Blockchain and cryptocurrency for barristers

By Emma Beechey

Litigation relating to blockchains, cryptocurrencies and 'ICOs' is inevitable. It is therefore worth knowing at least a little about them and how they work. This article aims to provide the briefest of introductions to this fascinating world.

Blockchain

A blockchain is a trustless, decentralised ledger. 'Ledger' as in a bookkeeping document in which one records credits and debits against each account within that ledger. 'Decentralised' in that copies of exactly the same ledger are stored on thousands of computers around the world. 'Trustless' in that one does not have to trust a centralised controller, such as a bank, to put correct entries onto the ledger. Rather, a network of computers work together following a set of fixed rules to process transactions. In this way, thousands of people can agree on who owns the assets recorded in the ledger and they can trade those assets with one another without having to go through an intermediary such as a bank.

Bitcoin and other cryptocurrencies

The original blockchain was bitcoin, which the inventor(s) (pseudonymously named Satoshi Nakamoto and anonymous to this day) called a peer-to-peer electronic cash system.[1] 'Peer-to-peer' meaning that, like cash, one person can pay another person without having to make the payment through an intermediary. Unlike cash, bitcoin and other cryptocurrencies are native electronic currencies. They are intangible. Each exists only on its own blockchain. Unlike cash, cryptocurrencies are not issued by a state. Like the currencies issued by modern states (fiat currencies), bitcoin and other cryptocurrencies are not backed by gold or anything else. Like fiat currencies, their value is based on a collective belief that they have value.

Cryptocurrencies use a system of cryptography called public key cryptography, which allows a person to publicise their public key (called an 'address' in relation to blockchains) so that people can send cryptocurrency to that address, while keeping completely private their private key. Only the person who knows the private key is able to withdraw cryptocurrency from the address. Owning bitcoin simply means that you have the private key to the address. To transact with bitcoin, a person signs a transaction request cryptographically using his or her private key, then broadcasts that transaction to the network. It is stored in the network as an unconfirmed transaction until it is placed into a block on the blockchain and the transaction is thereby executed.

Other cryptocurrencies include either (the native currency of the Ethereum network), XRP (the native currency of the Ripple network), litecoin, monero, zcash and tether (pegged to the valued of the US dollar).

"I'll give you a HUGE bonus in bitcoins if you can explain to me what the hell they are."

Legally speaking, what is cryptocurrency?

As with any asset, cryptocurrencies can have different characterisations for different legal purposes.

In Australia, cryptocurrencies are treated as money for the purposes of GST.[2] However, for income tax purposes, as with foreign currencies, cryptocurrencies are CGT assets that can trigger a CGT event on sale. [3]

ASIC does not consider cryptocurrencies to be financial products.[4] It appears that the US Securities and Exchange Commission agrees, at least so far as bitcoin and ether are concerned.[5]

The European Court of Justice has held that bitcoin is a currency and therefore its supply is exempt from the imposition of value added tax (VAT) in the European Union.[6] However, the United States Internal Revenue Service considers bitcoin and other cryptocurrencies to be commodities.[7]

In some US criminal cases, bitcoins have been treated as currency. For example, as the money in a money laundering conspiracy [8] or as the money transferred in an illegal money transferring business. [9]

ICOs and tokens

An ICO is an initial coin offering, a play on the concept of an IPO (initial public offering). The 2017 ICO craze has now died down but it has not died out entirely.

In an ICO, someone wishing to raise money – hopefully for a bona fide business venture – offers 'tokens' to investors who contribute money either in fiat currency or more commonly in bitcoin or ether. The tokens are said to have various rights attaching to them. For example, a right to a percentage of the profits of the business venture or a right to use the tokens to transact on a future digital platform to be created as part of the business venture. These offers are made to the world at large in a 'whitepaper' attached to the ICO and in other public statements by the offerors. Those buying the tokens probably believe that they have entered into a contract with the

Photo by Andre Francois on Unsplash

offerors and are entitled to the rights offered in connection with the tokens. However, the offerors are usually a loose and sometimes pseudonymous collection of people and the offered rights are both so vaguely described as to be incapable of enforcement and completely dependent on the commencement and success

"It's not fair. I get 10 years for counterfeiting and people make fortunes with cryptocurrency!"

of the business venture.

Regulators in many countries have been grappling with ICOs, in particular whether or not tokens meet the definition of a security in the US or a financial product or managed investment scheme in Australia.[10] The answer will be different for each different type of ICO.

