Distributed Ledger Technology: Implications of Blockchain for the Securities Industry[1]

JANUARY 2017

A REPORT FROM **THE FINANCIAL INDUSTRY REGULATORY AUTHORITY**

Contents

Introduction 1

SECTION I: Overview of Distributed Ledger Technology 2

SECTION II: DLT Securities Industry Applications and Potential Impact 4

- Applications Considered in Securities Industry 4
- Potential Impact on Securities Industry 5

SECTION III: Factors to Consider When Implementing DLT 7

- Implementation Considerations 7
- Regulatory Considerations 11

Request for Comments 20

- Endnotes 21

Introduction

Distributed Ledger Technology (DLT) (also known as blockchain technology or distributed database technology) has attracted significant interest and funding in the financial services industry in recent years. Several large financial institutions have established dedicated teams to explore the technology, and some market participants have formed consortia to create industry standards.[2] According to a 2016 report by the World Economic Forum,[3] over the past three years more than $1.4 billion has been invested in this technology to explore and implement uses in the financial services industry.

There are varying views in the securities industry on the magnitude of disruption DLT may cause. Some have argued that DLT has the potential to revolutionize the operations of the securities industry, while others have debated that any changes resulting from the use of DLT in the securities industry are likely to be incremental and take many years to develop. However, most agree that the technology has the potential to bring additional efficiencies and increased transparency to the industry while also presenting some novel risks such as those related to data security and privacy. Some analysts and research reports predict that we may start seeing adoption of the technology in limited market segments in a matter of months, with larger-scale industrywide adoption potentially occurring after several years.

Over the past couple of years, FINRA has actively engaged with various industry participants, including financial institutions, vendors and professional services firms, to monitor developments related to DLT and its potential impact in the securities industry. In particular, FINRA spoke to several FINRA member firms to better understand their current or potential future use of DLT. These broker-dealers highlighted their perspective on the potential benefits and challenges posed by DLT, and noted that they are considering how different DLT applications would operate within the current regulatory framework.

Many FINRA rules as well as some rules implemented by other regulators (such as the Securities and Exchange Commission (SEC)), that FINRA is responsible for examining or enforcing with respect to broker-dealers, are potentially implicated by various DLT applications. For example, a DLT application that seeks to alter clearing arrangements or serve as a source of recordkeeping by broker-dealers may implicate FINRA's rules related to carrying agreements and books and records requirements.[4] The use of

DLT may also have implications for trade and order reporting requirements to the extent it seeks to alter the equity or debt trading process.[5] Moreover, as more fully discussed later in this paper, other FINRA rules such as those related to financial condition, verification of assets, anti-money laundering, know-your-customer, supervision and surveillance, fees and commissions, payment to unregistered persons, customer confirmations, materiality impact on business operations, and business continuity plans also may to be impacted depending on the nature of the DLT application.[6]

As the securities industry continues to explore and adopt DLT, many market participants have indicated the impending changes are more than just those associated with the automation of a process or adoption of a new technology system, but instead represent the potential to create a paradigm shift for several traditional processes in the securities industry through the development of new business models and new practices. As a result, there has been a great desire among industry participants to have increased regulatory engagement, as they explore the technology and its possible applications.

FINRA welcomes an open dialogue with market participants to help proactively identify and address any potential risks or hurdles in order to tap into the full potential of DLT, while maintaining the core principles of investor protection and market integrity. Technological innovations in the industry, operating in accordance with these core principles, have the potential to provide investors with greater access to services and enhanced experiences, offer firms increased operational efficiencies and enhanced risk management, and enable further transparency in the marketplace.

This paper is intended to be an initial contribution to an ongoing dialogue with market participants about the use of DLT in the securities industry. Accordingly, FINRA is requesting comments from all interested parties regarding all of the areas covered by this paper.[7] FINRA also requests comments on any related matters for which it would be appropriate to consider additional guidance, consistent with the principles of investor protection and market integrity, based on DLT applications and their implications for FINRA rules.

In the sections that follow, FINRA provides a basic overview of DLT, highlights some key applications being explored in the securities industry and potential impact of the technology, and discusses key implementation and regulatory considerations for broker-dealers.

SECTION I: Overview of Distributed Ledger Technology

This section provides a high-level overview of DLT and its key features.[8] Distributed ledger technology involves a distributed database maintained over a network of computers connected on a peer-to-peer basis, such that network participants can share and retain identical, cryptographically secured records in a decentralized manner.

The operation of DLT may involve the use of a public or private network potentially containing digitally represented assets, where the participants on the network conduct and verify transactions, and record related data on the network in an encrypted format. In this section, we clarify this process by explaining: (1) the differences between public and private networks; (2) the use of digital assets; and (3) the general process for conducting and verifying transactions and recording them on a DLT network.

Public vs. Private Network

DLT uses either a public or private network. Public networks are open networks, accessible to anyone who wishes to join, without any restrictions on membership. Any data stored on a public network is visible to all network participants, in encrypted form. The first DLT network, centered on the issuance and exchange of bitcoins, was established as a public network. This network does not have any central authority; instead it relies on the network participants to verify transactions and record data on the network, based on a certain protocol.

In contrast to public networks, private networks are permissioned networks, and only those entities that have been granted access can join them. Private networks allow the network operator to restrict access and create an environment of known, trusted parties. On private networks, permission levels may also be tiered such that different entities and individuals may have varying levels of authority to transact and view data. There is a growing desire to employ private networks, particularly in the financial services sector, as various industries start to develop commercial uses of DLT while seeking to maintain greater control over network users.

Digital Assets on a DLT Network

A DLT network frequently contains assets that are digitally represented. The digital assets may be created on the network (*e.g.*, cryptosecurities, cryptocurrencies), or may be a digital representation on the network of a traditional asset that is stored offline (referred to as "tokenized assets").[9]

Assets on a DLT network, whether public or private, are cryptographically secured using a public-private key combination. A public key is the "address" where the digital asset is located on the network. A private key is the code that gives the holder access to the asset at the address represented by the corresponding public key. The private key is designed to be retained by the asset holder or its agent to access the asset.

Transaction Verification and Recording

A transaction may be initiated by any party on the network that owns assets on that network or has access to the assets on the owner's behalf. When a transaction is initiated, it is verified on the network based on a pre-determined verification process. The verification process generally involves confirmation from one or more nodes[10] on the network that the buyer and seller are the rightful owners of the assets they seek to exchange, based on transaction history records on the DLT network. The time required to verify and record a transaction on the DLT network can vary depending on the process employed. If the network uses a consensus-based[11] or proof-of-work-based[12] verification method, it may create some latency depending on the time required to achieve consensus and solve for proof-of-work requirements.[13] Some private networks are exploring alternative verification methodologies that would reduce the time needed for verification and recording. The settlement of the transaction may be contemporaneous with the verification process, whereby the new ownership of the asset or funds is reflected on the DLT network.

