Blockchain settlement

Regulation, innovation and application

Regulatory and legal aspects related to the use of distributed ledger technology in post-trade settlement

November 2016

Table of contents

Executive summary

Distributed Ledger Technology (DLT)[1] continues to generate significant interest within the securities markets, including with public authorities and regulators.

In February 2016, Euroclear and Oliver Wyman published a paper[2] which aimed to help leaders in capital markets understand the potential of the technology, the paths for potential adoption and the decisions facing industry participants. It also looked, briefly, at the major hurdles that would need to be overcome, including in the areas of law, regulation and policy.

Since the publication of that paper, many industry commentators have noted the potential for significant savings in the post trade industry and initiatives are now being launched to try to deliver those savings. ESMA is demonstrating a welcome and proactive engagement with the issues and has recently consulted on the application of DLT to securities markets[3] (we refer to this as the 'ESMA Discussion Paper'). Similarly, the European Central Bank (ECB) has published helpful contributions to the discussion.[4]

But there has, to date, been little market analysis of the detailed legal and regulatory challenges and opportunities faced by the post trade industry. This paper, prepared by Euroclear with support from fintech lawyers at Slaughter and May, aims at moving this discussion to the next level by examining in detail the regulatory and legal aspects of utilising DLT in a post trade environment. As a regulated Financial Market Infrastructure (FMI), Euroclear is well placed to analyse which elements of the DLT post-trade environment may require specific regulatory attention with a view to preserving financial stability and ensuring adequate investor protection. Our considerations focus mainly on the existing regulatory and legal framework and its underlying policy objectives. However, we recognise that the future adoption of DLT in post-trade settlement may, in due course, drive developments in the legal and regulatory landscape. Our thoughts on this long term future are included in an Appendix to this paper.

This paper addresses the following key issues:

1. While regulated market infrastructures must clearly continue to meet their existing numerous regulatory and legal obligations, the use of DLT by a central securities depository (CSD[5]), for example, should not by itself trigger any specific regulatory approvals. It is the CSD as an institution which is authorised, not its choice of technology platform. We therefore see no need for specific new DLT legislation or regulation in this field.

2. The current regulatory and legal environment is not designed to facilitate the wide-spread use of DLT in the securities post-trade process. Important open questions remain, such as:

   a. the participation of central banks in a DLT environment and the use of central bank money for securities settlement;

   b. legal certainty and, in particular, questions in respect of the legal concept of securities accounts and the law applicable to such accounts;

---

[1] The terms 'DLT' and 'blockchain' are not necessarily interchangeable. However, for the purposes of this paper, we assume that capital markets DLTs will use blockchain technology and, as such, we use the two terms interchangeably.

[2] Euroclear and Oliver Wyman Joint Report "Blockchain in Capital Markets – The Prize and The Journey" February 2016

[3] ESMA Discussion Paper 2016/773 "The DLT applied to Securities Markets" June 2016

[4] ECB Occasional Paper Series No 172 "Distributed ledger technologies in securities post-trading; Revolution or evolution?" February 2016

[5] References to CSDs include both national CSDs and international CSDs (ICSDs) such as Euroclear.

<ol type="a" start="3">
the extent to which one or more central authorities are required to perform certain functions such as the management of keys, smart contracts, and issuance of assets, and the regulatory treatment of such new central infrastructure functions;
the migration to DLT systems and interoperability between DLT and non-DLT systems which operate in several jurisdictions worldwide with numerous competent authorities involved; and
data protection and cyber resilience requirements, which may need to be revisited.

<ol start="3">
Any regulatory or legal analysis of a DLT solution will naturally depend on the use case and the precise design of that solution. At one extreme, all transaction data could be shared between all nodes with full transparency and no central authority. At the other extreme, transaction data could be sent to a central authority for validation and block creation, with participants having access only to data which they themselves have contributed. Between these two extremes, we would expect the adoption of DLT to have an impact on the role of CSDs. In some cases it could obviate the need for certain CSD services. In other cases, it could create a need for CSDs to provide additional infrastructure services that arise due to the adoption of DLT (such as private key and smart contract management), potentially in competition with other (non-CSD) providers of such services. Whatever the eventual role of CSDs in a blockchain-based settlement system, we believe that, in view of the regulatory and legal challenges discussed in this paper, it seems unlikely this could function as a completely decentralised system with no central authority.
Regulators and legislators, who are responsible for ensuring investor protection and financial stability, may wish to consider and propose an approach to some of the regulatory and legal issues raised in this paper. We believe that initially this may be best achieved through the issuance of guidance in the EU or by the establishment of formal principles to be adopted by the industry under the auspices of CPMI-IOSCO. In the longer term, a revision or even an overhaul of the regulatory rules and legal reform may well be required. We believe that this will also need to be coordinated at a global and EU level.

1 Introduction to blockchain and its possible use in clearing and settlement

The original Bitcoin blockchain was designed as a relatively simple distributed ledger for recording transfers of coin tokens between network participants in a semi-anonymous environment. Since at least early 2015, blockchain concepts have been adopted by entrepreneurs and mainstream financial institutions alike, which are collaborating and competing to find financial services use cases to which the concept could be applied. Use cases are now being explored in fields far beyond value transfer and payments, including portfolio management reporting, financial product distribution, collateral management, anti-fraud measures and KYC processes.

This paper focuses on the application of DLT to securities safekeeping and settlement services primarily in a European context. Securities represent a more complex use case than cryptocurrencies, both in terms of their mechanics (for example, how they are settled and held, and how ongoing contractual obligations associated with the securities are serviced) and in terms of the applicable legal and regulatory environment. As such, the application of DLT to a securities post trade environment yields a richer variety of questions and potential challenges than in the already well-established cryptocurrency industry.

These additional complexities have not escaped the attention of regulators. In April 2015, the European Securities and Markets Authority (ESMA) published a call for evidence regarding investment using virtual currency or distributed ledger technology.[6] The ESMA Discussion Paper, published in June of this year, specifically targeted the application of DLT to securities markets.

This paper is aimed at assisting ESMA and others to assess, from a regulatory standpoint, the opportunities and challenges arising from the adoption of DLT in this industry.

ESMA has not yet, however, taken a public position on the desirability or practicalities of using DLT in a securities post-trade environment. One of the aims of this paper is to contribute to the better understanding of the legal and regulatory consequences of such use.

This paper builds on the report published by Euroclear and Oliver Wyman, which articulated a settlement system use case for blockchain. Specifically, this paper drills down to look at key legal and regulatory aspects of that use case and in particular examines:

- the benefits that DLT can bring to securities safekeeping and settlement, assuming as a base case the model described in the Euroclear and Oliver Wyman report;

- the various legal and regulatory issues that CSDs and other industry players might encounter in their possible deployment of DLT;

- possible new central authority roles and activities that might develop in a DLT-driven securities post-trade environment and that could be performed by a CSD, other 'central authorities' or infrastructures (such as the management of securities issuances, keys, identities, smart contracts and protocols); and

- the potential future regulatory landscape for providers of post-trade services in a DLT environment.

---

[6] Available at https://www.esma.europa.eu/sites/default/files/library/2015/11/2015-532_call_for_evidence_on_virtual_currency_investment.pdf.

Introduction to the role of CSDs

CSDs are financial markets infrastructures that facilitate the efficient processing of securities transactions. CSDs maintain book-entry systems where legal records of securities and other assets can be held in digitised form. Their core services typically include notary and central account maintenance services as well as settlement services.

CSDs typically also provide a range of ancillary services such as corporate action processing, securities lending and borrowing and collateral management services. This paper will, in particular, focus on the CSD core services, i.e., top-tier account maintenance, settlement and notary functions.

In a CSD, settlement preferably takes place using central bank money, where payment is made from or received in an account maintained at a central bank. Less commonly, settlement can also occur in commercial bank money when central bank money is not practical or available.

Benefits of DLT in securities safekeeping and settlement

An oft-cited benefit of applying DLT to a securities market which has adopted a multi-tier securities custody model is reduced **settlement latency**. This is achieved by reducing the time required to align data prior to settlement (as the use of DLT would require parties to collaborate to maintain the same underlying data set). However, while reducing settlement latency also reduces settlement risk, liquidity risk may well increase as netting possibilities reduce.

