Understanding Blockchain Technology

Introduction

Disruptive technology continues to radically change the way the world operates whilst impacting, negating and creating new business models across industries. Blockchain is an example of a disruptive technology that could have the same transformational impact as the Internet. It has experienced a surge in interest and media coverage as a way for groups of organisations to come together to reduce costs, improve product offerings and increase speed.

Blockchain software offers a radically different approach to recording transactions in a way that is verified, immutable and accessible by all parties. Transaction records could represent value of many kinds – including payments, contracts or even wills. The technology promises faster execution at much reduced cost, removing the requirement for reconciliation and the necessity for trusted intermediaries.

It could have roles across industries, where multiple independent parties need to come to, and maintain, agreement about facts without involving a central arbiter. The technology essentially ensures two things 1) that what you see is what everybody sees and 2) that nobody can rewrite the historical record.

What is blockchain, how does it work and why does it matter?

Blockchain is simply software that provides a new way of recording transactions in a trustworthy way

Blockchain is just software. But it is a novel and special kind of software conceived to generate trust through programmatic techniques. It describes a set of instructions and rules that allow computers within a network to maintain a ledger of transactions.

The technology automates the recording of ownership and the transfer of value on a single replicated ledger without the need for a central arbiter. Transactions only need to be recorded in one place and are agreed at the point of recording through a process of consensus. Crucially while records can be added to the ledger, no existing transactions can be changed or removed. It is a permanent record that cannot be rewritten.

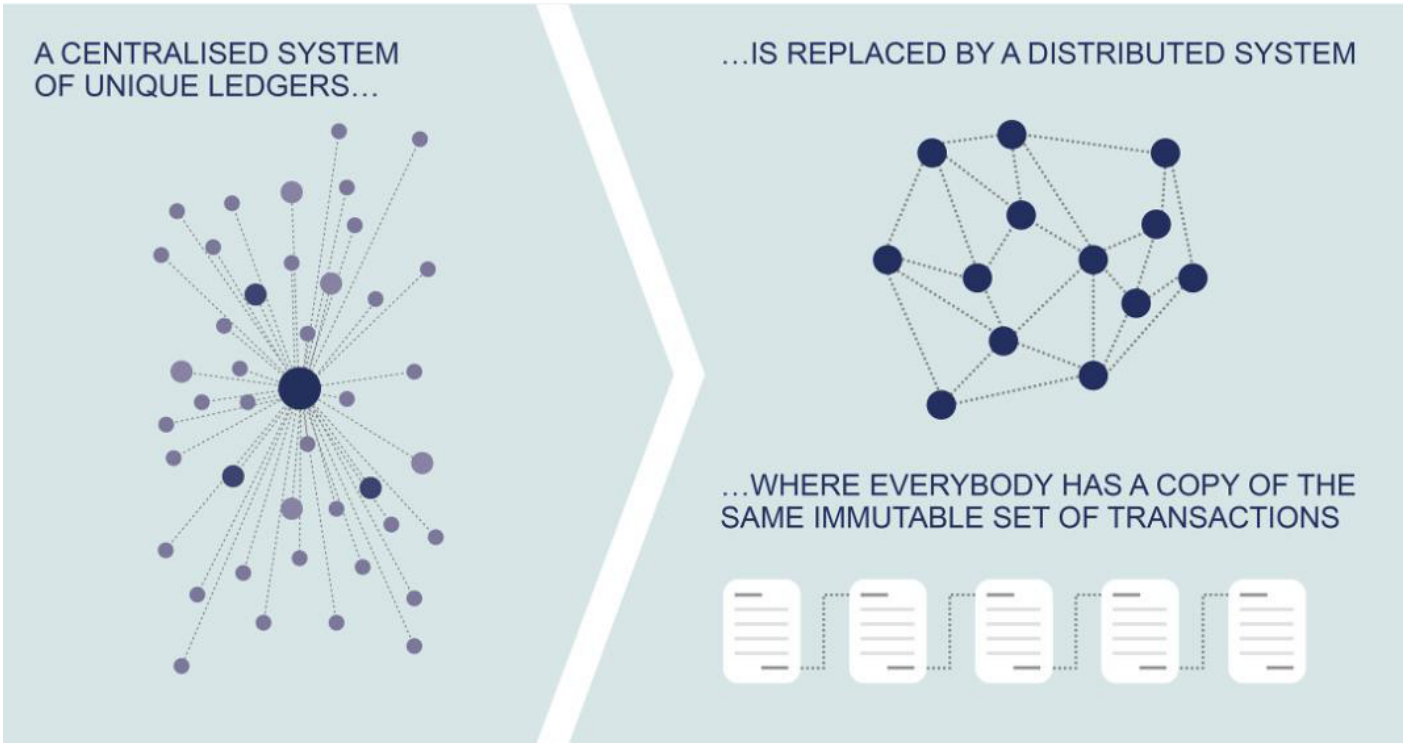
Blockchain works by trusting the science of mathematics rather than any individual institution or entity

