oxera
compelling economics

Agenda

Advancing economics in business

The debate about blockchain: unclear and unsettled?

Post-trading—the clearing and settlement of securities and money after a trade—has always been considered the dull but necessary part of 'trading and post-trading'. This is about to change. Blockchain technology offers a new way of creating, exchanging and transferring ownership of financial assets, and has captured the attention of the post-trading community in the financial services industry. What is the potential impact of blockchain technology on securities post-trading activities?

Post-trading refers to the transfer of securities and money following an agreement to trade, either over the counter (OTC) or on a trading platform. It has a number of characteristics that potentially allow it to benefit from blockchain technology.[1] This article focuses on the value chain of trading and post-trading services for transactions in equities. This is just one example, however—blockchain can also be applied to other securities such as bonds, derivatives, and asset-backed securities. A simple transfer of a share from investor A to investor B typically involves communication, over a period of up to two days, between various market participants (such as brokers, clearing agents, and local and global custodians) and infrastructure providers (the trading platform, central counterparties—CCPs, and central security depositories—CSDs). During this time, all of these parties will update the records on their own systems and verify that the information that they all hold is consistent and correct. They will then transfer ownership of the share and money between the two investors in accordance with the trade instructions.

Blockchain technology would partially replace all the fragmented systems and information sets managed by individual market participants and infrastructure providers with one logical ledger. Physical copies of this ledger would be distributed to all parties (nodes) involved (hence the alternative term, 'distributed ledger technology'), giving everyone in the value chain simultaneous access to the same (real-time) information set. This could potentially reduce system costs and shorten communication lines. It could also increase resilience, as the failure of one node or a subset of nodes would not affect the integrity of the system, since the blockchain-based system would continue to operate as usual on the basis of the other nodes.

The ledger is protected and kept up to date through a 'consensus' process, whereby new blocks of transactions that have been validated and approved by a majority of the participants are added to the existing chain of previously validated transaction blocks (hence the term 'blockchain').

Unclear and unsettled?

The debate about the application of blockchain technology to post-trading is currently in full swing. Some early reports discussed the potential for the technology in the post-trading space, and provided rough initial estimates of its potential benefits.[2] Later analysis focused on some of the challenges.[3] Most recently, regulatory authorities have set out the potential challenges from a regulatory perspective.[4]

It is not surprising that there are a range of views about blockchain technology. Not only is it a complex technology (perhaps only fully understood by a small number of IT experts who are unlikely to be very familiar with financial services), but post-trading itself also has a complicated value chain involving many players. As a result, for innovation to be successful a degree of coordination is often required (which can be particularly challenging if some players have a lot to gain and others a lot to lose).[5]

The financial services industry can be seen as a pioneer in exploring the uses of blockchain technology and, to some extent, its discussions reflect the more general underlying discussion in the IT community about the pros and cons of blockchain technology over traditional central databases. Central databases have become fast, cost-efficient and reliable, and some of the benefits that blockchain promises to deliver—such as real-time clearing and settlement, and

end-investor (rather than omnibus) accounts—are not unique to it but could also be delivered by these central databases.[6]

Why would we then move to blockchain technology? From a technological perspective, the idea is that blockchain can make ownership transfer between entities simpler, while increasing data security and resilience and decreasing dependency on a single central party. For example, companies that manage traditional central databases usually keep digital information secure by building a 'wall' around the data. Unfortunately, this means that the data is vulnerable to anyone who can find an access point and get inside the wall. Transactions and data in the blockchain ledger are protected and kept up to date through a 'consensus' process, whereby blockchain-based systems do not allow changes to data once it is created unless (almost) all of the participating nodes agree to the change. This is a significant departure from the traditional wall approach, and would decrease the potential for backdoor transactions.

Although it is still subject to debate, there is growing consensus on some aspects of blockchain technology. For example, there is increasing agreement that its application to post-trading would be based on a 'permissioned-based' system, which would be less costly and more manageable that an 'unpermissioned' ledger, such as that used in Bitcoin (see the box).

How could it work in practice?

There are likely to be several options for applying blockchain technology in the post-trading value chain. One model is a permissioned-based system where the nodes can be operated only by existing regulated entities such as trading platforms, CCPs, CSDs, brokers and custodians. These entities would be responsible for operating the distributed system, giving investors access to the post-trading system, and ensuring compliance with existing regulations, such as know your customer (KYC) and anti-money laundering (AML) rules. A version of this model by RISE Financial Technologies is presented in Figure 1 overleaf.[7]

For a practical and gradual adoption, existing financial securities and money would need to be able to flow into and out of the distributed ledger. There may be several options for achieving this interoperability, some of which are already used by financial institutions. For example, it might involve a system similar to global depositary receipts, whereby certificates are issued for shares in a foreign company.

