Market Insight

Blockchain – Disruptive or not?

London 27 June 2016, by Arjan van Bussel

The promise of blockchain, the technology behind Bitcoin, is to make financial services more efficient and secure. Clever coding and sophisticated cryptography are said to remove the need for middlemen and supervisors to validate transactions. Will blockchain-enabled Fintech start-ups indeed disrupt the financial services industry, or is a more collaborative approach more likely?

In God we trust, all others pay crypto-cash

Money requires trust – trust in central banks, governments, commercial banks and the companies registering and settling financial transactions. Blockchain technology makes this trust redundant, so the story goes. Blockchain technology, according to the Bank of England, "*allows people who don't know each other to trust a shared record of events*." Clever coding and sophisticated cryptography remove the need to have an authoritative, centrally guarded database to validate transactions. The services of banks to facilitate transactions between participants are no longer required.

Instead, distributed ledger technologies such as blockchain allow for participants to trade directly with each other (peer-to-peer) and record such transactions in a decentralised ledger to which all market participants have access all the time. The ledger is updated in real-time, contains the payment history of every transaction and is simultaneously replicated on thousands of computers around the world. Cheating is almost impossible, as it would require rewriting the complete history on all copies of the database saved on all these computers.

Blockchain goes mainstream

In November 2008, Satoshi Nakamoto (almost certainly a pseudonym[1]) launched Bitcoin, the crypto-currency. In the eyes of many, however, the key innovation was not the introduction of the digital currency but the development of the distributed ledger, which allows a payment system to operate in an entirely decentralised way, without intermediaries such as banks.[2] Since then, many investors and Fintech start-ups (and also banks defending their turf and looking for ways to reduce overhead costs) have been pouring money into various initiatives with the aim of monetising the seemingly limitless opportunities offered by blockchain technology.

[1] After years of speculation as to the identity of Sakamoto, Australian Craig Wright recently identified himself as the Bitcoin creator, but has backtracked on his pledge to provide proof, leaving his claim still subject to controversy.

[2] Please refer to the appendix for a more detailed description of Bitcoin and blockchain technologies.

According to Goldman Sachs, more than USD 482 million of venture capital was invested in blockchain initiatives during the first 11 months of 2015. Eye-catching initiatives include:

- *R3CEV* – a consortium of 43 global banks and Microsoft, aimed at establishing standards and protocols for blockchain activities.
- *Nasdaq Linq* – a blockchain-enabled Nasdaq platform to facilitate issuances and transfers of shares of privately held companies.
- *Abra* – blockchain for international money transfers. Abra recently raised USD 12 million from American Express and others.
- *Chain.com* – Visa, Nasdaq and Citi invested USD 30 million in the development of this blockchain share trading platform.

Blockchain applications go well beyond the financial market. *ADEPT* is an IBM and Samsung initiative that aims to merge blockchain with the 'Internet of Things' and *Everledger* is working on a blockchain register for diamond certifications and transactions history. The country Estonia announced a partnership with a private party to secure over 1 million patient healthcare records in the blockchain, and Honduras is testing the use of blockchain for land registration.

All these examples illustrate that blockchain is no longer the exclusive domain of tech-savvy early adopters; large global financial institutions, corporates and governments are increasingly embracing the new technology as well.

Three other recent developments highlight that especially in the financial services industry the blockchain is going mainstream. Firstly, in December 2015, the US Securities and Exchange Commission approved the use of the blockchain as a share ownership register for online retailer Overstock.com. Secondly, Goldman Sachs recently applied for a patent on a settlement system for trading shares, bonds and other assets that would employ its own cryptographic currency, the SETLcoin. Finally, JP Morgan Chase has tested blockchain technology for currency clearing and settlement for 2,200 clients transferring US dollars between London and Tokyo. The same bank was also involved in similar tests for credit default swaps, replicating, according to The Wall Street Journal, a month's worth of trades in the single-name credit default swap market. The test also included Bank of America, Credit Suisse, Citigroup and Markit.

