

Interleges 2019 Annual General Meeting**Blockchain: commercial use cases and the regulatory regime for cryptoassets
(10:40 on 7 June 2019 at Hotel Minareto, Siracusa, Sicily)**

In April – May 2019 I spent four weeks on secondment at Anderson Kill, a fellow Interleges member firm, at their head office in New York. During my time at the firm I worked with their Blockchain and Virtual Currency sector group and in particular alongside Stephen Palley, a renowned thought leader in the crypto industry.

My fireside chat with Stephen was published in the leading crypto news source The Block (see below for more details) and I spoke at the Blockchain Summit as part of Philadelphia Tech Week on cryptoassets, and why increasing engagement from regulators is a sign of a maturing market, and is not inherently something to fear.

Following the secondment I presented my findings at the Interleges Annual General Meeting in Sicily in June 2019. Detailed notes to support my presentation are below, which reflect the position as at 7 June 2019 and all hyperlinks were checked and were active as at 16 August 2019.

1. Blockchain – what is it?

The notion that there is only one blockchain is a myth, and I treat the use of 'the blockchain' with a healthy dose of scepticism. It is better to talk about blockchains (plural) or to refer to a specific blockchain (e.g. the Bitcoin blockchain or the Corda blockchain). Alternatively in the business world 'distributed ledger technology' (DLT) is readily understood and avoids any stigma or negative connotations associated with the word 'blockchain' which needs to be separated from blockchain technology more widely.

At present there are no agreed universal definitions for the key concepts and terminology. The ecosystem would benefit from global standards, and in particular established definitions for 'DLT', 'blockchain', 'cryptocurrency' and 'digital assets'. I spoke with numerous technical experts while on secondment in New York earlier this year and found you get a slightly different answer from each of them. It also has become clear that, as an inherently complex and novel technology, it is difficult to distil and simplify the terms into language that is readily understood by the public.

The simplest notion I have come across is to consider a 'blockchain' as an ***append-only distributed ledger / database***.

Append-only is used interchangeably with immutability. Generally speaking, once a record (otherwise known as a transaction) has been added (or appended) to a blockchain it cannot be amended or removed later down the line. This includes records that are added in error. The immutability of blockchains, including the fact that all records are time stamped, is one of the key benefits of the technology. Ultimately the development of blockchains has been based on a desire to build electronic systems to generate digital trust and reduce the reliance and costs (both financial and time) associated with the use of intermediaries.

Edward Chapman

Distributed means that the data does not reside on one central server. Rather, the blockchain is shared between all users (nodes) that are connected to the internet. On verification of a transaction, records are added to the blockchain and each user's 'copy' is updated. The frequency of the updates depends on the underlying protocols / rules for the specific blockchain. For example, the Bitcoin blockchain is designed to confirm a transaction in an average of 10 minutes, and in June 2019 the average confirmation time was 9.47 minutes¹.

In theory a distributed decentralised network can improve security as there is no one focal point of attack (as there is with conventional centralised servers). However it is also introduces new risks, including the '51% attack', whereby a party or group of parties acting in concert with a majority of the nodes and processing power can revise transaction history on a blockchain i.e. change the history and prevent new transactions from being added².

There is no magic around a 'database / ledger', this is simply the use of existing technology to record a particular state of affairs and transfers of ownership.

Blockchains are secured through the use of cryptography, which has led to the term 'cryptocurrency'. A process known as hashing creates a unique identifier, much like a QR code or a barcode. It converts any piece of data into a unique string of text, typically with the same length. This is combined with public / private key cryptography, which operates in a comparable way to online banking and email. A public key is visible to anyone you wish to share it with, like a bank account number or an email address. The private key is like the passcode for online banking or the password for an email account. As such the private key must never be shared, as this is where the value is held³.

2. Public / private blockchains (permissionless / permissioned)

Blockchains can be split into public (permissionless) and private (permissioned).

The most prevalent blockchains (Bitcoin and Ethereum) are permissionless, which means that there is no one owner. Anyone with an internet connection can participate, including viewing and adding records, and all participants are aware of all transactions. The information is generally pseudonymous thanks to the cryptography referred to above. Core themes are trust (or rather a lack of trust) and transparency.

