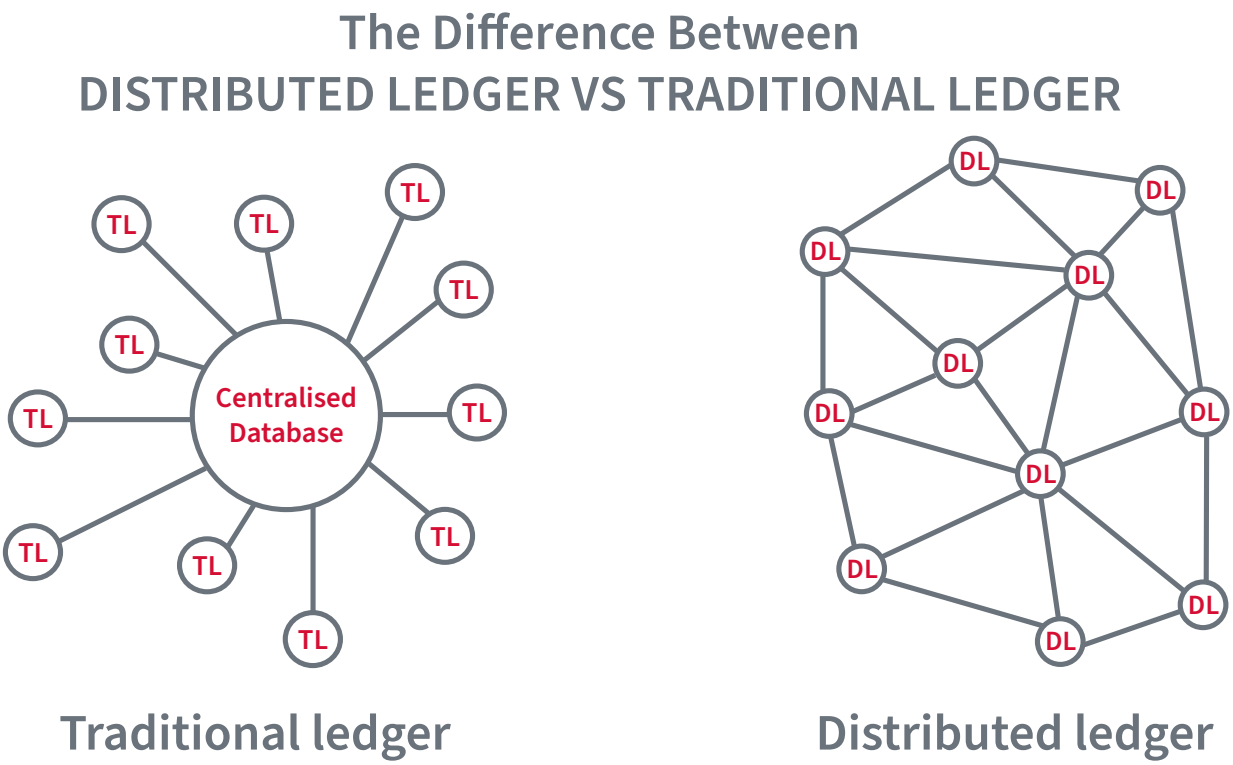
Satoshi introduced bitcoin as a counter to the central bank money printing in the wake of the financial crisis, which brought the fear of inflation and a threat to the value of the national fiat currencies used by millions of people every day. The idea underpinning bitcoin was one of 'programmable money', a peer-to-peer digital currency, not controlled by any central authority or entity, accessible to anyone with an internet connection, enabling frictionless transfer and having a known maximum supply limit of approximately 21 million coins encoded into its ruleset. This means it is 'deflationary' by design. In contrast to fiat currency, where supply is managed by central banks purposely seeking inflation, i.e. overt erosion of the real spending power of the currency, albeit at a low and stable level.

However, despite the development of bitcoin as a peer-to-peer digital currency to replace fiat currencies, it probably doesn't qualify to be labelled a 'currency', even though it can be used as a means of exchange, it can function as a unit of account and, for the bitcoin believers, it is hoped it will soon mature into a store of value as it undergoes wider acceptance and we approach the point of maximum supply. This also applies to almost all the crypto tokens that have since followed bitcoin's lead, with them fulfilling some, but not necessarily all, of the generally accepted criteria for money – whether due to volatility threatening the store of value element, or the slow and inefficient processing speeds threatening the medium of exchange argument in any real-world applications.