A private blockchain could also drive efficiencies in the settlement process, though from a purely technological perspective this may appear to be a surprising conclusion. The creation of a consensus-based distributed database should in principle be a slower process than the traditional centralised database technology by virtue of the fact that it requires multiple nodes to form a consensus rather than relying on updates to be verified by a single database controller.

But this belies the fact that in a multi-tier custody model (which is the model widely used to allow for cross-border holdings), settlement already proceeds according to a form of consensus reconciliation. As information and accounts are siloed between different banks or custodians, settlement requires execution and reconciliation between each layer of the holding chain. A DLT consensus-based settlement system could reduce inefficiencies associated with this process because information only needs to be recorded in a database maintained and accessed in a single distributed ledger, rather than in each separate database layer through the holding chain.

This leads us to another key advantage of applying DLT to multi-tier holding models. In a multi-tier holding model investors are exposed to **custody risk** – the risk that one of the custodians in the chain fails – and also to errors in the reconciliation of securities at any point throughout the custody chain. The blockchain model, by obviating the need for reconciliation, and removing database redundancies, could materially reduce the magnitude of these risks.

Use of DLT would also encourage straight-through **transparency** of the chain of custody. In the current multi-tier holding system, investors and other intermediaries typically have access only to the account kept by the intermediary closest to them in the chain. The potential of the blockchain is to merge these siloes of information into a single master record. This could, for example, be made fully transparent to the issuer and the CSD, and either fully or partially transparent to relevant regulators and intermediaries in the chain of custody. This could also provide investors with direct links to the issuer of a security, potentially facilitating the direct exercise of investor rights and actions with that issuer. Through the use of smart contracts, which would sit on top of the ledgers, certain corporate actions (at least those which are non-elective) could become automated.

These transparency benefits are very much in line with the evolutionary path of regulation. A drive towards increased transparency can be found in recent initiatives including the G20 High-Level Principles on Beneficial Ownership Transparency, the Shareholder Rights Directive and ISSA's Financial Crime Compliance Principles released in 2015. We would therefore expect the transparency benefits of a blockchain-based settlement system to be particularly attractive to regulators.

In markets which use a direct holding model, the putative benefits of using DLT described above are already available at CSD level. Yet, the direct holding model is not common in a global context as intermediaries closest to investors often access foreign markets through other intermediaries rather than directly.

Another frequently mentioned advantage of DLT is its potential to **disintermediate transactions**. Trading, clearing and settlement would become a single real time process updating a single ledger which does not involve multiple entities. However, this assumes that intermediaries in the chain of custody are mere record keepers. In

practice, intermediaries provide custody services as part of a broader package of services which may also include, for example, cash and liquidity management, credit lines, corporate action processing, compliance or related services, all of which investors value. They also have fiduciary responsibilities to end investors. Even in a direct holding model where investors' accounts are held at the top-tier level, custodians typically have the contractual relationship with the ultimate investors. Custodians are responsible for identifying account holders and, in practice, operate accounts on behalf of investors.

The key question, therefore, is how much investors will value the services provided by intermediaries in a DLT environment and if they will still require such services to the same extent. We believe that, at least in the short to medium term, customers' requirements for these services will enable custodians and other intermediaries to retain the broader customer relationship benefits of multi-level holding chains even where investors' holdings are maintained on a single ledger.

Application of DLT in securities safekeeping and settlement could yield substantial benefits:

- Reduced settlement latency

- Reduced operational and custody risk

- Increased transparency to issuers, end investors and regulators

- Reduced intermediation of recordkeeping

- Increased data security

Smart contracts

Part of the enthusiasm for blockchain use cases in the financial services industry is due to the potential for utilising so-called 'smart contracts.' Smart contracts are, in essence, computer protocols that record the terms of a contractual agreement and can be stored in an indelible, immutable blockchain so that, once agreed, they can be left to 'self-execute.' Smart contracts and blockchain are distinct concepts, and smart contracts can exist independently of the blockchain.

The key distinctions between smart contracts and automated services provided on traditional central systems are that:

1. smart contracts can (if the service model allows), be developed and deployed by users of the blockchain, to achieve specific bilateral business objectives; and

2. once deployed, a smart contract cannot be overridden without the specific agreement of all parties to the contract.

However, the incorporation of smart contracts into a blockchain could make them even more powerful. Once incorporated into blockchains, smart contracts can automatically execute a pre-determined action or transaction if prescribed conditions are verified (by the blockchain, or by reference to an agreed third party data source, known as an 'oracle') as having been met. Once executed, the action or transaction will be captured as a new block of data which is then irreversibly incorporated into the chain. In a securities market context, it is not difficult to see the potential for smart contracts to revolutionise securities and derivatives trading, collateralisation, close-out and settlement processes, as well as facilitating straight-through-processing of corporate actions, such as proxy voting.

Much effort is already being devoted to exploring smart contract use cases for securities markets. However, we are undoubtedly only in the very earliest stages of bringing smart contracts to the mainstream, as the recent 'DAO hack' event revealed (see page 14). In any event, it is also important to appreciate that smart contracts are unlikely to represent a 'silver bullet' leading to complete automation. Life cycles of securities cannot be completely automated as issuers typically make numerous decisions during the life of securities that cannot be anticipated at issuance (and therefore, which cannot be encoded precisely into a smart contract). This is particularly true of elective corporate actions where the holder of securities will need to make a number of decisions in order to participate in the corporate action.

A model for blockchain-based settlement

There are many ways in which DLT could be harnessed to deliver measurable improvements to securities settlement processes. For the purposes of this paper, we have focussed on exploring the legal and regulatory implications of an ambitious but realistic blockchain model for securities settlement. This broadly reflects the arrangements presented in the Euroclear and Oliver Wyman Joint Report as a 'utopian' blockchain model for securities settlement systems.

In this utopian model, the record of each security would be held on a blockchain asset ledger, which records the ownership details and transaction history of each security. Separately, a blockchain cash ledger records the cash (or cash equivalent) balance available for settlement purposes to each investor.

When Investor A and Investor B enter into a trade, they should (in a utopian world) both prove to each other, via the relevant ledgers, that each has the means to complete the transaction.

Utopian blockchain model for securities settlement systems

1. Securities transaction

Asset ledger stores ownership details and transaction history

In effect assumes the traditional custodian role

CSD is virtual layer coordinating the role of custodians

Pre-trade transparency and affirmation of holdings

Client A

Venue

Verification

Transaction hash

Client B

Trading platforms

Venues (e.g. exchanges, MTFs, bilateral voice conversations) still provide price discovery and match counterparties

Securely records ownership rights and encodes transaction details

Interoperable cash ledger enables near real-time settlement of asset transactions

Eliminates the need for CCP in cash transactions

Asset Ledger

Cash Ledger

€ $ £

2. Asset servicing

Reference database

Custody & portfolio management

Securities servicing

Fund management & accounting

Fund Ledger

Fund management and fund services operate on an interoperable fund ledger

Transfer agency replaced by distributed ledger consensus update

Risk management

Finance & accounting

3. Derivative transaction

Client A

CCP

Venue

Smart contract

CCP

Client B

Trading platforms

CCP still novates centrally cleared derivative trades and is entered into the ledger as the second counterparty

Contract programmed to execute automatically

Derivative ledger stores smart contracts and execution algorithms

Derivative Ledger

Collateral Ledger

Collateral management

Interoperable collateral ledger enables near real-time, efficient allocation of assets for margining

Reference data sources are agreed bases for calculating derivative positions and obligations (can be distributed ledgers or regular data sources)

Source: Euroclear and Oliver Wyman Joint Report, "Blockchain in the Capital Markets – The Prize and the Journey", February 2016

The two parties will then execute the transaction which could, if signed with their respective private keys, also provide all the information needed for settlement. The signed transaction is broadcast to all nodes of the two distributed ledgers to be verified, and a new block recording the transfer of ownership will then be added to all copies of the asset ledger and the cash ledger in line with the consensus mechanism. This would complete the transaction.