Transactions are added to the ledger by assembling them into a block and attaching a special label derived from the transaction data. Creating the label is deliberately mathematically challenging. There can only be one correct answer, but once solved the answer is easy to verify. The maths also links each block to the preceding block (hence 'blockchain'). The tiniest change in any information within any block will alter the label and break the chain.

The first participant to successfully create the label offers it to the rest of the network to check. Each network participant individually broadcasts their agreement to the network and consensus is reached. The transactions within the block are now confirmed as legitimate and authorised and the process begins again.

This replaces a system of independently developed, maintained and operated ledgers, clearing houses, complex message protocols and post transaction reconciliation, which are currently required to create a consistent record of transactions.

RBS™



(Figure 1: blockchain is a new model for recording transactions)

Blockchain has the potential to disrupt traditional business models by removing the need for complex reconciliations or trusted third parties

Blockchain offers a radically different approach to recording transactions in a way that is verified, immutable and accessible by all parties. It challenges established ways of recording and transferring value, providing efficiency and cost benefits.

All parties in the network derive their position from a single source of information. The costs of developing, maintaining and operating multiple proprietary systems are removed.

What is the potential impact of blockchain technology?

Blockchain has potential applications (and impacts) across industries, and within individual organisations

Not every instance of the blockchain is public (fully open and uncontrolled network), as is the case with bitcoin. It can work where there is an organisational requirement for a read only network (can be viewed but not amended) and private ledgers (access, read and write permissions are more tightly controlled).

There are several reported examples of blockchain exploration across industry and government. Examples such as voting, asset registers, company registrations, gambling, FX settlement, cross border payments and land registry are all being explored.

The first public applications of blockchain have been in payments and cryptocurrencies

The cryptocurrency known as Bitcoin was the first public application of blockchain technology. It was designed to provide a form of digital cash or bearer asset, resistant to censorship and external control.

Bitcoin and similar cryptocurrencies represent an alternative form of value transfer that is disrupting some aspects of traditional payments business by providing more choice in areas such as e-commerce and international remittance.

Cryptocurrencies claim to offer lower merchant processing fees than card-based alternatives and remove the risk of subsequent recharges. Significant merchants now offer Bitcoin payment including Microsoft, Dell and Expedia.

At this point, the overall adoption of cryptocurrency remains low due to the complexity levels for average users and confidence levels in the volatile, unregulated systems.

Attention is now firmly focused on using blockchain to establish 'smart contracts' (e.g. house buying, creation of wills etc.) offering an alternative to legal intermediaries

The same blockchain techniques offer many potential applications beyond payments. Blockchain technology is being developed to create smart contracts. This opens up the prospect of alternative use cases such as living

wills, house deeds, debt management, security assignation and voting systems.

These alternatives extend the basic transaction recording with business logic allowing agreements between parties to also be recorded. In smart contracts, a shared piece of code would represent the agreement between the parties with execution of the contract taking place on the ledger.

A smart contract sets out specific events and or conditions that must be met and once satisfied it immediately executes the agreed next steps. This could result in some legal and financial processes being removed or simplified such as the process of checking conditions and the invocation of next steps. For example, in the mortgage process smart contracts could automate property valuation; execute the transfer and updating of title deeds and release funds.

