

## Distributed ledger technologies (blockchain) in capital markets: risk and governance\*

### *Abstract*

Distributed ledger technologies (DLTs) have the potential to revolutionise securities trading and the capital market through removing reconciliation and other costs that are no longer needed with the trust and transparency that DLT brings. DLTs have been used to create virtual currencies (crypto-currencies), such as Bitcoin and Ether, and to create an alternative financial services system. DLTs are an innovation that can facilitate peer-to-peer trading, bringing about the democratisation of financial services markets. This promise is based on the assumption that the functionality of DLTs will result in two changes: decentralisation and disintermediation. To this end, the author investigates how DLT can be applied to the entire life cycle of securities trading – listing (issuing), trading, clearing, and settlement – currently operated by financial market infrastructure (FMI) providers. This paper attempts to answer the following questions: will DLT bring about the benefits it promises? Will decentralisation increase market risks? Will disintermediation create more obstacles to securities trading? In particular, this paper will assess securities trading on DLT networks against systemic risk, market conduct risk, and operational risk to the capital market and consider the appropriate regulations to enhance market integrity, operational safety and investor protection.

Key words: DLT, blockchain, smart contract, capital markets, RegTech, FinTech

### **1. Introduction**

Blockchain is a type of the algorithmic technologies and distributed ledger technologies (DLTs), as illustrated in Figure 1. It is a register containing information shared, recorded and replicated among nodes<sup>1</sup> that has been successfully applied to the creation of cryptocurrencies- value unit of transactions on the Blockchain ecosystem- such as Bitcoin and Ethereum.<sup>2</sup> Bitcoin and Ethereum are two types of cryptocurrency built on the blockchain. They are token-based and exchanged on Coinbase.com, a currency exchange brokering between digital assets - a cryptocurrency or reference to a record of the ownership of an asset on a Blockchain - and fiat currencies. It should be noted that there is

---

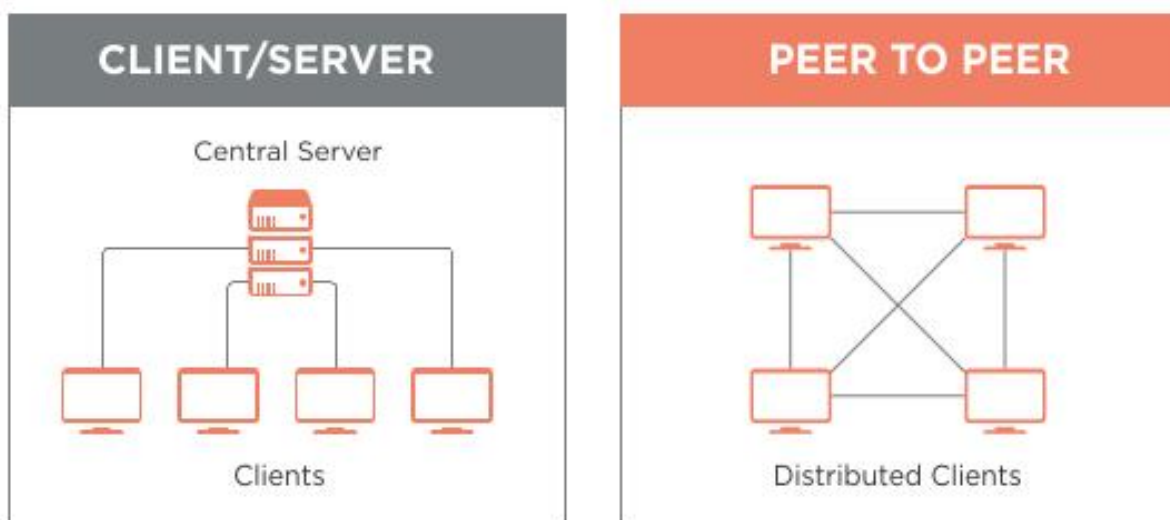
\* Dr Joseph Lee, Senior lecturer in law, University of Exeter. This article is based on a research project funded by the UK Economic and Social Research Council (ESRC).

<sup>1</sup> Nodes refer to the device participating in the peer-to-peer network by running a Blockchain client software and relaying information (transactions and blocks).

<sup>2</sup> The Economist, 'The promise of the blockchain: The trust machine', October 31, 2015 <<https://www.economist.com/news/leaders/21677198-technology-behind-bitcoin-could-transform-how-economy-works-trust-machine>> [Accessed November 6, 2017]; Philip Boucher, European Parliamentary Research Service, 'How Blockchain Technology Could Change Our Lives' (February 2017) [http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS\\_IDA\(2017\)581948\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf); Saman Adhami, Giancarlo Giudici, and Stefano Martinazzi, 'Why Do Businesses Go Crypto? An Empirical Analysis of Initial Coin Offerings' (October 20, 2017). Available at SSRN: <https://ssrn.com/abstract=3046209>; Satoshi Nakamoto 'Bitcoin: A Peer-to-Peer Electronic Cash System' 2008 available at: <https://bitcoin.org/bitcoin.pdf>

a distinction between public/permissionless networks (public chain) like Bitcoin and Ethereum and the private permissions world (private chain) where only permitted nodes can participate in the network. Public/permissionless ledgers are open to everyone to contribute data to the ledger and cannot be owned. Private and permissioned ledgers may have one or many owners and only they can add records and verify the contents of the ledger. The successful usage of blockchain in cryptocurrency, which transforms the internet information to internet value,<sup>3</sup> has promoted interest in also applying it as well to capital markets – mainly securities trading.<sup>4</sup> This is because such blockchain technology can be modified to incorporate rules, smart contract, digital signatures and other tools such as Artificial Intelligence to make contracts and financial transactions safer and more cost-effective.<sup>5</sup>

Figure 1 Central and distributed models



Some people are sceptical of such a use in capital markets and have discounted securities trading with blockchain as mere hype presented as a replacement for all the other technologies as a solution for all the problems in the financial industries.<sup>6</sup> As the blockchain network will need to use shared technology, some financial institutions have also pulled out from this development in order to develop their own blockchain initiatives.<sup>7</sup> Nevertheless,

<sup>3</sup> Dan Tapscott and Alex Tapscott, *How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, (Penguin Publishing Group 2016)

<sup>4</sup> Trevor Kiviat, 'Beyond Bitcoin: Issues in regulating blockchain transactions', (2016) 65 *Duke Law Journal*, p. 65; Philipp Paech, 'Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty' (2016) 21(4) *Uniform Law Review*, pp 612-639; and Taketoshi Mori, 'Financial technology: Blockchain and securities settlement', (2016) 8 (3) *Journal of Securities Operations & Custody* pp. 208-227.

<sup>5</sup> Digital Asset Holdings, a U.S. blockchain startup, is building business applications and market structure systems based on the distributed ledger, such as working with exchanges and post-trade providers ie Depository Trust & Clearing Corp., which provides settlement and clearing services.

<sup>6</sup> Paul Michelman, 'Seeing Beyond the Blockchain Hype: The potential for blockchain to transform how organizations produce and capture value is very real, but so are the challenges to its broad implementation', (2017) vol 58 (4) *MIT Sloan Management Review*, p17-19.

<sup>7</sup> Goldman Sachs, Santandar, and JP Morgan have left the blockchain consortium R 3. Bailey McCann, 'For Banks, 2017 Is Shaping Up to Be the Year of Blockchain', (2016) December, Institutional Investor.

major securities regulators have begun to look into relevant regulatory issues.<sup>8</sup> Some jurisdictions have also passed laws to increase their regulatory capabilities in dealing with any risks that arise once blockchain moves beyond the proof-of-concept stage.<sup>9</sup> In the UK, the Financial Conduct Authority (FCA) has set up an innovation hub and started a process of consultation. This is in addition to having created the regulatory sandbox currently in place for addressing the application of blockchain in the financial services sector,<sup>10</sup> for instance in the Exchange Traded Fund (ETF) and future markets as well as BTC (Bitcoin futures)<sup>11</sup> as an asset in conventional financial markets.<sup>12</sup> At the EU level, the European Securities and Market Authority (ESMA) has also begun a consultation process on the use of blockchain in capital markets.<sup>13</sup> In the US, the State of Delaware has also passed the first blockchain legislation, putting itself at the forefront of company law.<sup>14</sup> In Asia, China was becoming the largest market for cryptocurrency trade, with 17 cryptocurrency exchanges, until the issuance of a public notice by the Bank of China, China's banking regulator, in September 2017 caused many exchanges to suspend their trades.<sup>15</sup> This suggests two observations: first, that China has the technical infrastructure to create a model such as Ant Blockchain architecture, WeBank's syndicate loan reconciliation, and Wanda Blockchain architecture different from those used in the more advanced securities trading markets; and second, that the regulation of crypto-finance, such as an Initial Coin Offering ('ICO'), is forthcoming in China.<sup>16</sup>

---

<sup>8</sup> FCA Discussion Paper: Discussion Paper on distributed ledger technology, DP17/3; IOSCO Research Report on Financial Technologies (Fintech), February 2017; ESMA Discussion Paper on the Distributed Ledger Technology Applied to Securities Markets, 2 June 2016 | ESMA/2016/773 RF.

<sup>9</sup> Randolph Robinson, 'The New Digital Wild West: Regulating the Explosion of Initial Coin Offerings (September 1, 2017). University Denver Legal Studies Research Paper No. 17-41. Available at SSRN: <https://ssrn.com/abstract=3087541>'

<sup>10</sup> See FCA, Distributed ledger technology: Feedback statement on the Discussion Paper 17/03, <https://www.fca.org.uk/publication/feedback/fs17-04.pdf>

<sup>11</sup> Paul Vigna, 'Bitcoin Futures May Be Coming, But a Bitcoin ETF Is No Lock; SEC's opposition to bitcoin ETF proposals suggests bitcoin futures would need to build up a trading history before an ETF can be approved' *Wall Street Journal* (Online); New York, N.Y. [New York, N.Y.]01 Nov 2017.

<sup>12</sup> FCA, Regulatory sandbox, November 2015.

<sup>13</sup> Philipp Hacker and Chris Thomale, 'Crypto-Securities Regulation: ICOs, Token Sales and Cryptocurrencies under EU Financial Law' (November 22, 2017). Available at SSRN: <https://ssrn.com/abstract=3075820>; EU securities markets regulator ESMA also highlights ICO risks for investors and firms <https://www.esma.europa.eu/press-news/esma-news/esma-highlights-ico-risks-investors-and-firms>

<sup>14</sup> Andrea Tinianow 'Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance' (2017) Delaware Blockchain Initiative and Caitlin Long, Symbiont, on Thursday, March 16, 2017, Harvard Law School Forum on Corporate Governance and Financial Regulation. <https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/>

<sup>15</sup> China's bitcoin market alive and well as traders defy crackdown: Activity moves to peer-to-peer exchanges and messenger apps after Beijing's order to close exchanges earlier this month, South China Morning Post, Friday 29 September 2017 <http://www.scmp.com/news/china/money-wealth/article/2113401/chinas-bitcoin-market-alive-and-well-traders-defy-crackdown>

<sup>16</sup> Huasheng Zhu and Zach Zhizhong Zhou 'Analysis and outlook of applications of blockchain technology to equity crowdfunding in China' (2016) 2 (1) Financial Innovation pp 1-11.