That being the case, 'crypto-assets' is probably a better name for the collective asset class, as opposed to 'cryptocurrency', since we don't then make assumptions about the entire ecosystem and its possible use cases at outset.

Blockchain, distributed ledgers and decentralised networks

Besides cryptographically-signed transactions, what else powers crypto-asset technology? The answer is blockchain. But what is a blockchain? How does it relate to another term we hear in the space, 'distributed ledger', and what does 'decentralised networks' mean?

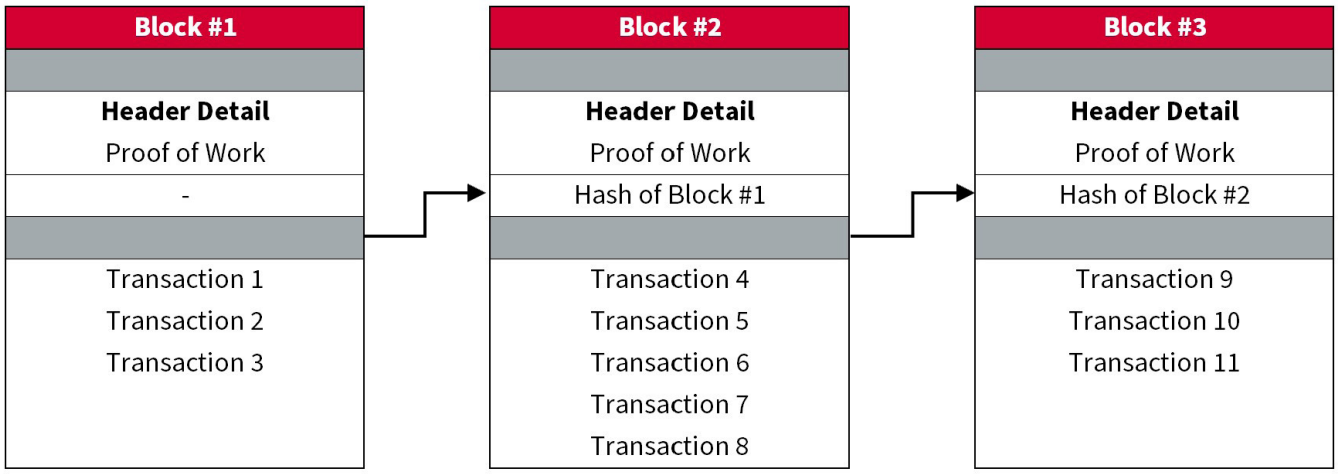


To start with, a blockchain is a type of distributed ledger, but not all distributed ledgers are blockchains. A distributed ledger is simply a transactional book of record that is shared between several different nodes, rather than being held as a database by one central controlling authority. The distributed nature of the ledger means all nodes have their own copy of the transaction record, which theoretically allows more efficient transactions, since every transaction doesn't have to process through the centralised controller.

In a centralised system, organisations must commit significant manpower and resources to maintain control and, as every location that contributes data to the ledger could become a source of fraud or errors, the ledger isn't always up to date due to checking and verification at the central repository. Distributed ledger technology, however, allows for real-time data sharing, which means the ledger is always up to date. It also enables transparency, as each participating node can witness changes in real time. Lastly, it is more secure by nature, because it eliminates the single point of failure and single target for hackers and manipulation that can exist with centralised ledgers.

Blockchain is a specific type of distributed ledger and one intimately associated with crypto-assets, since it is the type used in bitcoin and almost all crypto-assets. Blockchain combines transactions into a block and chains them together in an immutable linear record that is then publicly broadcast to the entire network. This means that once a transaction has happened, it is basically impossible to go back and edit it, since every subsequent block has the information from earlier blocks encoded in it. This makes blockchain technology very secure and hard to hack, which is very powerful for financial applications, where full visibility of the chain of ownership and transaction history is important.

An example of how a “Blockchain” connects past and current transactions



When you have distributed ledgers, multiple nodes, a large number of users and no central authority to run it, that is what gives us the idea of a decentralised network. But how are the network and the ledger kept up to date if there are multiple copies and everyone is transacting independently? The answer is via a consensus mechanism, e.g. cryptographic applications that allow nodes to compare their individual record books, to decide which is the true, latest state of the ledger.

