March 31, 2017

VIA ELECTRONIC MAIL (pubcom@finra.org)

Marcia E. Asquity
Office of the Corporate Secretary
FINRA
1735 K Street, NW
Washington, DC 2006-1506

Re: Distributed Ledger Technology: Implications of Blockchain for the Securities Industry

Dear Financial Industry Regulatory Authority:

R3 CEV Ltd. ("R3") appreciates the opportunity to respond to the Discussion Paper issued by the Financial Industry Regulatory Authority ("FINRA") on January 18, 2017, entitled "Distributed Ledger Technology: Implications of Blockchain for the Securities Industry". Should FINRA request further engagement on the best application of distributed ledger technology ("DLT") for the securities industry, R3 would welcome the opportunity to provide any and all subject matter expertise that may be of aid.

As background, R3 is leading a consortium that includes over 80 of the world's largest banks, financial institutions and regulators, working together to develop and apply distributed ledger-inspired technologies to global financial markets. The R3 team of financial industry veterans, technologists and distributed ledger and cryptocurrency experts collaborate with consortium members to advance this technology to meet banking requirements for identity, privacy, security, scalability and interoperability. The emergence of DLT provides an opportunity for banks and other institutions to break free from multiple generations of inefficient legacy technology and move toward a future where shared records of financial agreements are automatically managed in the cloud without error. R3 is making that vision a reality with our Corda platform.

Corda is an open source financial grade distributed ledger platform that records, executes and manages institutions' financial agreements in perfect synchrony with their peers. It was designed from the ground up to address the specific needs of the financial services industry and is the result of over a year of close collaboration between R3 and our consortium. The Corda software underpins the wider R3 Network, acting as the gateway through which institutions can access a wide ecosystem of interoperable distributed ledger applications.

Implementation Considerations

Governance:

When establishing the right governance structure for a DLT network, it is important to consider the ledger construct. Depending on its purpose, the ledger could be run by a central authority and governed by that authority or it could run as a decentralized network adhering to a set of governance rules created and adhered to by the members. The interest of end users would be protected by rules that are in place in today's world that need to be adhered to and enforced by participants on the DLT network. The participants in the network would agree to contractual obligations to ensure their interests and their clients' interests are protected. The day-to-day operation of the network and technical issues would be determined by the service level agreements in place between the DLT provider and the network participants. A Business Continuity Plan is essential for the network provider, as well as participants that should take additional steps to protect their own data. Similar to internal system disruptions, participants should develop recovery plans to restore material business functions caused by signification disruptions to a DLT network, however it is unlikely those disruptions are to occur.

Any conflicts of interest should be identified and addressed by the service level agreements in place between the DLT provider and the network participants. There should also be oversight of the operation by a regulatory body, and a board of directors

should appoint an independent auditor to review operations and other issues free from the influence of interested third parties.

The network operator should be transparent about their partners, relationships in the market, as well as their fee structures as part of the network participation agreement. Any disruptions or breaches of the distributed ledger should be promptly reported to participants and the appropriate regulatory authorities. The direct and indirect costs to maintain the network, which may be passed on to participants should be specified in the network participation agreement. For services utilizing Smart Contracts, there should be appropriate protocols in place to address performance issues with Smart Contracts on the ledger, and when there arises a need to suspend, exit and repair clauses that would permit further execution of code to be halted pending repair.

Operational Structure

On-boarding, off-boarding and access:

R3 is primarily considering the implementation of a private network and is mindful of the potential impact on investor protection and market integrity of the design and implementation of the permissioning process of each such network. It will be vital that only responsible participants obtain access to the network(s) and that clear rules are in place, memorialized and monitored to achieve these aims. It is also important that the governance structures and admission processes of the networks allow for fair access and open competition, and necessary access to data for regulators. To this end, the comments in the FINRA paper are very helpful, and align closely with our thinking on the requirements to be addressed in DLT design and implementation. R3 is already considering the options for operating entities that can support DLT networks and take responsibility for fair and effective on-boarding / off-boarding processes. At the earliest opportunity, we would welcome an open dialogue with FINRA as we develop our ideas in this area.