Following on from the expansion of permissionless blockchains, numerous private permissioned blockchains have emerged. These have also been termed 'enterprise blockchains', and offer organisations the ability to dip their toes into the world of blockchain without losing control of their data. Permissioned blockchains have enforced rules, role based access and privileges. They can be compared to an extranet or data room, like those used in mergers and acquisitions. Participants can only see information that is relevant to them. Core

¹ <https://www.statista.com/statistics/793539/Bitcoin-transaction-confirmation-time/>

² <https://Bitcoin.org/en/glossary/51-percent-attack> and <https://www.investopedia.com/terms/1/51-attack.asp>

³ For more information, see https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.13/gtps7/s7pkey.html

Edward Chapman

themes include privacy, efficiency and interoperability. The most prominent permissioned blockchains are Corda⁴, Hyperledger⁵ and Quorum⁶.

Using the terms public and private can cause confusion, which is why I prefer using permissionless and permissioned instead. From a technical perspective public = not within a firewall and private = within a firewall. This means that it is possible to have a permissionless private blockchain. As such it is better to focus on permissions and the visibility participants have, rather than using the terms public and private.

Ultimately, permissionless blockchains are used by participants who don't know and don't trust each other. Permissioned blockchains are for participants who know each other, but still don't trust each other.

3. Bitcoin

Bitcoin is intrinsically linked to blockchains and DLT as it is the initial and most prominent use of the technology to date. The Bitcoin blockchain was proposed as a peer to peer payment solution by a pseudonymous individual or group of individuals known as Satoshi Nakamoto in October 2008⁷. The Bitcoin network started on 3 January 2009, and the timing of this during the global financial crisis was no accident. Indeed, in the first block the headline '*Chancellor on brink of second bailout for banks*' is featured, which was taken from an article published in UK newspaper The Times on the same date.⁸

The simplest definition of Bitcoin is **peer to peer electronic money that can only be used once**. It solves the double spend problem and allows transactions to take place in trustless circumstances without intermediaries.

Despite being the most prominent cryptocurrency, Bitcoin is arguably more of a commodity than a currency. Scarcity has been built in to the underlying rules governing the Bitcoin blockchain, so that there will only ever be just shy of 21 million Bitcoins. The vast majority of Bitcoins are already in existence (i.e. have been 'mined') and it is projected the final Bitcoin will be mined in 2140. At the date of this presentation (7 June 2019) there were approximately 17.75m Bitcoins in existence⁹. The concept of mining makes Bitcoin more commodity like and the continuing volatility in the price of Bitcoin makes it a poor store of value. Bitcoin is also used a hedge against conventional fiat currency, and holders are likely to hoard and not spend their Bitcoins, which has led to the widespread use of the acronym HODL (which means to hold Bitcoins for the long term no matter the short term fluctuations in price).

⁴ <https://www.corda.net/> developed by the R3 consortium <https://www.r3.com/>

⁵ <https://www.hyperledger.org/> supported by the Linux Foundation

⁶ <https://www.goquorum.com/> developed by J.P. Morgan bank

⁷ The Bitcoin whitepaper can be found here - <https://Bitcoin.org/Bitcoin.pdf>

⁸ See <https://www.newyorker.com/magazine/2011/10/10/the-crypto-currency> for further information

⁹ <https://www.blockchain.com/en/charts/total-Bitcoins>

Edward Chapman

August 2019

As highlighted above, Bitcoin also suffers from slow transaction speed. On average the Bitcoin blockchain can currently process 4.6 transactions per second¹⁰. By comparison Visa processes around 1,700 transactions per second on average¹¹. Steps are being taken to address this scalability shortcoming (most notably through the Lightning Network¹²), and this is one of the key obstacles on the road to mass adoption. Other blockchains are faster than Bitcoin, but even the speediest fall well short of established payment systems.

Bitcoin has been recognised as money or a currency in a number of jurisdictions, and is only illegal in a handful of states (such as China). However this is not to be confused with legal tender status and the protections this brings. In April 2017 Japan became the first (and to date only) country where Bitcoin is legal tender¹³.

Legal tender status is what gives fiat currencies strength, as they are backed by the law. By contrast, Bitcoin and other cryptocurrencies are almost entirely unregulated (and are inherently difficult to regulate through conventional laws by design). This means there are minimal protections or safeguards when things go wrong. For example, if you send Bitcoin to the wrong account (due to a typo when entering the destination address, for example) the transaction cannot be reversed, and you would be relying on the goodwill of the recipient to acknowledge the error and send it back.

The concept of 'being your own bank' is touted as a major benefit of Bitcoin and other cryptocurrencies. While at first blush this may be an appealing notion, it involves taking on a significant level of personal responsibility to protect your assets and this, in my view, makes it unlikely to be viable or desirable for most people. Being a bank also paints a target on your back and, in the event cryptocurrency is lost or stolen, there is little to no recourse. If you lose your private key, there is no easy password reset button (since there is no central body to administer and keep track of private keys).