Bitcoin and various other protocols use ‘Proof of Work’ (PoW), which requires a participant node to prove that the work done and submitted by them qualifies them to receive the right to add new transactions to the blockchain and earn rewards as a result, i.e. mining bitcoins. They do this by solving simple but arduous mathematical problems. However, this mechanism has high energy consumption and a longer processing time, due to the increasingly difficult computations needed to process a block. This limits bitcoin to around seven transactions per second, which severely limits its use case as a means of exchange for goods and services. As a result, other alternative algorithms have developed, such as ‘Proof of Stake’ (PoS), which is used, along with other mechanisms, in newer networks such as Solana and will soon be adopted by the second largest network, Ethereum, in an upgrade to its protocol, as its consensus mechanism. This is a lower-cost, lower-energy-consuming alternative to the PoW algorithm and involves allocation of responsibility in maintaining the public ledger to participant nodes, in proportion to the number of crypto tokens held by it. PoS and newer mechanisms cut the processing time and energy usage down dramatically, allowing networks to process transactions much faster and increasing the throughput to levels beyond even the current VISA electronic payment network.

Network	Transactions per second
Bitcoin	7
Ethereum	20
Paypal	193
Visa	24,000
Solana	65,000

Source: howmuch.net/articles/crypto-transaction-speeds-compared (10 June 2018); gemini.com/cryptopedia/solana-blockchain#section-a-new-blockchain-architecture-proof-of-stake-and-proof-of-history (14 April 2021)

The expanding crypto universe – do too many cooks spoil the broth?

One argument proposed by those who don't believe in the value proposition of crypto-assets is that the sheer number of different tokens means that the network effect is diluted. They also contend that the finite supply and deflationary status hard-coded into network protocols such as bitcoin and a number of other tokens is moot, due to the almost limitless capability to fork, i.e. copy the open source ruleset code underlying a token, but then introduce edits to create a completely new asset. This has seen the universe of tokens grow to over 5,000 at this point, each with their own rulesets, design parameters and supposed use cases.

It should be said that the growing proliferation of crypto-assets does make crypto a more intimidating asset class for a newcomer to contend with, due to the breadth of networks, tokens and technology one must get up to speed on. However, the mere ability to fork or launch a token should not necessarily be taken to mean that the attractions of another token's use case are lost. For instance, take the case of bitcoin and its limited supply, which should mean it holds its value once they are all mined, a key design feature and raison d'etre; there are several variants of the bitcoin ledger, each with their own token – e.g. Bitcoin Cash, Litecoin, Dogecoin – but none of them have acquired the value and market capitalisation of the original ledger based on the Satoshi whitepaper. In a sense, creating an alternative may attract some users away, but it is akin to capitalism and copying the business model of a competitor; the existence of a new entrant business may impact the incumbent in the short term and may even usurp it or supplant it long term, but it isn't guaranteed to do so.

Crypto, criminals and regulation

One thing extensively covered in the media when discussing crypto is its attractiveness for criminal groups, who it is said use its borderless and supposedly anonymous transactional capability to conceal proceeds of crime. Then there are the fraudsters, who use the knowledge gap amongst participants in the space to extract and defraud users from their assets, due to the need for users to self-custody, i.e. manage the safekeeping of their assets themselves rather than outsourcing that role to a bank or asset manager. This saw, particularly in the early days of the asset class, some large frauds on crypto exchanges and a number of black-market transaction networks found to be using bitcoin for payments between users.

The decentralised nature of the networks – and the lack of any central authority mandating 'Know Your Customer' (KYC) or money laundering checks for source of funds once the initial fiat deposit has been converted into crypto-assets – has placed regulators and governments in an increasingly difficult position as to how they contend with the growing asset class. This is not only from the perspective of identifying proceeds of crime and protecting end users from fraud, but also from the perspective of collecting taxes and ensuring their own currency systems are not eroded and threatened by a parallel currency system.

As stated at the start of this article, like a lot of the key points of debate in crypto, the answer is not black and white on this subject. Whilst there are undoubtedly some criminals using crypto as a means to further their interests or transfer the proceeds of their crime, this is not something that is isolated to crypto, with fiat currencies also being used for the same means prior to the creation of the asset class. Neither is it the case that KYC ensures existing financial systems are immune to money laundering. It's an unfortunate circumstance that criminals are resourceful and will migrate and change their methods as the authorities catch up and it could actually be said that the open and transparent blockchains used by crypto-assets actually make them a convenient, yet poor, candidate for hiding criminal wealth, since any and every transaction put through the network can be tracked and traced.

