

## **Holding, clearing and settling securities through blockchain technology**

### **Creating an efficient system by empowering asset owners**

**Eva Micheler and Luke von der Heyde**

#### **Abstract:**

The paper analyses the current system of holding and transferring securities. It argues that the current model makes transactions safe by next to eliminating counter-party risk. This is done at the price of exposing the holding of securities to custody risk. Investors nowadays hold securities through chains of custodians and are exposed to risk of any of these failing. Custody chains also prevent them from exercising and enforcing rights against issuers.

The paper explains why somewhat counter intuitively the introduction of electronic settlement has led to an intermediated holding system which has significantly increased custody risk particularly in the UK.

The paper then argues that blockchain technology would make it possible to create a system that has the same level of transactional safety as the current system and that at the same time eliminates custody risk.

Existing custodians however are unlikely to bring about change that creates a system that is overall efficient. They are limited by their current business model. They are unable to fund the elimination of inefficiencies of the system as a whole when the elements that cause system-inefficiencies are factors that underpin their business model from their individual perspective.

The paper recommends empowering asset owners by requiring custodians to disclose that they have outsourced custody. Custodians should also make available to their customers details about the sub-custodians they have delegated custody to enabling investors to evaluate the chain that operates between them and the issuer. This will enable asset owners to evaluate the risk associated with the custody arrangements that are on offer.

The paper also encourages asset owners with market power to ask questions about the way in which the assets they look after are held. In addition to engaging with custodians, regulators should actively involve asset owners in their work on blockchain technology.

#### **Technology in Financial Markets**

Technology changes society, but sometimes in surprising ways. In the case of securities computers have all but eliminated transaction risk while at the same time introducing custody risk.

When computers were first introduced into financial markets there was a lot of excitement and urgency about replacing paper with electronic settlement. The transformation was not easy however. It took almost 10 years for the electronic settlement system CREST to come live.

Interestingly the reform did not lead to the creation of a new system from scratch that may have reflected the possibilities offered by the technology. As it turned out the system that was created closely resembled the paper settlement and holding system. The existing framework was preserved with the modification that communication by paper was replaced with communication by electronic instructions. The providers of the infrastructure remained in place and their processes were repeated on computers instead of paper ledgers.

The availability of almost instant electronic communication has had an additional and surprising effect. When securities were transferred by way of paper, investors used to have their name entered on the issuer register. It took some time for a transfer to be recorded on the register, but the investor had a direct connection with the issuer. While settlement of trades was cumbersome, it was easy to hold securities and exercise rights arising out of them.

The introduction of uncertificated (electronic) securities changed that balance. Settlement times were reduced allowing the speed of transferring securities to increase, but the holding of securities and the ability of investors to exercise their rights has become significantly more complex and risky.

Investors have become separated from issuers through intermediation. A framework emerged whereby the names of investors were removed from issuer register and replaced by nominees who hold securities on trust for investors or, more likely, other intermediaries.

This has made the enforcement of rights very difficult if not outright impossible. It stands in the way of shareholders exercising voting rights. Investors bear the risk associated with all intermediaries that operate between them and the issuer. Regulators struggle to keep up with increasing levels of intermediation spanning across borders. The introduction of computers has made trading easy, but holding assets more difficult.

Information technology has simplified connections. We speak to each other and send messages in real time and across borders without friction. Yet in relation to financial asset the opposite has happened. Investors have become separated from their assets. This is because computers by making it easier to connect and have also made it easier to intermediate. The ease with which

connections can be made has made it possible for chains of intermediaries to build up in the system.<sup>1</sup>

Intermediation has advantages for service providers. They facilitate innovation. Intermediation enables an innovating service provider to provide a service without having to persuade investors to switch. Through intermediation incumbent service provider can buy that service without making his clients aware of an alternative provider and will do so if it reduces his cost base. Between the two of them this creates an efficient outcome.

I have shown elsewhere that this does not necessarily need to an efficient result from the perspective of the system overall and in particular for investors who bear the cost and risk associated with the overall system.<sup>2</sup> In the case of securities the effect of intermediation has been to erode investor rights. In a direct holding system investors are only exposed to the risk associated with the issuer.

In an intermediated model, in addition to the issuer's risk investors bear the risk of all intermediaries that act between them and the issuer. When Bear Stearns was restructured an excess of 28% of shares compared to the shares issued by the company was discovered. The European Commission writes in the discussion paper justifying the Regulation on Central Securities Depositories that, 'Fortunately, Bear Stearns was rescued through a takeover by JP Morgan which bailed out the excess of securities.'<sup>3</sup> In reality this means, of course, that the price that JP Morgan was prepared to pay was distributed between all indirect investors diluting each of their shares. This is not efficient.