Cryptocurrency is held in a digital wallet, which can be software or hardware. These wallets can either be 'hot' or 'cold'. A 'hot' wallet is one that is online (i.e. connected to the internet), typically held through an exchange such as Coinbase¹⁴. A 'cold' wallet means one that is held offline, for example on a USB stick.

Cryptocurrency exchanges have routinely been hacked over the years, most famously the Japanese exchange Mt.Gox in 2014 when 850,000 Bitcoins were stolen¹⁵. They will continue to be a target as they are at the interception of crypto and fiat currency. As a result best practice is to only have the amount of cryptocurrency in a hot wallet that you would carry in cash.

¹⁰ <https://hackernoon.com/the-blockchain-scalability-problem-the-race-for-visa-like-transaction-speed-5cce48f9d44>

¹¹ <https://usa.visa.com/run-your-business/small-business-tools/retail.html>

¹² <https://cointelegraph.com/lightning-network-101/what-is-lightning-network-and-how-it-works>

¹³ <https://www.coindesk.com/japan-bitcoin-law-effect-tomorrow>

¹⁴ <https://www.coinbase.com/>

¹⁵ <https://cointelegraph.com/news/the-mess-that-was-mt-gox-four-years-on>

Edward Chapman

Earlier this year it was revealed that Canada's largest cryptocurrency exchange, Quadriga, was unable to locate or access approximately £105m of cryptocurrency after its founder, Gerald Cotten died in November 2018. The majority of the cryptocurrency was held offline in cold storage, and Cotten had sole responsibility for handling the funds and coins¹⁶.

The moral of the story is that if you do not hold your own private key, you do not truly own the underlying cryptocurrency and this makes your holding more susceptible to being stolen or lost by a third party.

4. Smart contracts

The term 'smart contracts' is something of a misnomer. They are not contracts in the traditional legal sense, instead being executable code. They are also not particularly smart, for now at least.

The idea with smart contracts is for code to partially or wholly automate a process, usually involving a transaction and a movement of a crypto token (whether that be a currency like Bitcoin or a utility token). Smart contracts enable transactions and agreements to be carried out between anonymous parties without the need for an intermediary or an external enforcement mechanism¹⁷.

Currently they are best at automating repetitive and low value transactions, but there is considerable potential for their use in a variety of sectors (including insurance, as set out below).

It can be said that a vending machine operates in a similar manner to a smart contract. It involves funds being put into the system, followed by a trigger event (pressing a button). Once that button is pressed, the process of dispensing the product cannot be stopped, and if any change is payable this is calculated and automatically dispensed with the product.

The Bitcoin blockchain is a simple cryptocurrency, in the sense that it can be used for recording ownership and transfers of ownership. However a blockchain can also include executable code (in the same way as macros can be run in centralised ledgers). The best known and most commonly used blockchain for this is Ethereum, which is a permissionless blockchain. Ethereum has 3 primary uses: 1) sending currency (Ether is a cryptocurrency) 2) deploying new code and 3) interaction with existing smart contracts.

Potential benefits include transparency (easier to audit), immutability (resilient data management) and the ability for multi party communication and interoperability.

¹⁶ <https://www.bbc.co.uk/news/world-us-canada-47123371>

¹⁷ <https://www.investopedia.com/terms/s/smart-contracts.asp>

Edward Chapman

Decentralised applications (DApps) can be run on Ethereum. In time it is likely that these apps will look like conventional apps, so that the front-end would be a mobile app or a website. The smart contracts (code) would run in the background and it is possible that the end user would be unaware of their existence. This would reflect the way that internet browsers are routinely used on a daily basis, but users do not need to have any knowledge or understanding of the HTML code 'underneath' the website which enables it to function.

One possibility in the future is for smart contracts to enable the establishment and operation of decentralised autonomous organisations, where human oversight would not be required. In May 2016 'The DAO' raised approximately \$120m in a token sale, making it the largest crowdfunding campaign in history¹⁸. However in June 2016, shortly after its launch, a hacker found a loophole in the code which meant they could steal around 3.6m Ether, worth circa \$70m at the time¹⁹. This happened as a result of a weakness in The DAO DApp, rather than Ethereum itself. It also highlighted a flaw in decentralised autonomous organisations, in that it is far more difficult to correct bugs and errors in the code (once it is deployed) compared with a centralised organisation.

While there is still a lot of hype around blockchain, smart contracts are now being used in real world scenarios, and below I have identified three major use cases for the technology.

