kynetix

7 Ways Blockchain Technology Could Disrupt The Post-Trade Ecosystem

Kynetix White Paper

Written by:

Paul Smyth, CEO

THERE IS DISRUPTION IN THE AIR

Over the last year we've seen a significant rise in interest, comment and speculation about two key technologies – *bitcoin* and *blockchain*. So much so that most of the major banks, and exchanges such as the LME, ICE, CME and NASDAQ, have launched initiatives to investigate how they can leverage these platforms.

Why are they investing in this research? What is it that these technologies offer that we haven't been able to do before? Why are major industry participants such as BNP Paribas saying publicly[1] that blockchain technology could make existing securities industry players redundant? Why do NASDAQ believe it will effect a fundamental change in the infrastructure of the financial services industry?

Hardly a day goes by now where there isn't some commentary about bitcoin and blockchain in the press. Even the BBC saw fit to include a piece on it in a Newsnight program[2].

The Bank of England have recognised the technology's potential saying that it is a "*significant innovation*" and that it could have "*far-reaching implications*."

In the words of Blythe Masters, the former head of global commodities at JP Morgan Chase & Co.

> *"How seriously should you take this? I would take it about as seriously as you should have taken the concept of the internet in the early 1990's. It's a big deal. And it is going to change the way that our financial world operates".*

So let's examine why this could be one of the most disruptive technologies to emerge since the spread of the internet.

WHAT ARE THESE TECHNOLOGIES?

Before we look at the reasons why these technologies could be so disruptive, let's first establish a set of definitions so that we can have a common understanding of them.

[1] BNP Paribas Quintessence http://bit.ly/1PiiLqL

[2] BBC Newsnight clip http://bit.ly/1UAjkzg

There are three key components that we will refer to:

1. **Bitcoin** (with a capital 'B') is a peer-to-peer network that allows for the proof and transfer of ownership without the need for a trusted third party.
2. **bitcoin** (with a lower-case 'b') is the unit of the Bitcoin network. Most references to bitcoin today refer to the crypto-currency but a bitcoin can also be used to reference other assets, both electronic and physical.
3. A **blockchain** is a distributed transaction database (ledger) shared by all computers (nodes) participating in a system based on the Bitcoin protocol. A full copy of a blockchain contains every transaction ever executed on it and is hardened against tampering and revision. A good way to think of the blockchain is as the 'rails' on which bitcoins are transferred.

Of these three technologies it is blockchain that is arousing the most interest in financial circles. It is what makes Bitcoin tick: Its unalterable (and transparent) record of all transactions in the chain makes it the potential foundation of many other applications.

To quote the Financial Times:

"At heart blockchain is a system that allows people that don't trust each other to trust each other".

Next we'll look at what how blockchains are secured and the different types of blockchain.

BLOCKCHAIN SECURITY

The core principle of the blockchain is the decentralised ledger. Unlike other currencies and payment networks, bitcoin is not controlled by a bank, government, or other financial institution. Instead, thousands and thousands of computers around the world (called "miners") independently verify and confirm transactions and manage every transfer on the network. This ledger can be accessed online by anyone.

Crucially, while records can be added to the ledger, no existing transactions can be changed or removed. It's a permanent record that cannot be corrupted. The ledger essentially creates an audit trail which removes the possibility for fraud, theft or compromising of sensitive data.

Once confirmed, each block on the blockchain is encrypted by a system of hashes[3]. Each new block begins by using the hash of the previous block to generate a new hash. Thus a chain is created. Because each block's hash is used to help produce the hash of the next block in the chain, any tampering with a block would also make the subsequent block's hash wrong too and the transaction would therefore be rejected.

Ownership of bitcoins is established through a private key. Every bitcoin address has a matching private key, which is saved in the wallet file of the person who owns the balance. The private key is mathematically related to the bitcoin address, and is designed so that the bitcoin address can be calculated from the private key, but importantly, the same cannot be done in reverse.

Even if somebody did get access to another person's private key they could only spend that person's bitcoins. They could not compromise the network. To attack the network they would need more than 50% of the computing power on the network to take control of it. This would require colossal computing power and speed. At current network mining difficulty levels, not even large-scale governments could easily mount a 51% attack.

Even if an attack on the network occurred and one entity took control they couldn't reverse transactions from long ago, create new coins out of thin air (except through regular mining), or steal coins from other people's wallets.

Permissionless versus Permissioned blockchains

The bitcoin blockchain is referred to as a "permissionless" model i.e. as a miner there is no requirement for you to have had a previous relationship with the ledger, and your vote does not depend on having a prior identity of any kind within the ledger. Miners compete to earn bitcoins for confirming transactions, and writing them into the ledger.

In a permissioned blockchain transactions are validated and processed by those who are already recognised by the ledger i.e. they have been authorised in advance and their identity is known. Their vote counts proportionally against everyone else's, based on the specific rules of the ledger.

There is much debate about whether permissioned blockchains are true blockchains. The purists believe that you cannot have a true blockchain without the bitcoin permissionless model which incentivises miners to do the verification work.