Participants in the settlement system can compile individual securities account balances by aggregating the transactions recorded in the blockchain associated with their identity on the network. Individual securities accounts could be updated whenever there is a validation on the network. Smart contracts could also be used to provide automatic updates to securities accounts, for example by automatically crediting dividends or adjusting margins, on the occurrence of pre-programmed events.

In this model, the need remains for coordinated oversight of asset issuances and ensuring orderly functioning of the market. The ledger may become the primary destination of asset issuances, although we might expect traditional CSDs to play the role of operational governance, responsible for coordinating the evolution of the ledger protocols, managing the introduction or cancellation of tokens on the ledger, regulator interface, and so on.

Overview of the most relevant laws and regulations

Securities settlement activities in Europe are governed principally by the Central Securities Depositories Regulation[7] (CSDR) and the Settlement Finality Directive[8] (SFD).

The CSDR came into effect on 17 September 2014, but has not yet been fully implemented. It was designed to harmonise aspects of the settlement process and to provide a common set of requirements applicable to CSDs. The CSDR provides several measures aimed at improving the safety and efficiency of the settlement process within the EU, all of which a blockchain settlement system would in principle need to satisfy. We cannot realistically envisage a policy basis or current policy appetite for the introduction of legislation to exempt a blockchain-based settlement system from these requirements.

The SFD unsurprisingly prescribes legal requirements designed to ensure finality in the settlement process. For example, the SFD provides that transfer orders entered into the EU's payment and securities settlement systems cannot be revoked or otherwise invalidated, even when a participant in the system becomes insolvent.

The SFD also provides that the rights of holders of collateral security shall not be affected by insolvency proceedings against the provider. In other words, the SFD gives market participants certainty that when a transaction is concluded, it is final, and its legitimacy cannot be affected by the solvency of either of the parties.

This primary law is buttressed by the CPMI-IOSCO Principles for Financial Market Infrastructures.[9] These priciples are relevant to the operators of any multilateral system among participating institutions used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions, regardless of the legal structure or technological foundation of that system. Amongst other things, the principles contain requirements relating to settlement finality, operational resilience, asset protection and recovery and resolution.

---

[7] Regulation (EU) No 909/2014 of 23 July 2014 on improving securities settlement in the European Union and on central securities depositories and amending Directives 98/26/EC and 2014/65/EU and Regulation (EU) No 236/2012.

[8] Directive 2009/44/EC of 6 May 2009 amending Directive 98/26/EC on settlement finality in payment and securities settlement systems and Directive 2002/47/EC on financial collateral arrangements as regards linked systems and credit claims.

[9] http://www.bis.org/cpmi/publ/d101a.pdf.

2 The legal and regulatory challenges for CSDs using DLT in the existing environment

DLT is a new potential technological solution to the challenges of providing low cost, highly efficient and secure settlement services.

CSDs require no specific additional regulatory permission or approval to utilise such solutions and nor should there be a specific DLT law, any more than there is a law to govern the use of traditional operating systems by CSDs. However, CSDs must ensure that, irrespective of the technology they use, they continue to meet their existing (and numerous) regulatory obligations and standards under, in particular, the CSDR and the CPMI-IOSCO Principles for FMIs.

In this section, we illustrate how a blockchain-based securities settlement system could be designed to meet those CPMI-IOSCO Principles which we believe are most relevant in this context, namely: settlement finality (Principle 8), exchange-of-value settlement systems, i.e. Delivery Versus Payment (DVP) (Principle 12) and operational risk (Principle 17). Similar requirements are included in the CSDR and are mapped to the associated CPMI-IOSCO Principle in the table below.

CPMI-IOSCO Principles	Similar CSDR requirement
Principle 8: Settlement finality An FMI should provide clear and certain final settlement, at a minimum by the end of the value date. Where necessary or preferable, an FMI should provide final settlement intraday or in real time.	**Article 39:** **Settlement finality**
Principle 12: Exchange-of-value settlement systems If an FMI settles transactions that involve the settlement of two linked obligations (for example, securities or foreign exchange transactions), it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other.	**Article 39:** **Settlement finality**
Principle 17: Operational risk An FMI should identify the plausible sources of operational risk, both internal and external, and mitigate their impact through the use of appropriate systems, policies, procedures, and controls. Systems should be designed to ensure a high degree of security and operational reliability and should have adequate, scalable capacity. Business continuity management should aim for timely recovery of operations and fulfilment of the FMI's obligations, including in the event of a wide-scale or major disruption.	**Article 45:** **Operational risk**

The need for certainty and correctability

The above Principles will require any blockchain-based securities settlement system to possess two key attributes: certainty and correctability. 'Certainty' is a broad noun, but in this context, CSDs and their regulators are principally interested in two types of certainty: certainty of settlement and certainty of operation.

Certainty of settlement

Certainty of settlement incorporates two concepts: first whether, at a given point in time, a transaction can be considered final and irrevocable and, second, whether the transfer of securities against cash at the point of settlement is final and irreversible (the concept of DVP). The CPMI-IOSCO Principles 8 and 12 cover settlement finality and DVP explicitly as requirements that a CSD must meet (and these requirements are also reflected in the CSDR).

There is a common misconception that DLT in general cannot offer settlement finality. This arguably is the case for a proof-of-work system for blockchain, such as that underlying Bitcoin, in which certainty of settlement builds progressively as more blocks are added to the chain until the probability that a given transaction will be undone becomes infinitely small. Nevertheless, this attribute is unhelpful in a securities settlement context. This is due both to the doubts it creates as to whether it is possible to comply strictly with the requirements of the SFD; and, insofar as, in practice, participants in the settlement system want to know that a transaction is settled at a given point in time, rather than relying on a probability that this is the case.

However, whilst achieving settlement finality presents significant challenges for the Bitcoin blockchain, it should not be a challenging obstacle for private, permissioned blockchains, whose protocols and architecture can be designed with the principle of settlement finality in mind. We therefore do not anticipate settlement

finality requirements to be inconsistent with the application of DLT to post-trade settlement processes.

As described above, securities settlement involves two ledgers: a securities ledger and a cash ledger. In order to ensure DVP settlement, if two separate blockchains are used to represent the ledgers, the system would need to ensure that block creation in those separate blockchains occurs simultaneously (a technical challenge rather than a legal one). The feasibility of this solution will therefore essentially be dependent on the technical interoperability and synchronisation of those two ledgers.

Certainty of operation

The CPMI-IOSCO Principle 11 and the corresponding rules in the CSDR are clear about the need for CSDs to demonstrate operational resilience even during potential recovery and resolution phases. A key aspect of operational resilience is certainty of operation. Another aspect is cyber resilience. The latter is covered in Part III on page 20.

Certainty of operation is not a concept unique to DLT, or to computer code more generally. The accuracy of computer code is no more a legal question than the accuracy of language in an 'old-fashioned' paper contract – it is an operational or drafting question, rather than a question of statute or regulation. That is to say, there is no real conceptual difference between considering whether the English used in a paper contract affords sufficient certainty for a given contract

to achieve its purpose, or whether the computer code underlying a smart contract overlaid onto the blockchain is 'bug' free and sufficiently precise to achieve the purposes of that smart contract.

However, it is still an important question from a regulatory viewpoint when dealing with FMIs. Regulators have two overriding objectives: protection of investors and stability of the financial system. Regulators will, therefore, be interested in the operational certainty of a blockchain model to the extent that this interferes with the achievement of either one of those objectives. This is particularly important in respect of settlement systems which are systemically important components of the worldwide financial architecture. Problems with these systems can have repercussions for the broader financial system. The certainty of operation of a blockchain-based settlement system will be dependent on the relevant blockchain protocol and its software code. Access to, and authority over, this code would therefore involve accountability for the operation of the system itself. This accountability would need to be allocated contractually (or by operation of statute) to a central authority.

A key question in respect of smart contracts is the extent to which legal contracts can adequately be represented by computer code. For example, is it possible for computer code faithfully to represent the nuances and 'grey areas' that frequently exist in complex commercial contracts? Solutions have been proposed whereby human arbitrators could intervene in defined circumstances through oracles. In the context of this paper, however, we envisage smart contracts facilitating the performance of easily defined operations such as ordinary course corporate actions, and we do not anticipate any particular technical challenge in achieving this modest goal.