Transaction Validation:

Validation on a distributed ledger can be achieved in multiple ways. There are different models where validators can be internal to a company or even a third party. Public blockchains utilize proof of work - a costly, inefficient solution used to establish voting order in an identity-free system.

In a private, permissioned distributed ledger network, with an authoritative gatekeeper for nodes joining the network ("doorman"), proof of work is not necessary. In a private, permissioned distributed ledger network, participants are known and can therefore be trusted to perform certain functions, as the relationship between entities is governed by legal contracts. Only trusted participants will be allowed on the network, but consensus is still necessary. Rules must be in place to provide the trusted third party legal authority.

The choice of the exact consensus algorithm – or protocol that network validating participants follow to determine agreement on the state of transactions in the system – may affect, latency and throughput. Additionally, for an identity-free system – where validating participants are pseudonymous like a public blockchain – because they lack explicit governance mechanisms, stakeholders have no formal method to hold pseudonymous validators accountable in the event disputes arise. For example, in many public blockchain systems, 51% of validating power could collude and change the next state of the blockchain without any recourse by other participants. While early iterations of public blockchain systems avoided trusted third parties, several different private distributed ledger platforms have a notary role that establishes one source of truth. This marks a dramatic improvement from today's systems where records may vary amongst multiple parties.

In distributed ledger systems, such as Corda, the concept of a notary provides the validating utility. The notary is responsible for transaction ordering and timestamping. Though a single node can represent the notary, the notary is typically comprised of multiple mutually distrusting participants who use a standard consensus algorithm. With a consensus algorithm, such as Raft[1], a

[1] The Raft Consensus Algorithm, (February 2017), *available at* https://raft.github.io/

leader is elected (and therefore in charge of pushing new transaction data to network participants) but other nodes vote on the next state of the ledger (i.e. which transactions are approved or rejected). Systems like Corda are designed to allow for the dynamic addition and removal of identifiable network participants.

The buzzword "immutable" is often used in discussing DLT systems. Yes, states can be changed, but only per the terms outlined in their governing Smart Contracts. In a system like Corda, state objects are controlled by pre-defined Smart Contracts. As state objects change, historic state objects are kept, but superseded by newer state objects.[2] If a Smart Contract allows for the future rectification of erroneous information – perhaps if a majority vote of involved participants agree – then the system will allow it. Otherwise, the data contained on the ledger cannot be modified. Theoretically, a distributed ledger system can allow some centralized party to override changes to the ledger.

Asset Representation:

Digitization of assets or representing assets on a DLT provides tremendous value for tracking, transferring ownership, automated execution of rules ("Smart Contracts") and providing secure and low friction movement. When both cash and assets are represented on the same (or interoperable) distributed ledger, there is a significant network effect allowing for delivery-vs-payment and payment-vs-payment, both domestically and internationally. Transactions can also split and merge states representing fungible assets. The ideal situation would be one where digital cash that is represented on the ledger is a form of central bank money.

Guidance on the legal and regulatory frameworks for both direct issuance of digital assets and of off-ledger assets, as well as guidance governing these movements, would be helpful, especially guidance indicating that a transfer of a digital asset using DLT represents a legal transfer of title.

---

[2] Richard Gendal Brown, The Corda Way of Thinking, (February 2017), *available at* https://gendal.me/2017/02/21/the-corda-way-of-thinking/

Further we would welcome consideration of a roadmap for a central bank digital currency. We have observed a significant value when working on joint projects including central banks, regulatory partners, industry schemes, commercial banks and academia. R3 has experience helping facilitate similar projects in multiple currency zones, including Canada and Singapore.

