Blockchain: Revolution or Bubble?

Written by Alexander Carter-Silk, Partner and Head of European Intellectual Property, Brown Rudnick LLP, London

Just as the evolution of the internet created new methods of communication and business models, the arrival of blockchain systems has enabled business to envision new ways of engineering transactions which are much less obvious than at first they would appear.

The evolution of digital commerce has two major impacts, disintermediation and dematerialisation. In any digital environment where one party is willing to make a payment remotely for property or services delivered against a digital promise, the need for intermediaries, brokers, trusted third parties and long supply chains is removed. The internet started a process which blockchain technology is likely to accelerate.

Physical intermediaries, high street stores and even wholesalers are inevitably reduced as part of the supply chain. The other element, dematerialisation, is less obvious and involves removing layers of infrastructure. Digitising transactions and automation of distribution centres facilitate matching the digital product identity with the financial transaction and the digital identities of the parties. Legacy business operations such as pick and pack and the reliance on the complex extended supply chain is inevitably dematerialised.

THREE TECHNOLOGIES

There are three elements to the new digital commerce environment; asymmetric cryptography, distributed ledger and blockchain. Whilst all three technologies come together in relation to cryptocurrencies they are not all individually necessary to other applications such as supply chain management.

Asymmetric cryptography also known as public key cryptography, uses public and private keys to encrypt and decrypt data. The keys are simply large numbers that have been paired together but are not identical (asymmetric). One key in the pair can be shared with everyone; it is called the public key. The other key in the pair is kept secret; it is called the private key. Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Distributed ledger technology (DLT) records the same transaction in multiple places at the same time. There is no centre data storage or control over what is recorded or when.

A blockchain ledger (database) consists of two types of records: individual transactions and blocks. The first block consists of a header and data that pertains to transactions taking place within a set time period. The block's timestamp is used to help create an alphanumeric string called a hash. When a blockchain is held on a distributed ledger each of the computers in the distributed network maintains a copy of the ledger to

prevent a single point of failure (SPOF) and all copies are updated and validated simultaneously.

After the first block has been created, each subsequent block in the ledger uses the previous block's hash to calculate its own hash. Before a new block can be added to the chain, its authenticity must be verified by a computational process called validation or consensus. At this point of the blockchain process, a majority of nodes in the network must agree the new block's hash has been calculated correctly.

THE FUNCTIONAL CHARACTERISTICS OF BLOCKCHAIN

Assuming that a transaction is concluded between two parties (remotely) by which a digital token is exchanged for property, the data which is created (the timestamp, parties' IP address, wallet ID, the amount of any token etc) are converted to hash and that data is added to the block. If a digital token is used in the transaction (such as Bitcoin) the system must reach a "consensus" to ensure that the same token is not spent twice; miners perform this function by validating the transactions and ensuring that only the first in time is joined to the current block.

As the blocks are chained and "distributed" there is no credible way of altering the transactional data. As the distributed ledger is not in the hands of a central administrator there is negligible risk of the data being altered. The Fintech experience offers a convergence of behavioural economics, artificial intelligence, big data, and the birth of a new era in commerce. This phenomenon will fundamentally affect lawyers and professionals, particularly those who continue to apply analogue skills systems and processes in a digital world. Blockchain introduces a new conceptual understanding namely that "trust" can be established with someone you do not know. Trusting transaction validated by a public network of computers is more than a technical evolution, it is a philosophical change, creating opportunities for business models that have yet to be conceived. Consensus ensures that all copies of the distributed ledger share the same state.

USE AND APPLICATIONS OF THE TECHNOLOGY

Applications based on these technologies have the capability to fundamentally affect lawyers and professionals, who transact remote trusted transactions. Trusting transaction validated by a public network of computers creates opportunities for business models that have yet to be conceived.

As with many disruptive technologies, the timing and adoption process can be unpredictable. It is often the product of changes in the ecosystem lying outside the control of the innovator. The application of these technologies is in a state of evolution. As Clayton Christianson pointed out, conventional valuation and risk analysis does not work when the application of the technology has no history.

The silent metamorphosis of digital infrastructure is likely to change business models and disrupt industries. The smartphone created a revolution in payment systems in Africa where conventional banking is simply not available and phone minutes became accepted as a medium of exchange. It is likely that cryptocurrency will evolve into an acceptable medium of exchange that reduces reliance on centralised ledgers. The

likely drivers will be speed and the need to reduce the hidden costs of transactions. This may take some time to identify a trusted token, which is likely to arise from a wealthy trading business, as happened with the rise of the Medici dynasty from trade in the 16th Century.