Our view is that regulators should not fear the use of smart contracts and DLT any more than any other automated computer-based process

prevalent throughout the settlement industry (all of which are vulnerable to mistakes in the underlying coding architecture).

Key regulatory questions will be:

- In a distributed system, who should be held responsible for any operational failures in the blockchain?

- Where a mistake is spotted, how should it be rectified?

In our view, CSDs could have an important role to play in a blockchain-based settlement system. As 'custodians of the code,' CSDs could exercise oversight of, and take responsibility for, the operation of the relevant blockchain protocol and any associated smart contracts.

Correctability

Another concept associated with settlement finality is 'correctability' – in other words, how easy it is to reverse a transaction, either in response to a mistake or a regulatory or legal mandate. In this context, the SFD provides that transfer orders entered into the EU's payment and securities settlement systems cannot be revoked or otherwise invalidated, even when a participant in the system becomes insolvent.

The mechanisms for 'correctability' will differ in a DLT system, depending on how the technology has been implemented. Transactions could be undone in a blockchain environment by creating a 'fork' in the blockchain, asking nodes to confirm a new sequence of transactions excluding or modifying a 'bad' transaction. This can be a challenging process on a public blockchain, as those chains are designed precisely with the

property of censorship resistance in mind; i.e., that it should not be possible for a central authority to reject or modify a given transaction. In practice, depending on the consensus method, a relevant majority would need to validate the fork, which is far from guaranteed in system with no central coercive authority.

The DAO hack, described in the call out box, provides further insight into the challenges that could arise in correcting or reversing transactions recorded on a blockchain in the absence of a central coercive authority. In the DAO case, a number of technical solutions to the hack have been attempted, none of which appear to have been completely successful, partly because the system was designed not to be amenable to central oversight or control. This example is not an intrinsic weakness of DLT per se, but illustrates that DLT is not a monolithic concept and that DLT

The story of the DAO and the sharp end of the 'code is law' principle

The Decentralized Autonomous Organisation (DAO) has used smart contracts on an Ethereum blockchain to establish a venture capital fund, without managers or employees. The DAO raised $150m through crowdfunding and the proceeds were to be invested in projects approved by the DAO's financial contributors (whose voting power depends on the size of their financial contribution). Funds are distributed according to the terms of smart contracts.

However, a flaw in the code underlying the DAO provided an opportunity for a 'hacker' to take control of $50m of the DAO's value. Whether this constituted a theft is a matter of some debate, with the hacker asserting

that he merely made use of an explicit feature (bug) in the computer code – i.e., he behaved entirely in accordance with the terms of the smart contract.

This example shows a possible danger of bugs in fully automated processes, as significant value was appropriated before any human intervention. It is also a reminder of the sharp end of the 'code is law' concept espoused by the DAO. It is not possible however, at least under English law, to oust the ultimate jurisdiction of the courts to determine disputes and we would expect English courts to deal with disputes founded on blockchain or smart contract bugs using the established body of contract law dealing with contractual mistakes.

protocols and systems can be designed in many different ways, to achieve myriad goals. The DAO's goal was partly philosophical – to achieve an autonomous governance structure with no central management.

However, in the context of securities settlement, where the ability to reverse transactions is an essential attribute, we would not expect regulators or market participants to embrace a model analogous to that underpinning the DAO. In the case of securities settlement, it seems to us likely that regulators will require there to be a regulated institution overseeing the operation of the settlement system blockchain with an authority to execute reverse transactions to correct mistakes or enforce court orders, for example.

In addition, it is conceivable that regulators could themselves have a node on the blockchain, with the power to propose forks in response to transactions entailing regulatory breaches. Conceivably this could lead to regulators being given additional regulatory powers to compel participants in a blockchain to take additional steps to verify regulator-initiated forks.

It should also be noted that the legal implications of reversing a transaction are more complex in a blockchain environment than where transactions are reversed on a bilateral basis or by a central authority. In contrast to the present system, where disputes are solved between interested parties, reversing transactions in a blockchain model could also implicate disinterested parties in the verification process. This potentially exposes those parties to legal claims if the reversal of a given transaction was successfully challenged. This issue has arisen in the context of the DAO example, where the 'hacker' threatened to take legal action against any party which took steps to support the reversal of the disputed transaction.

This issue could be addressed in an agreement entered into by parties participating in the blockchain system which could, for example, provide for indemnification of parties verifying a fork reversing a transaction in respect of which they had no interest.

In summary, we do not believe that SFD protections are compromised by the use of DLT in settlement systems. Rather, it depends on the design of the blockchain protocol and whether a central authority would be present. Correctability, if needed, is a concept that can be included in such a protocol.[10]

---

[10] See, for example, "Accenture to unveil blockchain editing technique" FT 19 September 2016.

3 Other regulatory and legal considerations

The meaning of a securities account in a distributed environment

The CSDR specifies a 'core' function of a CSD as being the provision and maintenance of securities accounts at the top-tier level in the holding structure. However, where all holdings are recorded in a blockchain, does it make sense to talk of securities accounts at all, let alone top-tier accounts? As most securities laws make reference to the notion of securities accounts, should these be adapted to deal with blockchain records? Apart from these important questions, identifying where a record is legally located and what the relevant applicable law would be in a distributed ledger environment is complex.

Pragmatically, the use of DLT does not compromise the ability to provide personalised information to participants at an investor (i.e. 'account holder') level, provided that the investors have been specifically identified in the ledger. Conceptually, holdings recorded on a blockchain could be seen collectively to constitute a securities account. However, a key additional requirement is a recognition that the record constructed by

the account provider is the 'golden record' with priority over any other records that could be constructed by other nodes. This stems from a requirement that the system operator, who is also an account provider, is required to be able to manage account holder (or in the event of CSD, participant) defaults or to execute court orders relating to assets held on the accounts.

A further consideration is that a number of national legal regimes require CSD legal records to be stored at least as a backup within the jurisdiction. To facilitate DLT settlement systems these jurisdictions could expressly permit records stored on a distributed ledger to satisfy local record-keeping requirements (provided, for example, that at least one node is within the relevant jurisdiction). Alternatively, CSDs could simply repeat the process described above and pull the relevant information from the blockchain for storage at the relevant local node or in a local 'mirror' data store.

Legal certainty

We discussed the importance of operational and settlement certainty on page 12, but legal certainty will also be of major interest to market participants. The law applicable to transactions undertaken on the blockchain will be a key legal question and specifically, which governing law should apply given that participants in the blockchain are likely to be distributed across a number of jurisdictions. Indeed, the combination of EMIR and the

forthcoming second Markets in Financial Instruments Directive (MiFID II) will impose open access requirements, including a requirement that investment firms and CCPs from other EU Member States will have the same access rights to settlement systems as domestic firms. This will ensure that, in most practical cases, participants will indeed be dispersed amongst EU Member States.

An important feature of the CSDR's open access requirements is that issuers have a right to arrange for their publicly-traded securities to be recorded in any CSD established in any EU Member State (assuming that the CSD has the appropriate passport). However, the CSDR also makes it clear that the corporate law of the Member State under which the securities are constituted will continue to apply. This demonstrates the 'patchwork' approach of EU securities law, of which we shall have more to say in the following paragraphs.

It is clear however that where securities are in digitised form and are stored at each node in a blockchain, an approach to address the conflict of laws operating at the level of the blockchain rather than at the level of individual securities accounts would be preferable.

Choice of jurisdiction is not a new issue when it comes to the settlement process. In the present model of securities settlement, investors and custodians are connected to each other through a chain of securities accounts maintained by custodians, ultimately ending at the central account ledger maintained by a CSD. In such cases, the CSD's records will not contain the name of the ultimate investor but instead the names of other intermediaries or nominee companies. The intermediaries in the holding chain are typically dispersed throughout a number of different jurisdictions. The question is then, given that the participants in the securities system are located in many different jurisdictions, which governing law should apply to a given security account?