Once a transaction is verified, the information is "cryptographically hashed"[14] and permanently recorded on the DLT network. The records are time stamped and displayed in a sequential manner to all parties on the network who have the appropriate access levels. It is claimed by many that this cryptographic hashing process secures the integrity of the data, such that once it is recorded on the network it cannot be modified; any errors would need to be fixed with new correcting amended entries. However, some technologists are reportedly exploring ways to create functionalities to edit DLT transaction records in certain circumstances. One vendor has reportedly developed a prototype of the capability to edit blockchain records in private DLT networks.[15]

SECTION II: DLT Securities Industry Applications and Potential Impact

This section highlights some of the applications of DLT that are being explored in the securities industry, and discusses the potential impact this technology may have on the securities industry.

Applications Considered in the Securities Industry

Market participants in the securities industry are contemplating various applications of DLT. Many of these participants have focused on discrete applications within the broader equity, debt and derivative markets.[16] By focusing on discrete applications and devising limited-scale experiments related to the implementation of DLT, they seek to avoid the potential risks associated with more wholesale changes. Moreover, many of these market participants have also focused on sectors they believe present significant inefficiencies, such as with respect to their clearing infrastructure, operational processes or administrative functions. This is largely driven by the view that focusing on areas with existing high levels of inefficiencies provides greater opportunities to demonstrate meaningful enhancements.

Reflected below are examples of discrete applications within the equity, debt and derivative markets where market participants are currently using or testing DLT applications. Also noted are examples of DLT-based shared utilities that market participants are exploring for certain common and repetitive functions.

Equity Market

- **Private company equities –** The administrative process of tracking transfer of private company shares and maintaining capitalization tables may be manual, expensive and subject to errors, and may expose private issuers to regulatory risks. In light of these stated concerns, some market participants are considering DLT-based applications to implement a system to track trading and ownership of private company shares. For example, in late 2015, one market participant launched a DLT-based platform for the issuance and trading of private company shares.[17] This platform aims to provide private company issuers with real-time transparency into the records or trading activity of its shares and shareholders of record.
- **Public company equities –** Some market participants are also exploring issuance and trading of public company stock on a DLT-based platform. For example, one public company issuer recently issued a new class of digital shares directly on a proprietary DLT network, such that the shares could be traded on the platform with same-day settlement.[18] Similarly, some vendors are developing DLT-based trading systems for publicly traded securities.

Debt Market

- **Syndicated loans –** Average settlement time for secondary trading of syndicated loans is around a month, given that the process is largely manual and involves multiple counterparties. Some market participants are exploring a private DLT network of various counterparties with the goal of facilitating faster clearing and settlement of these loans, and creating increased capital and operational efficiencies.[19]
- **Repurchase agreements (Repos) –** Regulators have focused recently on issues present in the repo market, including counterparty risk and a relative lack of transparency. Some market participants are exploring using DLT to facilitate clearance and settlement of repo transactions, with the goal of reducing settlement times and lowering the risk of settlement failures.[20]

- **Corporate bonds –** Some market participants are exploring issuance and trading of corporate bonds on a distributed ledger network, such that the terms of the bond are embedded as code on the digital asset. This would allow fully automated calculation and payment of coupons and redemption.

Derivative Market

- **Credit default swaps –** While certain derivative transactions trade and clear on exchanges, these instruments involve complex post-trade events. Market participants and regulators might benefit from enhanced transparency in this market. Some industry participants recently conducted a pilot to test how a DLT network could make these assets easier to manage and monitor, with automated processes and greater transparency.[21]

Industry Utilities

- **Product reference data –** DLT is also being explored to build industry utilities for common repetitive functions, to enhance and streamline other operational processes such as reference data management. Some market participants are collaborating to create and manage a DLT-based central repository of standardized reference data for various securities products. This may eliminate the need for each individual participant to maintain its own reference data repository and will facilitate the use of standardized reference data for securities products.[22]
- **Customer identity management utilities –** Some market participants are exploring setting up a centralized identity management function, such that they can manage their global customer identities through a single interface and share the information with other participants on the network.[23]

Market participants are also exploring enhancements to DLT networks by developing software applications that are overlaid on the DLT network. These software applications, frequently referred to as "smart contracts," are designed to automatically execute agreed-upon terms of a contract on the DLT network based on triggering events. A few examples of areas where market participants are seeking to apply the use of smart contracts within DLT networks include facilitation of collateral management (such as exchanging ownership interest in collateral upon a party's default), escrow arrangements (such as the automatic release of funds when requisite conditions have been satisfied) and corporate actions (such as coupon payment on a specific pre-determined date).

Potential Impact on the Securities Industry

DLT has the potential to affect various aspects of the securities market, including market efficiency, transparency, post-trade processes and operational risk. While it is too early to predict the exact nature of the changes that will result, some of the features of DLT that may influence each of these areas are highlighted below.

Market Efficiencies

One of the key stated features of DLT is that it has the potential to reduce settlement times for securities transactions by facilitating the exchange of digitally represented assets contemporaneously with the execution of a trade. However, independent of technological hurdles to reducing settlement times, it is unclear what the ideal settlement time would be for various segments of the securities market. Some market participants have indicated that the ability to net transactions occurring over a period of time (*e.g.*, end-of-day netting) is more advantageous compared to real-time settlement because it limits the frequency with which assets need to be transferred when taking on a temporary position. Any move toward real-time settlement would also influence how and if short sales or trade cancellations take place with respect to transactions

in the applicable securities, and thereby may affect the way in which market makers and others trade or hedge positions. Others have noted that real-time settlement (or the functional equivalent) would help to limit counterparty risks and would free up collateral, thereby creating increased capital efficiencies. However, considerations regarding settlement times are likely to vary based on the asset type, the volume of transactions, liquidity requirements, impact on market makers, and the current relative efficiency of a particular segment of the securities market. As a result, while the adoption of DLT may not necessarily lead to implementation of real-time settlement, it has the potential to make settlement time more a feature of the actual market needs of the parties instead of being based on operational constraints.

Transparency

DLT has the potential to promote increased transparency. The technology entails maintaining a database that contains the complete history of all securities transactions (and related information) that occurred on the DLT network.[24] All or a portion of this information could be made available simultaneously to all participants on the network. Similarly, the market participants and the investing public could be provided with access to relevant information on the network without the need to create a new reporting infrastructure.

However, while DLT may help facilitate transparency from a technological perspective, it would not resolve all questions about transparency from a policy perspective. The actual desired level of transparency will depend on factors unrelated to the use of DLT, such as the need to safeguard personally identifiable information (PII) and trade strategies. Further, in certain instances, transparency of the network may be detrimental to the market. For instance, in a private network, if information is shared only among the network participants, it could potentially create an informational disadvantage for non-network players. Conversely, market participants on a network may seek to keep certain transactional and position information anonymous and private, for competitive reasons.

Roles of Intermediaries

By facilitating the ability to blur the lines between execution and settlement, as well as by providing greater flexibility regarding data transparency, DLT has the potential to alter the roles and functions of intermediaries to securities transactions. For example, the various traditional post-trade processes used today by market participants could be affected. Specifically, DLT opens up new options for trade verification whereby confirmation may be sought from one or more participants on the network that the buyer and seller are the rightful owners of the assets using consensus-based, proof-of-work or other techniques. As a result, depending on the type of technique that is selected, the process for executing a trade and the role of intermediaries may be affected. Similarly, as noted in the earlier section, the process and timeline for settlement and clearing of transactions could be condensed, potentially impacting the use of certain functions such as transaction netting and maintenance of margin. As another example, reconciliation processes could potentially be simplified because participants on the shared network would each have the same set of transaction data.