5. Supply chain

Supply chains are frequently complex ecosystems with numerous stakeholders and intermediaries, operating across borders and continents. Due to the number of actors and steps involved there is a general lack of visibility, and although some aspects have been digitised there are still frequently analogue gaps. Transparency and auditability are key elements and blockchain technology is well placed to increase efficiency, and it can ultimately offer a real-time ledger of transactions and movements that all parties in the supply chain have visibility of²⁰. For example, the use of smart contracts can speed up payments, so that triggers mean automatic invoicing and near immediate payments provided specified conditions have been met.

There have been a number of industry collaborations in this space. One example comes from the world of shipping, where Maersk (the largest global container shipping company) and IBM joined forces to create TradeLens, which is based on the Hyperledger permissioned blockchain²¹. The structure of this collaboration as a joint venture between Maersk and IBM has caused issues in enticing more carriers to join. A particular problem is that Maersk and IBM have full and equal rights to all intellectual property in TradeLens²². In May 2019 there

¹⁸ <https://www.cnn.com/2016/05/17/automated-company-raises-equivalent-of-120-million-in-digital-currency.html>

¹⁹ <https://medium.com/swlh/the-story-of-the-dao-its-history-and-consequences-71e6a8a551ee>

²⁰ <https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/#20eb9b615fec>

²¹ <https://www.tradelens.com/>

²² <https://www.coindesk.com/ibm-blockchain-maersk-shipping-struggling>

Edward Chapman

was a significant step forward when the second and fourth largest global shipping companies globally joined the group²³. The success of any blockchain depends on reaching a critical mass of users, particularly in global supply chains, where the network effect is crucial and pronounced.

In the food industry IBM has collaborated with partners including Walmart, Nestle, Unilever and Carrefour with the launch of the Food Trust blockchain²⁴. It promises end to end traceability, from farm to factory to fork, launching in October 2018 after 18 months of development based on the Hyperledger blockchain. Around the same time Walmart wrote to its suppliers requiring its direct suppliers to sign up to its Food Traceability Initiative by 31 January 2019 and has mandated end-to-end traceability of leafy greens such as romaine lettuce by 30 September 2019²⁵.

Walmart also conducted a trial involving sliced mango, where Frank Yiannas (former Vice President of Food Safety) bought a pack of sliced mangoes from a Walmart store and asked his team to identify which farm they came from. It took almost seven days to locate the farm, calling and emailing various parties along the supply chain. Using the Food Trust blockchain to carry out the same task, the time required to trace the origin of the mangoes went from 7 days to 2.2 seconds!²⁶

LVMH, the luxury goods group behind brands such as Louis Vuitton and Christian Dior, is currently trialling a blockchain based on Quorum called AURA (partnering with ConsenSys and Microsoft). The idea here is to be able to take a leather handbag and be able to trace its provenance and lifecycle, from the alligator farm to the store where it was first sold, through to the multiple owners that bought and sold it. AURA will be a white label solution and it appears LVMH has learned from TradeLens when it comes to intellectual property. To encourage competitors to collaborate and use AURA all IP is to be transferred to a separate legal entity, which will be co-owned by participating brands²⁷.

6. Insurance

The insurance industry is well positioned to benefit from blockchain technology, and smart contracts in particular, to put the customer in control of the claims management process²⁸. One exciting live use case in this area is for flight cancellation insurance. Typically this is a process that can take many weeks and involves numerous forms, emails and phone calls before any compensation is actually received for late or cancelled flights.

²³ <https://www.coindesk.com/ibm-maersk-finally-sign-up-2-big-carriers-for-shipping-blockchain>

²⁴ <https://www.ibm.com/uk-en/marketplace/food-trust>

²⁵ The open letter from Walmart to its suppliers dated 24 September 2018 can be found here <https://corporate.walmart.com/media-library/document/blockchain-supplier-letter-september-2018/proxyDocument?id=00000166-088d-dc77-a7ff-4dff689f0001>

²⁶ <https://www.hyperledger.org/resources/publications/walmart-case-study>

²⁷ <https://www.coindesk.com/louis-vuitton-owner-lvmh-is-launching-a-blockchain-to-track-luxury-goods>

²⁸ <https://www.pwc.co.uk/financial-services/fintech/assets/blockchain-in-insurance.pdf>

Edward Chapman

Etherisc, a Berlin based start up²⁹, is offering fully automated flight cancellation, delay and diversion insurance cover through a DApp³⁰ which is fully licensed and operational.

Etherisc was accepted into the regulatory sandbox of the UK's Financial Conduct Authority for the second half of 2018 which gave them the opportunity to test their products in a controlled environment³¹. Payments for cover can currently be made in USD, EUR or GBP, and in time it is expected this will be expanded to the Ether cryptocurrency as well. If your flight is delayed by 45 minutes or more, the pay-out is automatically triggered and can be received immediately after landing.

