Decrypting the Jargon

Crypto Basics

Aaron & Partners
Solicitors

Introduction

Aaron & Partners
Solicitors

Cryptoassets, cryptocurrencies, blockchain, exchange tokens, NFTs, mining…. a virtual minefield.

The changing landscape of financial services and digital businesses brings with it the inevitable regulatory and legal challenges, obscured further by a lexicon that would not look out of place on the sci-fi shelves of a bookshop (or its app).

The starting point - cryptocurrencies are a digital payment mechanism. In an increasingly cashless world, it can be difficult to see how that differs from tapping a credit or debit card, or sending money on a banking app. However, there are some fundamental differences. Let's keep it simple, or at least try.

Quick Reference EasyGlossary

Aaron & Partners
Solicitors

The language of cryptoassets can be off-putting, so here are the key terms required to understand the concepts.

Cryptoasset
An umbrella term, which includes cryptocurrency (which is only one type of cryptoasset).

Cryptocurrency
Digital payment mechanisms, such as Bitcoin and Ethereum, also referred to as exchange tokens. For ease, bitcoin is used interchangeably with cryptocurrency.

DLT (Distributed Laser Technology)
A way of distributing data across a network, such as a record of ownership.

Blockchain
An example of a DLT – blockchain is a specific way of structuring data on a DLT platform, in a tamper-proof manner. Again, for ease, blockchain is used interchangeably with DLT.

Mining
This is how bitcoin is created. Computing power across a network is used to 'create' bitcoins, for example.

Wallet
Where bitcoin is stored. Think of a 'cold wallet' as similar to a USB, and a 'hot wallet' as a cloud-based bitcoin moneybox.

Private Key
The bitcoin equivalent of a PIN. This unlocks the wallet to enable a transfer. This is kept secret.

Public Key
This is akin to the recipient's bank account number. This can be freely published, as it can only be used to receive payment.

Node
A single part of a network, e.g., one connected computer.

Fiat
Just another name for any traditional currency, such as the pound, dollar, etc.

Airdrop
Unilateral distribution of cryptoassets to (usually multiple) recipients, principally for marketing or to increase usage.

DeFi
Decentralised finance – another umbrella term.

Key Characteristics of a Cryptocurrency Transaction

Aaron & Partners
Solicitors

A bitcoin transfer can be compared to a digital cash payment. The bitcoins (or fractions of a bitcoin) are sent by the holder to the recipient directly. The easiest way to conceptualise this is to think of a safety deposit box. The payor unlocks their box with the private key and enters the recipient's public key to enable the transfer. There is no intermediary bank – it goes directly to the recipient. Both parties are anonymised. The only identifying factor is the anonymous public key.

Details of the transaction are recorded on the blockchain. A block of data is added to a chain of ledger entries, tracing back to the original creation, or mining, of that particular bitcoin. The blockchain is an open ledger, so in theory everyone can trace the origin of bitcoin to where it is held today. This makes 'double spending' very difficult. The use of a network also makes it secure, in that to hack or manipulate the network, every node must be compromised, and blockchain is highly encrypted and records the data permanently.

When a normal debit card payment is made, it initiates a series of transactions. The net result is that the payor's bank owes less to the payor, and the recipient's bank owes more to the recipient. By contrast, a bitcoin transaction is a direct transfer of the bitcoin. In many ways, bitcoin works like people generally imagine debit cards to work, where the money just travels from one virtual safe to another.

> A bitcoin transfer can be compared to a digital cash payment.

What's the Attraction?

Aaron & Partners
Solicitors

Decentralisation, security, anonymisation are the often-cited attractions, even though the anonymous aspect is almost at odds with the traceability of bitcoin back to its original creation (which can be used to trace criminal proceeds).

The decentralisation (or DeFi) is the most romanticised reason for the existence of cryptocurrency, at least by IT enthusiasts. The inventor of bitcoin, Satoshi Nakamoto (a mysterious figure, whose very existence is disputed) is often quoted as having created it to 'take back financial control from the elites', in the aftermath of the banking crisis in 2008.