With the implementation of blockchain in cryptocurrency, new laws are being introduced in some jurisdictions,<sup>17</sup> regulators' preparatory work is underway,<sup>18</sup> and there is investment in this sector.<sup>19</sup> Blockchain thus seems to be a promising innovation that will revolutionise capital market structure, or at least have some impact on the post-trade segment of the securities trade.<sup>20</sup> It should be noted that DLTs are not a new technology and that blockchain has already been used to create peer-to-peer networks,<sup>21</sup> mainly in file-sharing in the entertainment industry. However, this technology has not taken off to become widely used in other areas because the central servers have to become more powerful and sophisticated in order to cope with massive data flows. As the central servers became more powerful, centralisation was then reinforced in many trades<sup>22</sup>. In capital markets, centralisation has allowed exchanges to process trading data and information.<sup>23</sup> Small capital holders will need to rely on financial intermediaries to participate in the securities trade. Hence, centralised market operators and financial intermediaries have become the bridge between businesses and capital providers. As the distribution channels have become multi-layered, as shown in Figure 2, in order to manage the risk, the distance between small capital holders and businesses has widened, thus making trading and investment costlier for small capital holders and placing increasing restrictions on the ability of small businesses to raise and access capital. Because blockchain is built on a distributed network, it has the potential to challenge market practices surrounding centralisation and the facilitation of intermediation. It may also challenge the surrounding regulation, which is based on a centralised model.<sup>24</sup> It may also bring a safe market ecosystem as highly centralised systems present a high cost single point of failure. They may be vulnerable to cyberattack and the data is often out of sync, out of date or simply inaccurate.<sup>25</sup> The current environment has many books of records at multiple levels in the hierarchy, and at its simplest, DLT can mean that just one distributed ledger, with suitable permissioning, can replace this hierarchy. If this is to happen, a suitable governance – i.e. regulatory framework

---

<sup>17</sup> Andrea Tinianow, Delaware Blockchain Initiative: Transforming the Foundational Infrastructure of Corporate Finance (2017) Delaware Blockchain Initiative and Caitlin Long, Symbiont, on Thursday, March 16, 2017, Harvard Law School Forum on Corporate Governance and Financial Regulation <https://corpgov.law.harvard.edu/2017/03/16/delaware-blockchain-initiative-transforming-the-foundational-infrastructure-of-corporate-finance/>

<sup>18</sup> FCA FCA Discussion Paper: Discussion Paper on distributed ledger technology, DP17/3; ESMA, Discussion Paper on the Distributed Ledger Technology Applied to Securities Markets, 2 June 2016. ESMA/2016/773 RF; IOSCO Research Report on Financial Technologies (Fintech), February 2017

<sup>19</sup> VC Blockchain Investments Approach \$300 million in H1 2016 as Banks Lead Deployments, M2 Presswire; Coventry [Coventry]12 Sep 2016.

<sup>20</sup> Euroclear and Oliver Wyman, 'Blockchain in capital markets: The Prize and the Journey' February 2016, <http://www.dltmarket.com/docs/BlockchainInCapitalMarkets-ThePrizeAndTheJourney.pdf>

<sup>21</sup> See Satoshi whitepaper, available at <http://nakamotoinstitute.org/bitcoin/>

<sup>22</sup> Manuela Geranio *Evolution of the Exchange Industry: from Dealers' Clubs to Multinational Companies* (Switzerland: Springer International Publishing 2016)

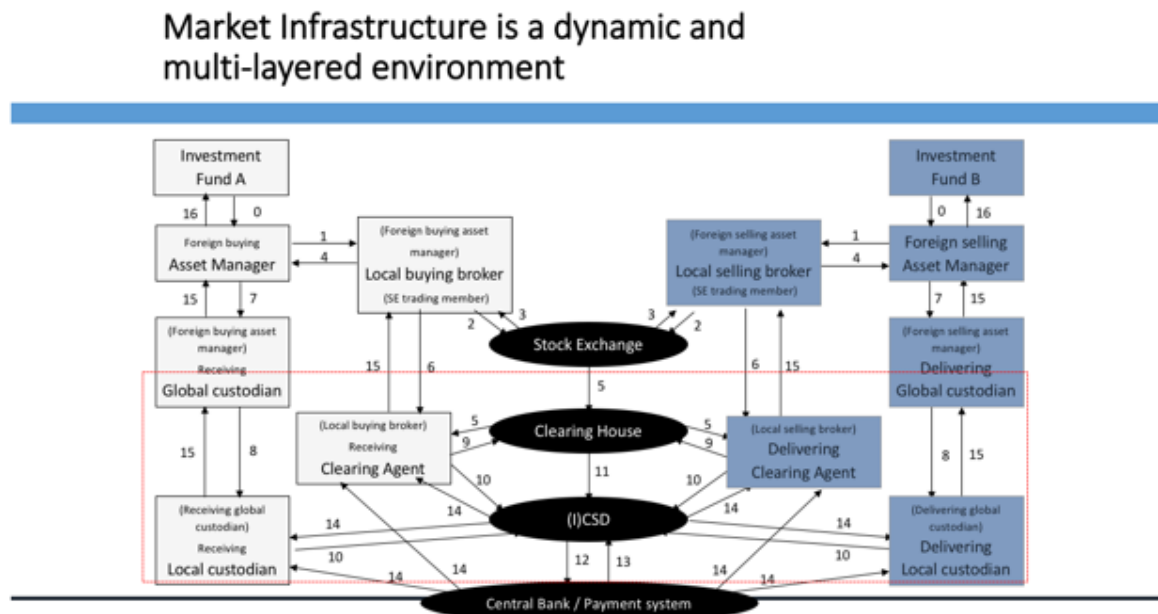
<sup>23</sup> Jane Winn, 'The Impact of the Internet on US Regulation of Securities Markets' (1997) 2 Yearbook of International Financial and Economic Law, pp. 409-426.

<sup>24</sup> Gerard Hertig and Ruben Lee, 'Four Predictions about the Future of EU Securities Regulation' (2003) 3(2) Journal of Corporate Law Studies, pp. 359-378.

<sup>25</sup> Government Office for Science, Distributed Ledger Technology beyond block chain, 2016 , p 6. Available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/gs-16-1-distributed-ledger-technology.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf)

– will need to be in place to ensure the interests of the owners of the network i.e. the participants and the broader interests of the society.<sup>26</sup>

Figure 2. Capital market infrastructure



## 2. The structure of distributed ledger technology in the capital market

For securities to be traded on the DLT network,<sup>27</sup> its structure must have two layers: the DLT network and the encoded smart contract. This latter is a set of conditions recorded as code on a distributed ledger and executed automatically by a computing system into which the security and the rules that apply to it are encoded<sup>28</sup>. There will be different nodes in the DLT network, and each one keeps a record of all (or a subset defined by policy) the transactions that occur on the network. For regulatory reasons and others such as tax,<sup>29</sup> not all nodes

<sup>26</sup> Philipp Paech, *The Governance of Blockchain Financial Networks*, (2017) 80(6) *Modern Law Review* pp 1073–1110.

<sup>27</sup> Som Shekhar Singh, 'How blockchain will change the way you trade in stock markets', *The Economic Times*, 15 January 2018, Available at

<https://economictimes.indiatimes.com/markets/stocks/news/how-blockchain-will-change-the-way-you-trade-in-stock-markets/articleshow/62161610.cms>; See also M. Kalderon, F. Snagg and C. Harrop, 'Distributed ledgers: a future in financial services?' (2016) 31 *Journal of International Banking Law and Regulation* 243, 247.

<sup>28</sup> G. W. Peters and E. Panayi, 'Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money' Working Paper, 18 November 2015 at [https://papers.ssrn.com/sol3/Papers.cfm?abstract\\_id=2692487](https://papers.ssrn.com/sol3/Papers.cfm?abstract_id=2692487), 3 (unless otherwise stated, all URLs were last accessed 30 November 2016).

<sup>29</sup> M. Kalderon, F. Snagg and C. Harrop, 'Distributed ledgers: a future in financial services?' (2016) 31 *Journal of International Banking Law and Regulation* 243, 247; Tom Bell, 'Copyrights, Privacy, and the Blockchain', (2016) 42(2) *Ohio Northern University Law Review*, 439–470; Belgian tax authorities investigate foreign cryptocurrency exchanges to find Belgian citizens who are required to pay 33% tax on their gains through crypto-trade. 2 March 2018

can have transactions, so the blockchain fabric will typically allow only parties to a transaction to see the transaction: other nodes may provide consent but not see the transaction itself. This is how Hyperledger Fabric and R3 Corda both work, by creating platforms through private networks for transferring digital assets among them.<sup>30</sup>

The network is maintained by all the nodes based on a consensus model (community consensus, or protocol consensus) rather than by a single entity. Each node will keep data files and, collectively, they will maintain the network (or on a premise if the participants elect to it run their node).<sup>31</sup> Unlike a centralised system, which is usually maintained by a single entity – such as the exchange – which has its own data centre, there will be no single data centre that keeps the data safe and authenticates the transactions. It should be noted that a blockchain network can be public or private. In a public chain, permission is not required to participate, thus creating a permission-less network with potentially anonymous participants. In a private chain, the participants can decide who should participate in the network, participants are known. In a permission-less model, how things operate on the network will be governed by a consensus of the network participants. Whereas in a private chain, rules can be set by the participants (also a consensus model) or by a commonly trusted third party. In other words, the public chain will bring about a higher degree of decentralised and disintermediated system than the private chain. A private chain,<sup>32</sup> if adopted by exchanges and other financial intermediaries, can continue the centralised market model but with improved functionality, but it offers non-incumbent operators the opportunity to provide services in this environment.

For the securities trade to gain synergy, an auto-executable smart contract, into which a security (e.g., a share) is encoded, will be used on the DLT network.<sup>33</sup> A smart contract is a pre-written computer code that it can be triggered by events, resulting in ledger updates. A smart contract can be seen as a 'digitised vending machine',<sup>34</sup> which is running according to the pre-written rules. Smart contracts will reduce the cost of transactions in various corporate actions, such as voting and the distribution of dividends.<sup>35</sup> However, in such a network, i.e., one without a centralised system, one must ensure that transactions are genuine and not made by a malicious third party, particularly if such transactions are to take

---

<https://www.rtl.be/info/belgique/economie/vous-investissez-dans-le-bitcoin-ou-une-autre-cryptomonnaie-attention-le-fisc-pourrait-vous-reserver-une-mauvaise-surprise-1000481.aspx>

<sup>30</sup> Hyperledger is to create a platform through the distributed database recording digital events with the batch of transactions timestamped to form a blockchain network. R3 also has an innovation that is the blockchain-based shared-ledger computer software platform known as Concord which allows companies to run high-scale financial applications on permissioned networks across organizations.

<sup>31</sup> In Fabric and Corda, there is through a central entity to sequence transactions onto the ledger: in fabric the ordering service; in corda the notary.