Operational Risk

DLT relies on several features that may have implications for operational risk, including sharing information over a network of various entities, use of private and public keys to obtain access to assets, and use of smart contracts to automate certain operations.

Given that DLT involves sharing of information with various entities over a network, it also poses important security-related risks. Participants would need to consider implementing enhanced security programs related to risks stemming from both internal and external sources. In the next section, we further expand on potential considerations with respect to such risks.

The use of a combination of private and public keys as a security measure to access assets on the DLT network is also likely to create risks associated with the management of those keys and may result in an even greater focus on network security issues. To deal with these risks, consideration would need to be given to where the keys are stored, who has access to those keys, what protocols are in place to access the keys, what occurs if the keys are misplaced or lost, and what safeguards are there to prevent improper use of the keys. In the next section, we further expand on potential considerations with respect to such risks.

The use of smart contracts is also likely to result in changes related to the nature of operational risks associated with securities transactions. While an automated process for executing terms of an agreement should generally help to streamline the transaction process, it is also likely to introduce the risk that undesirable actions may occur based on unanticipated events, without some type of human intervention.

SECTION III: Factors to Consider When Implementing DLT

The exploration of DLT applications in the securities industry has already begun and appears likely to pick up steam in the coming years. Many financial institutions have established in-house teams and research labs to build and test DLT networks, or are working with third-party vendors specializing in this space. In addition, firms have sought to participate in collaborative efforts with consortia to develop a common DLT framework and create industry standards.

As noted in the prior section, the types of DLT applications contemplated run the gamut of use cases involving the equity, debt and derivative markets. As the implementation of these DLT applications progresses, issues are being raised regarding how processes involving DLT fit within the current regulatory framework. In light of these trends, this section highlights some key considerations related to DLT implementation and regulation.

FINRA invites market participants to provide comments on how these DLT implementation and regulation efforts may be aided, including by any tailored guidance to support innovation, consistent with the principles of investor protection and market integrity, based on DLT applications and their implications for FINRA rules.

Implementation Considerations

Developing DLT applications in the securities industry can present many challenges. In seeking to overcome those challenges, some of the key considerations for market participants in implementing a DLT network may include governance, operational structure and network security.

Governance

One of the key governance principles of the Bitcoin Network was to establish a “trustless” environment open to the public, where no single party is responsible for, or empowered with, governing and operating the network. While this type of network may offer certain advantages such as providing a decentralized system that is not dependent on any specific party to operate, it may also pose some vulnerability if it leads to ineffective management of the system. For example, recent events have shown that lack of a central governing body for the evolving Bitcoin Network has created concerns for the network, as participants try to determine an approach to handle increased transaction volume. Therefore, a DLT network based on the use of a trustless network, where no party is responsible or accountable for the proper operation of the system, may present risks to markets and investors. Many market participants are seeking to use private DLT networks with a governance structure that takes into account that participants in the network are generally known and trusted parties.

When setting up or participating in a private DLT network, where multiple organizations across the industry are involved, some of the initial governance questions that need to be answered relate to the operation of the network and determining who bears responsibility for it. Below are the types of questions that market participants may want to consider when developing a governance structure for a DLT network.

- Would the governance structure for the DLT network be determined by a single entity or a group of firms? What role, if any, would participants in the DLT network play in shaping its governance? How would the interests of end-users, which are not participants on the network, be represented?
- Who would be responsible for ensuring adherence by participants to the requirements established for the DLT network, and how would this be conducted?
- Who would be responsible for the day-to-day operation of the network and resolving any technical issues on the network?
- Who would be responsible for establishing and maintaining a reasonable business continuity plan (BCP) for the network, to address any unexpected emergencies or significant business disruptions?
- How would any conflicts of interest in the operation of or participation on the network be addressed?
- How would errors or omissions on the blockchain be reflected or rectified?

Operational Structure

A key consideration for market participants in implementing a DLT network is determining the operational structure of the network. The operational structure of a DLT network would typically include developing a framework for: (1) network participant access and related on-boarding and off-boarding procedures; (2) transaction validation; (3) asset representation; and (4) data and transparency requirements. Below are some areas that market participants may want to consider when developing such a framework.

- **On-boarding, off-boarding and access:** It is critical for a DLT network to establish, as part of its operational infrastructure, the criteria and procedures for establishing and maintaining participating members and determining their level of access. Specifically, in developing a DLT network, applicable parties may wish to consider how they would:
  - establish eligibility criteria for participants to gain access to the network;
  - establish a vetting and on-boarding process for new participants, including creating an identity verification process and executing appropriate user agreements prior to on-boarding;
  - develop an off-boarding process for participants that may be non-compliant or disqualified for violating securities laws, rules and regulations or for violating network rules; and establish exclusion criteria to detect previous participants that may have been disqualified;
  - memorialize the terms of engagement and code of conduct required from all participants;
  - establish varying levels of access for different participant groups (*e.g.*, direct network participants vs. indirect users conducting transactions via direct participants)—this may include restricted access to certain data sets, and even restrictions on ability to read or write on the shared ledger; and if the network includes global entities or participants from different countries, it may be desirable to provide special attention to regulatory requirements in those different jurisdictions, particularly as it relates to privacy and information sharing; and
  - determine what type of access would be provided to regulators.

- **Transaction validation:** As described in Section I, different types of methodologies have emerged in recent years for validation of transactions occurring on a DLT network. Before establishing a transaction validation methodology, network operators are likely to assess the pros and cons of each methodology. In performing this analysis, some potential questions network operators may desire to consider are noted below.
  - If consensus-based, would it require a proof-of-concept or would it be a simple consensus algorithm? How much latency and complexity would that add to the validation process? What is the risk of collusion by multiple parties to validate a fraudulent transaction?
  - If single-node verifier (*i.e.*, one single node will be responsible for verifying all transactions), how would that verifier be determined? Is the speed and simplicity of a single-node verifier worth the concentration of risk in one party? What would be the back-up or recovery procedure in the event the single-node is unavailable or compromised?
  - How would the number of nodes needed for verification be determined? If alternative nodes or random nodes are set up as verifiers, how would the order be established? Does this process expose the network to potential risks from a variety of nodes? What would be the process if a required node is non-operational for whatever reason?
  - What process would the network adopt to rectify or correct any erroneous entry that may be recorded on the shared ledgers? What levels of approvals would be required—and by which parties—to process such a rectifying entry?