Information is obtained from the airlines and airports, and in the blockchain world these information sources are known as oracles. These oracles are the data source which provides the information for smart contracts to work. However there is a certain irony about a decentralised application relaying on data from centralised organisations and servers, and this is known as the oracle problem. In the flight delay context, this means that by taking out a policy through Etherisc and hacking the airline or airports involved it is possible to manipulate the smart contract into making a pay-out even if there was no actual delay. In all likelihood the cost and time involved for such a small reward is likely to put people off taking such action. There were also always be bad actors, however the risks can be mitigated by obtaining data from multiple sources (several oracles).

Etherisc also have a number of other products at various beta / testing phases, including crop insurance, hurricane protection and crypto wallet insurance.

7. Real estate

Being a relatively illiquid asset, real estate ownership is ripe for innovation and tokenisation, where an asset is fractionalised and represented by a digital token. This enables partial ownership and has the potential to democratise real estate ownership by lowering the cost of entry. In 2018 \$18m was raised through a token sale on the Ethereum blockchain, and the asset was the St. Regis Resort in Aspen, Colorado³². Aspen Coins were created (the tokens) which represent a share of the company Aspen Digital, which owns 18.9% of the Resort. The tokens could be purchased in USD, Bitcoin or Ether. This example provided for a real estate investment trust wrapper with the blockchain element enabling peer-to-peer investing.

Tokenisation also has the potential to create liquidity for investors³³. There will still need to be a market and willing buyers, but the principle is that tokens can be traded 24 hours a day across the globe. It should be noted that such business models are likely to be subject to

²⁹ <https://etherisc.com/#products>

³⁰ <https://fdd.etherisc.com/>

³¹ <https://www.fca.org.uk/firms/regulatory-sandbox/regulatory-sandbox-cohort-4-businesses>

³² <http://blog.realestate.cornell.edu/2019/04/30/tokenizing-real-estate-creating-new-investing-and-financing-channels-through-blockchain/>

³³ <https://cointelegraph.com/news/tokenizing-commercial-real-estate-and-the-promise-of-liquidity>

Edward Chapman

August 2019

increasing regulatory scrutiny and oversight, and tax advice should also be sought depending on which jurisdiction the investor and project is based in.

Another area where blockchain technology can have an impact is in speeding up the process of buying and selling residential real estate. As part of my training I spent around a year working on these property transactions and it is fair to say that the process was (and some 6 years later, still is) slow and largely opaque, where lawyers and banks still routinely correspond by letter and fax.

In the UK Her Majesty's Land Registry (HMLR) is actively investigating technological solutions to increase efficiency and to bring property transactions into the 21st century through its Digital Street initiative³⁴. Earlier this year HMLR built and run an end-to-end proof of concept with conveyancing firms Mishcon de Reya and MyHomeMove, payment intermediary Shieldpay, digital ID provider Yoti and Her Majesty's Revenue & Customs (HMRC) relating to a semi detached house in Gillingham. In March 2019 the sale completed using a conventional process and took 22 weeks.

HMLR and its partners ran the same sale process through its blockchain prototype, based on Corda and assisted by Methods, a digital transformation organisation with a public sector focus³⁵. Corda is a permissioned blockchain, so only chosen participants are aware and privy to transaction information (e.g. the buyer and seller, their advisors, banks and HMLR itself). Corda also allows for certain parties to see certain information. For example, HMRC only needs to know when a transaction completes, so that it can seek payment of the appropriate stamp duty land tax. HMLR also has this 'observer' status, where it does not participate in the transaction but is made aware of it completing, so it can then update its land register.

Each party was able to see the current status of the transaction, completed actions and outstanding aspects. HMLR concluded that blockchain technology could enable *'speedier property transactions, more trust in the transaction, higher levels of security and increased transparency for participants in the transaction'*³⁶.

8. Other use cases

There are a substantial number of other use cases for blockchain technology emerging on an almost daily basis. Some examples include:

- Remittances: this is a global industry dominated by legacy firms such as Western Union, who charge up to 10% commission on their services to transfer funds from employees back to their families in the developing world. There are a number of projects and prototypes aimed at lower the transaction fees and speeding up the process, as well as dealing with the well documented 'last mile' difficulties. However I

³⁴ <https://hmlandregistry.blog.gov.uk/tag/digital-street/>

³⁵ <https://methods.co.uk/>

³⁶ <https://hmlandregistry.blog.gov.uk/2019/05/24/could-blockchain-be-the-future-of-the-property-market/>

Edward Chapman

would argue that there has been little in the way of tangible results to date. It will be interesting to see what impact the proposed Facebook backed cryptocurrency Libra will have (if it ever launches).