<sup>32</sup> In ESMA blockchain review, it is the view that private chains are likely to be the basis of DLT progression in regulated markets. See Discussion Paper on the Distributed Ledger Technology Applied to Securities Markets, 2 June 2016 | ESMA/2016/773 RF.

<sup>33</sup> Reggie O'Shields 'Smart Contracts: Legal Agreements for the Blockchain' (2017) 21 North Carolina Banking Institute, pp. 177-194; Alexander Savelyev, 'Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law', (2017)26 (2) Information & Communications Technology Law, pp. 116-134.

<sup>34</sup> Nick Szabo, 'Formalizing and Securing Relationships on Public Networks' (1997) 2 First Monday <http://firstmonday.org/ojs/index.php/fm/article/view/548/469>

<sup>35</sup> Alexander Savelyev, 'Contract Law 2.0: Smart Contracts as the Beginning of the End of Classic Contract Law', (2017) 26 (2) Information & Communications Technology Law, pp. 116-134.



place on an open network (public chain) as opposed to a closed network (private chain). Hence, encryption technology is required to authenticate a transaction, i.e. a transaction in which A transfers 100 shares in Company Q to B.

The question is, therefore, how would smart contract technology affect centralised market practices<sup>36</sup> and would it reduce the need for financial intermediaries such as share services?<sup>37</sup> Second, how would encryption technology displace certain trusted third parties, such as the Certificate Authority (CA) and securities custodians, from centralised market practices? I will first discuss the mechanisms of smart contract and encryption technology and explore their utilities in capital markets on the DLT network. After discussing how DLTs will affect the life cycle of trades, I will then discuss the pertinent legal issues and challenges.

### **3. Smart Contracts and investor protection**

If activities that take place using blockchain technology are to achieve their intended effects, smart contracts must be used to facilitate the securities trade on the network.<sup>38</sup> For instance, a share can be encoded into a smart contract, which will be automatically executed upon the occasion of an event occurring. For instance, when there is a general meeting to decide certain issues, an investor will receive notices and votes according to the shares he/she holds on the blockchain network; When declared, dividends will be distributed automatically to the investors' cash (or other crypto-currency) account; when there is a new issuance of shares, those shares will be allocated automatically to those investors who exercised their pre-emption rights.

To give an example of how a smart contract can operate, imagine that a smart contract can trigger the removal of a director. The contract will contain the following essential clauses: 1) a shareholder can propose an action, i.e. the removal of a director; 2) other shareholders can join the proposal; 3) once the shares have reached a pre-set number, such as 5% of the total shares, a meeting will be called for shareholders to cast their votes; 4) the director will be removed if more than 50% of the votes cast are in favour of removing the director. For example, if a shareholder, Alice, thinks a director is in breach of duty or is unfit to lead the company, she can go through the following steps: step 1: she sends a message to the smart contract to propose a vote; step 2: another shareholder, Bill, also sends the proposal in a second message to the smart contract within one day, triggering a vote on the issue; step 3: shareholders send a message to vote in favour or against the proposal; step 4: once the votes in favour exceed 50 per cent of the votes cast, the removal of the director will be authorised.

---

<sup>36</sup> Thomais Kotta Kyriakou, 'Harmonizing Corporate Actions for the Achievement of a Capital Markets Union: An Analysis of the Shareholders' Rights Directive, the Green Paper Building a Capital Markets Union and TARGET2-Securities', (2017) 14 (3) European Company Law, 121-126.

<sup>37</sup> David Larcker, Allan McCall, Gaizka Ormazabal, 'Outsourcing Shareholder Voting to Proxy Advisory Firms', (2015) 58 (1) Journal of Law & Economics, pp. 173-204; Paul Rose, The Corporate Governance Industry, (2007) 32 (4) Journal of Corporation Law, pp. 887-926; Laura Noonan, Citi develops online shareholder voting system, 13 November 2017, <https://www.ft.com/content/31140600-c619-11e7-a1d2-6786f39ef675>

<sup>38</sup> Mark Giancaspro, 'Is a "smart contract" really a smart idea? Insights from a legal perspective' (2017) 33 Computer Law & Security Review, pp 825-835.

However, when and how a corporate action can be triggered still requires human judgement – in the illustrative case above, judgement of whether a director should be removed. A smart contract will not automatically trigger a corporate action: both human and legal judgement are required. In such a corporate action event such as the removal of a director, notice must be given to the director in question and shareholders will need to decide which director or directors are to be eligible to the vote. Shareholders may also need to state why the director is to be removed. If the reason is simply 'we don't like you', then the director may be entitled to compensation. However, if the reason is that there has been a breach of duty (not just a breach of rules), the director will not be entitled to compensation. If the reason pertains to 'breach of duty', shareholders may also be entitled to 'rectify' the wrong, and hence forgive the director. This is a general law that may also need to be written into the smart contract if it is to be used by a UK company.<sup>39</sup>

If a smart contract is set to be triggered automatically when a certain event occurs, a director may be wrongly removed, and such an act will render the company liable to pay damages to the director. In a different scenario, a company can call a general meeting to authorise an action if the company's assets fall below a certain threshold<sup>40</sup> and in this case, the smart contract would not be able to detect that the event that has happened. Detection of the event will be performed by an external 'oracle service'. At a stage when oracle services are still in the development stage, if the smart contract wrongly triggers an event that leads to auto-execution of share transfers, the investors can suffer irreparable damages.<sup>41</sup>

#### **4. Predicted deployment in the capital market**

Stock exchanges play a vital role in the capital market by facilitating listing (issuing), trading, clearing and in some cases settlement. They provide an efficient alternative financing mechanism to bank loans<sup>42</sup> or private equity financing<sup>43</sup>. Centralisation is key to the success of this financing mechanism,<sup>44</sup> as it enables the creation of larger capital pools and provides

---

<sup>39</sup> Thomais Kyriakou, 'Harmonizing Corporate Actions for the Achievement of a Capital Markets Union: An Analysis of the Shareholders' Rights Directive, the Green Paper Building a Capital Markets Union and TARGET2-Securities', (2017) 14(3) European Company Law, pp. 121-126.

<sup>40</sup> This resembles written resolution used in private companies under Companies Act 2006, s 288-300. However, such resolution cannot be used to remove company directors.

<sup>41</sup> Bitcoin divides to rule: The crypto-currency's split into two versions may be followed by others, (2017) The Economist, <https://www.economist.com/news/business-and-finance/21725747-crypto-currencys-split-two-versions-may-be-followed-others-bitcoin>

<sup>42</sup> Public markets provide enhanced visibility which is a factor that most European CFOs consider a benefit of going public. See Franck Bancel and Usha Mitto, 'Why Do European Firms Go Public?' (2009) 15 (4) European Financial Management, p844-884.

<sup>43</sup> In time of financial crisis, stock markets also provide an exit option for private equity firms. See Emil Plagborg-Møller and Morten Holm, 'IPO or SBO?: The Increasing Importance of Operational Performance for Private Equity Exits Following the Global Financial Crisis of 2007-08' (2017) 29(1) Journal of Applied Corporate Finance p115-121.

<sup>44</sup> The degree of centralisation can also affect transaction costs in securities trade. See Jean-François Gajewski and Carole Gresse, 'Centralised order books versus hybrid order books: A paired comparison of trading costs on NSC (Euronext Paris) and SETS (London Stock Exchange)' (2007) 31 (9) Journal of Banking & Finance p2906-2924.



integrated trading services. The major risk of decentralisation is liquidity fragmentation,<sup>45</sup> and it will exacerbate the fragmentation problem that blue chips companies already face<sup>46</sup>. The hope is that blockchain will be guided by a more peer-to-peer model, connecting businesses and investors. The question is, therefore, what type of peer-to-peer model will there be with blockchain? And, will such a model be more efficient or more distributed (fairer) than the existing centralised model?

#### **4.1 Listing and Issuing**

DLT is said to be able to bring about the democratisation of the financial market through a peer-to-peer network that will break through the current centralised capital market model, which is channelled to capital holders by financial intermediaries. This model is perceived to impose too high a cost on businesses and investors, especially SMEs and retail investors. As a result, few investors participate directly in securities trades or exercise their governance rights in the companies in which they invested. Additionally, businesses find that access to capital is obstructed by a very high regulatory threshold aimed at investor protection, as well as by the lack of support from intermediaries in terms of interest in making their trades. Furthermore, the underwriting cost is high, which has the effect of dissuading businesses from using the capital market as a way of raising funds. Because the investment environment is perceived as unfriendly to small capital holders, the potential of DLT to bring about decentralisation and disintermediation has spurred some financial innovations, such as the Initial Coin Offering ('ICO'), which relies on blockchain to raise capital.<sup>47</sup> A less-discussed use of DLT is in the area of issuance – using DLT as RegTech for book-building to enhance price transparency and fair dealings.

##### ***4.1.1. Initial Coin Offering (ICO)- public/private split***

An ICO involves a business issuing 'tokens' to investors on the open chain to raise cash, crypto-currency, or a mixture of both. The token represents an 'interest' that the investors have in the investee business.<sup>48</sup> There is a set of rights attached to the token that the token holders can exercise against the investee business. Initial coin offerings, therefore, have various parallels with Initial Public Offerings, private placement of securities, or crowd

---

<sup>45</sup> Yet, some argue that this depends how distribution happens and distribution does not necessarily mean that liquidity is distributed.

<sup>46</sup> Peter Gomber, Satchit Sagade, Erik Theissen, Moritz Christian Weber, Christian Westheide, 'Competition between equity markets: A review of the consolidation versus fragmentation debate' (2017) 31 (3) Journal of Economic Surveys p792-814.

<sup>47</sup> Jonathan Rohr and Aaron Wright 'Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets' (October 4, 2017). Cardozo Legal Studies Research Paper No. 527; University of Tennessee Legal Studies Research Paper No. 338. Available at SSRN: <https://ssrn.com/abstract=3048104>; Philipp Paech, 'Securities, Intermediation and the Blockchain: An Inevitable Choice between Liquidity and Legal Certainty' (2016) 21 (4) Uniform Law Review, pp 612-639.

