# Blockchain bricks and crypto cathedrals

## A breakdown of key terms

Sarah Archer

There is a saying in improv: 'Bring a brick, not a cathedral'.

While improv and the world of cryptocurrency are not readily comparable, the saying is a good reminder that you do not need to 'know it all' to participate in the crypto conversation.

Talk of blockchain and crypto is not new—but the voices are becoming more mainstream and credible. What was once thought of as a dangerous, scam-ridden fad is now being taken on by banks and governments around the world. And, while it may not yet be clear just how blockchain technology will become part of our day-to-day lives, its application and the infrastructure being built to facilitate it will become ubiquitous in the coming years.

While the message seems to be 'get on board'—the problem is that it is complex, and the terminology is inconsistent. This paper provides a breakdown of some of the key terms and concepts—'the bricks'¬—to help you piece together a framework¬—'the cathedral'—to engage in the conversation.

### What is blockchain?

A blockchain is a distributed digital ledger. And what is a ledger? In its most basic form, it is a system of recording information. A blockchain is essentially a digital system that records information, such as data and transaction records, which is added to and verified by the computers participating in that blockchain's network, and which cannot be changed.

There is no one central source and the blockchain transaction history can be accessed and seen by each participating computer. Each time new data is added to the ledger, that is, each time a new 'block' is added to the chain, it is time-stamped and digitally signed, making it transparent and verifiable. This can be thought of as a massive spreadsheet into which many people can input data—as long as they have the access key—in accordance with pre-agreed rules, and with every input requiring acceptance. Once an input is agreed to, it cannot be altered, although new inputs that add to the existing spreadsheet can, of course, be made. So, participants do not need to go through a 'trusted' central source such as a bank—a blockchain does not 'trust', it verifies.

There are public blockchains and private blockchains. Private blockchains allow only limited computers to participate—'VIP only' if you will. The most common public blockchains are Bitcoin and Ethereum, but there are thousands of different blockchains in existence given their widespread applicability. For example, a business

could use a private blockchain to facilitate invoicing, or blockchains could be used to record land titles, shares, medical records or to prepay and track an Uber.

The beauty of a digital decentralised ledger is that it creates a true record of transactions which is extremely difficult, if not impossible, to change. This removes the need for trusted central parties or intermediaries, such as banks.

## What are cryptotokens?

The terms digital assets, virtual assets, cryptotokens and cryptocurrency are all used interchangeably. For the purpose of this paper, these are all referred to as cryptotokens.

You will have heard the names of various cryptotokens bandied about—for example, Bitcoin, Ethereum, Dogecoin, Litecoin and Stellar. But what are they? Is a cryptotoken just like digital money? Is it an investment product? A digital representation of an artwork? Or is it something else entirely?

Although different cryptotokens might fit each of these descriptions, at its core, a cryptotoken is a record on a blockchain which can be found at a unique address. Depending on the blockchain on which it is recorded, the cryptotoken—or the record—might entitle its owner to other things. Why would the blockchain that a cryptotoken is recorded on matter?

Different blockchains have different cryptotokens and coding languages—much like countries have distinct languages and currencies. For example, Bitcoin is the native cryptotoken of the Bitcoin blockchain. Ethereum is a slightly more flexible blockchain, in that it allows cryptotokens that comply with its coding language to include coding within each cryptotoken—like a babushka doll—which in turn enables additional rights and functionality to attach to the record.

## Smart contracts

A 'smart contract' is not actually a contract at all—rather, it is a set of rules coded into a blockchain which self-executes. Remember that different blockchains, including Ethereum, enable a 'record' to be coded in that ledger. Smart contracts are essentially programmed, self-executing promises that can be used in transactions between participants on a blockchain.

## Stablecoins

A stablecoin is a type of cryptotoken with an inbuilt mechanism to keep its value stable. Different stablecoins use different mechanisms to achieve this. For example, some stablecoins attempt to peg their market value to physical assets, such as the US or Australian dollar, or gold, which are held by the issuer of that stablecoin. These types of stablecoin are often referred to as collateralised stablecoins. Other stablecoins seek to maintain their value by building in an algorithm which automatically 'mints' and 'burns' [that is, creates and removes from circulation] coins based on supply and demand.

Stablecoins are popular and play an important role in reducing volatility, however they give rise to a number of legal considerations. Their legal treatment will, among other things, depend on:

- the stablecoin's underlying assets
- whether the stablecoin is redeemable for the underlying assets
- the mechanism for maintaining the stablecoin's price stability
- whether the redemption value is fixed or variable.

Regulators are also wary of representations made in relation to the ability to redeem stablecoins and the credibility of the custodian.

## Non-fungible tokens

Firstly, let us deal with the term 'fungible'. If a thing is fungible, it is interchangeable.

For example, if two people each had a $100 note and decided to swap those notes, neither would mind. The value of one hundred dollars would not change and both could use the swapped notes without any problem. Those $100 notes are therefore fungible.