The blockchain start-up Ethereum is one example of this increasingly active area of innovation. It provides a platform upon which such smart contracts can be developed. Ethereum claims that anything that can be mathematically represented can be modelled, secured and traded. This is an active area of innovation and a range of blockchain start ups are gaining traction in this space such as Symbiont, ERIS, Clearmatics and Digital Asset Holdings.

This area is still being explored and there are reservations around holding legal agreements in code and whether they would be upheld if challenged.

What does the path to maturity look like, what has been the response across industries to date?

Blockchain is an 'emerging technology' that is yet to be tested at scale

The transaction volumes being processed by networks such as Bitcoin are tiny compared to the volumes processed by traditional players such as the banks and card schemes.

One aspect of scalability is the speed with which transactions can be processed. This is a function of how agreement is reached. The consensus method largely determines the speed with which the blockchain operates and the level of trust imparted by the technology. New models of consensus are emerging as the technology evolves.

Finding 'common cause' across industry will be key to success and take-up

Many of the potential blockchain benefits can only be realised by industry players working together. Whether blockchain is a threat or an opportunity will depend on the response of market participants. Intermediaries such as clearing houses (banking) and title search firms (real estate) could be threatened making common cause harder to engineer across industries. Nevertheless, there is an opportunity to eliminate costs that exist for many industry players.

Enterprise and industry adoption are also likely to be accompanied by regulatory and legal developments. Although most jurisdictions have reservations over the control of cryptocurrency, recent statements suggest that there is positive interest in blockchain technology from regulators and governments.

In January 2016, Mark Walport (UK Government Chief Scientist) released a report urging the Government to adopt blockchain technology for use cases such as tax collection and passport issuance.

The Bank of England is currently working with the University College of London on the development and control of a digital currency. The currency would be underpinned by blockchain but the Bank of England would hold an encryption key that could be used to control the supply of the digital currency available.

In March 2016, the Estonian eHealth Foundation partnered with Guardtime to deploy a blockchain-based system to secure over one million patient healthcare records.

Overcoming historic negative association with cryptocurrencies

Although the innovative and disruptive potential of blockchain is gaining traction in the media, it still suffers from negative association with cryptocurrencies.

Previous high profile Bitcoin Exchange failures such as Mt Gox and BitStamp, and the historic case of cryptocurrencies being used for illegal purposes on the 'dark web' marketplace known as Silk Road, initially created negative perceptions. It is only now that the importance of distinguishing the technology from the purpose to which it is applied is being recognised.

With financial services at the forefront, several industries are now increasingly exploring 'the art of the possible' with regards to blockchain

Interest in blockchain is rapidly becoming an active area for many industries, attracting significant capital investment and interest in the technology. The financial services industry is leading the way with extensive levels of commitment evidenced in the development of blockchain applications, however momentum is building across other industries.

In financial services, banks are starting to explore blockchain use cases for capital markets (e.g. settlement), consumer banking (e.g. mortgages, P2P lending and credit scoring) and bank processes (e.g. KYC as a shared service, client onboarding and intra-bank settlement).

Not all banks are exploring the technology in isolation. The Distributed Ledger Group consisting of 42 global banks, facilitated by R3, a consulting and venture group with a specialism in this technology is active exploring financial service use cases such as post trade settlement and identity management.

In the insurance industry blockchain is being explored to trace ownership and certify provenance. Allianz, along with blockchain vendor Everledger, is exploring blockchain to track diamonds from mine to retail sale in order to prevent fraud and illegal trading.

Smart contracts use cases are being considered by the music and media industry. For example, a smart contract could be used to add a condition to the transaction which will ensure that a reader will only gain digital access to an article upon receipt of payment. The technology could help in the battle against piracy and could also be used to facilitate royalty payments to artists and writers.

Conclusion

Blockchain is being hyped as having the same disruptive power as the Internet. 2015 brought most of this hype to the attention of several industries, mainly financial services, leading to a raft of press releases announcing areas of exploration.

However, the interest in blockchain hasn't been without concern or criticism. 2016 will be the year that evidence of real use case development will come to the fore, which will be required to negate those who remain to be convinced and for the technology to even be considered for mainstream applications.

April 2016 | RBS82691