- **Asset representation:** To the extent an asset is represented on a DLT network, operators will need to determine how those assets will be established on the network. Following are some factors operators may wish to consider in the analysis.
  - Will assets be directly issued and digitally represented on the network? Or would they be issued in traditional form and subsequently tokenized on the network? Would the network contemplate both types of asset representation?
    - If tokenized, what additional security risks and complexities are posed? How would any loss or theft of the traditional off-chain asset be handled? How would asset changes (*e.g.*, stock splits and conversions) be handled?
    - Will the network only permit new asset issuance or will it allow on-boarding of existing assets?
  - How would cash be represented on the network? Industry participants are contemplating various models to facilitate the cash side of a transaction settlement. For example, in a recent effort, a few banks are reportedly collaborating to create a virtual "settlement coin."[25]
    - If cash-backed settlement tokens are used, would these tokens be deemed as virtual currency? Could there likely be a scenario in which multiple such native tokens are created by different networks or firms? If so, will they be tradable?
    - If fiat cash (*i.e.,* currency that is established by the government of a country to be used as money) is used and settlement occurs off the network through a traditional cash payment process, how, when, and by whom will the trade and asset transfer be recorded on the network?
    - How will a participant's ability to meet the cash obligation be determined? Will a deposit be collected from network participants to be used in the event of non-payment? How will such a deposit be calculated?

- **Data and transparency requirements:** A DLT network will need to pre-establish, as part of its operational setup, its dataset requirements and transparency levels. Some related areas to consider include the following.
  - What data points will be recorded on the shared database? Of these, which data points would be deemed as mandatory and required for all records before they are validated? What additional data points may be recorded by participants as optional?
  - How transparent will the data on the shared ledger be? Will certain data fields or record types be transparent to all network participants? Will access to information be determined by user type?

Network Security

Security is a critical consideration for a DLT network, particularly given the distributed nature of the network and the potential participation from entities across the globe. Market participants are likely to desire assurances that the network is protected from external threats and insider risks before joining, given that they may be providing private information and engaging in transactions within the network. Accordingly, network operators may want to reflect on how the design, testing and maintenance of the system will address any potential concerns about the introduction of security issues, both from within the network as well as from outside the network, via its participants. For example, fraudulent transactions could be injected through a participant that falls victim to a cyber-attack (*e.g.*, email phishing or malware), and recovering from such an event may result in significant disruption to the entire DLT network's operation.

Distributed ledger technology is still in its nascent stages and as such, market participants are still trying to determine the full range of potential security risks posed by the technology and how to address such risks. Below are some questions that market participants may want to consider when developing, operating or participating in a DLT network.

- How are the cryptographic keys used to sign and encrypt blocks protected from unauthorized access, modification or loss throughout their lifecycle? Will keys be rotated regularly to guard against brute-force cracking attempts?
- What key sizes and cryptographic algorithms provide adequate protection against attacks on the cryptographic security of the DLT network?
- If a key is compromised, how will fraudulent transactions be identified and reversed? What parties will be responsible for this? Can historical transactions involving a compromised key be trusted?
- What are the incentives or disincentives to ensure completeness, integrity and accuracy of the blockchain?
- Who covers the cost of fraud? Will participants be made whole? How about customers/clients?
- How will appropriate notifications of security events be handled with respect to varying parties (*e.g.*, participants, customers/clients, regulatory bodies, law enforcement or insurers)?
- What methods (*e.g.*, multi-signature technology) have been considered to enhance the security of assets? What are the pros and cons of each method?

Network participants may also want to consider the following practices when developing, operating or participating in the network.

- Considering how the DLT fits into the firm's current recordkeeping framework, including facilitating the maintenance of back-up records in case the integrity of the DLT network is questioned or a network issue arises. Conducting appropriate business impact analysis and accordingly identifying the recovery point objective to determine back-up frequency.
- Considering how written policies and procedures reflect the use of or participation in a DLT network, including concerning the secure operation of the DLT network to account for threats and risks such as denial of service, hacking, phishing, malware, insider attacks, errors, fraud and data breach. Documenting policies and procedures related to detection of such threats and appropriate response, recovery and notification processes.
- Considering how the DLT fits into the firm's cybersecurity program, including establishing static, dynamic, and manual security testing (*e.g.*, penetration tests) to minimize the risk of software and infrastructure security flaws and vulnerabilities.
- Designing minimum security standards for network participants to adhere to on an ongoing basis and appropriately assessing compliance with those standards.
- Instituting multi-factor authentication for direct participants to access the network.
- Developing business process controls—such as verification steps triggered when a transaction value threshold is exceeded—to backstop the DLT network and catch fraud before transactions are executed.

Regulatory Considerations

Broker-dealers are exploring issuing and trading securities, facilitating automated actions (*e.g.*, coupon payments) and maintaining transaction records on a DLT network. When adopting this new technology and revamping current processes, broker-dealers should be cognizant of all applicable federal and state laws, rules and regulations, including FINRA and SEC rules.

In light of the potential for a paradigm shift for several traditional processes in the securities industry through the development of new business models and new practices incorporating DLT, this section highlights some of the major regulatory issues that broker-dealers may encounter. The discussion involves FINRA rules as well as some rules implemented by other regulators (such as the SEC) that FINRA is responsible for examining and enforcing. While we provide a framework for firms to consider application of various rules, this paper is not intended to provide specific guidance on facts and circumstances of any particular concept, arrangement or venture. Any potential application of blockchain technology in the securities markets may require independent legal advice and potentially interpretive guidance from FINRA, the SEC and other regulators.[26]

We invite market participates to engage in a dialogue with FINRA as they explore DLT and invite comments as part of this paper on matters for which it would be appropriate for FINRA to consider giving additional guidance, consistent with the principles of investor protection and market integrity, based on DLT applications and their implications for FINRA rules.

Customer Funds and Securities

A DLT network may create a new way to hold funds and securities, resulting in potential implications for custody and protection of customers' funds and securities.

Broker-dealers handling customer funds and securities are subject to a number of requirements, including Rule 15c3-3 under the Securities Exchange Act of 1934 (Exchange Act). The SEC has previously stated that one of the key requirements imposed by Rule 15c3-3 is that "the broker-dealer must maintain physical possession or control over customers' fully paid and excess margin securities."[27]

Securities transactions entered into, cleared and settled using DLT may also have implications for firms' obligations under Exchange Act Rule 15c3-1 related to net capital requirements, which is discussed later in this paper.[28]

When considering participating in a DLT network to facilitate securities transactions, firms will need to determine how, and by whom, customers' securities and funds will be received, delivered and held. For example, if the development of DLT applications resulted in the use of cryptosecurities, then broker-dealers would need to consider how they would account for obligations to maintain physical possession or control over these securities. Similarly, if any cash-backed token holdings or digital currency were used as part of a DLT application, broker-dealers would need to consider how this would affect their processes for complying with requirements under Rule 15c3-3, including the customer and proprietary account reserve formulas.

An otherwise introducing firm participating in a DLT network should also consider if certain activities and access levels (*e.g.*, holding private keys to customers' cryptosecurities, initiating and controlling customer funds) may be deemed as receiving, delivering, holding or controlling of customer assets.

Some potential factors to consider in this analysis include the following.