However, if each used their $100 note to purchase a piece of art from their favourite street artist, the exchange of the newly acquired artworks would not be as straightforward. Each piece of art is unique and is not directly interchangeable—it is therefore non-fungible.

A non-fungible token (NFT) is like a digital version—or more accurately, a record of ownership—of that unique artwork. NFTs have a uniqueness and scarcity value which means that ownership of a particular NFT becomes important. They play an interesting role in the digital landscape and bring traditional concepts like limited editions and intellectual property rights into the blockchain arena.

## Decentralised autonomous organisations

A decentralised autonomous organisation (DAO) is an entity native to blockchain without any central leadership. In essence, it is a collection of participating members—cryptotoken holders—acting in concert in accordance with rules coded into the blockchain. Somewhat like a company constitution, decisions are made, and actions taken in accordance with smart contracts.

In concept, a DAO is similar to a partnership, where thousands of people are coordinating resources and making decisions in accordance with smart contracts. How regulators around the world grapple with DAOs will be interesting—while the concept can be likened to a partnership or an unincorporated association, the question of liability is a tricky one. For example, how can you hold thousands of geographically diverse members accountable for the decision made by the DAO, particularly if only 51 percent of the members voted in favour of the offending decision.

**The quote**

*The beauty of a digital decentralised ledger is that it creates a true record of transactions which is extremely difficult, if not impossible, to change.*

**Sarah Archer**
**Holley Nethercote**

Sarah is a senior associate and works across the commercial and financial services practice areas. Her clients range from tech start-ups in the crypto space to large corporations in the financial services industry. Sarah predominantly advises on financial services law, anti-money laundering obligations and general commercial law, including employment.

## What is DeFi?

DeFi—or decentralised finance—is fundamentally the digital version of traditional banking and financial services, using blockchain for basic banking functions such as lending cryptotokens, accepting deposits and paying interest on cryptotokens.

'Staking' is a term frequently used in the world of DeFi and is similar to depositing money (cryptotokens) with the bank in order to earn interest. However, rather than there being the one central bank, there is a distributed set of computers following the rules coded into the relevant blockchain. The DeFi industry is already a USD 80 billion market and is growing rapidly.

## How is all of this regulated in Australia?

At present, activity relating to blockchain and cryptotokens is not thoroughly or consistently regulated. As with most new innovations, it is regulated insofar as it fits into existing regulatory frameworks including the Anti-money laundering-counter terrorism financing (AML/CTF), financial services and consumer protection regimes.

### AML/CTF obligations

Digital currency exchanges are required to comply with the Anti-money laundering regime. This means that an exchange needs to 'identify and verify' a customer's identity and assess the risk of the customer using the exchange to launder money or finance terrorism, before it provides its services to that customer. Exchanges also need to monitor customers' ongoing transactions for any 'red flags'.

### Financial services regime

The current financial services regime will apply to cryptotokens and accompanying services—including, for example, initial coin offerings—if they involve a financial service. Ordinarily, this will depend on whether or not the cryptotoken is deemed to be a financial product.

There is no single test as to when a cryptotoken is a financial product. Cryptotokens can generally be separated into two broad categories, as follows:

#### *Classic cryptocurrencies*

Classic cryptocurrencies are not financial products. These cryptocurrencies derive their value solely from supply and demand, and do not carry rights to any other thing. Bitcoin and Ether [the native cryptocurrency of Ethereum network] are both examples of classic cryptocurrencies.

#### *Other cryptotokens*

Other cryptotokens may be financial products. Other cryptotokens have an underlying or intrinsic value or right attaching to them. They may represent an entitlement to other assets or instruments, or carry rights to other things—for example, to shares in a company, a pool of assets, loyalty points or to a standing promise to exchange the cryptotokens for money. Other cryptotokens need to be considered in accordance with the definition of a financial product in the *Corporations Act 2001* (Corporations Act).

If a cryptotoken is a financial product under the Corporations Act, there is a range of licensing, disclosure and registration obligations that will apply to anyone who is issuing, selling, promoting, advising on or otherwise dealing in them.

### Consumer protection regime

The consumer protection laws that apply to all businesses under the *Competition and Consumer Act 2010*, which includes the Australian Consumer Law, also apply to cryptocurrency businesses. This includes the prohibition against misleading and deceptive conduct and false representations.

## What is next for regulation?

There is a race between a number of countries to attract blockchain and crypto businesses, which includes establishing regulation that is fit for purpose and strikes the right balance between encouraging innovation, providing certainty for investors and protecting consumers.

For Australia's part, there was a Senate Select Committee on Australia as a Technology and Financial Centre last year, which looked into how Australia should regulate cryptotokens and other uses of blockchain technology. As a result of this enquiry, the federal government has said it plans to consult on and implement a licensing framework for digital currency exchanges, and a custody or depository regime for businesses that hold crypto assets, by the end of 2022. Of course, this could all change with a change of government.

If it feels like this paper has been written in a foreign language, do not despair. The new terminology and concepts will become familiar over time as the blockchain revolution changes the way we do things, and the digital world becomes regulated and continues to permeate the everyday. Does anybody remember cash? **FS**