The general trend in conflicts of laws issues in securities settlement is to adopt a PRIMA – the 'place of the relevant intermediary approach' – i.e., the governing law is the law of the securities account to which the relevant securities are credited. This concept is explicit in certain European securities legislation. The SFD, for example, refers to rights "legally recorded on a register, account or centralised deposit system located in a Member State."

The PRIMA concept runs into difficulty in a fully disintermediated system because there is, of course, no 'relevant intermediary.' Taking the wording of the SFD, quoted above, as an example – where the securities register is stored on a blockchain, the location of that register is not a meaningful concept, as it is stored and reproduced at every node in the blockchain. The PRIMA concept, therefore, is unlikely to be helpful in its present form in solving conflict of laws issues in a distributed ledger context.

Whilst a strict application of PRIMA concepts may not be appropriate, in the context of the blockchain model discussed in this paper, there is a clear alternative choice of entity which can be used to anchor governing law – namely, a central authority such as a CSD. It may not make sense to speak of the location of the securities ledger per se, as a copy is stored at each node, but a securities register can certainly be placed under the ultimate governance of the central authority which oversees the coding and operation of the blockchain. Furthermore, we would expect such central authority to be a point of contact for regulators and, therefore, it would make sense from a regulatory perspective for the governing law and regulatory jurisdictions to be aligned.

An alternative to this approach would be for participants to sign up to a governing law clause when they agree to participate in the private securities settlement blockchain. However, we would anticipate that typically if a CSD is responsible for operation of a settlement platform,

the CSD would wish to select the law of the jurisdiction in which it is based. Furthermore, the governing law clause would apply only to the participants in the blockchain which, in a multi-

level holding model, would not necessarily include each entity in the chain of holdings. As such, the first approach described above is, in our view, the more preferable.

Insolvency of a participant

The CSDR requires CSDs to have effective and clearly defined rules and procedures to manage the default of one or more of its participants. In our view, a blockchain-based settlement system could be used to improve portability of securities and the transparency of ownership chains. This would allow a CSD to better respond to the insolvency of one of its participants.

Any lack of transparency of ownership information in a given holding chain, together with errors in records resulting from imperfect reconciliation through the chain, can both obscure ownership of securities and make it more difficult to move positions from a collapsed institution (i.e. lack of transparency reduces portability). Currently, transfer of positions occurs only when the insolvency practitioner of an insolvent participant takes action. This can be a lengthy process.

Another classic example of the risks inherent to chains of custodians in the multi-tier holding model is the restructuring of Bear Stearns. In this case, there were 28% more recorded shares than shares actually issued by the company, the excess presumably

arising due to mistakes in the reconciliation process through the custody chain. Ultimately, JP Morgan bailed out the excess securities when it took over Bear Stearns. By removing the need for reconciliation, distributed ledger technology can eliminate this kind of mistake and provide a stronger guarantee of issue integrity, not only at a CSD level, but also on an end-to-end level.

Where DLT is employed in settlement systems, as we envisage on pages 8 and 9, there would be both:

- transparency as to ownership of a given securities position; and

- a straightforward mechanism for transfer of underlying investors' accounts to solvent participants without the need to wait for action from an insolvency practitioner.

DLT could in principle, therefore, assist CSDs to provide a quicker, more efficient response to the insolvency of a participant.

Cash on the blockchain

As described above, in a typical securities trade there will be an obligation for the seller to deliver securities (the 'securities leg') and a corresponding obligation for the buyer to transfer cash (the 'cash leg'). In most European countries, settlement of the cash leg takes place in central bank money, though CSDs may also offer the option to settle in commercial bank money where central bank money is not practical and available. In the

latter case, specific requirements apply to the commercial bank money provider which needs to be a limited purpose bank.

In order to deliver a fully blockchain-based securities settlement system, therefore, there will need to be a way in which to settle the cash leg on the blockchain using central bank money. This could conceivably be facilitated by central banks

keeping a digital form of central bank money on a blockchain, albeit central bank blockchain money equivalents could equally be created through other models.[11]

The possibility of issuing central bank money on a blockchain – central bank digital cash – is being explored by a number of central banks and a pioneer in this area to date has been the Bank of England. In a recent speech,[12] Ben Broadbent, Deputy Governor for Monetary Policy at the Bank of England, described the opportunities and practicalities of issuing digital central bank money.

The central bank would essentially put commercial bank reserve deposits on a distributed ledger by, for example, sanctioning the use of tokens on a blockchain issued against fiat central bank funds. Settlement of the cash leg of transactions could then proceed by the exchange of these tokens in a blockchain environment.

At present, no central bank has put reserve deposits on a blockchain for the purposes of securities settlement, but the interest from central banks encourages optimism that this may become reality in the relatively near future.

Data protection, privacy and confidentiality

As DLT involves the storage, and therefore transfer, of what may constitute personal data between different nodes, a number of data protection issues are likely to arise.

In particular, EU data protection law places a number of requirements relating to the collection and transfer of personal data, which in some cases will necessitate collection of more expansive customer consents than is presently the case. The situation is even more complex where personal data is to be transferred between jurisdictions. This is particularly true if transferred outside of the EU, as certain national privacy laws and EU data protection law mandate that personal data can only be transferred across borders if an adequate level of protection is guaranteed. In addition, by default any financial information processed by CSDs is confidential, although there are exceptions as a result of regulatory reporting obligations.

It should be noted, however, that none of these data protection or confidentiality issues are particularly novel or unique to blockchain-based systems. They arise in many circumstances and most, if not all, of the firms which participate

in a securities settlement system will already be familiar with the requirements of the various pieces of EU data protection legislation and applicable confidentiality requirements. Nonetheless, compliance with data protection law and confidentiality rules will need to be considered as part of the design of a blockchain-based securities settlement system.

For example, one potentially thorny issue in the context of a blockchain system is the 'right to be forgotten.' In summary, this is the right of a data subject to request data which is stored in a manner which is no longer compatible with EU data protection legislation to be removed. This could be the case where, for instance, personal data is considered as no longer relevant, excessive or not kept up-to-date in relation to the purposes for which it was processed. A key property of a blockchain system, however, is that it displays the entire transaction history on a chain.

In practice, data protection legislation may not prove to be as difficult to comply with as is often assumed. For example, it is questionable the extent to which personal data needs to be openly displayed

---

[11] A number of banks are already seeking to develop a so-called "utility settlement coin" as an industry standard to clear and settle transactions; see "Banks seek to harness Blockchain technology for settlement system" FT 24 August 2016

[12] Available at http://www.bankofengland.co.uk/publications/Pages/speeches/2016/886.aspx. The Bank of England's Chief Cashier, Victoria Cleland, has also delivered an even more recent speech, available at http://www.bankofengland.co.uk/publications/Documents/speeches/2016/speech919.pdf.

on a blockchain, or whether transaction histories can be anonymised for the purposes of the shared ledger.

The ability to anonymise ledger entries is another important point. There are circumstances in which it would not be commercially, or even legally, desirable to share the identities of parties to a certain transaction, or the complete transaction history, with all participants in the blockchain. The ability to anonymise certain transactions is not, however, inimical to use of a blockchain – it is, primarily, a technical challenge rather than an insurmountable legal hurdle. However, this may necessitate the involvement of third parties, such as CSDs, to validate the identities of market

participants who are semi-anonymised parties to transactions on the blockchain.

Nonetheless, participants in any blockchain system should also be aware that pseudo-anonymity, where transactions are visible to all blockchain participants but the identities of the counterparties are anonymised, is an increasingly weak method of protecting identity. This may give rise to some challenges in practice, for example, in securities markets where, on the one hand, some transactions are required to be made public by law while, on the other hand, transaction data as a main rule is treated by applicable laws as confidential information.

Cyber security

A key selling point of DLT over more traditional databases is its enhanced resistance to cyber-attack. This derives principally from:

- the redundancy built into the blockchain (i.e. there is a copy of the ledger at each node); and

- the fact that in order to alter the ledger, any attacker would need to control greater than a certain threshold number of nodes.

Both of these attributes should be attractive to regulators. We note however that other points of failure could appear in a DLT environment, e.g. in a fully decentralised environment, a cyber-attack destroying private keys leaves the investor with no possibility to recover its assets.