<sup>48</sup> Monetary Authority of Singapore, A Guide to Digital Token Offerings, 14 November 2017, <http://www.mas.gov.sg/~media/MAS/Regulations%20and%20Financial%20Stability/Regulations%20Guidance%20and%20Licensing/Securities%20Futures%20and%20Fund%20Management/Regulations%20Guidance%20and%20Licensing/Guidelines/A%20Guide%20to%20Digital%20Token%20Offerings%20%202014%20Nov%202017.pdf>

sales.<sup>49</sup> ICOs have attracted much regulatory attention and action. For instance, the Securities Exchange Commission (SEC) of the US, in the case of DAO hack, decided that the DAO tokens were securities, according to the Howey test of whether something can be considered as a security under their securities acts given by the Supreme Court of the United States decision in 1946 which is now called as the Howey test.<sup>50</sup> China<sup>51</sup> and South Korea have also banned them; the UK,<sup>52</sup> Hong Kong, and Singapore<sup>53</sup> are taking a 'wait-and-see' approach but have issued a risk warning to investors; France has launched a public consultation process<sup>54</sup> and has introduced a law on the transfer of property in securities on the blockchain network.<sup>55</sup>

The SEC's treatment of ICOs is based on the notion that such a method of capital-raising outside the exchanges circumvents the transparency and disclosure regime aimed at protecting the investor.<sup>56</sup> The issuance of a token, as a type of crypto-security, is not *per se* illegal<sup>57</sup> and indeed the state of Delaware has provided a legal basis for crypto-security enabled by smart-contracts transposed on the blockchain. That is to say that DLT can be used by businesses to raise capital under proper legal and regulatory frameworks, thus offering a way to provide a legal basis for an ICO token. The token can be legally recognised on a *sui generis* basis, as though it were a share. The rights attached to a token should also be regulated so as to provide confidence in this kind of crypto-security and also in the working of the ICOs as a legitimate aspect of crypto-finance. The regulatory framework and legal protection, equivalent to those offered to shareholders in an IPO, should also be offered to investors in an ICO. Whether a more or less onerous transparency regime should be applied to ICO will depend on the policy objective and on other safeguards provided by the operators. Although ICOs do not go through crypto-currency exchange operators, this does not mean that those operators or other financial institutions cannot set up a platform

---

<sup>49</sup> Financial Conduct Authority, 'Discussion Paper DP17/3 on distributed ledger technology (DLT)', April 2017 <https://www.fca.org.uk/publication/discussion/dp17-03.pdf>

<sup>50</sup> 'SEC Issues Investigative Report Concluding DAO Tokens, a Digital Asset, Were Securities. U.S. Securities Laws May Apply to Offers, Sales, and Trading of Interests in Virtual Organizations' SEC Press Release, published 25/07/2017. Available at: <https://www.sec.gov/news/press-release/2017-131>.

<sup>51</sup> 'Central Bank of the People's Bank of China PBC Office of Industry and Information Technology Administration of Industry and Commerce China Banking Regulatory Commission China Securities Regulatory Commission CIRC Notice on Preventing Financing Risk of Tokens Issue' (Translated from Chinese' Published 04/09/2017, available at: <http://www.circ.gov.cn/web/site0/tab6554/info4080736.htm>

<sup>52</sup> Financial Conduct Authority, 'Consumer warning about the risks of Initial Coin Offerings ('ICOs')'. Published 12/09/2017, available at: <https://www.fca.org.uk/news/statements/initial-coin-offerings>

<sup>53</sup> Monetary Authority of Singapore, 'MAS clarifies regulatory position on the offer of digital tokens in Singapore' Published 01/08/2017 available at: <http://www.mas.gov.sg/News-and-Publications/Media-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-Singapore.aspx>

<sup>54</sup> The French financial markets regulatory, AMF, publishes a discussion paper on Initial Coin Offerings and initiates its UNICORN programme

[http://www.amf-france.org/en\\_US/Actualites/Communiqués-de-presse/AMF/annee-2017?docId=workspace%3A%2F%2FspacesStore%2F5097c770-e3f7-40bb-81ce-db2c95e7bdae](http://www.amf-france.org/en_US/Actualites/Communiqués-de-presse/AMF/annee-2017?docId=workspace%3A%2F%2FspacesStore%2F5097c770-e3f7-40bb-81ce-db2c95e7bdae)

<sup>55</sup> France, the first among European countries, introduces law regarding the transfer of property in securities on the blockchain network. <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000036171908>

<sup>56</sup> Christoph Jentzsch, 'Decentralized Autonomous Organization to Automate Governance' White Paper 2016 available at: <https://download.slock.it/public/DAO/WhitePaper.pdf>

<sup>57</sup> Securities and Exchange Commission 'Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO' Published 25/07/2017 available at: <https://www.sec.gov/litigation/investreport/34-81207.pdf>

to facilitate ICOs in order to confer legal status on the platform a legal status as a regulated market or as an organised market to help start-ups or SMEs to raise capital.<sup>58</sup>

#### **4.1.2. Book-building process**

One possible application of DLTs in the IPO is in the area of the book-building process, where DLTs can increase transparency and fair dealing in the IPO process. The current practice involves a stage in an IPO where the investment bank (the underwriter) can allocate shares at a certain price to buy-side investors, such as brokers. How the price is set and to whom shares will be allocated are not transparent.<sup>59</sup> That is to say that the underwriter can decide, at its own discretion, to whom shares should be allocated, at what volume and at what price. This can create potential conflicts of interest and unfairness, especially if the shares are considered to be highly desirable.<sup>60</sup> For example, underwriters may allocate shares to brokers who will trade those shares on a certain trading venue<sup>61</sup> and to whom the shares have been allocated before the IPO may not be known to the market. Using DLT in the book-building process within the IPO can help give a higher degree of transparency to the allocation of shares, minimise potential conflicts of interest and increase fair dealing in the market.<sup>62</sup> The use of DLT will involve the lead underwriter inviting brokers and investors to a private chain network.<sup>63</sup> A smart contract detailing the rights and obligations will be designed by the lead underwriter. The smart contract will also specify the book-building volume, the price and the allocation rules. The brokers and investors will submit their bids specifying the volumes of the share desired at a particular price. Once the lead underwriter determines the price based on the bid information, the shares will be automatically allocated according to the bids and rules of the smart contract. The investors and brokers will be notified of the allocations, and the information on the allocations will be recorded on the distributed ledgers. Banks can also join the network in order to provide payment guarantees and facilitate payment transfers. In this way, DLT can act as an *ex ante* measure to regulate conflicts of interest as well as other market misconduct, such as insider dealing and market manipulation of the IPO. Using book-building in this private chain is a type of regulation technology (RegTech) - technologies that facilitate the delivery of regulatory requirements -<sup>64</sup> for the IPO.

---

<sup>58</sup> Oscar Williams-Grut, 'Crypto exchanges are charging up to \$1 million per ICO to list tokens: 'It's pure capitalism' Business Insider, 12 March 2018

<http://uk.businessinsider.com/cryptocurrency-exchanges-listing-tokens-cost-fees-ico-2018-3>

<sup>59</sup> Ann Sherman, 'IPOs and long-term relationships: an advantage of book building Sherman' (2000) 13 (3) Review of Financial Studies, pp697-714

<sup>60</sup> See Manuela Geranio, Camilla Mazzoli, and Fabrizio Palmucci, 'The effects of affiliations on the initial public offering pricing' (2017) 51 International Review of Economics and Finance, 295-313.

<sup>61</sup> Financial Conduct Authority, Investment and corporate banking market study, (2016) Final report, MS15/1.3 <https://www.fca.org.uk/publication/market-studies/ms15-1-3-final-report.pdf>

<sup>62</sup> Financial Conduct Authority, Investment and corporate banking market study, (2016) Final report, MS15/1.3 <https://www.fca.org.uk/publication/market-studies/ms15-1-3-final-report.pdf>

<sup>63</sup> Private chain is favoured by some regulators. See European Central Bank, 'The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration' (2017) [https://www.ecb.europa.eu/paym/intro/governance/shared/pdf/201709\\_dlt\\_impact\\_on\\_harmonisation\\_and\\_integration.pdf](https://www.ecb.europa.eu/paym/intro/governance/shared/pdf/201709_dlt_impact_on_harmonisation_and_integration.pdf)

<sup>64</sup> FCA, 'Call for Input: Supporting the development and adoption of RegTech' (2015) <https://www.fca.org.uk/publication/call-for-input/regtech-call-for-input.pdf>

## 4.2 Trading

One of the public utilities performed by the stock exchange and the trading venue is price-discovery.<sup>65</sup> That is, through trading on the secondary market, the prices of securities can best reflect their value. Without such a trading mechanism, it would be difficult for investors, especially retail investors, to appreciate the value of companies. For this reason, the securities trade needs the support of financial intermediaries,<sup>66</sup> if it is not to lose visibility in the marketplace, and lead to reduced interest in securities trading on the part of investors. The efficiency of such a trading mechanism is attributed to the matching engine (a central server) provided either by the exchange or the trading venue. The more sophisticated this matching engine is, the more trades it can process. It can also process trades in milliseconds in order to support the strategies used by high frequency traders (HFTs).<sup>67</sup>

What will happen to the trading segment given the potential of DLT to de-centralise trade? DLT is able to facilitate peer-to-peer trades without the centralised market system operated by the exchanges and the trading venues. So the question is not whether DLT can facilitate securities trades, but rather whether it can achieve the same function as the centralised market system in terms of price-discovery,<sup>68</sup> liquidity,<sup>69</sup> and maintaining market integrity against market misconduct<sup>70</sup>, such as insider dealing and market manipulations.<sup>71</sup> In the securities trade market, investors will take different trading positions – long or short – depending on their views of the future market. It is this long-short dynamic that brings about the function of price discovery. Trading on the DLT network will make shorting a security an impossible task because stock-lending will not be possible.<sup>72</sup> Although, in some cases, shorting securities might destabilise the market and economy in times of financial

---

<sup>65</sup> Benjamin Clapham and Kai Zimmermann 'Price discovery and convergence in fragmented securities markets' (2016) 12 (4) International Journal of Managerial Finance pp381-407.

<sup>66</sup> Amber Anand and Avaniidhar Subrahmanyam, 'Information and the Intermediary: Are Market Intermediaries Informed Traders in Electronic Markets?' (2008) 43 (1) Journal of Financial & Quantitative Analysis, p1-28.

<sup>67</sup> Viktor Manahov; Robert Hudson, 'The implications of high-frequency trading on market efficiency and price discovery' (2014) 21 (16) Applied Economics Letters, 1148-1151; Kristin Johnson, 'Regulating Innovation: High Frequency Trading in Dark Pools' (2017) 42(4) Journal of Corporation Law, 833-886.