- Trade finance³⁷.
- Escrow – smart contracts can fully automate simple escrow services, which could increase efficiency in a number of industries
- Identity – the district of Zug in Switzerland offers blockchain based digital IDs to all of its circa 30,000 citizens using the uPort DApp³⁸. Once a person's identity is confirmed this becomes publicly attested on the Ethereum blockchain (without the underlying personal information being made public).
- Internet browsers – Brave³⁹ is a free open source browser which blocks ads and website trackers. It also incorporates its own native token, called the Basic Attention Token. By choosing to watch or be subjected to adverts users of the browser obtain BAT⁴⁰, and end users obtain 70% of the proceeds which are automatically added to their Brave wallet on a monthly basis.

9. Dole Food case study

In 2013 a class action case was brought against Dole Food in the USA, the largest producer of fruit and vegetables in the world. The action was based on the conduct of David Murdock (then the chairman, CEO and largest shareholder of the company) who, in short, took the company private at what was considered to be an artificially low price. The class action was successful and in 2015 the Delaware Chancery Court ordered Murdock to pay each shareholder an additional \$2.74 per share (plus interest). Claims were made by around 4,600 shareholders, holding around 49 million shares between them. However, there were only 36,793,758 issued shares at the time. Upon investigation it was established that nearly all of the claims were valid (rather than people lying about holding shares)⁴¹.

This episode shone a light on the way shares are held in the USA. There are a number of intermediaries involved, each using separate and unlinked ledgers of shareholders and holdings. In short, a Dole Food shareholder had an entry in their broker's database, the

³⁷ https://cib.db.com/insights-and-initiatives/flow/trade_finance_and_the_blockchain_three_essential_case_studies.htm and <https://www2.deloitte.com/content/dam/Deloitte/global/Documents/grid/trade-finance-placemat.pdf>

³⁸ <https://www.uport.me/> and <https://www.ethnews.com/zug-and-uport-see-first-citizens-identity-registered-on-the-ethereum-blockchain>

³⁹ <https://brave.com/>

⁴⁰ <https://lifelhacker.com/get-paid-to-watch-ads-in-the-brave-web-browser-1834332279>

⁴¹ <https://www.bloomberg.com/opinion/articles/2017-02-17/dole-food-had-too-many-shares#footnote-1487284943950>

Edward Chapman

August 2019

broker had an entry in the Depository Trust Company's (DTC)⁴² ledger and finally the DTC has an entry in Dole Food's ledger of shareholders.

Blockchain technology could help provide a solution to prevent this situation happening in future, by offering a real time shared ledger which would also help speed up the current (and frankly archaic) standard 3 day settlement period for stock acquisitions.

In 2017 Delaware passed legislation that allows corporations to maintain shareholder lists, along with other corporate records using blockchain technology⁴³. The legislation is not prescriptive; it does not mandate a particular blockchain or provider. This reflects a wider trend of statutory company records becoming digitised. Blockchain technology is particularly attractive for this purpose because of its immutability, which will help with auditing and due diligence during an acquisition process.

10. Regulatory landscape

As with any emerging technology, regulators and legislators across the world are racing to understand blockchain and considering how best to regulate it (if at all). There is a tension between regulation and innovation, and (broadly speaking) the preferred approach by regulators to date appears to be reactive rather than proactive. It can be characterised as giving market participants freedom to operate, issuing guidance which will ultimately end in legislation arising out of test cases. That said, different jurisdictions are taking different approaches. For example, France and Germany want a regulatory framework in place⁴⁴, whereas the UK and US seem more likely to let participants innovate up to a point and only legislate once it becomes necessary.

The inherently transnational nature of blockchain technology presents jurisdictional issues. It can be argued that distributed networks equal distributed liability, and it will be fascinating to observe how traditional government and law enforcement adapt to a technology which is fundamentally designed to operate without state oversight.

11. United Kingdom⁴⁵

In the UK three regulatory bodies formed a Cryptoassets Taskforce in early 2018, being the Bank of England, Financial Conduct Authority (FCA) and Her Majesty's Treasury (HMT). It issued its final report on DLT in October 2018, concluding that *'while DLT is at an early stage of development, it has the potential to deliver significant benefits in financial services and other sectors in the future'*⁴⁶.