Given the scale and high frequency of transactions processed, the financial services industry indeed seems to be the market where for blockchain the stakes are high: In June 2016, Santander issued a report stating "*that distributed ledger technology could reduce banks' infrastructure costs attributable to cross-border payments, securities trading and regulatory compliance by between USD 15-20 billion per annum by 2022.*"

Benefits and roadblocks

The benefits of blockchain technology are well documented. They include the peer-to-peer transaction enabling via the decentralised and wide distribution of time-stamped ledgers, the broad applicability in the financial services industry and beyond, and the possibility to programme and incorporate '*smart contracts*' that will only be executed if certain conditions have been met. Smart contracts can facilitate payment of interest, principal or dividends, and also allow for margin calls to be automatically executed by and registered in the blockchain.

However, there are also drawbacks such as the enormous use of energy to run a large, sophisticated blockchain: one single Bitcoin transaction uses the same amount of energy as an average American household per day.

Setting aside energy requirements, blockchain-enabled platforms are also currently not able to

deal with the large volumes traded on global capital markets. For blockchain-enabled platforms to become a real alternative, they would not only have to become scalable but also embed functionalities offered by current systems. For example, in addition to settling transactions and maintaining databases, a platform will have to offer post-trade functions and the control environment needed by banks.

The blockchain, rather than Bitcoin, is widely seen as the more ingenious invention of the two. However, it is difficult to see how one can operate without the other. '*Miners*', as described in the Appendix, keep the blockchain secure. For this they receive Bitcoins. Without the crypto-currency they would not be incentivised to perform this service. But Bitcoin has its own set of challenges and has failed to address these, according to many. On 14 January 2016, Mike Hearn, one of its most well-known developers, declared Bitcoin a failure and disclosed that he had sold all of his Bitcoins. According to The Washington Post, the price of Bitcoin fell 10 percent in a single day in reaction to that news. Bitcoin's challenges include:

- The increasing concentration of 'miners' jeopardises security – Mining capacity has been accumulated by a limited number of Chinese parties who could rewrite ledgers if they control over 50% of all mining capacity.
- Currently operating at near-full capacity complicates further growth – Current miners are accused of hijacking the Bitcoin network by not allowing it to grow further.
- Lack of speed – The Bitcoin network can only support 3 to 7 transactions per second and it takes 10 minutes to commit to a transaction.

Within the Bitcoin developers community there is much discord about how to tackle these issues. Most of these Bitcoin-issues seem to be solvable in the medium to long-term, but for the time being they form a weak-link in the blockchain.

Another drawback of blockchain-enabled systems is the leakage of information. In today's market, investors use brokers to trade securities, providing anonymity to investors who typically do not want others to know that they are accumulating or unwinding positions. However, at the heart of any blockchain application is a decentralised ledger accessible by everybody.[3] Even though investors would not be known by name but by a pseudonym identifier, their long or short trading behaviours will be visible to everyone. The visibility could trigger a response by other participants that might offset the profitability for the initial investor, who might therefore refrain from investing in the first place, thereby reducing liquidity and market efficiency.

The pseudonymity itself is a problem too. In the blockchain, there are no regulated entities tasked with verifying the sources or uses of money, the appropriateness and suitability of the financial products being bought and sold, or checking whether participants are subject to sanctions or criminal or tax investigations. Platforms that do not provide safeguards for compliance with laws, rules and regulations will not be accepted by professional counterparties, and will therefore not be scalable. Instead blockchain-entrepreneurs will need to ensure that their business models and systems are compatible with the standards all professional financial institutions are required to meet.

We are of the opinion that the most prominent drawback of any blockchain application is indeed that very lack of governance and the absence of a legislative and regulatory framework. The roots of the blockchain technology are in the anarchic world of virtual currencies that operate outside the conventional financial system. Ironically, this is also its Achilles heel. Unless blockchain

[3] An exception would be restricted ledgers that are closed systems whose members are identified and accountable entities.

applications choose to operate within existing regulatory structures, their role in the financial services industry will be limited to a role on the fringes. In the words of the ECB: "*The characteristics of blockchain technology that were so important for the purposes of the Bitcoin network – pseudonymity of market participants, immunity from supervisors, copies of the ledger being accessible to anybody all over the world, and irreversibility of unlawful transactions – are not relevant to the financial industry. Market players instead need a system that is compatible with the standards they are required to meet – implementation of know-your-customer (KYC) rules, transparency and accountability vis-à-vis regulators, respect of the rule of law and confidentiality of trading strategies – and that is relatively cheap to maintain*."[4]

Blockchain applications that aspire to a meaningful role in the financial markets will have to subject themselves to centralised regulatory frameworks. Even though this might run counter to the believes of blockchain pioneers, we believe that this will accelerate acceptance by the financial community as it will allow financial institutions to embrace the numerous possibilities, mitigate the 'fear of the unknown', and improve governance and therefore provide a framework against unlawful or unethical uses and resilience against crises.