Bitcoin is most famous for its superlative 'exchange rate' – as of March 2023, one bitcoin is worth c. £22,000, and has been as high as £48,000. As such, it has been bought and sold by speculators more than it has been used as an exchange token. The value is in its scarcity – the algorithm limits the amount of bitcoin that can ever be mined to 21 million. In that way, it cannot be affected by inflation in the same way that the value of fiat is affected by quantitative easing (printing more money). That is not to say its value is not volatile, as has recently been demonstrated.

"Whilst cryptocurrency remains unregulated, cryptoassets do fall within existing and proposed regulatory frameworks. It helps to first consider how each type of cryptoasset is categorised before considering the applicable regulatory regime."

Classification and Regulation

Aaron & Partners
Solicitors

The UK Government formed a Cryptoassets Taskforce consisting of the Bank of England, the Financial Conduct Authority, and HM Treasury. The Taskforce produced a report in October 2018 for the classification of cryptoassets. In February 2023, HM Treasury published a Consultation and Call for Evidence. It is likely that the Financial Services and Markets Bill will introduce a phased approach to further regulation.

As to the present state of play in terms of regulation as at April 2023, the main categories are:

Exchange Tokens (Cryptocurrencies)	Security Tokens	Utility Tokens
The present position is that cryptocurrencies are not regulated and are not recognised as money or e-money, primarily as they do not meet the core criteria of money and are not backed by a central government. As such, they are not seen as of themselves a store of value. Their value is subjective and volatile, and almost comparable, in investment terms, to trading in antiques.	These are akin to shares, in that they confer specified ownership rights and obligations, and as such are regulated by the Financial Services and Markets Act 2000 and the regulatory regime, which it enables, including the Regulated Activities Order, meeting the criteria of a specified investment.	These can be thought of as similar to vouchers for services and can be used in crowdfunding. They are also unregulated. However, in certain circumstances, these could meet the definition of e-money.

In contrast to cryptocurrencies, e-money is regulated because it is a store of value represented by a centrally-backed currency (e.g. a top-up debit card). The Electronic Money Regulations 2011 and the Payment Services Regulations 2017 apply.

Consumers in particular need to beware. The fact that cryptocurrency is unregulated means that those who lose money will not benefit from the compensation regime.

A simplified starting point is deciding whether the asset creates a right of ownership (security token), or whether it is pegged to a fiat currency. Any system which creates a new unit of value, like bitcoin and others, is likely to be an unregulated exchange token.

Promotions and Other Regulated Activities

Aaron & Partners
Solicitors

It is important to carefully consider the provisions of the FSMA relating to promotions separately, and how the rules that apply, depend on the type of cryptoasset and whether it falls within the regime.

Similarly, the use of unregulated cryptoassets as payment for regulated services will not escape regulation. In short, there is no standalone comprehensive regime for cryptoassets at present. Advising on the regulatory impact on any dealings involving cryptoassets will require a very clear understanding of the cryptoasset itself and the prevailing FCA or taskforce guidance at the time on its classification. The upshot is that it is the nature of the cryptoasset itself that determines how it is treated under the existing framework.

Although not explored in detail here, regulated financial services firms need to note the requirements with which they are still required to comply, when carrying out unregulated activities (e.g. Principles for Business Rules). The FCA published Guidance (Policy Statement PS19/22) in July 2019. The detailed regulatory requirements for market participants in relation to any type of cryptoasset are complex and detailed consideration is required.

It is worth noting that, whilst cryptocurrency is lawful despite being unregulated, there is presently an outright ban on the sale, marketing, and distribution to retail customers of certain financial products (e.g. derivatives) which reference unregulated cryptoassets.