<sup>68</sup> Bank for international settlement, 'The implications of electronic trading in financial markets', (2001) <https://www.bis.org/publ/cgfs16.pdf>; David Lawton, Price: the cornerstone of markets, Speech by Director of Markets of the FCA at the International Capital Market Association (ICMA) Capital Market Lecture Series 2014 on Monday 3 February 2014 <https://www.fca.org.uk/news/speeches/price-cornerstone-markets>

<sup>69</sup> Liquidity refers to the degree to which a market allows assets to be bought and sold without affecting the asset's price. For stock exchanges, lower liquidity tends to result in a more volatile market (especially when there are block trades and there is a huge spread between bid price and ask price), and it causes prices to change more drastically; whereas higher liquidity creates a less volatile market, and prices do not fluctuate as significantly. Evangelos Benos, Richard Payne and Michalis Vasios, 'Centralized trading, transparency and interest rate swap market liquidity: evidence from the implementation of the Dodd-Frank Act' January 2016, Bank of England Working Paper No. 580 <https://www.bankofengland.co.uk/working-paper/2016/centralized-trading-transparency-and-interest-rate-swap-market-liquidity-evidence-from-the>

<sup>70</sup> Oscar Williams-Grut, Market manipulation 101: 'Wolf of Wall Street'-style 'pump and dump' scams plague cryptocurrency markets, 14 November 2017, Business Insider, <http://uk.businessinsider.com/ico-cryptocurrency-pump-and-dump-telegram-2017-11>

<sup>71</sup> Jay Clayton, 'Governance and Transparency at the Commission and in Our Markets' Chairman of SEC Remarks at the PLI 49th Annual Institute on Securities Regulation, 8 November 2017 <https://www.sec.gov/news/speech/speech-clayton-2017-11-08>

<sup>72</sup> Some argue that it is possible to undertake stock borrowing and short-selling on DLTs.

crisis, short-selling can also be a legitimate investment strategy. DLT can also reduce the level of liquidity caused by the latency problem. Speed is a critical element for brokers who execute orders for their clients. Latency is the reason why there is no interconnected trading venue between the London Stock Exchange and the Borsa Italiana, even though both markets use the same IT system, (applications from the Millennium subsidiary of LSEG), for trading.<sup>73</sup> The Milan-based traders felt that they would be put at a disadvantaged position compared to the London-based traders because the server (the matching engine) would be based in London. The latency of DLT can cause unfair competition between traders. Furthermore, without a centralised market system, i.e. a regulated market<sup>74</sup>, or a more organised market such as a multilateral trading facility<sup>75</sup> or organised trading facilities,<sup>76</sup> market misconduct will be more difficult to detect and regulate.<sup>77</sup> Under the current system, each trade can be linked to a particular investor. However, on a DLT, especially on an open chain network, trades will be made anonymously due the technology of encryption<sup>78</sup>. This can create a major challenge to law enforcement agencies in their investigation and prevention of market misconduct and crime, such as money laundering<sup>79</sup>. In terms of market safety, a circuit breaker cannot be implemented to create market stability for trades conducted on an open chain network.

Some suggest that DLT can be used for trading in certain venues, such as over-the-counter for large-volume trade, and for certain traders, for instance in dark pools. This can potentially reduce the non-transparency of dark pools, in which the parties do not need to make pre-trade disclosures about the price and volume of their securities trades. However, trades in dark pools still require speed. Even if the parties use the private chain network to trade, DLT can be used as a RegTech only if it can overcome the latency problem.

### 4.3 Clearing

---

<sup>73</sup> Joseph Lee, 'Synergies, Risks and the Regulation of Stock Exchange Interconnection' [2017] 11(2) Masaryk University Journal of Law and Technology pp. 291-322 <https://doi.org/10.5817/MUJLT2017-2-5>

<sup>74</sup> A regulated market is a multilateral system operated by a market operator, which brings together or facilitates the bringing together of multiple third-party buying and selling interests in financial instruments. The list of RMs currently includes the London Stock Exchange Main Market.

<sup>75</sup> Article 4 (15) of MiFID II. An MTF is a multilateral system, operated by an investment firm or a market operator, which brings together multiple third-party buying and selling interests in financial instruments.

<sup>76</sup> Article 4(1)(23) of MiFID II. An OTF is a multilateral system which is not a regulated market or an MTF and in which multiple third-party buying and selling interests in bonds, structured finance products, emission allowances or derivatives are able to interact in the system in a way that results in a contract in accordance with Title II of MiFID II. Equity cannot be traded on OTFs.

<sup>77</sup> Kristin Johnson, 'Regulating Innovation: High Frequency Trading in Dark Pools' (2017) 42(4) Journal of Corporation Law, pp. 833-886.

<sup>78</sup> Jan Henrik Ziegeldorf, Roman Matzutt, Martin Henze, Fred Grossmann, and Klaus Wehrle, 'Secure and anonymous decentralized Bitcoin mixing' (2018) 80 Future Generation Computer Systems pp 448-466 <https://doi.org/10.1016/j.future.2016.05.018>

<sup>79</sup> Mark Carney, 'The Future of Money' Speech by Governor of Bank of England <https://www.bankofengland.co.uk/-/media/boe/files/speech/2018/the-future-of-money-speech-by-mark-carney.pdf?la=en&hash=A51E1C8E90BDD3D071A8D6B4F8C1566E7AC91418>, p 9.

The Central Counterparty (CCP) is an important liquidity provider as well as an important risk management provider to securities traders.<sup>80</sup> It provides the function of netting which, through the legal technique of novation, reduces multiple trades (buying and selling) into one single position.<sup>81</sup> The netted position improves efficiency in the settlement segment performed by the Central Securities Depositories ('CSDs'), where a transfer of securities against payment is not required upon each trade that takes place on a trading platform. This improves trading efficiency and allows more trades to be placed for the purpose of price discovery.<sup>82</sup> The better the quality of the price discovery mechanism, the more informed is the investor's decision making. Secondly, the CCP provides risk management, whereby it will use its defence mechanism to resolve the problem of one party's default in a trade.<sup>83</sup> Such resolution will usually involve the CCP 'stepping into' the defaulting party's position to ensure a smooth trade. This can prevent a blockage in the trading system.

How will the blockchain network change the CCP's function in the complete life cycle of the securities trade? The blockchain network, a peer-to-peer network, will facilitate securities trade among different network nodes. Smart contracts can be used to execute transactions, i.e. auto-execution of securities and payment transfers. The blockchain network and smart contract will result in a new trading model where securities trading and securities transfers can take place simultaneously, as opposed to the current practice whereby a securities transfer takes place two days after the trade (T+2).<sup>84</sup> If the current practice of delivery versus payment (DvP) is to be followed,<sup>85</sup> funds will need to be in place before the trade can take place – i.e. there must be pre-funded trades. This scenario will contrast with the current trading and clearing arrangement where the CCP provides the funding (partial financing) in the trade for the traders. That is, the trader does not need to have the full amount of funding in its payment account before it can place a trade. However, the CCP will require the collateral and collect margins according to the risk of the trader. In other words, a trader can engage in a securities trade with a value that exceeds the funding the trader has placed in this cash account. With the blockchain network and smart contract, CCP will lose its functions as a liquidity provider<sup>86</sup> and a risk management mechanism. Hence, removing CCP from the trading cycle will not improve trade efficiency or price-discovery

---

<sup>80</sup> Jo Braithwaite and David Murphy, 'Central Counterparties (CCPs) and the law of default management' (2017) 17 (2) Journal of Corporate Law Studies, 291-325, DOI: 10.1080/14735970.2016.1254448

<sup>81</sup> European Central Bank, Standards for Securities Clearing and Settlement in the European Union, September 2005 <https://www.ecb.europa.eu/pub/pdf/other/escb-cesr-standardssecurities2004en.pdf?46d110f6ad9e1ea050fa1de9b47a372d>

<sup>82</sup> Viktor Manahov and Robert Hudson, 'The implications of high-frequency trading on market efficiency and price discovery', (2014) 21 (16) Applied Economics Letters, p1148-1151.

<sup>83</sup> EuroCCP Risk Management overview, 7 March 2018 <https://euroccp.com/document/euroccp-risk-management-overview/>

<sup>84</sup> Regulation (EU) No 909/2014 of the European Parliament and of the Council of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories (CSDR). The CSDR requires that the settlement date for transactions, the date on which the assets have to be transferred to the owed party, must be no later than the second business day after the trade takes place (T+2 requirement).

<sup>85</sup> IOSCO Recommendations for securities settlement systems, 2001, <https://www.iosco.org/library/pubdocs/pdf/IOSCOPD123.pdf>

<sup>86</sup> Froukelien Wendt, 'Central Counterparties: Addressing their Too Important to Fail Nature' IMF Working Paper, January 2015 <https://www.imf.org/external/pubs/ft/wp/2015/wp1521.pdf>



efficiency. There will be fewer trades on the platform, as the funding requirement will reduce trades and result in reduced liquidity. The reduced liquidity will affect the critical function of price discovery performed by the exchanges or other trading platforms. Furthermore, trading on the DLT with T instant rather than T + X would increase difficulty in execution, resulting in execution blockage.<sup>87</sup> This will reduce trading at the exchanges and, consequentially, affect their revenue. As exchanges have fixed costs for maintaining their infrastructure and other compliance costs, they will increase trading fees which will be borne by the end investors.

However, DLT can also facilitate the transfer of collateral to the benefit of the CCPs. As the collateral posted by the clearing members can only be transferred during the opening time of the central securities depositories (CSDs), CCPs need to collect the collateral of their members from a CSD during its opening time.<sup>88</sup> Currently, a European CCP would need to collect collateral of their members against their trading risk during the non-opening time of the European CSD from a US CSD. If DLT can continue allowing collateral to be transferred after the opening time of the CSD, this can potentially increase efficiency of CCP's risk management function. The question is whether transfers of such collateral on the DLT during the non-opening time of the CSD will be legally recognised and whether such transfer on the DLT will be the same as transfers between accounts by the CSD.

#### 4.4 Settlement

The industry's view seems to suggest that the benefit of DLTs lies in the post-trade segment<sup>89</sup>, particularly the settlement of securities.<sup>90</sup> Blockchain will improve efficiency to securities settlements by reducing the settlement time from the current T+2 to T+0, meaning that blockchain can provide almost real-time settlement.<sup>91</sup> How this will be achieved with blockchain has not been detailed and tested, although some of the exchange operators have partnered with tech companies to experiment on selected un-listed companies on a permission-based chain ('private chain'). Therefore, it is reasonable to assume that it is possible to carry this out – be it on an open chain ('permission less-based chain' or 'public chain') or a private chain – to achieve the intended outcome of T+0. The

---

<sup>87</sup> Diana Chan, 'Moving from T+2 to T-instant: Blockchain distributed ledger technology could cut the costs and complexity of post-trade processing' Financial News, 28 September 2015

<https://www.fn.london.com/articles/blockchain-moving-from-tplus2-to-t-instant-20151002>

<sup>88</sup> European Central Bank, 'The potential impact of DLTs on securities post-trading harmonisation and on the wider EU financial market integration' (2017)

[https://www.ecb.europa.eu/paym/intro/governance/shared/pdf/201709\\_dlt\\_impact\\_on\\_harmonisation\\_and\\_integration.pdf](https://www.ecb.europa.eu/paym/intro/governance/shared/pdf/201709_dlt_impact_on_harmonisation_and_integration.pdf)

<sup>89</sup> Andrea Pinna Wiebe Ruttenberg, 'Distributed ledger technologies in securities post-trading: Revolution or evolution?' European Central Bank, Occasional Paper Series No 172, April 2016.

<https://www.ecb.europa.eu/pub/pdf/scpops/ecbop172.en.pdf>

<sup>90</sup> EuroClear and Slaughter and May, Blockchain settlement: Regulation, innovation and application, November 2016, <https://www.swift.com/file/34341/download?token=qqx60Nus>

<sup>91</sup> Hong Kong Exchanges and Clearing Limited (HKEX) introduced realtime DvP for northbound stock connect trading- its mutual market access programmes with the Shanghai and Shenzhen stock exchanges- in November 2017. Realtime DvP is expected to be used by institutional investors.