---

<sup>1</sup> A similar development occurred in the relation to payments. Payment providers such as paypal or apple pay have created services that facilitate payment by adding an additional layer to the existing infrastructure.

<sup>2</sup> E Micheler, Custody Chains and Asset Values - Why Crypto-securities are worth contemplating, [2015] CLJ 533; available from [http://eprints.lse.ac.uk/62609/1/Micheler\\_Custody%20chains%20and%20asset%20values.pdf](http://eprints.lse.ac.uk/62609/1/Micheler_Custody%20chains%20and%20asset%20values.pdf)

<sup>3</sup> Commission Staff Working Document Impact Assessment accompanying the document 'Proposal for a Regulation of the European Parliament and of the Council on improving securities settlement in the European Union and on Central Securities Depositories (CSDs) and amending Directive 98/26/EC /\* SWD/2012/0022' - COD 2012/0029 para 8.9. Annex 9.

Investors also encounter problems when attempting to exercise their rights. Issuers may find that a custody chain protects them against claims from issuers,<sup>4</sup> but also experience problems when they need to reach investors to restructure debt. This can delay insolvency proceedings.

A situation has arisen where the economics that operate between intermediaries have created externalities for investors and issuers leading to an overall inefficient system.

## **Blockchain technology**

With blockchain technology a new technology for keeping securities registers and for updating them has become available. The technology has been said to make it possible for trading, clearing and settlement to merge into one real time process that does not involve relationships with multiple intermediaries. There is no need for separate trading, clearing and settlement venues. There is no exposure to the risk of any one central provider failing. Buyer and seller can interact directly with each other. They can exchange securities and cash directly and in real time.

In terms of user interface not much needs to change. Investors would access their portfolio like they are now through a computer or through some other electronic device. But while at present the interface they see is a record kept by an intermediary who is connected to another intermediary who is connected to yet another intermediary, what they see in a distributed ledger/blockchain environment would be the master record.

The same could become true on the money side. At present investors view a balance of an account held by a bank. In the future their view could be of a master record of money held at the central bank. This raises important questions about the role of banks. At present bank deposits fund lending. If individuals stop providing banks with deposits, lending will have to be funded in other ways. But then who says that that is impossible.

This development is exciting. It would reduce complexity and remove intermediary risk from financial markets for both assets and cash. There would still be counter-party risk but with only one (shared and distributed) master record, the risk of double-spending reduce to almost zero by way of blockchain technology, and payment linked to delivery, this appears to be very low.

---

<sup>4</sup> *Secure Capital SA v Credit Suisse AG* [2015] EWHC 388 (Comm).

It looks like blockchain technology could create a world where transaction risk is minimised and intermediary risk is eliminated.

There is, of course, a risk that the computers break down or will be hacked into, but because every node has an identical copy of the ledger that risk has been referred to as very small.

We do not know yet what the technology is capable of, but let us assume for the purpose of this paper, that computer science can deliver an un-intermediated ledger allowing investors to hold and transfer securities and money in real time.

And while we are making assumptions let's also assume that national border can be overcome by technology or perhaps better that the technology is scalable in a way that accommodates the volumes of domestic as well as cross border holdings and transfers.

The question then is, will this happen?

Before we attempt to look into the future it is worth having a quick look at bitcoin for which blockchain technology was invented.

## **Lessons from Bitcoin**

Bitcoin built is an open source un-permissioned blockchain ledger. Anyone can join and maintain the blockchain. Those maintaining the chain are paid by a combination of new coins and fees. Overtime the system will switch over to a fee only reward to those maintaining the chain. The combination of open access and a fee provides an incentive for miners to maintain the ledger. The software is updated by a group of developers on an informal basis taking into account the views of miners.

There is apparently no or rather very little concern that this openness will enable the wrong kind of computer scientist to manipulate the system. The risk of miners manipulating the content of the ledger is low. This is because there is a significant number of them and manipulation would require for anyone of them to have more than half of the computing power available on the system.

Compared to the current system where manipulation could and has occurred in the past at any level of the intermediation chain and could go/has gone undetected for some time Bitcoin's technology promises significant improvement. Slightly tongue in cheek it is worth remembering that Bitcoin's technology has proven remarkably temper resistant in markets that are challenging even compared to financial markets.

Bitcoin's blockchain distributed ledger then provides users with a direct way of holding something that we can, without having to answer the question of what bitcoin are, call a token, but that might as well also be an asset. Bitcoin's ledger enables direct holdings. It operates peer to peer, no intermediaries are required.

The technology can, however, also be used in a way that creates a closed network of permissioned participants who hold assets as intermediaries.

In the context of Bitcoin, for example, an intermediated option has become available. The bitcoin software was not designed to be appealing to users that are spoilt by smartphone technology. Individuals hold bitcoins through wallets. Wallets are a type software that connect to the bitcoin main software.