⁴² <http://www.dtcc.com/about/businesses-and-subsiaries/dtc>

⁴³ <https://fortune.com/2017/08/01/blockchain-shareholders-law/>

⁴⁴ <https://uk.reuters.com/article/us-france-cryptocurrencies/france-to-ask-eu-partners-to-adopt-its-cryptocurrency-regulation-idUKKCN1RR1Y0?rpc=401&>

⁴⁵ See my interview with Stephen Palley published on 1 May 2019 for more details -

<https://www.theblockcrypto.com/2019/05/01/crypto-and-law-a-view-from-the-other-side-of-the-atlantic/>

⁴⁶ The full report is available here <https://www.gov.uk/government/publications/cryptoassets-taskforce>

Edward Chapman

The FCA went on to issue draft guidance in January 2019 with the final guidance due to be released in the summer. While this will not be binding it will have persuasive value in the courts of England and Wales, and therefore its findings are highly likely to be followed by judges.

Based on the draft guidance the FCA does not propose to regulate what it calls 'exchange tokens' such as Bitcoin or Litecoin, or 'utility tokens' in the majority of cases (provided that there is genuine utility). However it does propose to regulate 'security tokens' by reference to existing capital markets legislation. In short, if a token looks like a security (e.g. it has share or debt instrument like characteristics) it is likely to be caught by the extensive and burdensome securities regime in the UK.

HMRC has also stated that cryptoassets are liable to capital gains tax on disposal if a profit is made, and individuals will also be liable to pay income tax on cryptoassets received from an employer as a non-cash payment or via mining.

In light of the draft FCA guidance a key question will be whether a token is classed as a 'security'. It is a hallmark of regulation to label and box new innovations by reference to existing understood concepts (each with their own legislative regimes). For blockchain this has so far included regimes for securities, commodities and currencies.

Even if a token is not subject to FCA oversight (i.e. falls outside of its regulatory perimeter) market participants will need to consider the upcoming implementation of the EU 5th Anti-Money Laundering Directive (5MLD). 5MLD extends KYC and AML checks to cryptoasset exchanges, which are defined as 'providers engaged in exchange services between cryptoassets and fiat currencies'. In April HMT launched a consultation on the implementation of 5MLD⁴⁷, and is considering whether the scope of 5MLD should be extended so that customer due diligence (CDD) is needed for the following:

- Cryptoasset ATMs;
- Crypto to crypto exchange services;
- Peer to peer exchange services;
- Issuance of cryptoassets (i.e. initial / security / hybrid token offerings); and
- Publication of open-source software.

The final proposal is the most alarming, and it is unclear how this would work in practice or what it is intended to achieve⁴⁸.

As it stands crypto exchanges and token issuers have had minimal AML / CDD requirements. 5MLD and associated regulation in England and Wales is likely to make identifying and verifying the identities of investors a key risk factor for exchanges and issuers. I expect 5MLD

⁴⁷ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/795670/20190415_Consultation_on_the_Transposition_of_5MLD_web.pdf

⁴⁸ https://www.theregister.co.uk/2019/06/11/open_source_money_laundering_directive/

Edward Chapman

to be transposed into English and Welsh law regardless of the outcome of the ongoing Brexit negotiations / impasse, not least because the UK was heavily involved in drafting and negotiating 5MLD).

It is possible that the UK may enact more stringent AML laws than the rest of Europe. If this proves to be the case this could drive participants to lighter touch jurisdictions. Alternatively a more robust regulatory regime may lead to increased confidence in the UK as a cryptoasset destination (as is the case with existing public offerings and the wider FinTech industry).

12. Wyoming, USA

The peculiarities of the US legal system, in that regulation can vary widely on a state by state basis, present opportunities for innovative states to gain an early mover advantage. Wyoming is aiming to take the lead in the USA by creating a business friendly cryptoasset regime, driven by ex Wall Streeter Caitlin Long.

There is no state tax (i.e. no property or sales tax) payable on cryptoassets and there is also an exemption from stringent money transmission legislation.

Several bills were passed in February 2019, including legislation for security tokens and defining utility tokens as intangible personal property⁴⁹ to separate them from security tokens (an approach now adopted by the Securities and Exchange Commission). Montana has since followed suit⁵⁰.

The state has also approved the introduction of a FinTech regulatory sandbox⁵¹, no doubt inspired by the success of the UK's FCA sandbox.

13. The route ahead and key challenges

Blockchain technology is still very much in its infancy and has yet to truly break out from a small passionate group of developers, evangelists and entrepreneurs. As with other emerging technologies there have been teething pains, most notably during the initial coin offering craze of 2017, where hope value saw the price of Bitcoin and other cryptocurrencies sky rocket almost overnight.