Figure 2 illustrates the steps in the transaction processing. Investors send trade orders to their brokers, which send them on to trading venues for execution. When the orders are matched to form a legally binding obligation, the trading system passes on the trade details to the blockchain-based system for clearing and settlement. Another option would be to first send the trade details to a clearing house for clearing and netting,[8] and then send novated details to the blockchain-based system.

It's not like Bitcoin—we don't need the miners!

Any blockchain-based system entails a verification process for any changes and a consensus model among the nodes, to enable agreement on separately verified changes to the ledger. How costly these processes are depends on the level of trust that can be assumed between the nodes.

By design, the Bitcoin blockchain is an unpermissioned ledger—that is, no permission is needed to become a node and to participate in the verification process. Anyone with the appropriate equipment can become a node, and there is no verification of their real identity. It is therefore not possible to know whether a single person is running multiple nodes. This is the reason behind the relatively costly consensus process known as 'mining'. To disincentivise 'cheap talk' and incentivise truth-telling, the consensus mechanism in effect requires nodes to incur costs in order to verify a new block. This is done by requiring nodes to solve difficult cryptographic puzzles, which, in turn, may require significant computing power, resulting in energy costs to the nodes.[1] To make these costs worthwhile, a reward needs to be offered, which is largely financed through an increase in the money supply at this point: the node that solves the puzzle first and verifies the new block is awarded Bitcoins.

The use of permissioned ledgers is an alternative for when a certain degree of trust already exists between the nodes. It allows the transactions to be verified and secured through a more limited consensus process that is less resource-intensive than mining.

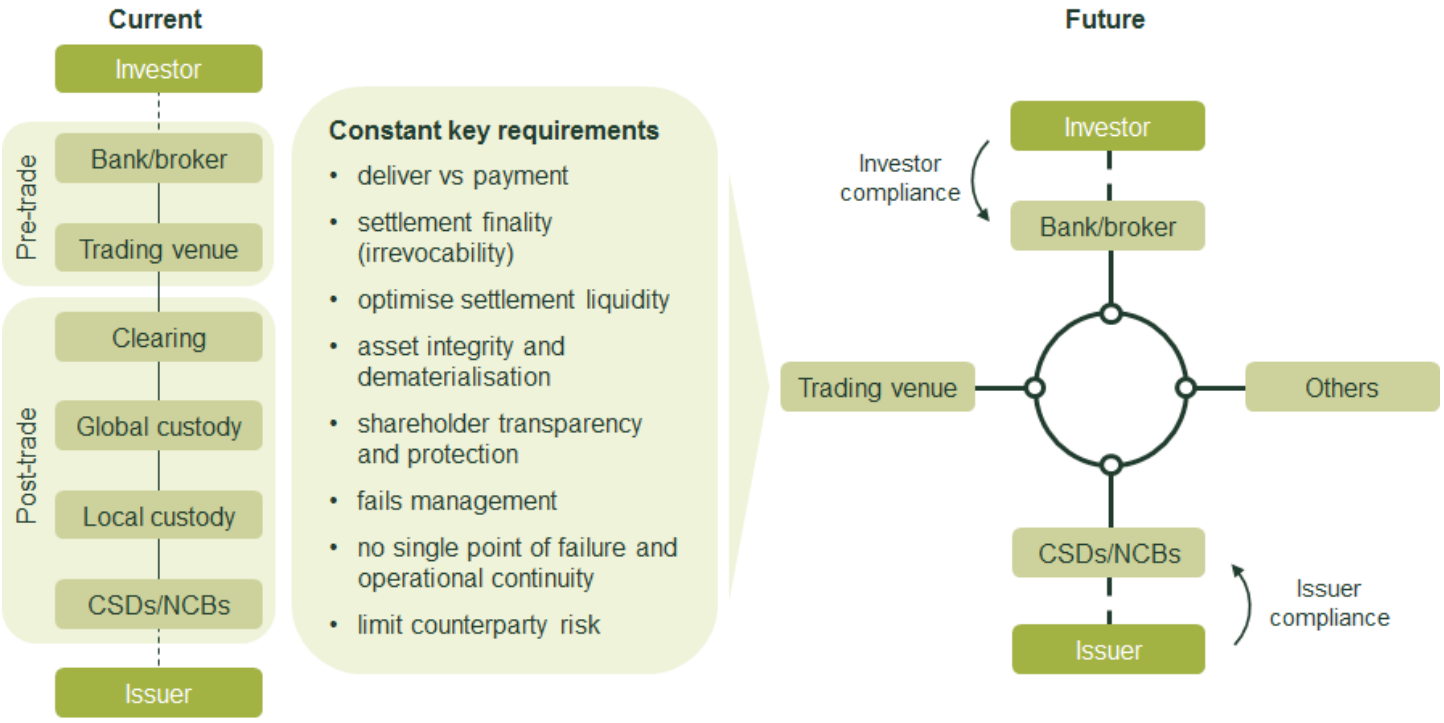
Source: [1] The average power consumption of the mining process has been estimated to be similar to the average power consumption of a country the size of Ireland. See O'Dwyer, K.J. and Malone, D. (2014), 'Bitcoin Mining and its Energy Footprint', Hamilton Institute National University of Ireland Maynooth, https://karlodwyer.github.io/publications/pdf/bitcoin_KJOD_2014.pdf, accessed 11 April 2016.