Bitcoins are transferred by way of a private key. A private key is a series of numbers and letters. To the completely uninitiated it could be referred to as a very long password.

The private key needs to be typed into the Bitcoin software to authorise a transfer of coins. While it appears to be next to impossible to hack into the blockchain software, it is not impossible to lose a private key to theft. It is important to store the key safely. The weakest point of the bitcoin network is the storage of the private key. Reports about theft of bitcoins refer to thefts of private keys. This occurs when a hacker succeeds in extracting a private key from a computer.

Storing the private key only on the hard drive of a computer that is connected to the internet is not a good idea. Neither is destroying your hard drive without first making a note of your private key. Ideally you store it cold, ie in some way that is not connected to the internet. Writing it down and putting it in a safe comes to mind.

Wallet software helps with creating and storing private keys. There is a range of services available. On one end of the spectrum is software that only connects to the bitcoin software and does not look after private keys at all. The wallet holder looks after his private key. This is direct way of holding bitcoin. It is sometimes referred to as non-hosted wallet.

On the other end of the spectrum is an intermediated solution referred to as hosted wallet. Coinbase, for example, is a wallet provider whose customers do not know the private key associated with their coins. Coinbase is a custodian of private keys. They keep wallets for customers. These show bitcoin balances. But they only record claims against Coinbase. Their general terms state that transactions can take up to 48 hours when private keys are sourced from their cold storage facility.

Coinbase also operates an exchange and in that capacity is entitled to settle transactions between customers that both have wallets with Coinbase internally. This is sometimes referred to as a sale 'off blockchain'.

Those who are familiar with securities settlement systems would refer to Coinbase as an intermediated holding and transfer system for bitcoins. MtGox, a bitcoin exchange that is now in insolvent liquidation, also operated custody services for coins and cash. It too established an intermediated model.

Hosted wallets have, however, not gone down well with the bitcoin community. Coinbase have recently been placed on the bottom of a ranking of wallet providers published by an organisation referred to as Open Bitcoin Privacy Project. The reason was their custodianship of customer funds. Interestingly their response was to point out that they view themselves more as a retail exchange rather than a wallet provider.

It remains to be seen if the bitcoin environment will also go down the route of intermediation over time.

## **Looking into the future**

There has been significant interest in and great excitement about blockchain technology. The last few months have seen a number of announcements about making use of blockchain technology

for securities settlement. Major market players are investing in the technology. Here are some themes that emerge from this material.

Euroclear, for example, has published a paper in which they envisage that in the future blockchain technology will underlie the holding and transfer of financial assets. They stress that the very fact that the ledger is distributed means that different providers can be accommodated. This will make it easier for the technology to be adopted. They, however, also point out that there is a risk that the technology will challenge the business model of incumbent custodians.

Michael Mainelli and Alistair Milne have published a survey of participants in the settlement and custody industry. This reveals a variety of interesting points.

One comment is that turkeys are unlikely to vote for Christmas. Interviewees also mention that they are comfortable allowing their clients to hold assets on a disintermediated basis enabling them to form relationships with competitors.

Perhaps the most important outcome of the survey is that business processes are a significant barrier towards any update of technology. The issue is not just demonstrating technical feasibility but rather achieving the necessary co-ordination in the adaptation of the business processes.

Another interesting insight from emerging from this recent material is that real time settlement is possible with current technology. It seems that business processes and legacy systems are responsible for the standard T+2 (London) or T+3 (New York) timeframe. The problem is that trades are made before buyers and sellers have the cash and the securities in place. This is interesting because from the retail end brokers are unlikely to enter into transactions before the money and the securities respectively are in place.<sup>5</sup>

An important outcome of the discussion of blockchain technology for securities has thus been that existing technology does not appear to stand in the way of a more efficient framework. Technology is not the problem.

---

<sup>5</sup> Look up standard terms.



Unsurprisingly then it has been observed that existing projects, as far as is visible at the moment, appear to combine elements of blockchain technology in a way that causes the outcome to revert to the existing framework. There is a significant focus on permissioned systems. This means that the keepers of the ledger are only participants that have received permission, perhaps by a central authority. Once a network is permissioned the question arises if it is necessary to create a blockchain. Does every new transaction really have to be checked against and joined up with all previous transactions? Is it not enough to have trusted participants keep the register? There is also and once again significant focus on transactions, but not much interest in the perspective of investors and their rights.

There are therefore reasons to be pessimistic about the emergence of an overall efficient framework. This also fits with past experience with technological innovation. It has already been mentioned that the changeover from paper to electronic settlement in the UK was fraught with difficulties. The incumbent market participants tried to build a computer system called Taurus and failed. The Bank of England took over and established CREST. Reform took some 10 years. A significant amount of money was spent on a project that had to be abandoned. It is not easy to see through reform if that means disturbing the business model of established service providers.