Some key hurdles to be overcome on the road to mass adoption are, in no particular order:

- User experience – at present the interface needs to be more user friendly and simpler to use, with the ultimate aim that users are unaware they are using and interacting

⁴⁹ <https://cointelegraph.com/news/wyoming-passes-bill-to-recognize-cryptocurrencies-as-money> and <https://www.coindesk.com/wyoming-lawmakers-pass-three-bills-in-boost-for-states-crypto-industry>

⁵⁰ <https://cointelegraph.com/news/montana-passes-bill-to-recognize-utility-tokens-and-exempt-them-from-state-securities>

⁵¹ <https://www.coindesk.com/wyoming-lawmakers-advance-blockchain-sandbox-bill>

Edward Chapman

with a blockchain (browsers made this leap with the internet which led to mass adoption).

- FAANG incumbents⁵² - these companies have and will continue to investigate blockchain as they have the funds to do so; their business models hinge on the harvesting and exploitation of personal data, which will become increasingly sophisticated (and potentially disturbing) through the use of machine learning and AI. From the information available at present Facebook's mooted cryptocurrency is about the future of payments, and crypto just happens to be the tool.
- Interaction with legacy IT systems – blockchain solutions should be seen as augmenting rather than replacing existing architecture. That said, the success of a blockchain depends on the quality and relevance of the data being inputted; it will not inherently make data more useful.
- Governance – Bitcoin and Ethereum core developers have significant power and influence, as they are creating the rules for the most popular and most used blockchains. Ethereum is particularly susceptible, as it has had numerous 'hard forks' where users have been effectively forced to switch to a new version of the blockchain to comply with new rules set by core developers. This type of governance will come under increasing scrutiny, particularly when one of the key objectives of decentralised ledgers is transactional transparency.
- Interoperability – there is a need for agreed definitions and standards for the ecosystem to move forward and for it to reach a critical mass of users.
- Scalability – as highlighted in the Bitcoin section above, this is a major concern for most blockchains. The technology is inherently slow when compared to centralised systems. Whether agreement is required from all participants is a key question. If so there is a risk that a blockchain becomes overloaded with transactions and participants. Since every node (or user) has a complete historical record of a permissionless blockchain more transactions makes a blockchain more cumbersome.
- Cost-effectiveness and environmental impact – there are well publicised issues around the 'proof of work' consensus mechanism that powers Bitcoin and a number of other cryptocurrencies⁵³, due to the processing power and the resultant electricity required. There are numerous competing consensus mechanisms, most prominently proof of stake, which Ethereum is planning to move to in the near future.
- Privacy – there is an increased awareness of the value of data, particularly in light of the Cambridge Analytica scandal. Protecting personal data is going to become ever more important as the use cases of blockchains become increasingly exotic (e.g.

⁵² This presentation was given before Libra was officially announced and before publication of the whitepaper

⁵³ Mining is beyond the scope of this paper

Edward Chapman

storage of health records). Regulations such as the European GDPR and the upcoming Californian legislation need to be carefully considered too.

14. Conclusion

Blockchain technology cuts across many industries, and its impact is likely to be felt far beyond its 'natural' use case of financial services. As such lawyers and other professional advisors will benefit from having an awareness or understanding of it (without needing to be technical experts or coders). This may lead to new practice areas being created, as was the case with data protection. I expect there will be litigation around mis-selling of investments and the classification of tokens, in particular whether a token is to be classed as a security.

Cryptoasset exchanges will come under increasing scrutiny from regulators, with a focus on anti-money laundering processes and demonstrating compliance with increasingly stringent regimes.

Securitized token offerings (STO) will become part of the investment landscape, and this is a welcome development from the initial token offerings. That said, it must be remembered that the quality of the underlying business venture or proposition is what matters and that a poor business model is not magically improved or remedied by virtue of raising funds via a STO.

I expect to see the continued development and adoption of permissioned enterprise blockchains, and expect to see legal contracts and smart contracts to increasingly co-exist as part of a new hybrid legal framework.

If cryptoassets become more widely adopted, inheritance will become a key issue given the importance of holding and safeguarding private keys. Innovative new products and companies are likely to emerge that will challenge existing thinking in this area.

Blockchain needs its Netscape moment⁵⁴ in order for mass adoption to take place. If and when this happens previous technological leaps (like the internet) tell us that the pace of change is likely to be rapid and the consequences will be far reaching.

⁵⁴ <https://www.poynter.org/reporting-editing/2015/the-netscape-moment-20-years-on/>