Within the blockchain-based system, both brokers then re-confirm the settlement details by signing the settlement transaction. As soon as the settlement instruction is complete, it is submitted to all nodes in the system for final verification. Once the settlement instruction is verified, it is added to the distributed ledger as 'settled'.

The verification process across the distributed network can ensure that transactions are booked in a compliant manner and regulations are enforced. It includes checks on the availability of assets, the eligibility of assets, KYC compliance of trading parties, and compliance with trade restrictions.

Context-free verification by all the nodes in the system is not sufficient for settling the transaction, as two equally valid transactions may be sent at the same time and involve the buy or sale of the very same securities. Each of these

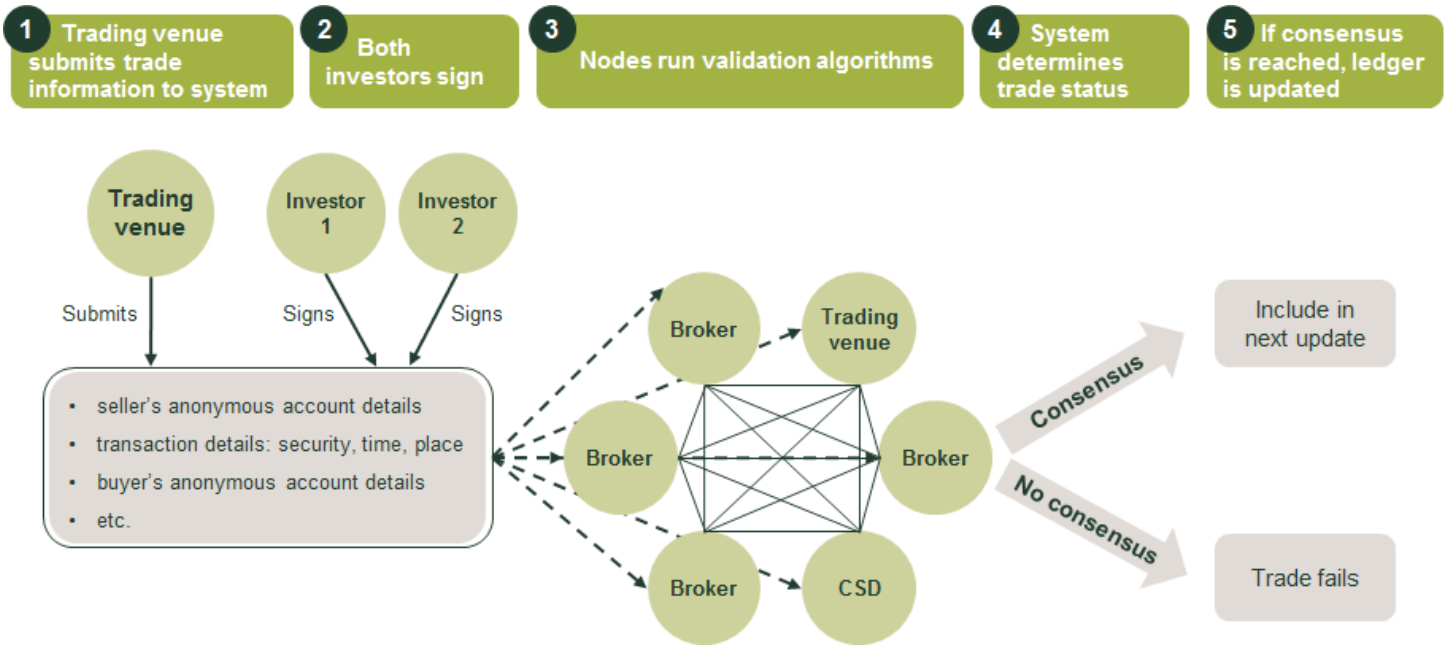
Figure 1 Blockchain technology applied to post-trading: an illustration



Note: NCB, National Central Bank.