Data and Transparency Requirements:

A key benefit of a permissioned network is that it may be designed so that data is only shared with participants involved in the transaction. If you are a participant in the transaction, then you will be able to see the new state object – financial agreement – as well as the transaction graph which displays changes and owners of where this state object was first created and shared. Network participants can only see this information if they are explicitly given permission to copy this state object to their node.

R3's Corda allows for regulatory nodes to receive state objects on a per-transaction basis. These can be granularly controlled (e.g. flow can require a regulatory node to get a copy of states; movement of states between jurisdictions can also allow different regulators' oversight).

Network Security:

With a traditional blockchain, security is a construct determined by the participants capable of dictating which transactions are approved, per the software governing the system. Even if a network participant exhibits prudent security regarding their private keys, unaccountable miners can decide the fate of their wallets by attacking the minority chain and preventing transactions from being included into blocks.

With a private, permissioned distributed ledger, there are several features in place to ensure the integrity of the system. At R3, network security is one of our top priorities and focus areas. R3's Corda recommends that users store keys and run cryptographic operations inside hardware security modules ("HSMs") - devices that safeguard and manage private keys. Like

with traditional systems, Corda participants will have the ability to request new private keys from the network administrator in case of a proven loss.

Corda supports very strong encryption and signature schemes, much like other blockchain systems. Corda currently supports five different schemes for the signing of transactions, each of which uses SHA-256 or SHA-512. There has never been a known "collision" – when two different inputs, given the same hashing function, return the same output – of either a SHA-256 or SHA-512 hash. Corda is proactively secure against quantum computers through its support of SPHINCS-256, which benefits from avoidance of number-theoretic problems that are known vulnerabilities of quantum computers.

Regulatory Considerations

Customer Funds and Securities:

For a valid transfer of beneficial ownership to occur on a distributed ledger, keys need to be exchanged between sender/receiver of the asset/obligation. The exchange of keys is a prerequisite for the transfer of value. The rules established for network participation may require additional safeguards / controls such as a pair of key signatures (e.g. one from a maker and a second from a checker) to allow entities to transfer value, applying a four eyes principle. Control or access to the distributed ledger where the assets are held is dependent on both the technology of the ledger construct and the master agreement and network participation agreement that govern the ledger.

In the event of a loss or destruction of assets, we advise that all DLT Smart Contracts contain an encoded dispute resolution mechanism. In the case of fraud, effective security policy controls need to be developed to reduce the impact of the potential fraud. In the event of a destruction of a record, the expectation is that the record can be restored from backup. In general, participants to the ledger should refer to the master agreement or electronic trading agreements that govern such events.

In the event a financial institution on the network fails, the distributed ledger would hold an immutable record of all beneficial owners of assets to prevent assets from being put at risk. In addition, the network participation agreement could include rules dictating how to handle default of a participant, including escrow of default funds or other procedures to make participants whole. If participants partner with third parties to serve as their backups and/or to carry out critical functions on their behalf in the event of emergencies, appropriate controls need to be in place to govern when and how the third party would have access. For example, the access to private keys would be dependent on the nature of the distributed ledger construct; the permissions provided to third parties to access assets on the ledger would need to be clearly specified in the rules under this construct. As a rule, third parties should be permissioned in the distributed ledger systems for authorized actions only, and keys to the assets of ultimate beneficiaries on the ledger should be protected by this permissioned system. A network participation agreement should detail rules that govern how customer's assets are protected in case of a default.

Clearance and Settlement:

In a traditional settlement system, two (or more) participants record, book, and confirm a trade in separate silos, then communicate to verify if the details are accurate. If there's an error, the information typically flows back up the chain from the back office eventually to the trader (or person who entered the trade), where corrections are made, and then the process repeats.