The distinctive benefits of blockchains and cryptocurrencies

Decentralised and censorship-resistant

Bitcoin is decentralised. There is no authority that can be ordered to shut down the network, to modify transactions or to refuse certain types of transactions or transactors. Its decentralisation also makes it censorship-resistant. Other blockchains achieve decentralisation and censorship-resistance to lesser degrees. Some, such as private corporate blockchains, do not aim for censorship-resistance and are decentralised only to the extent required to prevent there being a single point of failure which can be targeted by attackers.

Permanent and immutable

A blockchain is a permanent and immutable record of past transactions. For bitcoin and many other cryptocurrencies, the records are made permanent and immutable by a system called 'proof of work'. In a proof of work system computers compete to find a large number that meets certain specific criteria (mining). Finding the number takes a significant amount of computing power and hence a significant amount of electricity. It is therefore costly. The reward for the successful computer is known as the block reward, currently 12.5 bitcoins per block. The successful miner broadcasts the new block which contains transactions from the unconfirmed transaction pool. Those transactions become confirmed transactions and all miners move on to trying to find the next block. An additional feature which makes all blockchains difficult to retrospectively alter is that all blocks on a blockchain are cryptographically linked together. Any attempt to change one block would require changing all subsequent blocks to be effective. It is not literally impossible to modify a secure blockchain such as bitcoin. Rather, it is so costly and computationally impractical that it is impossible in practice.

Complete history

A blockchain contains a complete history of all transactions ever undertaken in the cryptocurrency which is native to that blockchain.[11]

Digital

Because cryptocurrencies are native to the digital world, they can be transferred rapidly through digital communications systems such as the internet. Because they are both digital and peer-to-peer, they can be sent across national borders as easily as they can be sent to a person in the next room.

Pseudonymous (not anonymous)

There is a common misconception that cryptocurrency transactions are anonymous. They are not.[12] Rather, they are pseudonymous. A name is not required to transaction with cryptocurrency, but a cryptocurrency address is required. Anyone looking at the blockchain can see the amount and source of any cryptocurrency arriving at an address or departing from that address. Telling people one's cryptocurrency address – a necessary step in receiving payments – also allows those people to see all past and future transactions from that address. A person may have many cryptocurrency addresses on one blockchain but a careful analysis of the blockchain will be able to link together many such addresses. A US company called Chainalysis specialises in providing this sort of de-anonymising service for the bitcoin blockchain to governments and corporations.

Exchanges

If a person wants to convert cryptocurrency into fiat currency (rather than spending the cryptocurrency directly), that person will either need to trade their cryptocurrency for cash, or they will need to use the services of at least one intermediary: a cryptocurrency exchange or a bank, or both.

A bitcoin exchange is an online marketplace where buyers and sellers of bitcoin can trade with each other via an orderbook managed by the exchange. To use an exchange, a user creates an account with the exchange. The user then deposits either traditional currency or bitcoin. Traditional currencies are deposited by way of a bank transfer to the exchange's bank account. Bitcoin is deposited by sending bitcoin to a bitcoin address nominated by the exchange. The relevant amount is then credited to the user's account. The user can then sell the bitcoin for traditional currency, or vice versa. Having bought or sold, the user can then withdraw the proceeds from their exchange account to their preferred destination by way of a bank transfer or bitcoin transfer.

Almost all exchanges now require users to prove their identity when signing up for an account, in order to comply with anti-money laundering requirements imposed on the exchanges by most countries. This makes

exchanges an excellent target for preliminary discovery or subpoenas.

Other applications of blockchain technology

'Smart contracts'

The Ethereum blockchain markets itself as being able to perform smart contracts. Cryptocurrency lawyers are fond of saying that 'smart contracts' are neither smart, nor are they contracts. A smart contract is a computer program which instructs a blockchain to make a certain transaction if certain criteria are met, for example at a certain time, or if a certain number of digital signatures have been provided (used to operate a multi-signature cryptocurrency wallets), or if a certain authority has provided a certain input (used to execute escrow transactions or bets). ICO tokens are almost all issued as smart contracts on the Ethereum blockchain.