What we are seeing are different countries and regulators taking different stances on the asset class, with some embracing participation and acceptance as a way to generate economic interest in their country, whilst others are more guarded, putting high barriers to adoption in place, to discourage use. The regulatory space will continue to be very dynamic around crypto-assets, given the relatively new technology and very different problems regulators are having to contend with and, for that reason, it is difficult to cover it in any detail here. It isn't necessarily the case, however, that increased regulation would automatically hinder growth in the space, as some regulation and assurance may actually open up the asset class to wider adoption from institutions and retail users. Suffice to say, extensive research should be carried out before embarking on any transactions in the space, to ensure that the user has an adequate level of awareness around the legalities, regulations and financial implications, e.g. tax, of transacting in the crypto-asset space.

Central bank digital currencies

The natural point to end the article is the emergence and future potential of central bank digital currencies (CBDCs), as the technology underlying the ecosystem becomes more widely understood and the potential applications and benefits of it for financial institutions and central banks become clearer. Currently, central banks are the sole issuers of currency in a country and they use this ability to control the money supply in order to enable them to fulfil their mandates, which can include financial stability, inflation targeting and even employment levels. With the use and circulation of paper money to pay for goods and services reducing year over year and electronic payments, credit and the digital economy growing, it's almost inevitable that we will move to digital currency in almost all developed countries in the near future. The interesting question will be whether this is a decentralised, digital currency established by the free market which becomes widely adopted and used, or whether it is established by the authorities, with centralised control, and then enforced upon the population in place of paper currency. There isn't a clear answer as to how this will play out since there are strong drivers for both routes, so at present it's unclear if they will co-exist or whether one will win out over the other.

On the CBDC side, national central banks and governments, for instance, benefit from 'seigniorage', which is a way for a central bank to earn revenues, without taxation, due to their power to ascribe value to physical currency. As an example, in the US, it costs the Federal Reserve around 11 cents to produce a $20 bill and 14 cents to produce a $100 bill. The difference between physical production costs and the value placed on the note when issued is effectively earned by the Fed. Suffice to say, central banks are likely to be unwilling to give up the benefit of this arrangement to the private sector, seeing them mint a new crypto token, which then becomes more valuable than its production cost when it is issued to the public. This is one factor that lends weight to the idea that the central banks will issue their own token and use regulations to enforce adoption, removing competitors. The full adoption of a CBDC would also be advantageous from a data and tax collection angle, since all transactions would be visible, allowing better insight into economic performance and also much more efficient and effective tax collection, assuming that mechanisms weren't found for the dishonest to circumvent the system. Lastly, a theoretical benefit to central banks, but one which is maybe less attractive for citizens, would be the ability to overcome the 'zero bound' on interest rates in the pursuit of their mandates. Whilst the last few years showed us that the zero bound on interest rates is not necessarily zero, with some economies having negative rates, there is still a floor level that once rates fall below, the existence of paper currency would disincentivise the use of banks and the financial system in favour of the hoarding of the paper currency which isn't easily subjected to the negative rates. In the theoretical case of a full CBDC economy, there is no alternative to the digital token and, as such, interest rates could go as negative as the central bank deemed necessary, whenever they deemed it necessary!

On the idea of a market-based digital currency being adopted, whilst it may at outset seem the authorities would be unlikely to sanction a free market solution as the main digital currency in an economy, it could be said that the fact we have allowed various other asset classes to exist in tandem with the centralised state means as yet alternative forms of co-existence and cooperation could be found, whereby central banks and governments prefer to allow the collective creativity of the free market to solve the scaling and technological issues at hand, but with some of their own inputs, requirements and guard points factored in to ensure they retain control of elements that they deem necessary for preventing crime and protecting their sovereignty.

Summary

The crypto-asset space is already a vast and varied ecosystem which has sparked fierce debate amongst not only financial market participants but also the wider population in general. The extreme returns and falls seen on some assets, the intense speculative fever and an increasingly technically savvy population have all contributed to the increased adoption from consumers, column inches in the media and regulatory scrutiny amongst authorities. Whilst we do not know what the future will hold, the fact that the total market cap in the asset class is currently over $1.5 trillion and growing rapidly means that it will continue to garner attention and generate conversation and, for that reason, some exploration of the space, the technology involved, the tokenomics of the coins, the regulations surrounding the asset class and the future use cases is recommended to ensure that, whatever happens in the future, the adjustment is a more comfortable one for advisers, their clients and the industry as a whole.