- What entities are the holders of the "private keys" in the DLT network that would be required to gain access to the cryptosecurities, cash-backed token holdings or digital currency? Are multiple keys needed to gain access or is a single key sufficient?
- Who controls or has access to the DLT network where the assets are held?
- What happens in the event of a loss or destruction of assets (either due to fraud or technological malfunction) on the network?
- If the broker-dealer was to fail and is liquidated in a proceeding under the Securities Investor Protection Act of 1970, as amended, how would customers' securities and funds be treated, and how would customers access their assets?
- In instances where firms have established partnerships with other firms to serve as their back-ups and to carry out critical functions in the event of emergencies, what type of access would those back-up firms have to the private keys?
- How will customers or a Securities Investor Protection Corporation (SIPC) trustee access the customers' assets in the event of a defaulted broker-dealer? What parties will be involved, and what are their roles and responsibilities?

Broker-dealers would also need to consider how they would comply with asset verification requirements, such as under FINRA Rule 4160 (Verification of Assets) and Exchange Act Rule 17a-13, in the context of DLT applications resulting in the use of cryptosecurities. For example, depending on the structure of the DLT network, firms may need to assess whether assets would be viewed as being held by another institution, and if so, develop appropriate processes for the provision of written verification of the maintenance of those assets in accordance with FINRA Rule 4160.

Broker-Dealer Net Capital

Certain activities and responsibilities of a firm participating on a DLT network may impact the firm's net capital requirements.

The SEC has previously stated that Exchange Act Rule 15c3-1 "requires broker-dealers to maintain a minimum level of net capital (consisting of highly liquid assets) at all times."[29] FINRA Rule 4100 Series (Financial Condition) lays out various requirements for broker-dealers to ensure compliance with the SEC's net capital rules and related reporting and notification requirements to FINRA.

Broker-dealers typically calculate the minimum amount of net capital they must maintain and the amount they actually maintain. Part of the process for computing net capital involves determining whether an asset is an "allowable" or "non-allowable" asset (*i.e.*, whether it is eligible to be used for purposes of the net capital calculation) as well as taking certain haircuts from the market value of various allowable assets to account for various risks.

If a broker-dealer were to hold cryptosecurities, digital currency or other cash-backed token holdings, then the firm would need to consider how they would affect its net-capital computation under Rule 15c3-1. Given the relatively novel nature of these products and the ways in which product liquidity may potentially be impacted based on the type of DLT network that is developed, firms will likely need to consider their own particular facts and circumstances when determining how to apply the net capital rule requirements.

Broker-dealers may wish to consider these factors in the analysis:

- How does the use or application of the DLT network affect the market risk, liquidity or other characteristics of the asset?
- How do the characteristics of a particular cryptosecurity, digital currency or other cash-backed token holdings fit within the principles of the net capital rule?

Books and Records Requirements

Broker-dealers are subject to recordkeeping requirements under Exchange Act Rules 17a-3 and 17a-4 and FINRA Rule 4511 (Books and Records: General Requirements), which outline minimum requirements regarding the types of records that must be made, as well as the length of time that broker-dealers must maintain relevant records and other documents pertaining to their business.

The development of DLT networks may afford market participants the ability to develop and maintain certain records on the network itself. However, broker-dealers may want to carefully consider the capabilities and limitations of the DLT network before determining whether they are able to rely on the records developed within the network to fulfill their minimum recordkeeping requirements. Moreover, to the extent broker-dealers seek to maintain books and records on the DLT network, they would need to consider whether this approach would meet the requirements of Rules 17a-3 and 17a-4 (*e.g.*, write once, read many (WORM) requirement, accessibility of information and third-party attestations).

Some factors to consider in the analysis include the following.

- What information is maintained using the DLT network?
- What will be deemed as the physical location of the firm's records maintained on a node of a DLT network that may extend over multiple countries?
- What parties have control or access to the firm's records? What are their rights, obligations and responsibilities related to those records, and how are they governed?
- What is the firm's (and other participants') level of access to the data, and in what format would it be able to view the data?

- How does the DLT network interact with the firm's own systems for recordkeeping purposes?
- How would the records be made available to regulators?
- How will the firm's traditional exception reporting, used to supervise transactions, be generated from a DLT network?
- How will the firm protect any required records from tampering, loss or damage?

Clearance and Settlement

The development of DLT applications in the securities industry has the potential to alter the clearance and settlement process. Careful consideration should be given regarding how any application fits within the current regulatory framework for clearance and settlement of securities transactions.

For example, under a DLT environment, clearing and settlement of securities transactions may occur outside of the traditional infrastructure, with a potentially less clear distinction between trade execution and settlement. Depending on how trade execution and settlement is ultimately structured, broker-dealers and other market participants may wish to consider whether any of their activities in the DLT environment meet the definition of a clearing agency and whether corresponding clearing agency registration requirements under Section 17A of the Exchange Act would be applicable.[30]

The development of a DLT environment that alters the clearing and settlement process for securities transactions may also impact introducing broker and clearing broker (*i.e.*, the carrying firm) relationships.[31] FINRA Rule 4311 (Carrying Agreements) requires, among other things, that "the carrying firm shall submit to FINRA for prior approval any agreement for the carrying of accounts, whether on an omnibus or fully disclosed basis, before such agreement may become effective. The carrying firm also shall submit to FINRA for prior approval any material changes to an approved carrying agreement before such changes may become effective." Accordingly, broker-dealers will need to consider how using a DLT trade and settlement platform may change their existing carrying/introducing firm roles and responsibilities and affect their carrying agreements, and if so, seek appropriate approval consistent with FINRA Rule 4311.

Anti-Money Laundering and Customer Identification Programs

In a DLT network, firms may be connected with various unknown parties and their customers on the network, including entities domiciled in foreign jurisdictions. Firms should consider how this may impact their compliance programs associated with various anti-money laundering (AML) and customer identification related regulatory obligations.

The Bank Secrecy Act of 1970 (BSA) requires all broker-dealers to, among other things, implement compliance programs to detect and prevent money laundering. In addition, FINRA Rule 3310 (Anti-Money Laundering Compliance Program) requires all broker-dealers to develop and maintain a written AML program to comply with the requirements of the BSA. The BSA also requires that, as part of the AML program, broker-dealers must establish, document and maintain a reasonable customer identification program (CIP)[32], which, among other things, requires broker-dealers to verify identities of all parties with which they establish a formal relationship to effect securities transactions.

FINRA Rule 2090 (Know Your Customer (KYC)) requires broker-dealers to "use reasonable diligence, in regard to the opening and maintenance of every account, to know (and retain) the essential facts concerning every customer and concerning the authority of each person acting on behalf of such customer."

As noted earlier in Section II, some market participants are exploring setting up a centralized identity management function, such that once the identity of a customer is verified by an entity on the network, that information may be made available to all parties on the network. The motivation here is to potentially eliminate duplication of effort by various entities to verify customer identities and thereby create efficiencies. Various models are being contemplated for setting up such a centralized identity management function, including sharing the verifications conducted by regulated entities on the network, or potentially having a third-party vendor serve that function on the network on behalf of all participants.