We believe that the recently published CPMI-IOSCO Guidance on Cyber Resilience for FMIs (June 2016) represents a sound starting point for assessing the cyber resilience of DLT when employed by an FMI. The guidance emphasises the importance of implementing an adaptive cyber resilience framework that evolves with the dynamic nature of cyber risks to enable effective management of those risks. This should ensure that FMIs employing DLT are sufficiently equipped to monitor and manage any specific cyber risk aspects related to this technology.

As described above, a DLT settlement system would rely on public/private key cryptography, with participants in the settlement system using their private keys to validate transactions.

The security around private keys is, of course, vital to the success of a DLT infrastructure, as was seen by the recent hacking of the Bitfinex blockchain exchange. Given that public/private key cryptography has been around for some time, however, we do not expect this to present a novel technical challenge. We would expect requirements relating to the security of private keys to be addressed in any relevant cyber-security regulation or guidelines. However, even in the absence of specific rules addressing this issue, regulators might reasonably expect CSDs and their participants to adopt relevant security measures as part of meeting their day-to-day obligation of ensuring the security of their IT systems.

In any event, we would not expect a DLT settlement system to represent an inherently weaker cyber security proposition than any present system, which is not immune to cyber-attacks, including in particular attacks on the system launched by exploiting weaknesses in the defences of individual participants.

Links and interoperability

Links between CSDs are vital for delivery of efficient cross-border settlement. They also enable a domestic issuer CSD to offer settlement services in securities issued in other issuer CSDs established in other countries.

Such links are regulated tightly by CPMI-IOSCO Principles 18 (Access and Participation) and 20 (FMI links) and the CSDR (Articles 33, 48, 50, 51, 52 and 53). The CSDR requirements in respect of interoperability specify that a CSD must provide access to its securities settlement systems on a non-discriminatory and transparent basis to a CCP or a trading venue.

It could well be technically more challenging for a traditional CSD (for example) to gain access to a CSD which operated in a DLT environment. As well as possibly violating the regulatory requirements in respect of interoperability described above, this could potentially also create anti-competitive barriers to entry. Common technical standards and business rules will be essential to meet interoperability requirements.

New technology risk

Technical challenges and unforeseen vulnerabilities often accompany the application of new technologies to financial markets, and we would expect the use of DLT in settlement to be no exception. Many of these challenges and vulnerabilities may only become apparent when DLT is applied to 'real life' situations or used on a market-wide scale.

One clear challenge is the migration of securities and participants from legacy systems to DLT systems. Were DLT to be adopted in a systemically important settlement system, we would expect CSDs, market participants and regulators to give significant attention to the technical process of migration. A staged approach would likely to be preferable to reduce the systemic risk which could result from a large-scale one-time migration from a legacy to a DLT environment.

As DLT is adopted in settlement systems, regulators and market participants will need to be both flexible and agile to identify and respond to any emerging technical issues. Any risks in this regard could, however, be mitigated by cooperation between regulators and market participants to enable innovators in this space the latitude to thoroughly test their ideas – technically, legally and practically – before large-scale implementation. Recent innovations in approaching regulation, such as the FCA's 'regulatory sandbox' in the UK and similar initiatives by other regulators in supporting innovation, could be particularly helpful in this regard. This is a theme we return to on page 25.

4 Responses to an evolving landscape – regulatory (r)evolution?

The use of DLT in securities settlement may entail significant simplification of the settlement process as well as cost savings. DLT would undoubtedly constitute a technological revolution. The question for regulators and market participants is whether it would also require a regulatory revolution.

The evolving role of CSDs

From the preceding discussion, it is clear that the use of DLT in settlement will change the role of CSDs. Depending on the precise implementation of the DLT system, the need for CSD services could be more limited than today (e.g. limited to the notary function or oversight of the asset issuance process) or could even be removed altogether. CSDs may also start to provide other central authority infrastructure services which may be required in a DLT environment (such as 'gatekeeping' the ledger or private key and smart contract management), potentially in competition with other (non-CSD or non-FMI) providers of such services.

Perhaps the key infrastructure roles in our vision of a blockchain-based post-trade system are that of 'gatekeeper' and 'overseer.' By definition, in a private ledger, one entity would need to control access to the ledger. Regulators, focussing on their priorities of investor protection and market stability, are unlikely to embrace a blockchain-based securities settlement system without a robust well-capitalised entity being responsible for vetting and validating the identities of prospective participants in that system.

More broadly, a central authority would also need to be responsible for, amongst other things, setting, supervising and updating system rules; imposing relevant sanctions; taking responsibility for the processes designed to ensure correctability described above; managing smart contracts on the ledger; taking action in the case of operational incidents; and implementing the necessary procedures to respond to an issuer's or a participant's insolvency.

From a legal perspective, we would consider the performance of the gatekeeping and oversight roles to be very close to the performance of the 'core CSD functions' specified in the CSDR.[13] We would therefore expect a CSD to be a natural candidate to perform such roles in a DLT environment. In this case, there would be no need to create an additional regulatory framework or additional regulated activities relating to the performance of the gatekeeper and oversight functions, as we would expect them to fall within, and for regulators to regard them as falling within, the existing scope of the core CSD functions.

---

[13] These being the operation of a securities settlement system (the "settlement service"), the recording of securities in a book entry-system (the "notary service") and providing and maintaining securities accounts at a top-tier level (the "central maintenance service").

From a practical perspective, CSDs are trusted and central entities which do not participate in the settlement system as a 'customer,' but rather their role is to facilitate the settlement process. Overseeing the blockchain system would be a natural evolution of this facilitation role. Furthermore, CSDs are required to comply with numerous requirements under the CSDR and the CPMI-IOSCO Principles, which practically may only be possible if CSDs were able to perform an operational oversight role. Finally, we would expect the selection of CSDs to perform the gatekeeper and oversight roles to be an attractive proposition to regulators, given that CSDs are heavily regulated entities, subject to stringent prudential, cyber security and other relevant requirements.

In this world, CSDs will continue to perform an important role as trusted, centralised FMIs, providing gatekeeping services and oversight of the relevant blockchain. Participants, as nodes, would each hold the latest version of the ledger, and therefore could readily provide access for its clients (and regulators) to account and transaction data, including where required by applicable law. Participants, in turn, would need to maintain contractual relationships with underlying clients, to whose accounts the participant would facilitate access (unless and until the client wished to transfer its account relationship to another participant) on the CSD-controlled top-tier ledger.

The use of DLT in securities settlement would likely create a host of other technologically-focussed roles – for example, the design and technical management of the DLT platform – and it is a question for regulators whether these roles should be regulated directly. Our view is that they should not; existing legislation is technology independent and functional in nature, regulating the activity rather than the underlying technology. We see no reason why this approach should change in a DLT environment.

Considerations for regulators

The adoption of DLT in a settlement context, as presented above, should not require a radical overhaul of the existing regulatory architecture. The regulation applicable to a CSD is independent of the technological basis of that settlement system. Whilst regulation may inform the type of technology which is suitable – for example, settlement finality requirements may currently preclude the use of proof of work public blockchains – we are not aware of any law or regulation that would be outright incompatible with the blockchain model discussed in this paper.

While a CSD is a natural actor to perform the gatekeeping and oversight roles (certainly in the short to medium term), we nevertheless believe that such infrastructure roles could technically also be performed by other entities. Therefore, whilst we would not expect the contents of relevant law and regulation to be rewritten to accommodate the use of DLT in post-trade settlement systems, the application of such law and regulation may need to extend beyond CSDs if any of these new infrastructure roles are performed by entities other than regulated FMIs.

This does not, of course, mean that there will be no friction at all between the current system of law and regulation and adoption of DLT in settlement systems. As discussed above, there are certain areas where adoption of DLT raises legal issues that would not be implicated by the present non-distributed ledger system. In particular, the nature of a securities account on a blockchain and whether application of the PRIMA approach to the selection of governing law is suitable.

The use of a DLT system in securities settlement does, however, present regulators with a new and perhaps more effective method of exercising supervision. Regulators could participate in (or more likely, merely observe) a blockchain-based settlement system by themselves becoming a node in the distributed network.