[https://www.hkex.com.hk/news/news-release/2017/1711062news?sc\\_lang=en](https://www.hkex.com.hk/news/news-release/2017/1711062news?sc_lang=en)

benefits the DLT can offer are not unquestionable in terms of their impact on price-discovery, participation in the market, and the objective of democratising the financial market.

Most contemporary modern financial markets use a central securities depository (CSD) to settle securities trades based on the delivery versus payment system ('the DVP system'), where securities are transferred in the centralised ledgers maintained by the CSD against transfers of payment maintained by a bank (i.e. a central bank). CSDs may or may not legally hold the securities – which are beneficially owned by the end-investors – in the ledgers they electronically maintain, depending on the law under which the CSD operates. If the CSD is to be replaced by DLT, how is the default risk of settlements to be mitigated, and who can guarantee the ownership of securities?

#### ***4.4.1 Mitigating default risk***

Settlement efficiency is achieved by the CSD netting all the trades – setting off trades between parties such as members of the CSD ('normally investment banks') – rather than making a transfer for each trade.<sup>92</sup> The current settlement time is two days after the trade ('T+2'),<sup>93</sup> and this time period allows securities traded on different venues and markets to be settled with sufficient time. This also allows members of the CSD, usually the investment banks and brokers, sufficient time to consolidate the information on the trades within their organisation to be given to the CSD to effect transactions on the centralised ledgers.<sup>94</sup> This can mitigate the default risk that is more likely to arise in a market system operating on a same-day settlement basis ('T+0'). If the purpose of the DLT is to bring about a settlement system of T+0, default risk may increase and can cause a blockage in the trading system, as one trade depends on the successful trade of another. In addition, there are markets that operate on a T+0 basis without the use of DLT, such as China and Hong Kong.<sup>95</sup> Thus, if the financial participants in a market can agree to operate on a T+0 basis, this can be achieved without the assistance of DLTs. The current T+2 model benefits certain intermediaries who can utilise the cash realised from the sale of securities. The removal of the centralised ledgers system performed by the CSD will reduce settlement efficiency by netting multiple transactions into one single position. Furthermore, CSDs can perform functions ancillary to settlement facilities, such as custodian services and security gate-keeping. These functions, and the way in which DLT can be used to realise efficiency and benefits, will be discussed in the following sections.

#### ***4.4.2 Custodian services***

---

<sup>92</sup> The Giovannini Group, Second Report on EU Clearing and Settlement Arrangements, April 2003 [http://ec.europa.eu/internal\\_market/financial-markets/docs/clearing/second\\_giovannini\\_report\\_en.pdf](http://ec.europa.eu/internal_market/financial-markets/docs/clearing/second_giovannini_report_en.pdf)

<sup>93</sup> Article 5, EU Central Securities Depository Regulation (CSDR).

<sup>94</sup> Boston Consulting Group, 'Cost benefit analysis of shortening the settlement cycle' 2012 Commissioned by The Depository Trust and Clearing Corporation.

<sup>95</sup> Hong Kong Exchanges and Clearing Limited (HKEX) introduced realtime DvP for northbound stock connect trading- its mutual market access programmes with the Shanghai and Shenzhen stock exchanges- in November 2017. Realtime DvP is expected to be used by institutional investors.

[https://www.hkex.com.hk/news/news-release/2017/1711062news?sc\\_lang=en](https://www.hkex.com.hk/news/news-release/2017/1711062news?sc_lang=en)

As CSDs maintain a centralised ledger system that records the ownership of securities, they can also act as managers of these securities by holding them for the benefit of the end-investors.<sup>96</sup> In the UK, the CSD does not act as a securities custodian, but rather as a notary of the securities, recording the ownership of the securities held by members.<sup>97</sup> The financial intermediaries, who are members of the CSD, hold the securities in trust for their immediate clients (who are not necessarily the end-investors). Under the current model of securities intermediation, the identities of the end-investors – even the domestic ones – are difficult to ascertain. This can make it difficult to enforce the law against market misconduct, such as money laundering, market abuse, and tax evasion. DLT is potentially a regulatory technology (RegTech) that increases the level of transparency in securities trading. However, such a guarantee of transparency can only be achieved through a private chain – a permission-based chain – whereby a trusted third party will act as an authentication authority. The authentication authority will provide the public key infrastructure that prevents fraudulent transactions, i.e., forged transactions. While on the private chain, participants may wish to maintain a certain level of privacy so as to prevent others from knowing their trading positions/strategies as well as their individual personal wealth. At the same time, personal data may need to be made available for law and enforcement purposes.<sup>98</sup> The authentication authority will be able to act in such a way that both protects personal data against data theft and protects market integrity against misconduct.

## 5. A de-centralised network

The blockchain network can revolutionise market practice in securities trading, which is essentially a centralised model, be it an exchange, an organised trading platform, or an alternative trading platform. In these centralised trading platforms, trade orders will be matched centrally, netted by a central counter party (CCP), and settled by a central securities depository (CSD). Decentralisation by DLT means that these operators or their functions could be made redundant. Consequentially, systemic risk, market conduct risk, and operational risk would be left unmanaged. First, the markets will become fragmented on the open chain. It is not certain whether the capital market, when on the DLT, will increase competition, as seen in the rise of the alternative trading platforms. The peer-to-peer model does not promise more liquidity, ensuring the price-discovery function of the market. This model can also lead to a higher cost for the investor seeking to exit the company or the market. Because a CCP will not perform its netting function, the market on the DLT will operate on a pre-funded basis, losing the function of an open market. Furthermore, the nodes on the open chain will act independently in keeping the ledgers. It will take approximately 20 minutes to update the ledgers on the chain. Because the nodes will be based on different locations around the world, it will be more difficult to coordinate their actions in dealing with market shocks and other instances of market turbulence, such as Black Swan events. When securities trades happen without coordinated action, there will

---

<sup>96</sup> Diana Chan, Florence Fontan, Simonetta Rosati and Daniela Russo, 'The securities custody industry', European Central Bank Occasional Paper 68, 2007.

<https://www.ecb.europa.eu/pub/pdf/scpops/ecbocp68.pdf?5ff757225862fdd1894d8dab08815b19>

<sup>97</sup> Madeleine Yates and Gerald Montagu, *The law of global custody: legal risk management in securities investment and collateral*, (4th edn Bloomsbury Professional 2013) pp 243-286.

<sup>98</sup> Matthias Berberich and Malgorzata Steiner, 'Blockchain Technology and the GDPR - How to Reconcile Privacy and Distributed Ledgers' (2016) 2 (3) *European Data Protection Law Review* pp. 422-426

be mismatches in trade, as some nodes may validate a trade without an update on the ledgers. This can lead to systemic problems on the capital market.<sup>99</sup>

Market conduct risk will be difficult to control. Capital market rules have been designed to protect investors and ensure fair dealings. The rules relate to such matters as conflicts of interest,<sup>100</sup> insider dealing, market manipulation,<sup>101</sup> disclosure<sup>102</sup> and transparency regimes.<sup>103</sup> These essential rules apply to listing, issuing, trading, clearing and settlement. For listing, the prospectus regime applies to ensure that the issuing companies pass a certain quality control threshold to protect the investor. The exchanges and other intermediaries, such as underwriters, financial analysts, and lawyers in the IPO, all act as critical capital market gatekeepers. On the DLT, especially on an open chain, the location of the issuing entity will be difficult to ascertain. Yet, the issuing of the securities can still reach investors who have access to the nodes on the chain. However, there will be reduced or no protection for investors. For trading, because trades will be made on an encrypted basis, no disclosure of information will be made to the market. Pre-trade and post-trade disclosure about price and volume need to be made for trades on regulated markets. This is to ensure that investors obtain the best price available. Without this information, the prices of the securities offered will be easily manipulated. For trades on DLT, the investor who loses out through price manipulation will have no access to regulatory assistance to obtain compensation. This can be seen in the LIBOR scandal, where pricing could be manipulated because there was no regulatory oversight. For clearing, the CCP performs critical risk management functions for the capital market, and DLT will cause the decentralisation of this risk management function. The current regulatory regime at the EU level shows the risks of CCP's operations in the areas of interoperability, transfer of open interest, and third country supervision. If each node on the chain is also to perform such risk management functions, recovery and resolution will be a challenging task, as coordination will be more difficult. For settlement, if the DLT can make delivery-versus-payment (DVP) instantaneous, the question that arises is when, under the law, is settlement recognised? As there will be a time lag between the actual transaction and the validation of the settlement on the nodes, such a time lag represents a risk. Because transactions on the chain are encrypted, trades will be

---

<sup>99</sup> Bank for International Settlement, 'Distributed ledger technology in payment, clearing and settlement: An analytical framework' (2017) <https://www.bis.org/cpmi/publ/d157.pdf>

<sup>100</sup> Ferrarini, G. and Moloney, N. (2012) Reshaping Order Execution in the EU and the Role of Interest Groups: from MiFID I to MiFID II. *European Business Organization Law Review*, 13 (4), pp. 557-597.

<sup>101</sup> Council Directive 2003/6/EC on insider dealing and market manipulation; Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse.

<sup>102</sup> Directive 2003/71/EC of the European Parliament and of the Council of 4 November 2003 on the Prospectus to be Published when Securities are Offered to the Public or Admitted to Trading and Amending Directive 2001/34/EC. *Official Journal of the European Union* 31 December. Available from: <http://data.europa.eu/eli/dir/2003/71/oj>

<sup>103</sup> Directive 2013/50/EU of the European Parliament and of the Council of 22 October 2013 amending Directive 2004/109/EC of the European Parliament and of the Council on the harmonisation of transparency requirements in relation to information about issuers whose securities are admitted to trading on a regulated market, Directive 2003/71/EC of the European Parliament and of the Council on the prospectus to be published when securities are offered to the public or admitted to trading and Commission Directive 2007/14/EC laying down detailed rules for the implementation of certain provisions of Directive 2004/109/EC. *Official Journal of the European Union* 6 November.

made on the basis of anonymity. In other words, it would be difficult to trace fraudulent transactions. Although settled transactions are not reversible under the current law and market practices, there are exceptions to such irrevocability, one of which is the case of fraudulent transactions. Trades recorded on the ledgers cannot be easily reversed, as they are immutable. This can lead to the ‘hard fork’ problem, as seen on the Ethereum platform – a cryptocurrency trade platform. When nodes on the platform cannot agree whether fraudulent trades can be reversed, two parallel systems can be created as a result. If a ‘hard fork’ occurs in the securities trade, it can cause a company’s securities to be doubled and traded on two systems. Furthermore, because the trades will be encrypted and the transactions enabled by the use of public and private keys, if the investor loses the private key, they will not be able to recover the assets. If the system is subjected to cyberattacks,<sup>104</sup> there will be no guarantee of recovery of the investors’ assets.