Each broker-dealer bears its own responsibility to comply with relevant AML and customer identification rules[33], regardless of whether or not a DLT network is used to process a transaction. While broker-dealers may choose to outsource certain functions to a central utility or a third party on the network, firms need to be aware that they may not outsource their responsibility associated with the performance, or lack thereof, of those functions (*see, e.g.,* *Notice to Members 05-48* (Outsourcing)).

Firms may want to assess the implications of the various approaches available to them to fulfil their AML/CIP/KYC obligations, when operating on a DLT network. Some factors to consider in the analysis include:

- How would the broker-dealer verify identities of parties that it transacts with on the DLT network?
  - Will customer and counterparty identities be verified offline, outside of the network?
  - Will any CIP information be shared or stored on the network? If so, how would broker-dealers ensure compliance with SEC Regulation S-P (Privacy of Consumer Financial Information and Safeguarding of Personal Information)[34] and other privacy-related rules and regulations?
- Will the broker-dealer outsource any related functions to a central identity management facility operated by the DLT network? If so:
  - Are the procedures used by this central facility sufficient and adequate for the broker-dealer to meet its AML and CIP/KYC requirements and fulfill related obligations?
  - How will the broker-dealer supervise and test any functions outsourced to other parties to ensure they continue to comply with requirements?
  - How dynamic is the customer verification process and how frequently will customer information be updated for changes?
  - How frequently will the customer information be tested or verified (*e.g.*, quarterly, yearly)?
  - Who will be responsible for managing such a central facility? Will it be the network operator, a third-party vendor or a collective effort by all participants? Will all the involved parties be subject to regulation by the Financial Crimes Enforcement Network (FinCEN)?
  - How will the roles and responsibilities of the parties be memorialized in a contract?
  - How will broker-dealers conduct AML tests as required by FINRA Rule 3310(c), to verify the process adopted by the central facility?
  - Will the broker-dealer have the option to opt out of such a facility and establish its own independent AML and identity management programs? If so, how will this impact the transaction validation and settlement process?
- How will transaction monitoring be conducted and incorporated into a broker-dealer's existing AML monitoring processes and systems?

Customer Data Privacy

In a DLT network, data, including certain customer information and transaction records, may be shared by all parties on the network. Even where such data is encrypted, it may be vulnerable to being exposed or accessed by undesired parties on the network.

Protection of financial and personal customer information is a key responsibility and obligation of FINRA member firms. As required by Regulation S-P, broker-dealers must have written policies and procedures in place to address the protection of customer information and records. Specifically, as detailed in NASD *Notice to Members 05-49* (Safeguarding Confidential Customer Information), the policies and procedures must be reasonably designed to:

- ensure the security and confidentiality of customer records and information;
- protect against any anticipated threats or hazards to the security or integrity of customer records and information; and
- protect against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer.

The rule also requires firms to provide initial and annual privacy notices to customers describing information sharing policies and informing customers of their rights. Additionally, SEC Regulation S-ID (the Red Flags Rule) requires broker-dealer firms that offer or maintain covered accounts to develop and implement written Identity Theft Prevention Programs. Further, many states have specific rules and requirements related to customer data privacy. (Refer to FINRA's Customer Information Protection web page.)

Broker-dealers would need to consider and account for the application of such customer data privacy requirements to the information maintained or shared on the DLT network. When joining a DLT network, firms should assess whether the network and its policies and procedures are designed appropriately, such that participating firms can meet their obligations associated with customer data privacy. Further, firms may want to consider how to update their own policies and procedures to reflect changes in how customer information may be stored and any new procedures that may be adopted to protect against new forms of threats to customer data and privacy on a DLT network. Similarly, firms may also want to consider what updates will be required to their Identity Theft Prevention Programs. Firms may also wish to consider whether related training for their employees or communications to their customers may be appropriate in light of any changes.

The following are some potential related questions for firms to consider.

- When participating in a DLT network, what procedures and security measures will the broker-dealer need to adopt to ensure compliance with customer data privacy related rules and requirements?
  - What restrictions will be placed on network participants' access to such information?
  - What security measures and protocols need to be considered to ensure data privacy and to ensure that PII is not compromised or stolen?
  - As noted in the previous section, to the extent PII is shared on the network, how would broker-dealers ensure compliance with Regulation S-P and other privacy-related rules and regulations?
  - What disclosures will be made to customers regarding the privacy of their information?
  - In the event the DLT network facilitates transactions and information sharing with entities in foreign jurisdictions, how would broker-dealers ensure compliance with foreign privacy requirements and potential conflicts in related requirements across different jurisdictions?

Trade and Order Reporting Requirements

FINRA operates several facilities to facilitate order and trade reporting for regulatory purposes, and to provide transparency in equity and debt securities markets. Pursuant to various rules, FINRA member firms are obligated to report certain order- and trade-related information into these FINRA facilities. Broker-dealers should be mindful of how such reporting obligations may apply when participating or transacting in a DLT network.

Equity Securities

The current reporting framework for over-the-counter (OTC) transactions in listed and unlisted equity securities requires market participants to report information to one of FINRA's facilities (such as a Trade Reporting Facility® (TRF®), the Alternative Display Facility (ADF®) or the OTC Reporting Facility™ (ORF™)), depending on the type of equity security involved in the transaction.[35] For trades in listed stock, FINRA reports data to a centralized Securities Information Processor for consolidation and public dissemination.

According to news reports, one potential application of DLT may involve the facilitation of OTC transactions in equity securities. For example, one use case that is reportedly in development would allow market participants to engage in OTC trading of NMS stocks by creating tokenized (digital) representation of existing NMS stocks on a DLT network and trading those digital shares on that network. Market participants appear to also be considering using DLT to facilitate trading of newly issued digital shares that would not be tokenized representations of existing NMS stocks and could represent a distinct class of a company's stock.

Market participants considering such uses should evaluate the extent to which those applications would be subject to the rules that govern quotation and trading practices and reporting obligations. For example, activity on these platforms may be subject to FINRA Rule 6100 series (Quoting and Trading in NMS Stocks) or FINRA Rule 6400 Series (Quoting and Trading of OTC Equity Securities), depending on the type of securities transacted on the platform. Additionally, to the extent broker-dealers participate in a DLT network to facilitate OTC securities transactions, they would also need to consider and account for any other applicable order and trade reporting requirements including those for FINRA's Order Audit Trail System (OATS™) and FINRA's equity trade reporting facilities noted above (the TRFs, ADF and ORF).

Other SEC or FINRA rules may apply, for example, FINRA Rule 4550 Series (Alternative Trading Systems (ATSs) Reporting) or rules governing securities offering and trading standards and practices (FINRA Rule 5000 Series). As with any market participant that engages in non-DLT equity trading, FINRA encourages firms to conduct a comprehensive review of all applicable securities laws, rules and regulations.

Debt Securities

Under FINRA Rule 6700 Series (Trade Reporting and Compliance Engine® (TRACE®)), all FINRA member firms are required to report transactions in eligible fixed income securities[36] to FINRA via TRACE. Generally, FINRA disseminates transaction information for most trades in fixed income securities that are reported to TRACE. To the extent broker-dealers participate in a DLT network to facilitate fixed income securities transactions, they also should consider reporting requirements under TRACE rules as part of their comprehensive analysis.