By allowing regulators to participate as a node in the blockchain system, they could have complete oversight of all the transactions occurring within the settlement system and receive transparent transaction data in real time. This could represent a significant improvement in data provision to regulators than is presently possible and may allow them to exercise tighter and more granular supervision of activities in the securities market. This could also initiate a reconsideration of the various reporting obligations in law and regulation, as reports would either be made automatically or regulators would have direct access to the necessary information.

It is inevitable that regulators may wish to adjust their approach to deal with some of the regulatory and legal issues raised in this paper. The open issues will need to be addressed to the satisfaction of the market (in terms of efficiency) and regulators (in terms of security and safety). In this context, ESMA's discussion paper, and its willingness to work with industry participants to further understand the industry and develop an appropriate regulatory framework is very encouraging.

Conclusion – What can regulators do now?

We believe that there are two approaches which regulators could adopt now, whilst ensuring investor protection and systemic stability.

First, by developing industry guidance, either with the EU, through the EBA[14] and ESMA, or more globally using CPMI-IOSCO. This 'principles-based' regulation may be particularly suitable at this early stage in the adoption of DLT, compared to 'black letter law.' Principles are more flexible and easier to modify in response to unforeseen issues as the technology beds in. It is also generally easier to achieve international consensus in respect of principles-based regulation and consensus will ultimately be required for DLT to be successfully applied to international securities settlement. For example, we would expect such principles to address the 'new' infrastructure functions in a blockchain world, described above.

Secondly, and perhaps in parallel, regulators could also work with firms to foster disruptive innovation in this area and to help firms overcome the significant monetary, technical and regulatory barriers to wide-scale adoption of DLT in this industry. Regulatory 'sandboxes' are one example of this, but other regulatory approaches can be as valuable. While we would not, of course, expect a loosening of the regulatory standards that apply today to existing market participants, there are a number of worthwhile actions regulators could take to stimulate progress in this industry.

At the same time, market participants must consider the adoption of common technical standards (for example, standardising the technical specifications of blockchain networks and harmonising coding platforms) to assist interoperability of the various platforms. A more unified technical approach would also allow a single set of principles (or, in the future, bespoke regulation) to apply more straightforwardly to all settlement systems.

There is much for regulators and market participants to like about a blockchain-based settlement system – from the significant savings that would result in the removal of latency and redundancies in the system to the stronger guarantees of reconciliation – and therefore how to foster innovation in this area is a pressing question for regulators and market participants alike.

[14] Similarly to the European Banking Authority's Opinion on Virtual Currencies, EBA/Op/2014/08, February 2014

↘

Post script

Looking from the outside in

So far in this paper, we have stayed within the realms of the present regulatory and legal environment. We have considered current legislation and how a distributed ledger securities system could be made to fit within it, concluding that there is no fundamental incompatibility provided that the basic institutional arrangements of the market look similar to those that exist today.

In other words, we have assumed the technology is constrained by the world as we know it.

But...

↘...What if we take a different approach and set the technology free?

Imagine a world with the following:

- Reliable, encrypted, peer verified data storage and transaction management available on demand, as a public ledger.

- Smart contract systems that could interact with the secure data ledger and enable anyone to write and publish complex, contingent commitments that would change the state of the data layer in the future.

- Well-established oracle services that provide data inputs for smart contracts and interfaces for human interactions in cases where uncertainties cannot be resolved with data and judgement is required.

- Sophisticated wallet applications that enable users to manage their interactions with the system and their identity, as well as provide safekeeping of keys and access to (near) real time reporting and transaction management functions.

If this appears far-fetched consider that, although it may not be finished, Ethereum is designed precisely to offer the kind of core data and smart contracting infrastructure outlined above.

So what might securities services look like in such an imaginary world?

Start with the issuers. It would be easy to create a security via the deployment of smart contracts on the ledger. Issuers (or more likely, specialist suppliers) would programme smart securities contracts as they wrote their prospectuses and then set them free on the blockchain to manage the lifecycle of the security. These contracts could contain both transaction and lifecycle management features. For example, DVP could be achieved through the smart contract, utilising features in the blockchain.

Investors could hold their securities directly on the ledger, managed via their wallet applications: no need for intermediaries. They may still need specialist services to help them manage their investments, such as investing their liquidity and managing collateral accounting. They may also need fiduciary services, for example, to protect keys against loss or to verify the contents of the wallet on behalf of third party investors. But they could now buy these services as and when they need them, since they are in full control of their records of ownership. The relationships between buyers and suppliers could therefore look very different to those that exist today.

Cash would be interesting. There could be many different forms of cash, all jostling for attention. Perhaps some central bank money tokens would be in circulation, alongside commercial alternatives issued by various banking entities, and pure cryptocurrencies. But perhaps other forms of short-term liquidity would also be available, backed by gold or HQLA, for example.

Such a model would be truly disruptive to the current system. But would it be legal?

The first thing to note is that it would not necessarily be completely unthinkable. Issuers can already create securities privately in either bearer or registered form and distribute them to shareholders via private placement. It may be possible to issue securities on a blockchain adapting these techniques.

Of course, there would be constraints to this approach. Under the current regime, for example, securities held privately outside of a CSD would not be eligible to be traded on recognised trading venues under MIFID. But this problem might be bearable in some cases. The issuer could, for example, create a private order matching facility for its investors using a smart contract.

Nevertheless, if the world did move in this direction, it would create some interesting challenges:

Accountability

Where securities are issued privately, the issuer is normally held fully responsible for maintaining the ownership ledger. Given that securities market operations are not core to the business of most issuers, they may be reluctant to take on this responsibility and, indeed, today many outsource share registration to specialist registrars or CSDs. Perhaps registrars would re-invent themselves as technology firms, creating the smart contracts and then accepting liability for their ongoing operation. Note however, that this liability could extend to the underlying data backbone itself, so would not necessarily be a trivial role. We discuss this further in 'Roles and Responsibilities' below.

Systemic risk and efficiency

The model outlined above is essentially composed of a set of atomic, independent, automated securities registers and settlement systems. That is all very well, but investors tend to own and trade portfolios, meaning, for example, that they use the proceeds from the sale of one security to fund the purchase of another. CSDs, custodians, central banks and regulators today expend a lot of effort trying to minimise the total liquidity required to make the system as a whole work. Would this be possible if every security was its own mini settlement system? And what about the risk that many smart contracts, written and deployed by different people, interact in unexpected ways to jam the system, or make it unstable?

Identity

Bitcoin, notoriously, is pseudonymous with identities hidden behind the public keys used to identify individual transactions. It is possible – in some jurisdictions – for securities to be issued in bearer form, enabling anonymous holding and transacting. But regulators are strongly in favour of more transparent models as evidenced by, for example, the G20 High Level Principles of Beneficial Ownership Transparency.

In our future world, it is hard to imagine issuers wanting to do KYC on everyone who wants to buy their securities. However, services to enable verification of identities by trusted third parties could be purchased, and use of such services could perhaps be mandated within the smart contracts. But would these identity providers themselves be regulated? And what kind of liability would they need to accept for errors or fraud, not to mention AML requirements?

Finality

As we discussed above, finality is an important consideration in securities transactions. To a large extent it is a matter of definition. However, having a definition everyone can agree on before transactions start is much better than arguing in the courts after the event. Current legislation on finality (SFD) applies through established FMIs, which can then build their settlement systems accordingly. How would this work if every security was created as an individual smart contract, potentially with its own settlement model? Without specific regulation, uncertainty is added to all transactions. For example, in the event of an investor's bankruptcy, the bankruptcy estate could request a court order to reverse certain transactions it considered were not executed according to ordinary commercial terms.

Default and correctability

Default by either major holders or issuers themselves are challenging events in the life cycle of a security, and certainly require action on behalf of settlement systems and custodians. Who would have the power and responsibility for calling defaults and for managing such interventions in our future world? It could not be the issuer – at least in the case of their own default. And, as was shown on page 14 the issue of correctability goes far beyond default. So perhaps a regulator would need to take on the role of correction agency? But if they did, how would they gain access to the relevant smart contracts, let alone organise the verifiers to accept the changes?