> **The advent of the Financial Services and Markets Bill 2022-2023 is likely to usher in a raft of new measures and regulations applicable to the crypto sphere.**

Britcoin and Stablecoin

Aaron & Partners
Solicitors

Central Bank Digital Currency (CBDC) is where cryptocurrency is issued by the central bank of a state. The Bank of England is exploring the launch of 'Britcoin' (which would follow other examples including Chinese 'Rembini' and the 'Sand Dollar' in the Bahamas, both already in circulation, to differing degrees). A distinguishing feature is co-existence with existing currencies, rather than as alternatives (indeed, in China, cryptocurrency is banned).

Stablecoin is a term given to a cryptocurrency backed by or pegged to the value of another asset or fiat currency, and as such may fall within the category of e-money, or (depending on the underlying asset), a security token. HM Treasury will likely develop the outline of a separate regulatory regime for stablecoins.

Non-Fungible Tokens (NFTs)

Something fungible, like a physical coin, can just be replaced for another. An original Picasso is non-fungible. NFTs are the digital equivalent, and are cryptoassets in a similar way. Within this category are event tickets and digital artworks, for example.

Initial Coin Offerings (ICO)

ICOs are the equivalent of IPOs (initial public offerings, e.g. shares when a company is first listed). These can be used to promote the launch of a new cryptocurrency, or as a means of attracting crowdfunding or initial investment.

Data Protection

Aaron & Partners
Solicitors

The distribution of even anonymised data in blockchain or any other DLT is a real challenge. Consent is a factor, but so is the right of erasure, and also that data is transferred outside the EEA. DLT is not exempt from the GDPR and the Data Protection Act, and any introduced right of erasure will damage the integrity of the permanence of the ledger.

Anti-Money Laundering

From the perspective of law firms, cryptocurrency poses a real challenge in terms of AML compliance. There is no specific Law Society Guidance.

The Law Society's response to a question in August 2022 seems to have been misunderstood by the press. In response to being asked whether a solicitor could act for a client purchasing a £795,000 property in bitcoin, as a 'cash' transaction, the response was that Enhanced Due Diligence (EDD) was required. It was then reported that the Law Society had suggested that cryptocurrency should be treated as cash.

Whilst that may or may not have been the intended response, it is more likely that the response has been misinterpreted to a degree, because the need for EDD is also triggered by 'cash' transactions (i.e. purchases without a mortgage), regardless of the actual method of payment.

Nevertheless, it seems that EDD should be applied where there is a crypto element somewhere in the mix. It is prudent to consider not just the source of the cryptocurrency 'funds' themselves, but also the source of wealth with which it was acquired.

It is of course more likely that the proceeds of bitcoin sales will be the issue, rather than cryptocurrency itself, especially in the short term, as law firms are ill-equipped to actually receive cryptocurrency directly. It remains to be seen whether the Law Society will release any specific guidance as to how to deal with these issues, especially given that the trading platforms themselves, from which the proceeds are likely to pass before being used in any fiat transactions, are obliged to comply with the prevailing AML regimes.

Taxation

Aaron & Partners
Solicitors

HMRC has published its internal Cryptoassets Manual. The rules relating to taxation are no less complicated than the rules applicable to other trading and assets. The manual covers taxation of individual and business owners, with consideration for the position relating to corporation tax and income tax, right through the spectrum including VAT, stamp duty and inheritance tax. The position can be summarised in their own words:

> **The tax treatment of all types of tokens is dependent on the nature and use of the token and not the definition of the token. HMRC does not consider cryptoassets to be currency or money. This reflects the position previously set out in the Cryptoasset Taskforce report. On its own, owning and using cryptoassets is not illegal in the UK and does not imply tax evasion or any other illegal activities.**

Other Uses of DLT

DLT and blockchain can be used for anything which requires automation or the recording of rights. It can be used to effect and record transactions in a manner that has self-validating integrity and security, with permanence. Its uses could extend to land registries, voting, and smart contracts (see below).

It is important not to lose sight of the challenges in terms of data protection and the need for universal computer literacy, as well as the ever-increasing need for processing power and its environmental impact, given the need for huge amounts of energy for the requisite computing capability.