Conclusion: Enabling, not disrupting

Blockchain technology has the potential to fundamentally change the cost structure and operational processes in the financial services industry. But in our view the potential shake up will not come from start-up Fintech disruptors taking on established financial institutions. Concerns regarding scalability, security and particularly the lack of governance would make this an unsustainable business model. Instead, blockchain technology is more likely to transform the industry from the inside, by increasing efficiency, decreasing transaction times, lowering transaction costs, improving straight-through processing, and minimising fraud. Recognising that IT efficiency is critical to their competitive position[5] and the far-reaching impact that blockchain technology could have in this respect, banks are rapidly teaming up with Fintech partners. Such collaboration is also favourable to blockchain start-ups as banks offer the client access necessary to quickly scale-up, a reputation for trustworthiness, and, importantly, a well-established, and institutionalised regulatory compliance environment.

If you agree with our views in this Market Insight, and even if you don't, we would be delighted to hear from you (info@bishopsfieldcapital.com).

[4] ECB, "*Distributed ledger technologies in securities post-trading*", April 2016

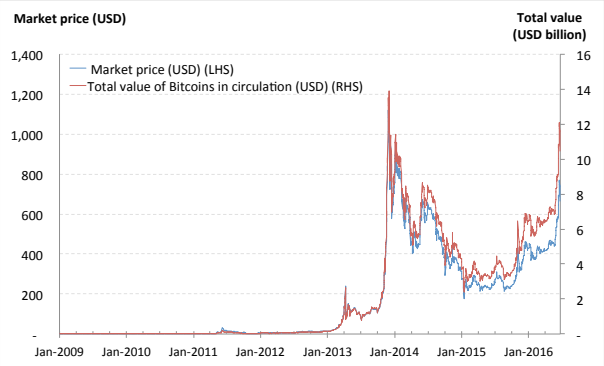
[5] In 2015 IT staff made up 22% of bank employees in the Netherlands (up from 12% in 2010) according to KPMG's Banking Systems Survey 2015/2016

Appendix – Bitcoin and the blockchain explained

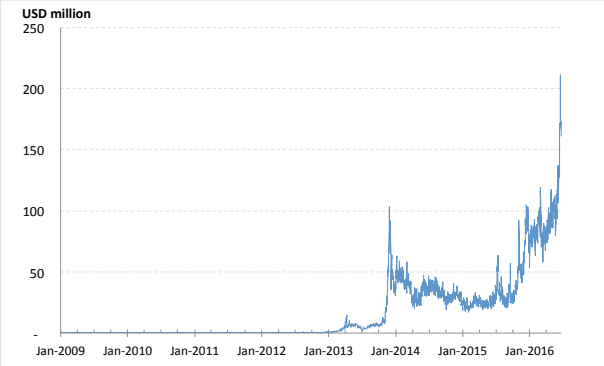
Bitcoin was launched in November 2008 and remains the most wide-spread internet-based currency. More than fifteen million Bitcoins, with an aggregated value in excess of USD 10 billion, are currently in circulation. So far this calendar year, between 123 thousand and 282 thousand Bitcoin transactions have been executed each day. This corresponds with a daily turnover between USD 53 million and USD 211 million. See Exhibit 1.

Exhibit 1: Market size

Market price and market cap



Value of transactions per day



Source: www.blockchain.inf

The blockchain enables Bitcoin owners to pay digital cash directly to one another without needing a financial institution to facilitate the payment. Moreover, it ensures that an owner cannot spend the same Bitcoin twice, and it removes the need of a centrally stored ledger maintained by a trusted third party. This is how it works:

