Blockchain: An enigma linked to Bitcoin mania or a transformational technology?

By William Ball

When thinking about Blockchain technology, bitcoin is the obvious first thing that comes into one's mind. Seldom does a week go by without some mention of Bitcoin or another so-called cryptocurrency (there are currently over 1300 in existence) in the news, various media outlets or by the average person on the street.

Bitcoin is the most widely recognised of all the cryptocurrencies (digital currencies) and leads the way in terms of market capitalisation, popularity, and sheer amount of users. What a bitcoin (and its rivals) is, can be thought of just as virtual money, used to buy and sell items, as you would in a shop with a five pound note: they are simply a means of exchange. Whereas a central bank stands behind and stabilises traditional currencies, there is no bank, corporation or government acting as a backbone to bitcoin. Cryptocurrencies are a very good way of circumventing capital controls, in countries such as China, and a way to transact in illegal trades.

Bitcoin is not a functional currency. In reality there is no one pricing the goods or services they sell in bitcoins. Any merchant that accepts a cryptocurrency is in fact pricing them in any fiat currency, such as the pound, and then accepting payment in bitcoins. Secondly, the extreme volatility in the price movements means that any cryptocurrency has no real store of value. Ultimately we value an asset based on its future discounted cash flows that it generates and/or its physical value determined by variables such as supply and demand. Unlike a finite asset like gold, the price of a cryptocurrency is determined by how much someone else is prepared to pay for it. Another important distinction is that they are not traded instruments on a regulated exchange, however you can enter into derivative contracts.

What we find interesting is the technology that underpins cryptocurrencies, which is called blockchain. This is a nascent technology, to be used by businesses, that was, according to Wikipedia, originally created in 2008 by an anonymous person or group known as Satoshi Nakamoto. It is a decentralised database and public trusted digital ledger system that can be relied upon as authoritative records. According to the Bank of England "*blockchain is a technology that allows people who don't know each other to trust a shared record of events.*" Information in a blockchain system is a shared and continually reconciled database therefore creating a distributed network of information.

Chart 4: Centralised vs. distributed ledgers

b1.png

Source: Credit Suisse

The concept is to have a single impartial authority that guarantees the security and accuracy of transactions as data is stored across a network rather than a single source. Updates made are permanently recorded on every ledger, so the record transactions cannot be modified retrospectively without alteration of all of the subsequent blocks in the chain, and agreed by participants on a network.

As a 2017 paper by the Center for Global Development describes it: *"Cryptography (encryption) is used to ensure that previously verified data modifications are safe against tampering by any participant or minority of participants, and that no new modifications can be made without detection. As a result, participants can trust the data held on a blockchain without having to know or trust one another and without having to rely on a central authority like a bank, credit card company or government."* Every transaction is visible to all participants on the system, but crucially only those who have permission (via a unique 30-plus character alphanumeric identifier) can amend and update the data on the ledger. Unlike a centralised system, through a central node, communication occurs directly between each node (user) in the block chain. Each block added to the chain is securely hashed (rendering into a digital representation) and stored in the next block, making it virtually tamper proof. Consequently, by design, it makes it incredibly difficult for the data to be hacked or stolen.

Chart 5: Blockchain: the digital ledger in one chart

Increasing attention is being paid to the potential impact of blockchain, but will this justify the hype? Investors have poured billions of dollars into blockchain start-up and ventures, while many companies are making significant investments into this technology. One such example is when four of the European insurance giants (Aegon, Allianz, Munich Re and Swiss Re) formed a joint project to explore this technology in 2016.

This remains a nascent technology that has the potential to profoundly impact a host of industries. We are in the early days of understanding, developing and adopting this technology into a wide-spread commercial setting. Perhaps this explains the range of growth rates and total values for the blockchain market from the consultancy/market intelligence firms. One such firm Netscribes estimates that the market will compound at 42.8% between 2017 and 2022, reaching $14 billion in global revenue. Whereas MarketandMarkets forecast that the market will grow at a 71.5% CAGR over the same period to reach $4.4 billion in revenue. In a couple of decades, blockchain could turn out to be similar to the internet, in regard to its impact, and similarities. Both were born as protocols that were developed to be decentralised and open, and like the internet, blockchain is at its strongest when everyone is using the same network. One word of caution: the public commercial use of the internet may have commenced in 1989, but only truly became a developed technology for mainstream use and as a viable commercial opportunity until over a decade later. From an investor's perspective, in the 1990's there were a plethora of pre-internet and dot.com companies, nevertheless there is only one Amazon and only one Google! Broadly, it is more appropriate to think of blockchain as a transformational technology rather than a disruptor. The successful developers of blockchain technology could well be future disruptors by using this as a foundation to change the way business is done.