There are considerations for how technological evolution is factored into the equation. It may well be the case that blockchain itself may one day become obsolete with the advent of quantum computing. Nevertheless, blockchain is the presently disruptive technology and its reach is extending well beyond money transfer.

Smart Contracts

Aaron & Partners
Solicitors

Smart Contracts are not a separate type of contract, nor are they outside the scope of English contract law as it presently stands. In fact, they are not contracts; they refer to the method of performance. It is a use of, for example, blockchain technology to automate an outcome, or a string of outcomes, if a certain condition is met. This enables potentially rapid performance of contractual obligations, even internationally, in accordance with the program which is written and stored on a blockchain.

> **In short, the program is essentially written so that, for example, "if A does X, then B gets Y".**

Simple enough, in theory. Consider however the length and depth of a traditional set of contractual terms and conditions, and the fact that the program needs to deal with each one. It is not always easy to allow for subjectivity, such as impossibility, force majeure, or even reasonableness. However, 'oracles' (sources of external information) can be used to determine certain conditions (e.g. stock performance, weather conditions, consumer engagement) which may be in-built conditions precedent to performance, for example.

Legal Status of Cryptoassets

Aaron & Partners
Solicitors

The UK Jurisdiction Taskforce (chaired by Sir Geoffry Vos) published its Legal Statement on Cryptoassets and Smart Contracts in November 2019. IP rights in the underlying technology itself are of course a separate matter and present a familiar problem by way of a very simplified summary of the statement:

- A cryptoasset, despite its intangibility and not being a 'chose in possession' or a 'chose in action', is still property (it should be noted that the Law Commission is considering the introduction of a third category: 'digital objects'). The result of that is that:
  - They can be the subject of theft, succession, trusts, assets in personal and corporate insolvency.
  - Certain types of security can be granted over them.
  - However, although they are property, they cannot be possessed, so they cannot be the subject of bailment, for example, and not all types of security can be granted over them.
- Private keys are not property, because they are information.
- Smart Contracts are enforceable and, where required, in principle satisfy the requirement of being 'in writing', though that depends on the type of code. There is already provision in the existing English law of contract to deal with anonymised or pseudonymised parties.

The case law on cryptocurrency has reflected this approach:

- In *AA* v *Persons Unknown*, it was accepted that bitcoin was property in the context of a proprietary injunction.
- In the matter of *Torque Group Holdings Limited* (In Liquidation), cryptocurrency was considered as an asset in the liquidation.
- In *Lavinia Deborah Osbourne* v (1) *Persons Unknown* and (2) *Ozone Networks Inc t/a Opensea [2022],* a hot wallet was hacked into and an NFT was stolen, and was considered to be property capable of being the subject matter of theft.
- In *Ion Science Limited* v *Persons Unknown*, the High Court decided, in the absence of precedent, that the lex situs relating to cryptocurrency (i.e. the applicable law), is the law of the place where the owner is domiciled.

Legal Status of Cryptoassets (cont'd)

Aaron & Partners
Solicitors

It has also been accepted by the Courts in principle that cryptocurrency can be the subject matter of a trust (in concordance with the Taskforce) and it is possible that it can be used as security for costs, although the volatility of bitcoin has so far precluded it (Tulip Trading v Bitcoin).

This is by no means a summary of all the case law concerning cryptoassets, but it can be seen that it is becoming more prevalent and the legal profession will need to become comfortable with dealing with the novel issues that continually arise.

To that extent, let's conclude with a cautionary point as a sign of the times.
In *D'Aloia* v *Binance Holdings and Others [2022]*, the Court held that a Court Order could be served as an NFT by airdrop into a public wallet via the DLT.
Please refer to the glossary to de-crypt that jargon.

Aaron & Partners
Solicitors

AaronsLegal

Aaron & Partners LLP

aaronandpartners.com

Chester: 01244 263051
Shrewsbury: 01743 838067
Greater Manchester: 0333 241 6886
Wirral: 0333 241 6886