Knowing that an industry is about to be disrupted is not the same as predicting what the effect will be, how fast it will happen, or who will be the winners or losers. Examples can be cited to evidence that managers in the most affected industries are the last to accept the inevitable. This may be because they do not have the influence to change their individual environment, or because they cannot realign their skills to do so.

Those who predicted the end of days for music when digital music took hold lived to see the volume of published music rise exponentially, stars created on YouTube and greater access globally to media than could have been conceived. At the same time as iTunes reached 14 million downloads a month, the stock price of music retailer HMV was still rising. It was some time until the conventional retail distribution matrix responded.

BLOCKCHAIN AS AN ENABLING TECHNOLOGY

The combination of these three technologies has created the opportunity for parties to exchange digital tokens remotely with certainty that the token they receive has not been used in any other conflicting transaction.

Just as when one passes cash from one banking ledger to another, or one party hands over physical currency, a token that is passed through a blockchain/distributed ledger system is validated using asymmetric encryption cannot be spent twice and has the characteristic of a currency transaction.

It is for the parties to decide what a digital token represents and what it can be exchanged for. A unit of fiat currency has a value because people accept it as a medium of exchange, and that has a lot to do with being backed by a central or sovereign bank as the "lender of last resort". With the explosion of new crypto currencies, it is perhaps inevitable that a handful will survive as the chosen medium of exchange.

Once the ledger code has been "launched", and is proliferated across multiple platforms and computers, it cannot be controlled. Changes to the way tokens operate is undertaken by "forking" the token's underlying code and creating a new variant.

As an enabling technology blockchain enabled tokens can be applied in any circumstances where two (or more) parties wish to engage in a digital transaction remotely without needing to trust the other party to do what they have promised to do. Transactions are executed automatically using computer code.

TOKENISATION AND PROVENANCE

In principle, the title to any physical asset can be represented by a digital token. For example, the serial number on a high value luxury item such as a watch can be converted to a hash using public/private key encryption.

Only the holder of the private key can create that hash and only the public key holder can verify it. In principle therefore, the title to the physical asset can be tokenised, and

title passed in a digital transaction. If the owner's personal data is given the same treatment, it is possible to create a "hash" from the property data combined with that created as a hash of the owner's identity.

Starting with the manufacturer the "hash" could be a combination of the manufacturer's identity and the serial number of the asset. A new owner would be "added" to the block giving a complete chain of provenance that can be validated online by any prospective owner who is provided with the public key (only the key pair will validate).

If one extrapolates this thinking it can be understood that a provenance can be provided for any high value asset. That provenance will only ever identify the current owner, there cannot be two owners of the same asset. Presentation of an asset by a third party whose "hash" is not presented on the chain will not validate.

PUBLIC AND PRIVATE BLOCKCHAIN

Whilst the use of a distributed ledger is an attractive way of ensuring that tokens that are exchanged remotely have not been duplicated, and that the transactions on a blockchain are valid, it is not necessary for this to be the case.

The blockchain database can be held on a single instance database "privately" and provide certificates which evidence that transactions took place and were recorded on a specific date.

LENDING ON MOVEABLE ASSETS

Whilst perhaps a less obvious application, assuming that one has sufficient data to create a unique digital hash that identifies an individual, and the same for a physical asset, it is possible to create a registry that can be used to identify assets which are pledged for a debt. The challenge to such systems is whether such registries operate as legal "notice" to third parties who may purchase assets without notice of the lender's rights. On the premise that the owner cannot pass better title than he has, such applications would appear to be attractive. Some jurisdictions such as the USA already recognise pledges of moveable assets.

EVOLVING LAW

Since the advent of the internet there have been remarkably few new laws. In the early days of the internet there were accusations of it being unregulated, that the Wild West etc. would abound. Now, we take it for granted that we will deal remotely with companies and buy and sell high value assets across web portals.

The basic principle of the law relating to trade has not changed since it was codified in Roman Law. Whether it is by common law or civil law, the principles of contract are remarkably similar. The laws relating to misrepresentation, unfair contracts and the like apply as much in the digital world as they do in the analogue world. There is however the need for the courts to reinterpret the law to apply it to the new paradigms.