The world exists on contracts, transactions and deeds that are defined in legal and economic systems to facilitate the transfer and protection of assets. Technology is evolving at a rapid pace and the world is becoming more digital. There is necessity for the fabric of our economic and legal systems to keep up and adapt to change. An article titled The Truth about Blockchain (2017) in the Harvard Business Review puts the immense potential well:

"*With blockchain, we can imagine a world in which contracts are embedded in digital code and stored in transparent, shared databases, where they are protected from deletion, tampering, and revision. In this world every agreement, every process, every task, and every payment would have a digital record and signature that could be identified, validated, stored, and shared. Intermediaries like lawyers, brokers, and bankers might no longer be necessary. Individuals, organisations, machines, and algorithms would freely transact and interact with one another with little friction.*"

The way blockchain works makes its very applicable to systems that keep static records; from tax and health care records to supply-chains. What industries is blockchain technology most applicable to and who are the early adopters in this nascent technology? Some conceivable examples are:

- Finance and banking: trade settlement and validation of transactions, exchange of documents, digital asset transfer, financial and regulatory reporting, client on-boarding and online verification (i.e. anti-money laundering checks).

- Insurance: fraud reduction, smart contracts that pay-out on an event without the policy holder having to make a claim, effective pricing of car insurance based on actual risk/events and travel insurance only activated at the time of purchase of a ticket.

- Auditing services.

- Public sector: simplification of the management of trusted information (land, health care, tax/social security data and records and digital property ownership).

- Music, video and movies: reduces piracy and benefits the online streaming services and content owners/providers such as the artists, Apple Music, Spotify and NetFlix.

- Manufacturing/logistics: automatic monitoring of prices, delivery times and the automatic negotiation and completion of transactions in real-time.

One industry that has been an early adopter of blockchain technology is shipping. The Danish conglomerate AP Moller-Maersk (world's largest container shipping business) has teamed up with marine insurers (including Amlin and Catlin) to develop a block chain platform to better manage its supply-chain. This would allow all the participants in a vast and complex network of parties to accurately view and monitor data they need to see in real-time at different stages of the supply-chain. Smart contracts **(Chart 6)** would encapsulate a spectrum of variables from temperatures/weather changes to cargo inspections, docking and haulage, seamlessly in real-time on a trusted and verified network. Whilst the pool of data within the network would reside with Maersk, it will also be incorporated in a digital (smart) contract for each relevant participant. Maersk is looking at this technology as an effective way to cut costs and reduce cyber risk. The insurers can also cut costs as it would remove the dependency on paper-based

administration and contracts whilst enabling more efficient and effective pricing.

AP Moller-Maersk has not just stopped there, and has recently announced a joint venture with IBM to develop the platform. The aim is to make company supply-chains more efficient and safer and in the process make their platform the standard for global trade. Multinational companies such as P&G, DuPont and General Motors are already involved or interested in the platform.

Chart 6: Using blockchain for smart contacts

Source: Deloitte University Press, DUPress.com

Whilst we share many people's enthusiasm for the exciting possibilities of this technology, for wider adoption there are a several challenges that need to be overcome:

1. Proof of concept and understanding of the potential limitations of the technology.

2. Regulation and governance keeping pace with technological change.

3. Awareness and learning process: consensus across the network.

4. The trade-off between data security vs. cost: the network is heavily data dependent and therefore secure maintenance of that data may be difficult. The more permissioned writers/participants using the network, the lower the cost to run it.

5. Privacy as every transaction is in the public domain.

6. The integrity of data can be prone to being compromised; for example banks are attempting to create a permissioned network where certain administrators have greater power to modify transactions at their will.

7. Vulnerability of networks at an early stage: a hashrate attack where anyone who controls 51% of the networks computing power can hack the chain.

8. The need for a database, shared write access and anonymous writers to verify.

9. Scalability: strong enough computing power to handle and verify mass amounts of transaction data.

10. Immutability: prone to human error.

11. Trust transferred to an anonymous writer: integrity and quality of input data must be high.