Supervision and Surveillance

A DLT network designed to facilitate securities transactions may present new and unique challenges related to maintaining appropriate supervisory policies and procedures and surveillance systems in accordance with applicable rules (*see, e.g.,* FINRA Rules 3110 and 3120).

For example, FINRA's supervisory rules require the review of customer account activity as well as the review of post-trade transactions, such as account designation changes, to correct order errors. When establishing and maintaining supervisory and compliance surveillance systems in a DLT network, broker-dealers would need to consider whether appropriate supervisory and compliance personnel have sufficient levels of access to DLT network records. Moreover, broker-dealers may wish to consider whether such systems would provide evidence of review that is properly recorded and attributable to designated supervisors, or whether a broker-dealer would develop its own parallel process.

As noted earlier, some market participants are contemplating offering centralized facilities on DLT networks to perform certain repetitive and shared functions (*e.g.*, having a node on the network serve as a verifier of investor's accreditation status, setting up a centralized identity management function, etc.). To the extent broker-dealers choose to outsource any functions to these facilities on the network, they would be required to include in their written supervisory procedures how they will ensure compliance with applicable securities laws and regulations and FINRA rules (*see, e.g., Notice to Members 05-48* (Outsourcing)). Broker-dealers may also want to review the covered functions first, to ensure that the functions are not prohibited from being outsourced.

Firms may also wish to consider providing specialized training to supervisory personnel and internal auditors, so that they can reasonably navigate the system and effectively perform their assigned functions.

Fees and Commissions

To the extent that participating in a DLT network results in additional or increased customer fees or charges (*e.g.*, for wallet management, key management, on-boarding), broker-dealers should ensure that any changes in their fee structure comply with applicable regulatory requirements. For example, FINRA Rule 2122 (Charges for Services Performed) requires that any charges for services performed must "be reasonable and not unfairly discriminatory among customers." Likewise, any commissions or mark-ups on DLT-derived products would be subject to standards outlined in FINRA Rule 2121 (Fair Prices and Commissions).

The following are some areas for firms to consider.

- What changes, if any, may occur in the fees or charges that firms impose on customers? How will these changes be communicated to customers?
- For new types of fees or charges (such as key management), how will they be structured and assessed (*e.g.*, one-time, per transaction, based on assets under management)?
- How will these fees and charges be reflected on confirmations and account statements?

Separately, to the extent a broker-dealer may make payments to third parties (whether on the network or outside of the network) that are not registered as broker-dealers, the firm should consider the structure (*e.g.*, transaction-based) and purpose of these payments, and whether they may implicate broker-dealer registration requirements for those third parties. FINRA Rule 2040 (Payments to Unregistered Persons) specifies requirements and restrictions related to transaction-based payments made to unregistered parties.

Customer Confirmations and Account Statements

Exchange Act Rule 10b-10 requires firms to disclose certain information to their customers before or at the completion of a securities transaction. Such information includes certain specific details about the transaction (such as date and time of transaction, identity, price and number of shares purchased), whether the firm is acting as an agent for any party, and the remuneration received by the broker from the transaction. In addition, FINRA Rule 2232 (Customer Confirmations) requires firms to, at or before the completion of a transaction, provide customers with written notification in compliance with Rule 10b-10. FINRA Rule 2340 (Customer Account Statements) imposes requirements on firms to provide customers with account statements at least quarterly, with certain specific information such as cash balances, security positions and any activity in the account since the last statement.

Broker-dealers operating or participating on a DLT network should ensure that the operational procedures and systems account for compliance with these requirements. To the extent broker-dealers are considering using the features of a DLT network (such as the maintenance of shared records on the network) to help facilitate compliance with these requirements, such firms should analyze how any new methods comport with existing obligations related to trade confirmations and customer account statements.

Some factors to consider in the analysis include:

- If multiple firms are involved in a customer transaction (*i.e.*, introducing and clearing firm), who would be responsible for sending trade confirmations and account statements to customers?
- Will the responsible firm have sufficient access to data on the network to generate such confirmations and account statements?
- As noted in the previous section, how will information about broker compensation and fees be reflected on confirmations and account statements?

Materiality Impact on Business Operations

NASD Rule 1017(a)(5) requires broker-dealers that undergo a material change in business operations to file a Continuing Membership Application (CMA) prior to implementing the material change.

Broker-dealers should consider whether the changes in the firm's operations, capital requirements, carrying/clearing status, and infrastructure when employing DLT are material and whether it implicates NASD Rule 1017, potentially requiring the firm to file a CMA with FINRA. If a firm is uncertain, it may seek a materiality consultation from FINRA (*see* FINRA's Continuing Membership Guide and NASD *Notice to Members 00-73*).

Business Continuity Planning

FINRA Rule 4370 (Business Continuity Plans and Emergency Contact Information) requires broker-dealers to create and maintain reasonable business continuity plans. Firms would need to consider how participation in a DLT network may impact its BCP and whether the network has sufficient measures in place to ensure business continuity in the event of a significant disruption.

Request for Comments

FINRA will continue its efforts to foster a deep dialogue with the industry, including with broker-dealers, other regulators and key stakeholders, to proactively identify and address any potential risks that new financial technologies may pose to investors and markets.

As the securities industry continues to expend time and resources in exploring DLT, it is imperative that market participants and regulators collaborate early in the process, to address any potential regulatory gaps that may pose risks or hinder the adoption of the technology. This will allow the industry to fully reap the benefits of the technology, while ensuring protection of investors and maintenance of market integrity.

FINRA encourages all interested parties to provide comments on all aspects of this paper. FINRA also requests comments on related matters for which it would be appropriate to consider additional guidance, consistent with the principles of investor protection and market integrity, based on DLT applications and their implications for FINRA rules.

Comments are requested by March 31, 2017. Member firms and other interested parties can submit their comments using the following methods:

- Emailing comments to *pubcom@finra.org*; or
- Mailing comments in hard copy to:
  Marcia E. Asquith
  Office of the Corporate Secretary
  FINRA
  1735 K Street, NW
  Washington, DC 20006-1506

To help FINRA process comments more efficiently, persons should use only one method to comment on the proposal.

Important Notes: All comments received in response to this paper will be made available to the public on the FINRA website. In general, FINRA will post comments as they are received.

Direct inquiries regarding this paper to Haimera Workie, Senior Director, Office of Emerging Regulatory Issues, at (202) 728-8097; or Kavita Jain, Director, Office of Emerging Regulatory Issues, at (202) 728-8128.

Endnotes

1. This paper is not intended to express any legal position, and does not create any new legal requirements or suggest any change in any existing regulatory obligations, nor does it provide relief from any regulatory obligations. While the paper highlights certain operational and regulatory areas that broker-dealers may wish to consider as they explore adopting distributed ledger technology, the paper does not cover all applicable regulatory requirements or considerations. FINRA encourages firms to conduct a comprehensive review of all applicable securities laws, rules, and regulations to determine potential implications of operating or participating in a DLT-based operation.