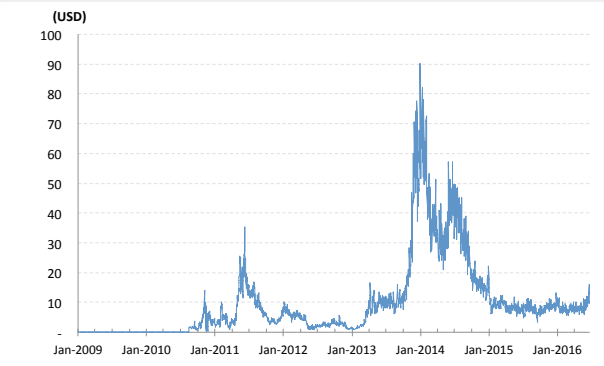
People can open an electronic wallet online and start filling it with Bitcoins by accepting them as payment for goods or services. Additionally, users can buy Bitcoins directly from an exchange with their bank account. Having opened an electronic wallet and acquired Bitcoins, participants can spend Bitcoins by making payments to other Bitcoin users around the world. Every 10 minutes, all payment instructions are gathered in a 'block' ready to be bolted-on to preceding blocks, creating a chain. However, before a block can be added to the chain it must be verified. This is done by turning the block into a complex mathematical formula that embeds the characteristics of the payment instructions in the block but also refers to preceding blocks, thereby permanently time-stamping the chain and preventing anyone from altering the ledger. The cryptographic formula can only be solved by trial and error. The first computer in the global Bitcoin network to solve the problem will communicate the solution to the other computers in the network. These other computers verify the solution and if sufficient computers approve, the payments are made and the block is added to the chain. The new blockchain is subsequently replicated on thousands of computers around the world, visible to everybody. It is this blockchain that replaces the trusted third-party in traditional banking

systems. The blockchain ledger not only shows, in pseudonyms, who owns how many Bitcoins at this very moment, but it also provides proof of who owned what at any given point in time.

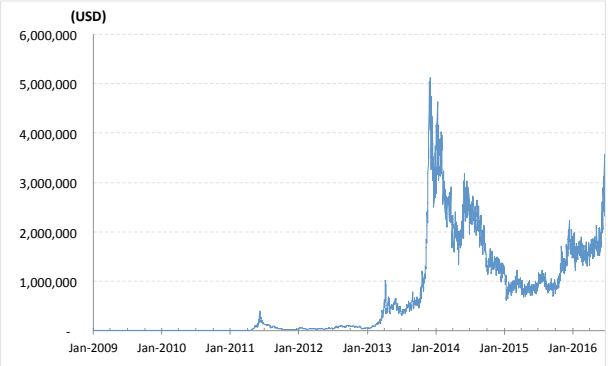
To incentivise people to make computing power available, the computer (in Bitcoin jargon called a 'miner') that found the solution receives 25 new Bitcoins, which on 21 June 2016 equated to USD 16,650, for its services. These transaction costs have fluctuated significantly in the past. But as shown in Exhibit 2, more recently, the costs have stabilised at a level of around 8 to 10 US dollars per transaction. These transactions costs form the revenues for the owners of the 'mining' computers.

Exhibit 2: Costs

Costs per transactions



Daily mining revenues



Source: www.blockchain.info

The right hand graph in Exhibit 2 shows historic mining revenues. With daily revenues fluctuating between 1.5 and 3 million US dollars this is no longer the domain of the lone computer whiz. Most mining power today is provided by large groups of miners pooling together their computing power to increase their chance of wining the reward. Mining Bitcoins requires very large computing power and is therefore very energy intensive, which is why pools are concentrated in countries where energy is cheap, such as China. This consolidation jeopardises Bitcoin's existence: Any pool that controls more than half of the network's computing power can rewrite the history captured in the blockchain. Such a '51% attack' was up until recently considered practically impossible, but with more and more computing power being concentrated (and consolidated) in countries where electricity is cheap this is a threat that can no longer be ignored.[6]

China is often mentioned as one of the countries in which Bitcoin's computing power is being amassed. In addition to geo-political risks this has the material adverse effect of China's great firewall slowing down the Bitcoin network. And speed is of the essence if Bitcoin wants to disrupt established financial service providers: The Bitcoin network is said to be able to handle 7 payments per second, whereas Visa is able to handle 56,582 transactions per second if needed.

[6] According to The Economist one of such pools (called GHash.IO) had in June 2014 "*the bitcoin community running scared by briefly touching that level before some users voluntarily switched to other pools*."