## 6. A disintermediated network imagined

Other than exchanges, clearing houses (CCP), CSDs, and custodian banks, there are also brokers, banks, and asset managers who intermediate securities trades in the investment world. Without their functionality, cross-border trades and cross-border investment would not be possible in trade across different centralised markets. When DLT creates a decentralised market space, the functions of financial intermediaries are said to be redundant. Brokers would no longer need to execute orders for their clients. Custodian banks would no longer need to hold securities for their clients. Asset management would not be required to create an investment scheme with a portfolio to facilitate cross-border investment to meet the needs of international investors.<sup>105</sup> Proxy advisors and shareholder services would not be in demand, as investors would be able to exercise their own voting rights on the blockchain. The issuing company would be able to know who holds its securities and how much they hold. This information could help the company facilitate corporate actions such as voting rights and other economic entitlements. The peer-to-peer blockchain network has the potential to achieve shareholder transparency and to reduce the cost and risk of intermediated securities. The International Central Securities Depositories (ICSDs) that currently facilitate securities trades at cross-border level would be unnecessary. As a result, discussions about the insolvency of an intermediary and the effect of that insolvency on the rights and entitlements of the end investor would be redundant.<sup>106</sup>

---

<sup>104</sup> Major bitcoin exchanges hit by cyberattacks as record rally makes them a target, see <https://www.cnbc.com/2017/06/14/major-bitcoin-exchanges-hit-by-cyberattacks-as-record-rally-makes-them-a-target.html>

<sup>105</sup> With the invention of Robo-advisors - which use algorithms to recommend a portfolio of funds based on an investor’s answers to an online questionnaire- asset management role as advisor will be gradually diminished. See Jonathan Leaf, ‘The Rise of Robo-Advisors Financial Planning’, (2012) 41 (8) pp 39-42; However, some asset management firms have invested in the development of robo-advisors. See Aliya Ram and Robin Wigglesworth, ‘When SiliconValley came to Wall Street: Mainstream asset managers have begun using big data and machine learning’ Financial Times; London (UK) 30 Oct 2017: 6; Also see Ian Hunt and Chris Mills, ‘Distributed Ledger Technology – An Emerging Consensus on the Buy-Side’ The Alternative Investment Management Association (AIMA) Research Report, 2018 <https://www.aima.org/uploads/assets/uploaded/dd2326bb-b9ed-4be2-b5b905e29d3dfa63.pdf>

<sup>106</sup> Luc Thevenoz, ‘Intermediated Securities, Legal Risk, and the International Harmonization of Commercial Law’ (2008) 13 (2) Stanford Journal of Law, Business & Finance, pp. 384-452.

## 7. How to regulate trades on DLT: a consensus model or a private chain?

### 7.1 A consensus model

With the blockchain network, each node will act as a data node, and all the nodes will form a network of data centres. Participants maintain the integrity of the ledger by reaching a consensus about its state - the accuracy of a ledger- by using the consensus algorithm. That is the algorithm for mutually approving a distributed ledger using Proof of Work and Proof of Stake. It is difficult to know which law will govern and which regulator will have enforcement power over activities and transactions that occur over the network.<sup>107</sup> If there is a risk of cyber attack, which relates to cybersecurity, the state has a role in ensuring safety over the network (the territorial governance). The state may use criminal law to deter cyber attacks and may use its sovereign power to cooperate with other state entities in ensuring security at the cross-border level. There are other areas where state intervention –as opposed to self-regulation of network participants – is justified. These may include market abuse, data protection, and competition law.

Assume that network participants were able to make their own rules to ensure market safety, stability, and investor protection (to ensure participant confidence). The participants would need to decide 1) who is allowed to join the network; 2) the level of transparency in the network; and 3) how disputes are to be resolved.<sup>108</sup> It is submitted that even a consensus-based network blockchain would need regulation. The question is, therefore, who should regulate and what is to be regulated?<sup>109</sup>

It is submitted that a public-private regulatory collaboration would be the best model to provide the network with rules, adjudication, and enforcement.<sup>110</sup> There is nothing new about such a collaborative model. Indeed, there are many areas where such a collaborative regulatory model provides the basis of governance.<sup>111</sup> What may be emerging or shifting is the line of demarcation between state and private regulation.<sup>112</sup> With distributed ledgers connecting between nodes that are based in different jurisdictions, traditional conflict-of-law rules may not, without further development, be applicable to incidents that occur over the network.<sup>113</sup> For instance, which law should be applicable to the transfer of securities in

---

<sup>107</sup> Gabrielle Patrick and Anurag Bana, 'Rule of Law Versus Rule of Code: A Blockchain Driven Legal World' (November 2017) available at: <https://www.ibanet.org/Document/Default.aspx?DocumentUid=https://>

<sup>108</sup> Pietro Ortolani, 'Self-enforcing Online Dispute Resolution: Lessons from Bitcoin' (2016) 36 Oxford Journal of Legal Studies 595, 608.

<sup>109</sup> Elizabeth Sara Ross, 'Nobody Puts Blockchain in a Corner: The Disruptive Role of Blockchain Technology in the Financial Services Industry and Current Regulatory Issues' (2017) 25 (2) Catholic University Journal of Law and Technology, pp. 353-386

<sup>110</sup> Dominique Custos and John Reitz, 'Public-Private Partnerships' (2010) 58 American Journal of Comparative Law pp. 555-584.

<sup>111</sup> Julia Black, 'Enrolling Actors in Regulatory Processes: Examples from UK Financial Services Regulation' (2003) Public Law 63-91

<sup>112</sup> Carla Reyes, Nizan Geslevich Packin, and Benjamin Edwards, 'Distributed Governance' (2017) 59 William & Mary Law Review pp. 1-32

<sup>113</sup> World Economic Forum, 'Realizing the Potential of Blockchain: A Multistakeholder Approach to the Stewardship of Blockchain and Cryptocurrencies' White Paper, June 2017 [http://www3.weforum.org/docs/WEF\\_Realizing\\_Potential\\_Blockchain.pdf](http://www3.weforum.org/docs/WEF_Realizing_Potential_Blockchain.pdf)



such a distributed ledger network?<sup>114</sup> Since there are different laws across different jurisdictions, the legal status of smart contracts would need to be clarified by introducing a standard that will facilitate compliance issues such as privacy requirement and anti-money laundering control and allow for a life-cycle management of smart contracts.

## ***7.2 The need for a trusted third party – authentication and identification management***

It has been said that blockchain has the potential to replace a system that requires a trusted third party with a system that is itself a trusted model. This statement is based on two essential promises: decentralisation and disintermediation. Currently, the trust system is built on a centralised system in which the exchanges, CCPs and CSDs will ensure operational safety. A certification authority, which acts as an intermediary between traders and exchanges, authenticates trade orders (proves you are who you say you are).<sup>115</sup> The CCP acts as a trusted third party that will step into a default trade, and the CSDs can authenticate the record of securities ownership. Instead of such a centralised trust system, blockchain hopes to bring about a distributed trust system whereby trust is maintained by all the participants (the nodes) through a consensus model. In this distributed trust system, as opposed to a centralised trust system maintained by a third party, authentication will be based on algorithms. In effect, records cannot be tampered with (or be nearly tamper-proof) and fraudulent transactions cannot be made without putting in a substantial amount of time and energy, thus making such fraudulent activities not cost-effective. However, to maximise the power of distributed ledgers, there will need to be interoperability of authentication which, in turn, will require, at international level, agreements about data interoperability, policy interoperability and the effective implementation of international standards. Leaving this question aside, there are a number of issues that blockchain technology has not yet managed to address, including the prevention of money laundering, identity theft, violation of data protection laws, the problem of settlement finality, the hard fork problem, recovery and resolution, and cyber security issues. It is submitted that mechanisms will need to be developed to map blockchain transactions to individual users and entities in a secure manner. Furthermore, credentials on the blockchain will need to be stored and or aligned to a sidechain (off blockchain) to be carried out by trusted third parties.

### ***7.2.1 Risk of fraud and money laundering***

On the blockchain network, transactions can be made anonymously because participants can use ‘Private Key Cryptography’ and ‘Public Key Cryptography’ to make transactions. Although the transactions are transparent on the shared ledgers, the person who initiates the transaction will not be traceable. In a decentralised network where each node can facilitate securities trading, using the system to launder the money would be more easily facilitated compared to the present system, where the intermediary can act as a gatekeeper

---

<sup>114</sup> This is one of the risks in ICO as the UK Financial Regulator may not have jurisdiction over transactions over DLTs. See Financial Conduct Authority, ‘Consumer warning about the risks of Initial Coin Offerings (‘ICOs’)’. Published 12/09/2017, available at: <https://www.fca.org.uk/news/statements/initial-coin-offerings>

<sup>115</sup> Scott Shackelford and Steve Myers, Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace (2017) 19 Yale Journal of Law and Technology, pp. 334-388.

under Know Your Customer (KYC) rules.<sup>116</sup> Bitcoin trades have demonstrated that there are 'dark web' trading sites,<sup>117</sup> known as the Silk Road,<sup>118</sup> which associates with criminal transactions,<sup>119</sup> so standards will need to be developed to ensure that the confidentiality, integrity and availability of users and entities are maintained.<sup>120</sup> Compliance to money laundering and Know Your Customer (KYC) requirements will need to be embedded.<sup>121</sup> This will also include standardising electronic KYC processes.<sup>122</sup>

### **7.2.2 The risk of Public and Private Key infrastructure: loss of assets**

In the blockchain network, there will be no central body (or trusted third party) to authenticate transactions and safeguard the information/data. Instead, there will be hyper-ledgers distributed among participants. To transmit, authenticate, and access information, both public keys and private keys will be used. Public keys will be used to encrypt documents/messages and private keys to decrypt them.<sup>123</sup> For instance, as illustrated in Figure 3,<sup>124</sup> if A wants to send a message to B, A needs to use a private key to encrypt the message, and only A's public key can decrypt it. A can send B a public key to authenticate the message (i.e. to confirm the message is from A). However, if the parties lose these keys or allow others to access them –causing theft – they would lose assets as a result, and it would be impossible to recover those assets.

Figure 3. Mechanism of public key cryptography

---

<sup>116</sup> However, DLT, if designed properly, can also be used as RegTech to perform the duty of KYC.