It has already been mentioned that as far as the UK domestic market is concerned there already exists an un-intermediated infrastructure. It is possible in the UK for investors to have accounts with CREST enabling them to hold uncertificated securities directly at the level of the master record. Notwithstanding the fact that this option has been available, an intermediated model has emerged.

Interestingly the same was historically true for the now intermediated German system. It was for some time possible for individual investors to maintain accounts directly with the German CSD, now Clearstream Banking Frankfurt.

Given the disadvantages associated with intermediated holding structures, it is hard to explain why investors have accepted a framework that causes them significant problems.

Michael Milne has pointed out that technological innovation is subject to a phenomenon entitled 'excess inertia'. This is a form of market failure. An inefficient market infrastructure persists if the cost of change for individual participants is higher than their individual gain. This prevents technological innovation that would reduce the cost for the industry overall.

This explains why it is hard to introduce innovation. It does not explain, however, why a direct paper model has transformed itself into an intermediated electronic model.

It has already been mentioned that intermediation is facilitated by computer technology. What remains to be explained here then is why asset owners appear to have accepted the intermediated model in circumstances where there was a direct alternative. This applies in particular to investment managers some of whom have significant market power.

Here is an attempt to shed light on what might be going on.

One possible explanation for the success of the intermediated model could be price. It is sometimes said that fees associated with direct holdings are higher than fees associated with indirect holdings.

It is true that in a paper environment intermediation saved cost because it reduced the amount of paper that had to be physically moved. This is what explains why intermediation occurred in Germany. This was at a time where there was no electronic alternative. In the UK however, there intermediation coincided with the elimination of paper.

In an electronic environment the cost of maintaining one account should be lower than the cost of maintaining and reconciling several accounts over multiple levels.

What then explains lower prices for intermediated electronic accounts? Intermediaries do more than keep accounts. They normally provide and charge for a bundle of services. Record keeping can, for example, be bundled together with foreign exchange services.

Holding securities can also produce income that enables an intermediary to offer low fees. For example, recent regulatory changes requiring explicit client consent for securities lending can provide evidence for the fact that intermediaries may have benefitted from lending income in the past without clients necessarily understanding that this was the case.<sup>6</sup>

---

<sup>6</sup> Securities lending has, of course, also benefitted from computerisation. The emergence of a framework that allows electronic transfers makes it possible for assets to be moved across markets

Bundling makes it difficult for investors to evaluate the price for an intermediated service.

Statements do not reveal that there is a chain of intermediaries operating between the investor and the issuer. Custody terms enable intermediaries to outsource the holding of securities, but do not show if the power has been exercised and who the holding of securities has been delegated too. They also do not disclose how many intermediaries operate between the client and the issuer.

The combination of bundled services and the lack of transparency about the structure of the chain makes it next to impossible for investors to evaluate the prices offered against the service levels and the associated risk.

### **Facilitating an efficient market – lessons for regulators and asset owners**

From the perspective of regulators it is important to understand what can be done to facilitate the emergence of an efficient infrastructure.

This cannot and should not be done from scratch. It is important to take advantage of the expertise and resources that are available in the existing system. It would however be wrong to forgo the opportunity to improve the efficiency of the existing model by constructing new technology with a view to minimising the disturbance of existing business model. Incumbent service providers are unable to eliminate inefficiencies of the system as a whole when these are efficient from their individual perspective.

Regulators and in particular the European Securities Markets Authority are likely to take a keen interest. The key is to encourage investment in infrastructure that are designed with a view to improving efficiency for those who pay for the infrastructure and bear the risk associated with it.

The cost and the risk of the infrastructure is borne by asset owners. It is important to ensure that asset owners are consulted. That, for example, did not happen in the case of the EU's Legal Certainty Project which was set up to improve the legal framework supporting the market

---

with ease. It also makes it easier for service providers to explore business opportunities inserting themselves into the chain.

infrastructure for the holding and transferring of securities. Advisers to project consisted mainly of experts associated with the custody industry. There were experts without an affiliation to particular custodians, but asset owners were not represented.

At present asset owners only receive statements showing that securities are held for them. It has already been mentioned that general terms permit outsourcing, but do not inform investors if that power has been exercised. Investors are unable to evaluate the risk associated with the services they are offered.

The regulator should enable investors to form a view on the risk associated with and the price offered by the current infrastructure. A straightforward way of achieving this would be way of disclosure. Custodians should be required to disclose to investors that they have outsourced custody. They should not only reveal that custody has been outsourced but also enable investors to evaluate the chain that they are associated with. They should reveal details about the service providers that operate between them and the issuer.

And finally leaving regulators aside the ball is in the court of asset owners some of whom have the muscle to ask questions about how their assets are held. They are also able to involve themselves in the current discussion about how the new technology, if it is to be used, should be implemented.