2. For example, FinTech start-up R3 is leading a consortium of over 50 financial organizations, to create a distributed ledger technology framework for its members. Similarly, the HyperLedger project hosted by the Linux Foundation is a collaborative effort by various cross-industry market participants to develop a DLT framework and make it available open source.

3. "The future of financial infrastructure: An ambitious look at how blockchain can reshape financial services," World Economic Forum, August 2016.

4. *See* FINRA Rule 4311 and Rule 4510 Series.

5. *See* FINRA Rule 4550, as well as the 5000, 6000, 7200, 7300 and 7400 Series.

6. *See* FINRA Rules 3310, 2090, 3110, 3120, 2121, 2122, 2040, 2232and 4370; the 4100 Series; and NASD Rule 1017.

7. *See* Request for Comments section on page 20 of this paper.

8. This paper is not intended to provide an in-depth technical explanation of the technology. Instead, it explains certain key concepts to set context, such that the reader can understand the regulatory implications we discuss in later sections.

9. Digital securities on a DLT network are different from traditional uncertificated securities.

10. A node refers to a participating entity on the network that maintains a copy of the ledger on the network.

11. A consensus-based verification process requires that a majority of the network participants confirm the integrity of the data in a transaction before that transaction is verified and recorded on the blockchain.

12. A proof-of-work-based verification process typically requires participants on the network to conduct some work and establish an economic interest (*e.g.*, opportunity to obtain a bitcoin) in the process of validating the integrity of the data in the transaction.

13. For example, on the Bitcoin Network, which uses a combination of proof-of work and consensus-based verification method, each transaction confirmation takes between a few seconds and 90 minutes, with 10 minutes being the average time. *Source:* Bitcoin.org, https://bitcoin.org/en/faq#why-do-i-have-to-wait-10-minutes

14. Hashing is the process of applying a mathematical formula to a set of data and converting it into a short binary value. A cryptographic hash produces a unique and non-predictable value. Also, a cryptographic hash is non-reversible, in that one can verify that the hash represents the corresponding dataset, but cannot identify the data by looking at the hash value.

15. "Accenture Debuts Prototype of 'Editable' Blockchain for Enterprise and Permissioned Systems," Accenture Press Release, September 20, 2016.

16. While the focus of this paper is primarily on the direct applications of DLT in the securities industry; securities products that invest in bitcoin or other blockchain-based virtual currencies represent another type of DLT application in the securities industry.

17. "NASDAQ Enables First-Ever Private Securities Issuance Documented with Blockchain Technology," NASDAQ Press Release, December 20, 2015.

18. "Overstock Closes Historic Rights Offering," Overstock.com Press Release, December 15, 2016.

19. "Blockchain Demonstration Shows Potential Loan Market Improvements," Credit Suisse Press Release, September 27, 2016.

20. "DTCC and Digital Asset to Develop Distributed Ledger Solution to Drive Improvements in Repo Clearing," DTCC Press Release, March 29, 2016.

21. "Successful Blockchain Test Completed by Axoni, DTCC, Markit, and Multi-Bank Working Group, " DTCC Press Release, April 7, 2016.

22. "Anoxi Creates Successful Reference Data Proof of Concept with R3, SIFMA, and Seven Financial Institutions," Anoxi Press Release, September 20, 2016.

23. "Global Banks and R3 Test DLT for KYC Services," Finextra, November 10, 2016.

24. One of the proposed benefits of DLT is the ability to offer a time-stamped, sequential, audit trail of transaction records. This may provide regulators and other interested parties (e.g., internal audit, public auditors) with the opportunity to leverage the technology to view the complete history of a transaction where it may not be available today and enhance existing records related to securities transactions.

25. "Big Banks Band Together to Launch 'Settlement Count'," CoinDesk, August 24, 2016.

26. As noted earlier, this paper is not intended to express any legal position, and does not create any new legal requirements or suggest any change in any existing regulatory obligations, nor does it provide relief from any regulatory obligations. While the paper highlights certain operational and regulatory areas that broker-dealers may wish to consider as they explore adopting distributed ledger technology, the paper does not cover all applicable regulatory requirements or considerations. FINRA encourages firms to conduct a comprehensive review of all applicable securities laws, rules and regulations to determine potential implications of operating or participating in a DLT-based operation.

27. *See* SEC Securities Exchange Act Release No. 70073 (July 30, 2013) (Order Approving File No. S7-23-11).

28. Exchange Act Rule 15c3-1(a)(2)(i) states that a "broker or dealer (other than one described in paragraphs (a)(2)(ii) or (a)(8) of this section) shall maintain net capital of not less than $250,000 if it carries customer or broker or dealer accounts and receives or holds funds or securities for those persons. A broker or dealer shall be deemed to receive funds, or to carry customer or broker or dealer accounts and to receive funds from those persons if, in connection with its activities as a broker or dealer, it receives checks, drafts, or other evidences of indebtedness made payable to itself or persons other than the requisite registered broker or dealer carrying the account of a customer, escrow agent, issuer, underwriter, sponsor, or other distributor of securities. A broker or dealer shall be deemed to hold securities for, or to carry customer or broker or dealer accounts, and hold securities of, those persons if it does not promptly forward or promptly deliver all of the securities of customers or of other brokers or dealers received by the firm in connection with its activities as a broker or dealer."

29. *See* SEC Securities Exchange Act Release No. 70073 (July 30, 2013) (Order Approving File No. S7-23-11).

30. Section 3(a)(23)(A) of Exchange Act provides the definition of a clearing agency. Section 3(a)(23)(B) of the Exchange Act provides exclusions from the definition of a clearing agency.

31. Introducing brokers may wish to consider how any additional responsibilities they take on in the context of operating in a DLT environment may impact their status as an introducing broker, particularly if they are undertaking any functions typically associated with a carrying firm.

32. 31 C.F.R. § 1023.220.

33. *See* SEC no-action letter to Mr. Ira D. Hammerman, Securities Industry and Financial Markets Association (January 9, 2015), providing relief to broker-dealers that rely on a registered investment adviser to perform some or all of its customer identification program obligations.

34. 17 C.F.R. Part 248.

35. The TRFs are facilities through which members report transactions in NMS stocks, as defined in SEC Rule 600(b)(47) of Regulation NMS, effected otherwise than on an exchange. The ADF is both a trade reporting and quotation display and collection facility for purposes of transactions in NMS stocks effected otherwise than on an exchange. The ORF is the facility through which members report transactions in OTC Equity Securities and certain transactions in Restricted Equity Securities, as those terms are defined in FINRA Rule 6420.

36. Refer to FINRA Rule 6710(a) for the definition of "TRACE Eligible Security." Beginning July 10, 2017, FINRA member firms must begin reporting transactions in U.S. Treasury Securities to FINRA via TRACE. (*See* FINRA *Regulatory Notice 16-39*, Reporting Transactions in U.S. Treasuries Securities, October 19, 2016.)

Investor protection. Market integrity.

1735 K Street, NW
Washington, DC 20006-1506

www.finra.org

17_0020.1 –01/17