However, there is another camp of blockchain advocates who believe that a permissioned model is essential to meet the needs of a number of industry sectors.

[3] Hashing is a method of taking data, encrypting it, and creating unpredictable, irreversible output making it secure from tampering.

In particular, in the financial service sector, compliance regulations don't allow for anonymity in transactions. So a permissionless model would present challenges to financial institutions for know-your-client (KYC) and money laundering obligations amongst other things.

Those supporting the permissioned model believe that that the bitcoin enthusiasts don't fully understand how settlement and title transfer work within the highly regulated finance sector, in particular the need to identify people. Conversely, the bitcoin enthusiasts believe that the financial services sector is antiquated in its processes.

Public versus Private versus Consortium blockchains

A public blockchain has a fully de-centralised ledger and is open to everybody. It is permissionless as there is no requirement to have a prior relationship with the blockchain to be able to take part in it. The bitcoin blockchain is one of a number of public blockchains.

A private blockchain on the other hand has a centralised ledger under the control of one organisation. Access to the blockchain is controlled by the organisation and may be completely restricted within the organisation or may allow limited public access. As such, it is a permissioned blockchain.

A consortium blockchain is one where a number of permissioned organisations have access to the blockchain. The consensus process, required to verify and confirm transactions, is written into the rules of the ledger. Read access to the blockchain can be public or restricted to the consortium participants. Examples of a consortium blockchain could be an exchange and its members, an insurance company and its brokers etc.

Now let's now look at the ways in which blockchain technology could disrupt the post-trade ecosystem.

1. Lower operational costs and risk

Use of blockchain technology can modernise, streamline and secure cumbersome administrative functions, eliminate errors and lower operational costs and associated risks.

In today's post-trade environment market participants have to maintain a whole range of interfaces and reconciliation procedures. Every step of the clearing and settlement process is loaded with cost and complexity.

With a centralised ledger that publicly records the movement of every asset, along with proof of ownership and the authenticity of assets protected by a coded secure cryptographic framework and with confirmations of new trades identifiable by a unique crypto stamp, there is a significant reduction in manual processes.

It's not hard to see how a single, trusted, ledger would reduce costs and would remove the need for duplicated reconciliation processes as well as reducing the number of interfaces that need to be maintained.

Some people envision a world with no middle or back-office, and no registry, which would clearly have a major impact on costs.

Ultimately, this could lead to a large number of 'back-office' roles common in today's banks becoming extinct.

To illustrate the potential savings that blockchain technology could bring a recent report[4] co-authored by Santander estimated that it could reduce banks' infrastructure costs by up to $20 billion (£12.8 billion) a year.

2. Reduced regulatory reporting

The bitcoin blockchain already has a publicly available record of all holdings and transactions so anybody could audit the blockchain.

In private or consortium blockchains it would be a relatively simple process to give read access to the regulators to a comprehensive audit trail that allows any movement of assets to be traced back to their origin which could enable organisations to meet regulatory reporting obligations in a more efficient way.

Obviously there are regulatory and legal hurdles to overcome to get to this point but the potential is obvious.

3. Instantaneous confirmation and settlement

Shortening settlement times for trading would reduce the risk that counterparties would not be paid, while also cutting the amount of collateral used to back trades. Collateral would also move around the system quicker. (Of course a potential downside to faster settlement is that investors may have to pay for some trades far earlier than they have become accustomed to).

[4] Rebooting Financial Services http://bit.ly/1ShMHFg

Bob Greifeld, CEO of NASDAQ had this to say on the topic:

> *"I am a big believer in the ability of blockchain technology to effect fundamental change in the infrastructure of the financial services industry. Clearing houses are a wonderful invention, but if you have a public ledger that is trusted, you can evolve back to a bilateral (trading) world but proceed with instantaneous settlement. We currently settle at T+3. Why not settle in 5-10 minutes?"*

This of course raises other issues about the trading value-chain. If a blockchain can replicate a settlement and custody infrastructure at lower costs then ownership could be transferred without the need for expensive intermediaries. Which conveniently leads us to our next point.

4. Disintermediation of the market

If properly implemented across financial services blockchain would eliminate much of the slow and expensive post-trade and clearing ecosystem. When this happens it would also remove the need for much of the market intermediary structure.

Some intermediaries are more at risk than others. These include the CSD, sub-custody or prime broker sectors. As an example, because the blockchain would hold the registration details of each trade, there would no longer be a need to distinguish between custodian, CSD and registrar.

As mentioned earlier, NASDAQ envision a world where clearing houses can be by-passed. Using a concept called "smart contracts" (computer protocols that verify or enforce contracts) intermediation between buyer and seller would be eliminated. This leads us nicely to our next point.

5. Transformation of Delivery versus Payment

The majority of financial assets – such as bonds, stocks, loans, and derivatives– only exist in electronic form, which means that the financial system itself is already simply a set of digital records.

With bi-lateral trading in place then simultaneous exchange of assets, or transfer of title, can occur with peer-to-peer Payment-versus-Payment (FX) or Delivery-versus-Payment (Securities Settlement).