Timestamping

A much more interesting application of blockchain for barristers is its ability to provide evidence of the time before which a certain event must have occurred. Each block on a blockchain is added one-by-one over time. Each block has a time stamp. In its simplest form, timestamping exists for every cryptocurrency transaction. There is an immutable record that a certain transaction occurred at a certain time. In its more advanced form, any data (e.g. a contract, a novel, a digitised picture) can be converted into a cryptographic hash of that data. Then, the cryptographic hash can be recorded on a blockchain. There are various commercial operators providing this service and almost all of them use the free and open source OpenTimestamps protocol which has been timestamping data to the bitcoin blockchain since 2012.[13]

Asset ledgers

Blockchain is also being used to create immutable, tamper-resistant ledgers of the provenance of certain high value goods, such as diamonds.[14] The success of such initiatives depends on two critical factors: whether the initial data inputs onto the blockchain can truly be trusted and the level of security of the chosen blockchain.

Other implementations

Blockchains are also being used or developed for many different implementations, some of which may be successful, others of which may prove to be too costly, too inefficient or too easily de-anonymised to be useful. Examples include online voting systems,[15] shipping supply chain ledgers,[16] patient health records,[17] medical data for researchers,[18] digital identity systems and an 'Australian National Blockchain' being developed by Herbert Smith Freehills, CSIRO and IBM for management of commercial contracts.[19]

"This is Pete, our cryptocurrency expert."

ENDNOTE

1 Satoshi Nakamoto (2008), Bitcoin: A Peer-to-Peer Electronic Cash System (Bitcoin whitepaper), available at https://bitcoin.org/bitcoin.pdf.

2 Budget 2017 Fact Sheet: Backing innovation and FinTech: Australia as the innovation and FinTech nation, available at https://www.budget.gov.au/2017-18/content/glossies/factsheets/html/FS_innovation.htm.

3 Australian Tax Office guideline, Tax treatment of crypto-currencies in Australia - specifically bitcoin, 29 June 2018, available at https://www.ato.gov.au/General/Gen/Tax-treatment-of-crypto-currencies-in-Australia---specifically-bitcoin/.

4 Australian Securities and Investments Commission, Submission to the Senate inquiry into digital currency, December 2014.

5 William Hinman (SEC Director, Division of Corporation Finance), Digital Asset Transactions: When Howey Met Gary (Plastic), speech delivered at the Yahoo Finance All Markets Summit: Crypto (14 June 2018), available at https://www.sec.gov/news/speech/speech-hinman-061418.

6 *Skatteverket v David Hedqvist Case* C-264/14.

7 Inland Revenue Service, Notice 2014-21, available at https://irs.gov/pub/irs-drop/n-14-21.pdf.

8 United States v Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014). Australia has its own Silk Road inspired case (R v Collopy; R v Cooley [2017] SASCFC 64) but the character of the bitcoins received as payment was not in issue as the charges were trafficking, possession and supply of controlled substances.

9 *United States v Murgio*, 209 F. Supp. 3d 698 (S.D.N.Y. 2016).

10 ASIC Information Sheet 225: Initial coin offerings and crypto-assets, published March 2017, updated March 2018. In March 2018, the ACCC delegated its powers to ASIC to enable ASIC to take action under the Australian Consumer Law in relation to crypto-assets.

11 There is one exception: where a person hands over a private key to another person, thereby transferring ownership of the cryptocurrency which is accessible by using that private key. This is the cryptocurrency equivalent of a cash transaction.

12 Except on privacy coin blockchains such as monero and zcash.

13 See https://opentimestamps.org/. This project, created by well-known bitcoin contributor Peter Todd, is in my opinion one of the best examples of a free, non-profit public service built on the bitcoin blockchain.

14 For example, the Everledger project, which operates on the Ethereum blockchain, see https://www.everledger.io/.

15 West Virginia will apparently use blockchain for online voting by military personnel servicing overseas in the 2018 mid-term elections: Mike Orcutt, 'Why security experts hate that 'blockchain voting' will be used in the midterm elections', *MIT Technology Review,* 9 August 2018, available at https://www.technologyreview.com/s/611850/why-security-experts-hate-that-blockchain-voting-will-be-used-in-the-midterm-elections/. Various other groups, including Horizon State (https://horizonstate.com/) are also trialling blockchain voting platforms.

16 https://www.prnewswire.com/news-releases/maersk-and-ibm-introduce-tradelens-blockchain-shipping-solution-300694642.html.

17 Adam Green, 'Blockchain offers cure for patients' fragmented medical records', *Financial Times,* 6 June 2018, available at https://www.ft.com/content/6f138722-47d4-11e8-8c77-ff51caedcde6.

18 Asha Mclean, 'Australian Department of Health using blockchain for medical research records', ZDNet, 20 May 2018, available at https://www.zdnet.com/article/australian-department-of-health-using-blockchain-for-medical-research-records/.

19 https://www.australiannationalblockchain.com/.