Roles and responsibilities

Today's regulation tends to be framed around intermediation and broad functional descriptions that map to particular market roles. CSDR covers CSDs, EMIR CCPs, MIFID investment firms and trading venues and so on. It is also noteworthy that the idea of a securities account is based on intermediation, assuming that ownership rights are exercised by an intermediary on an account holder's account. But in the world sketched here, some of these roles start to merge and break down. We would have issuers setting up trading and settlement platforms for their own securities. At the very least this would be confusing and we could end up with a completely fragmented financial system. Could regulators effectively oversee such a system? Perhaps new technology, such as big data analytics, could help them make sense of it?

Maintenance of the underlying infrastructure

Finally, we have assumed that the underlying infrastructure on which our new world operates is generic and runs independently of our securities market use case. Presumably data and smart contracts relating to medical records could be sitting alongside securities data and the underlying nodes process them all according to their protocols without visibility on what they mean – a true 'Internet of Value.' Yet it is naïve to think that this underlying protocol would require no coordination or management. So how would this be achieved?

The Internet is sometimes cited as a model for how an un-coordinated system can deliver a service of great social value. It is certainly true that there is no central Internet authority, although there are bodies such as the Internet Corporation for Assigned Names and Numbers (ICANN), which manages name and address conventions. However, with the Internet, each website is responsible for its own data and sites only need to interact with each other at the margin. As a result, all that is needed to make the system work are simple address protocols and data formats. This allows any website to change what it does and how it does it any time.

Our new architecture has a fundamental difference: it is 'stateful.' That is, the network as a whole is responsible for the present state of the data. This means that all nodes need to process the data and propose changes to it in the same way, at any given point in time. The experience of the Ethereum DAO shows how difficult it can be to herd participants to manage changes in an uncoordinated stateful system. Can a technical solution to this problem be devised, or does the Internet of Value end up requiring a universal regulator of data?

All of this is to say that...

Even in the most evolved state of a distributed ledger system, it is difficult to imagine that questions of governance, accountability and liability will disappear. So perhaps the ultimate question is who should be responsible for answering them? No doubt the answer to this question will emerge from a complex interaction between existing market players, new entrants, regulators and politicians. Will it lead to a landscape that looks much like the world of today or will something completely different emerge? And if the latter, what is the path that takes us there? The only way to answer these questions is to take it one step at a time.

About the authors

For Euroclear

Paul Symons
Head of Government Relations
paul.symons@euroclear.com

Ilse Peeters
Director, Government Relations
ilse.peeters@euroclear.com

Jorma Yli-Jaakkola
Director, Legal
jorma.yli-jaakkola@euroclear.com

André-Marc Delhez
Director, Strategy and Corporate Planning
andre-marc.delhez@euroclear.com

Angus Scott
Director, Head of Product Strategy and Innovation
angus.scott@euroclear.com

Visit **www.euroclear.com**

For Slaughter and May

James Mead
Associate, Fintech group
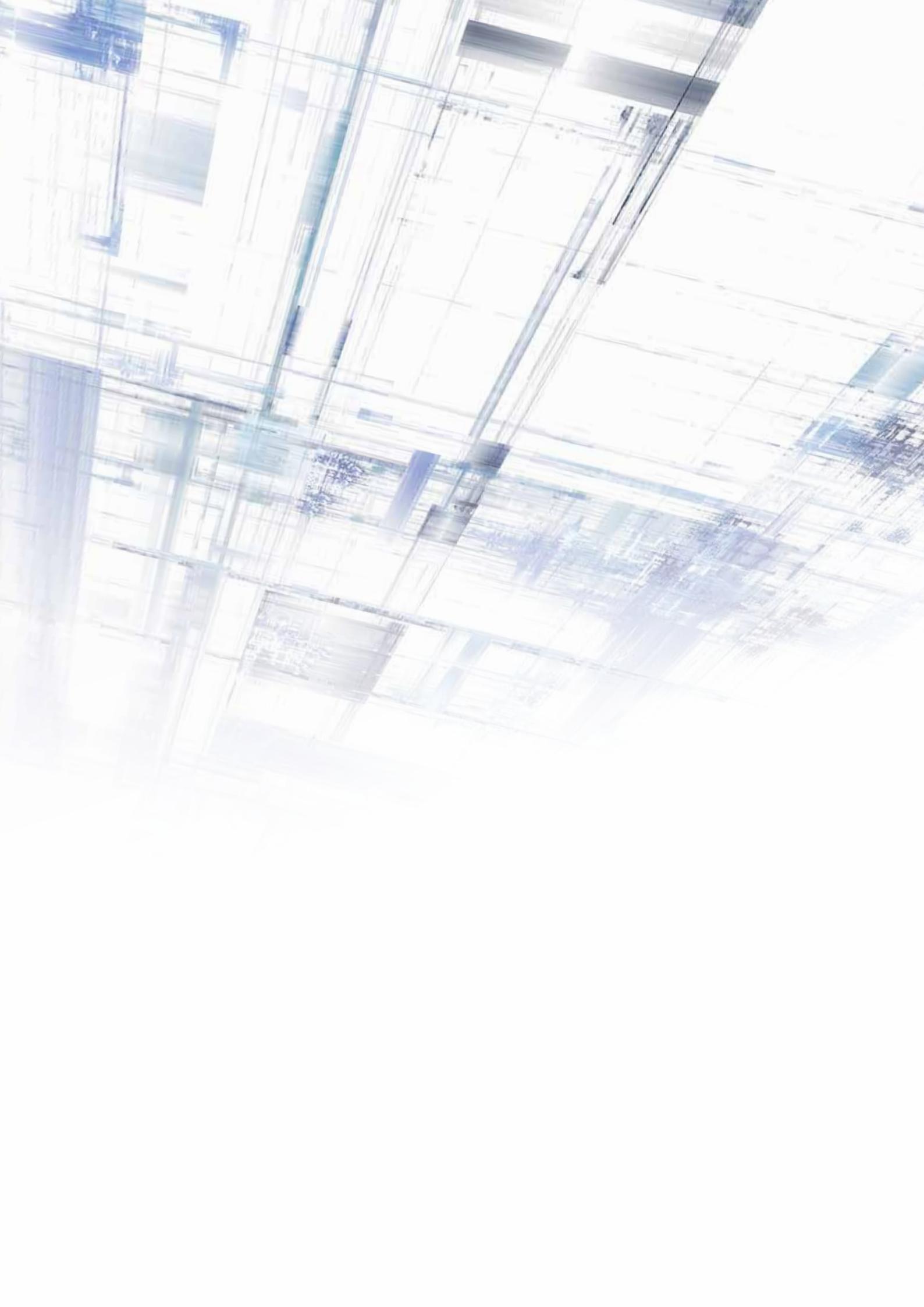*james.mead@slaughterandmay.com*

Ben Kingsley
Partner, Fintech group
ben.kingsley@slaughterandmay.com

Visit **https://www.slaughterandmay.com/what-we-do/legal-services/industry-sectors/fintech/**

Euroclear group is the financial industry's trusted provider of post trade services. At the core, the group provides settlement, safe-keeping and servicing of domestic and cross-border securities for bonds, equities and derivatives to investment funds. Euroclear is a proven, resilient capital market infrastructure committed to delivering risk-mitigation, automation and efficiency at scale for its global client franchise.

The Euroclear group includes Euroclear Bank - which is rated AA+ by Fitch Ratings and AA by Standard & Poor's - as well as Euroclear Belgium, Euroclear Finland, Euroclear France, Euroclear Nederland, Euroclear Sweden and Euroclear UK & Ireland. The Euroclear group settled the equivalent of EUR 675 trillion in securities transactions in 2015, representing 191 million domestic and cross-border transactions. By December 2015, the group held EUR 27.5 trillion in assets for clients.   **www.euroclear.com**

Slaughter and May is a leading, full service, international law firm headquartered in London. Our Fintech Team supports clients across the full spectrum, ranging from established international financial institutions and global technology and telecoms providers, to investors and start-ups with the potential to become market disrupters. We advise on the legal implications of developments in the fields of technology, intellectual property, data use, and financial regulation, but our interest spans any and all legal implications for innovation and growth in the fintech sector.   **www.slaughterandmay.com**