With no clearing house involved the challenge of delivery versus payment (DVP) could become a frictionless process.

In the physical world, commodities for example, DVP might be addressed using multi-signature escrow. This would enable additional trusted parties (e.g. a warehouse keeper) to confirm delivery of goods thereby triggering verification of a transaction.

As a side note here, there are other initiatives involving the Internet of Things (IoT) that will enable better monitoring and tracking of goods that could also help automate DVP. Smart sensors will monitor the condition of goods and will track their location via GPS. In due course data from these sensors are likely to become part of a smart contract linked to a blockchain.

6. Lower risk of fraud

In China in 2014 the Qingdao port scandal rocked the world of commodity financing. It was discovered that some firms had been using fake receipts to obtain multiple loans against a single cargo of metal at the port. This is the classic double-spend problem recognised by the Bitcoin network.

Whilst double-spending a bitcoin is theoretically possible it is extremely difficult to achieve and to cover it up. There are far more counterfeit currency notes in circulation for example than instances of successful double-spending of bitcoins.

Because of the blockchain's distributed consensus approach, in which multiple copies of a shared single ledger are constantly evaluated to prevent fraud or error from entering, there is a high degree of security built in.

The Qingdao port scandal might never have happened if the financing of metal had been operated through a distributed ledger.

7. Easier access to trade finance

Blockchain technology and bitcoin will not only change the way we do payments it will also lower the costs of finance and ultimately should increase market liquidity.

Currently cross-border payments remain slow and expensive. Using bitcoins (or other digital currency) significant savings can be made by banks and end-users by bypassing existing international payment networks.

Blockchain technology could be used to digitise and authenticate the paper-intensive Letters of Credit process thereby saving both money and time whilst providing secure access to the various participants in the trade transaction.

Furthermore, lenders are more likely to lend in a secure trusted environment. The Qingdao port scandal in China led many banks to re-evaluate the risks they face and has resulted in higher interest rates and a reduced appetite for collateral financing.

With a distributed trust system based on blockchain technology the risks of fraud are mitigated. This should free up capital and lead to easier access to finance, lower interest rates and ultimately greater liquidity.

SUMMARY

The first thing to say is that the whole blockchain landscape is changing rapidly right now. As mentioned at the top of this paper most of the major financial institutions have initiated pilot projects to investigate how blockchain technology can be applied in their businesses.

Whilst bitcoin is a proven and tested example of blockchain usage, examples of its use in financial services are very thin on the ground. Most of the work being done today is still at the prototyping stage.

We are seeing huge amounts of venture capital being poured into this area. We are also seeing an explosion of vendors moving into the space. Some of these vendors are focussed on using the Bitcoin network while other are focussed on creating permissioned distributed ledgers to deal with the regulatory and latency challenges we face in financial services.

Technology is only one part of the equation. The legal and regulatory hurdles that have to be overcome will also affect the adoption rate of blockchain technology, particularly for permissionless blockchains.

One shouldn't overlook the political implications that might also come to the fore. Some jurisdictions might seek to introduce restrictive legislation preventing the disintermediation of their market infrastructures.

Our view at this stage is that major financial institutions will probably begin by running private or consortium blockchains until the legal and regulatory landscape is clearer and they have trust in permissionless blockchains.

The buzz around blockchain feels like the buzz we experienced in the mid-90s as the Internet began to be commercialised. There was lots of hype and lots of predictions at how it would change the world. They were right that it would change the world but many (if not most) of the predictions were wrong about exactly what the changes would be.

What we actually saw was a whole new raft of companies emerge that grabbed huge market share and threatened established players e.g. Amazon, eBay, Alibaba etc. We've seen the music and film/TV industries disrupted by Napster, Apple, Netflix etc. In 1995 nobody could have foreseen the effect that internet-connected smartphones would have on our daily lives.

One thing we can be reasonably certain about is that blockchain technology in some form is going to cause significant disruption.

The post-trade ecosystem is in the line of sight for much of this disruption. If you operate in this space then you really should be taking action now to understand how this technology could benefit your business.

HOW WE CAN HELP

Kynetix are global leaders in technology solutions that unlock the physical economy. Working exclusively within the commodities sector has allowed us to grow a deep understanding of the challenges and risks faced by our clients. In particular, we have extensive experience of the post-trade clearing and settlement processes.

With our industry knowledge, our deep technical skills and our agile approach we can help you evaluate blockchain technology so that you can make decisions on how to best implement it in your business.

If you'd like to find out more then please call us on 020 7836 1800.

_____

About the author

Paul Smyth is CEO of fintech specialist Kynetix. He can be contacted at *Paul.Smyth@kynetix.com*.

Kynetix is the City's leading provider of software solutions for the physical economy. For 20 years we've been delivering solutions to our clients providing them with the bedrock for growth, flexibility and competitiveness. Operating on web, cloud and mobile platforms our solutions are trusted to run mission critical processes for some of the world's best-known financial institutions.