Source: Oxera and RISE Financial Technologies.

Figure 2 Illustration of front-to-back transaction processing



Source: Oxera and RISE Financial Technologies.

transactions would be valid in isolation, but allowing both to confirm would produce a 'double spend', whereby the same securities or money is spent twice. This requires a consensus mechanism beyond the validity of individual transactions. The consensus mechanism ensures that all nodes agree on a new state of the world (contained in the ledger) that is: (i) consistent with the history of that ledger; and (ii) consistent in terms of the new transactions, which ensures that one, and only one, of a number of conflicting transactions is confirmed, and that transactions comply with certain regulatory rules.

Blockchain could offer additional functions, such as a 'regulator window' that allows the regulator to look beneath the veil of cryptography and monitor all trade data; the possibility of 'codifying' regulatory rules and building them directly into the validation process; and the ability to add 'smart contracts' to facilitate corporate actions and the processing of more complex securities.

Cost savings?

The potential cost savings from blockchain technology are subject to debate. It could replace all of the fragmented systems that are managed by individual market participants and infrastructure providers with one big ledger, which would be likely to reduce system costs and shorten communication lines. Further efficiency savings could be achieved by reducing fail management costs[9] and achieving economies of scale in the compliance of certain regulations (which could potentially be incorporated into the blockchain). There is less clarity on the order of magnitude of these cost savings.

One could also argue that a blockchain-based system would be relatively expensive compared with the central processing systems that are currently used by CCPs and CSDs (and many other companies, such as payment processing companies), where fees have reduced substantially in the last ten years due to economies of scale and reduced technology costs. From a technological point of view, a central database may indeed be cheaper to run than a blockchain-based system, partly because it avoids duplication in terms of the hardware and software required to process transactions at each of the nodes.

To really understand the potential cost reductions, however, the costs along the entire value chain (i.e. those of fund managers, brokers, clearing agents, custodians, CCP and CSD) would need to be estimated and then compared with the costs of a transaction processed by a blockchain-based system. There are few available estimates of the costs of the entire current value chain, and estimates of the costs of a blockchain-based system (operating at a similar scale) have not yet been published.[10] The cost savings are likely to vary by the type of security and by financial centre, and each application would need its own business case.

Challenges

The application of blockchain to post-trading may bring with it significant challenges.

Technical challenges

As well as scale and speed,[11] the system would need to ensure 'confidentiality'. Blockchain-based systems rely on the fact that entities in the network can validate third-party transactions. This requires a knowledge of the content of the transactions (such as the types of asset and amounts to be exchanged and, if regulatory rules need to be validated, knowledge of the identity of the sender and recipient), which might directly violate the confidentiality requirement in financial systems. Blockchain-based systems must therefore incorporate mechanisms that allow validators to verify transactions without full knowledge of their content—a task that is theoretically and practically challenging but is currently being addressed by financial technology companies.[12]

Industry choices

Although blockchain technology does not prescribe the design of the central architecture for trading and post-trading, it does raise a number of design questions. For example, although the technology could potentially deliver real-time or near real-time clearing and settlement, there is no need to impose this. There may be benefits to real-time settlement, but it would arguably require pre-funding of securities and money (which could potentially be facilitated by a lending facility on the blockchain), which would come with its own costs. Similarly, a blockchain-based system could clear and settle all individual transactions (without netting) or netted transactions (which might be more attractive in cases such as derivatives, where traders could benefit from margin offset).

Regulatory challenges

If a blockchain-based system is introduced within the current market structure of intermediaries and infrastructure providers (which would continue to fulfil the functions of clearing and settlement) then it might be able to operate within the existing regulatory framework. However, if blockchain were to evolve and remove some of the existing players from the value chain, the regulatory framework might have to evolve as well to support the full benefits. In any case, a blockchain-based system would require a governance structure to ensure that the interests of the different users were represented and taken into account in decisions about its further development. This would represent an area of innovation for start-ups in the industry.