<sup>117</sup> Michael Chertoff, 'A public policy perspective of the Dark Web' (2016) 2 (1) Journal of Cyber Policy, pp 26-38 <https://doi.org/10.1080/23738871.2017.1298643>

<sup>118</sup> Andrew Norry, 'The History of Silk Road: A Tale of Drugs, Extortion & Bitcoin' Blockonomi 29 November 2017 <https://blockonomi.com/history-of-silk-road/>

<sup>119</sup> James Ball, Charles Arthur and Adam Gabbatt, 'FBI claims largest Bitcoin seizure after arrest of alleged Silk Road founder' The Guardian, October 2013, <https://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin>

<sup>120</sup> Inside Bitcoins, 'Blockchain Identity: Solving the Global Identification Crisis', 27 September 2015 <https://insidebitcoins.com/news/blockchain-identity-solving-the-global-identification-crisis/35028>

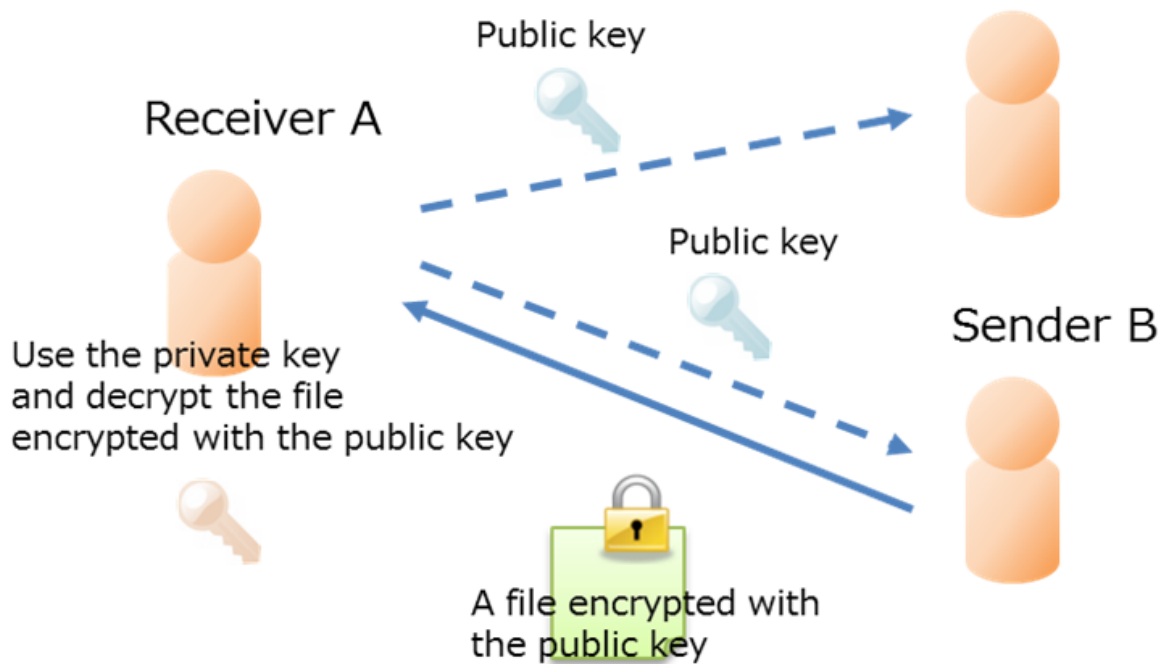
<sup>121</sup> Neepa Patel, 'Blockchain KYC/AML Utilities for International Payments: A Regulatory Solution for Anti-Money Laundering and Financial Inclusion? R 3 Report, 6 November 2017 [https://www.r3.com/wp-content/uploads/2018/02/blockchain\\_kyc\\_aml\\_utilities\\_R3.pdf](https://www.r3.com/wp-content/uploads/2018/02/blockchain_kyc_aml_utilities_R3.pdf)

<sup>122</sup> International Telecommunication Union, 'Successful use of security standards, ITU-T Technical Report, 7 September 2016. [https://www.itu.int/dms\\_pub/itu-t/opb/tut/T-TUT-SEC-2016-PDF-E.pdf](https://www.itu.int/dms_pub/itu-t/opb/tut/T-TUT-SEC-2016-PDF-E.pdf)

<sup>123</sup> Public key cryptography, IBM Knowledge Center

[https://www.ibm.com/support/knowledgecenter/en/SSB23S\\_1.1.0.14/gtps7/s7pkey.htm](https://www.ibm.com/support/knowledgecenter/en/SSB23S_1.1.0.14/gtps7/s7pkey.htm): What is public-key cryptography? A look at the encryption algorithm and its security benefits, GlobalSign, <https://www.globalsign.com/en/ssl-information-center/what-is-public-key-cryptography/>

<sup>124</sup> Nomura Research Institute, Survey on Blockchain Technologies and Related Services FY2015 Report. Available at [http://www.meti.go.jp/english/press/2016/pdf/0531\\_01f.pdf](http://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf)



### 7.2.3 One world, one internet, and the network effect (Fork problem)

As seen in the crypto-currency world, disagreement between participants can lead to a break-up of the network that causes a ‘fork’.<sup>125</sup> A fork involves splitting the path of a blockchain by invalidating transactions confirmed by nodes that have not been upgraded to the new version of the protocol software.<sup>126</sup> This is illustrated in Figure 4. A hard fork can be implemented to correct important security risks found in older versions of the software, to add new functionality, or to reverse transactions. This can also be a major risk for capital markets that use DLTs. For instance, Company X has 100 shares on Blockchain 1. When a fork occurs, Blockchain 2 will also have 100 shares of Company X (the mirror image of Company X’s shares on Blockchain 1), with the same shareholders. Because there will be no central registration of the company’s shares, e.g. Companies House in the UK, the fork problem can create duplicate shares which may confuse shareholders, markets, and companies. When there is a corporate action, instead of one vote, a shareholder will get two. A gets one vote on Blockchain 1 and one vote on Blockchain 2. When shareholders sell their shares to others on different chains, this can cause major disruptions to corporate governance that is currently built on shareholder action. A can sell shares of Company X to B

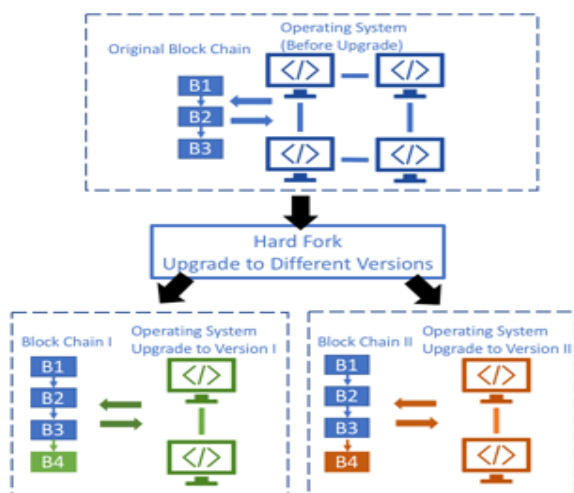
<sup>125</sup> J. I. Wong and I. Karr, ‘Everything you need to know about the Ethereum “Hard Fork”’ Quartz 18 July 2016 at <http://qz.com/730004/everything-you-need-to-know-about-the-ethereumhard-fork/>. ; A crypto-currency civil war. Making Bitcoin work better: A compromise over the currency’s future may not last. Jul 29th 2017, The Economist

<https://www.economist.com/news/finance-and-economics/21725598-compromise-over-currencys-future-may-not-last-making-bitcoin-work-better>

<sup>126</sup> Nomura Research Institute, Survey on Blockchain Technologies and Related Services, p 11. FY2015 Report. Available at [http://www.meti.go.jp/english/press/2016/pdf/0531\\_01f.pdf](http://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf)

on Blockchain 1 and A can sell to C on Blockchain 2. In other words, a share that was owned by A before the fork is now owned by B on Blockchain 1 and C on Blockchain 2. This creates a problem: who has the voting rights recognised by Company X and by law? There is a need to implement interoperability – allowing transfer of messages and assets across the blockchain. Furthermore, there is a need to incorporate interoperability between different blockchain networks and to non-blockchain networks. In other words, a global approach to data governance is critical in addition to technical interoperability between different blockchains.

Figure 4. A hard-fork



### 7.2.4 Recovery and Resolution

Financial institutions need to have a recovery and resolution regime in order to continue their business in times of crisis.<sup>127</sup> For instance, in the event of a major attack or extraordinary event such as flash crashes, exchanges must be able to take measures to secure their operations and main market safety. It is said that distributed ledgers are inherently harder to attack because instead of a single database, there are multiple shared copies of the same database, so a cyber-attack would have to attack all the copies simultaneously to be successful.<sup>128</sup> However, some argue that centralised systems will have better recovery and resolution capabilities. According to this argument, in a decentralised and distributed system where there are several nodes – several exchanges and many more banks – the coordination required to design a business continuity plan would be more difficult to achieve, and it would be more difficult to take action at the time of an attack, for

<sup>127</sup> The EU Recovery and Resolution Directive (RRD) DIRECTIVE 2014/59/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, under which financial institutions are required to prepare and regularly update recovery plans that set out the measures they would take to restore their financial position following a significant deterioration.

<sup>128</sup> Government Office for Science, Distributed Ledger Technology beyond block chain, 2016 , p 6. Available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/492972/gs-16-1-distributed-ledger-technology.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf)

instance due to software bug or loophole. On the other hand, one may also argue that the blockchain network is itself a recovery and resolution regime. Because blockchain is a distributed ledger network, it would be more difficult for an attacker to make a successful attack, which would require that a majority of nodes be affected. This is a contentious issue, and we must wait and see how DLTs evolve. Yet, one should also consider how blockchain participants would be protected from joint liability if adoption of blockchain is to be increased.<sup>129</sup>

## 8. Conclusion

DLTs have the potential to transform the conduct of public and private sector organisations particularly in areas of highly regulated industry with increased private-public governance partnership.<sup>130</sup> The benefits of DLTs to the capital market are premised on decentralisation and disintermediation. However, a careful examination of the life cycle of the securities trade shows that decentralisation and disintermediation would not bring about the intended benefits – i.e. lowering the costs of securities trading, facilitating more peer-to-peer trade at the domestic or cross-border level, and enabling more access to capital for SME enterprises. That is not to say that DLTs, in their current form, cannot be used to correct some of the market failures by making trades more transparent, the system more secure, and, at the same time, making the system more cost-efficient for the participants. In this sense, DLTs can be a Regulation Technology (RegTech)- that uses technical code (software and protocols) to assure compliance with legal code (rules consisting of legal obligations), and, in so doing, reduces the costs of legal compliance.<sup>131</sup> Yet this would still require trusted third parties to maintain the DLT's network in order to mitigate market and operational risks and act as *de facto* regulators. Furthermore, the term 'distributed' is used to describe the effect to the blockchain network, however, it does not denote that there is no overall controlling authority or owner. There are various distributed ledger models, with different degrees of centralisation and different types of access control, to suit different business needs. The question is, therefore, who should act as the trusted third parties – governments, incumbent financial market infrastructure operators, banks, technology companies, or the new FinTech companies? As DLTs will operate at the cross-border level, how is the governance of such networks, akin to the Internet world, to be coordinated at a transnational level?

---

<sup>129</sup> Dirk Zetsche and Ross Buckley, and Douglas Arner, 'The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain' (August 13, 2017). University of Illinois Law Review, 2017-2018, Forthcoming; University of Luxembourg Law Working Paper No. 007/2017; Center for Business & Corporate Law (CBC) Working Paper 002/2017; University of Hong Kong Faculty of Law Research Paper No. 2017/020; UNSW Law Research Paper No. 52; European Banking Institute Working Paper Series 14. Available at SSRN: <https://ssrn.com/abstract=3018214> or <http://dx.doi.org/10.2139/ssrn.3018214>

<sup>130</sup> Julia Black, 'Paradoxes and Failures: 'New Governance' Techniques and the Financial Crisis' (2012) 75(6) *Modern Law Review*, 1037–1063.

<sup>131</sup> Government Office for Science 'FinTech Futures: The UK as a World Leader in Financial Technologies' 2015. Available at [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/413095/gs-15-3-fintech-futures.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/413095/gs-15-3-fintech-futures.pdf)