CRYPTOCURRENCY AS A MEDIUM OF EXCHANGE

One of the concerns that has been raised is whether government control of the money supply will be materially affected as means of economic management. The first

countries to lead with regulation have been those who are most concerned at preventing assets from leaving the country. Tight central control is challenging if commercial operators are willing to accept tokens for payment which do not need to pass through conventional foreign exchange control mechanisms.

DOCUMENT AND PROJECT TOKENISATION

The philosophy behind distributed ledger technology creates the opportunity to validate digital documents, and to record events and transactions which could in principle abrogate the need for the production of millions of documents in court proceedings and the unrewarding experiences of thousands of hours spent on manually trawling through these to establish legal rights. These systems are likely to take many years to develop and adopt.

It is entirely possible to build business ownership models using tokenised equity which are subject to smart contracts built on algorithms that echo conventional company law (this would need to accord with tax and securities laws). There is no reason why pre-emption rights issues and the like could not be achieved digitally. Similarly, there is no reason why rewards structure cannot be linked securely to almost any event that can be recorded. In this way the internet of things could well be the catalyst for new reward systems that generate tradeable tokens.

PROJECT MANAGEMENT

The potential to disrupt conventional contacting is significant and complex projects are capable of being converted into a digitised process replacing thousands of hours of narrative agreements into code. In a "smart-contract"/blockchain environment a central project plan can be tied to a CAD design, project plan, diary and to sensors, smart validation of work done and payment algorithms which release funds automatically.

As each task is completed a token can be created, and, when the criteria for release are loaded, the transaction is time stamped and cannot be reversed or duplicated. Digital models would need to be created, but once created the recording system is programmed, and the core program need never be rewritten. The "contract" records its own progress: reading invoices, project plans and asking for authorisation by the appropriate stakeholder. The timeline stores multimedia timestamped records of each work product and authorises payments.

A legal team is required to create such a "smart contract" and to develop it, but the time spent in negotiation would be directed to operating the project rather than arguing over the narrative.

This narrative is an explanation as to what is possible. Whether it is economically viable or probable, I will leave to others. Elements of this speculation are likely to be achieved and some are already happening, with contracts being made remotely and events recorded in a way which cannot be altered or reordered. Businesses that sell media rights and other easily digitised assets are some of the first to develop systems which permit each transaction and resale to generate and distribute value to the original creator as well as the immediate vendor. Something which is possible if the "hash" records the full title of the digital asset.

These contracts are already in existence in the financial markets where the terms of the trades are standardised and the importance of recording the exact timing and sequence of transactions is critical. The development of XML schemas for the narrative of legal agreements means that automated contract review is within reach. If documents are drafted within the constraints of standardised XML schemas and all of the events, transactions and agreements of a business are digitised and digitally signed, then the records of transactions and interactions with suppliers, customers and employees could be analysed using the AI methodologies and payments made automatically.

GAME THEORISTS

Game theorists have for decades been mapping human economic behaviour but struggled to correlate cause and effect. In the blockchain era, game theory comes of age. The rules of competition and behavioural response can be preordained.

With the internet of things and the analytics engaged by "no-sql" opens the potential to move from static to dynamic commercial agreements, where specific behaviour can trigger a price change, create a reward or limit a risk. The cause and effect of any change can be analysed in real time using big data analytics.

The design of these "dynamic" contracts has been underway for some time as the travel industry commoditises aircraft seats, hotel rooms and car hire to respond instantaneously to demand changes. The same has been going on for some time in digital advertising where digital assets are auctioned in hundredths of milliseconds.

Algorithms derived from game theory and behavioural economics can be coded to recognise and respond to events. As the movement of people and goods and value becomes increasingly digitised, data analytics can analyse and predict behavioural change in real time.

The evolution of smart cities and the allocation of resources from a parking space to road use no longer requires crude predictions of how consumers will respond to regulation many months after the event. Parking costs in a smart city can be altered in real time to respond to demand, payments can be tokenised and personalised and programmed to respond to the status of the driver.

Regulation of the use of these technologies will be reactive depending on perceived abuses as they are identified. European payments legislation, money laundering, corporate transparency rules and cross border regulation are likely to be modified to protect the innocent, disadvantaged and unwary. It is also likely that a new body of law may evolve around the ethics of data use and misuse. It is by no means obvious that data privacy will be fit for purpose in an environment where the transactional data discloses real time responses to environmental and financial changes.

Just as this technology makes many new business processes and models possible, it is also right to say that just because you can do something, does not mean you should do it…