There are still significant challenges that need to be overcome for a blockchain-based system to be fully operational in post-trading. The potential of the new technology, however, is immense, and the significant amount of funding and the numerous start-ups in this area attest to this. Blockchain technology may be one of the key drivers of innovation in post-trading, and it has the potential to shake up parts of the value chain.

[1] The terms 'blockchain technology' and 'distributed ledger technology' are often used interchangeably. Strictly speaking, 'blockchain' describes a technology, while 'distributed ledger' describes a functionality. Blockchain is the technology that allows the different (and 'distributed') parties to achieve consensus on a data set, effectively achieving a distributed ledger which can be considered as a database shared between the entities participating in a common blockchain-based system.

[2] For example, see Santander InnoVentures, Oliver Wyman and Anthemis Group (2015), 'The Fintech 2.0 Paper: rebooting financial services', 15 June. This paper uses data on the cost of post-trading activities for cash equities from Oxera (2011), 'Monitoring prices, costs and volumes of trading and post-trading services (MARKT/2007/02/G)', report prepared for European Commission DG Internal Market and Services, May, http://www.oxera.com/Latest-Thinking/Publications/Reports/2011/Monitoring-prices,-costs-and-volumes-of-trading-an.aspx, and makes certain assumptions about the potential cost savings.

[3] For example, see Mainelli, M. and Milne, A. (2016), 'The impact and potential of blockchain on the securities transaction lifecycle', SWIFT Institute working paper No. 2015-007, 9 May.

[4] Pinna, A. and Ruttenberg, W. (2016), 'Distributed ledger technologies in securities post-trading: revolution or evolution?', European Central Bank Occasional Paper 172, April; and European Securities and Markets Authority (2016), 'The Distributed Ledger Technology Applied to Securities Markets', Discussion Paper, 2 June.

[5] For a discussion of similar issues around coordination in the payments system sector, see Oxera (2014), '"Money-go-round": insights into the economics and regulation of payment systems', *Agenda*, May, http://www.oxera.com/Latest-Thinking/Agenda/2014/Money-go-round-insights-into-the-economics-of-pa.aspx. On the role of coordination and standardisation in trading and post-trading, see also Oxera (2009), 'What are the benefits of the FIX Protocol? Standardising messaging protocols in the capital markets', prepared for FIX Protocol Limited, December, http://www.oxera.com/Latest-Thinking/Publications/Reports/2009/What-are-the-benefits-of-the-FIX-Protocol.aspx; and Oxera (2008), 'Building efficiencies in post-trade processing: the benefits of same-day affirmation', June, http://www.oxera.com/Latest-Thinking/Publications/Reports/2008/Building-efficiencies-in-post-trade-processing-th.aspx.

[6] For example, end-investor accounts are already delivered by CSDs in some financial centres, such as Brazil and Malaysia.

[7] There are a number of other blockchain start-ups in this area, including Setl, Digital Asset Holdings, Epiphyte and Bankchain.

[8] Netting refers to the process of combining multiple transactions into a single settlement instruction.

[9] For an analysis of the cost of processing failures (with a specific focus on corporate actions), see Oxera (2004), 'Corporate action processing: what are the risks?', sponsored by The Depository Trust & Clearing Corporation, May, http://www.oxera.com/Latest-Thinking/Publications/Reports/2004/Corporate-action-processing-what-are-the-risks.aspx.

[10] Oxera (2011), 'Monitoring prices, costs and volumes of trading and post-trading services (MARKT/2007/02/G)', report prepared for European Commission DG Internal Market and Services, May, http://www.oxera.com/Latest-Thinking/Publications/Reports/2011/Monitoring-prices,-costs-and-volumes-of-trading-an.aspx. See also Oxera (2012), 'What would be the costs and benefits of changing the competitive structure of the market for trading and post-trading services in Brazil?', June, http://www.oxera.com/Latest-Thinking/Publications/Reports/2012/Introducing-competition-into-the-capital-market-in.aspx; and Oxera (2014), 'Global cost benchmarking of cash equity clearing and settlement services', prepared for ASX Clear Pty Ltd and ASX Settlement Pty Ltd, June, http://www.oxera.com/Latest-Thinking/Publications/Reports/2014/Global-cost-benchmarking-of-cash-equity-clearing-a.aspx.

[11] The system currently used for Bitcoin would not have sufficient scale and speed for post-trading.

[12] For example, RISE Financial Technologies has developed a solution that allows distributed validation based on participant identity, while at the same time using cryptographic obfuscation to hide transaction details, including amount and participant identity, from the validators.