The use of DLT allows for the efficient simplification of the clearing, settlement, and reconciliation processes that are required of the participants privy to a transaction. The design of the distributed ledger arrangement can vary; for instance, a design may allow for only the sharing of information to all material participants to a transaction. Alternatively, a distributed ledger can also be designed to achieve full end-to-end settlement, through the exchange of information between material participants and then through the exchange of value, or assets on ledger. Using a distributed ledger system, you have shared business logic and the shared processing of that business

logic, to create a single set of shared data. Corda shares that data on a need to know basis only, but the idea remains consistent.

Anti-Money Laundering and Customer Identification Program:

Allowing identities to update their own information on the ledger and control access to it ("self-sovereignty") would greatly improve data accuracy, richness, and support sharing - all of which are essential to the development of KYC/AML tools far more powerful and efficient than anything in the marketplace today.

A common question within this theme is how government actors would be able to interact with DLT solutions that handle KYC/AML, and what level of access would make the most sense given sensitivities around government access to certain personal information that makes up a digital identity. R3 has designed Corda to support a flexible approach in this area, giving participants the ability to set permission levels and thereby protect information that is not relevant to other participants on the network, including regulators. Data on the distributed ledger can be attested to by reliable third parties further strengthening the quality of information and help enhance compliance with "using reasonable diligence" as stated in FINRA Rule 2090. Users relying on the data would be notified if data changes. This feature would greatly benefit jurisdictions where regulators require entities to upload information to central registries.

Further clarity of AML responsibilities related to ongoing monitoring for a distributed ledger network provider would be beneficial.

Customer Data Privacy:

R3 takes the subject of data privacy extremely seriously and has specifically designed its own DLT solution with all relevant data privacy laws and guidelines in mind. On R3's Corda platform, data is not shared with all participants, but only with those with the appropriate authority / permissioning. R3 believes that DLT -

involving as it does the use of cryptography to authenticate, protect and secure records as well as Smart Contracts to provide great flexibility in control of access to, and modification of records (including the records of those identities able to access and use the distributed ledger) - substantially improves the ability of banks and other financial institutions to act responsibly with respect to client data records under their control. By not sharing data records widely, Corda enables the restriction of data record location to the appropriate jurisdictions.

Trade and Order Reporting Requirements:

The process of booking a trade (e.g. recognizing the definitive profit and loss on a bank's books and records, and the intermediate steps to assure an orderly exchange of value) involves multiple IT systems and departments across a bank. Processing trades on a common distributed ledger offers significant efficiencies over current practice. Instead of capturing data from a trading platform and copying / storing it in a separate database, a trade processed on the distributed ledger can be validated and time stamped by a notary to confirm both participants are recording the same trade attributes. This eliminates the need for external reconciliation and creates a "golden source" of trade facts to feed internal processes as well.

For trades on Corda, the presence of a regulatory node would allow regulators to have supervisory oversight of transactions processed by banks in their jurisdiction. This would empower regulators to receive real-time information on cancels, corrects and amends and could eliminate the need to create a distinct reporting process. Post trade reconciliation performed by banks and regulators would be substantially less onerous. For example, TRACE Report Cards will no longer need to report mismatched and late trades. Regulators and banks can focus on the single source of truth and spend less time reconciling transactions and understanding the individual systems of record involved with trade processing. A significant amount of time and effort is currently spent by regulators to simply understand the data sets provided by different banks: a single source of record shared

across banks would reduce this effort and free up time for deeper analysis.

Business Continuity Planning:

Business Continuity Planning is essential and mandatory: participants of the network must be able to continue conducting their normal activities regardless of external events. Hardware failures, natural disasters and loss of data integrity must not interrupt business activities. The criticality of shared ledger applications must be assessed in terms of their impact on the members' mission and overall systemic risk. This assessment will dictate which availability / criticality level is required and which corresponding recovery plan must be implemented.

Supervision and Surveillance:

DLT offers more transparency and analytical oversight. R3 believes DLT has the potential to improve reporting and assist compliance departments with many of the written supervisory procedures required by FINRA 3110. FINRA 3110 and many other regulatory requirements rely heavily on documenting controls. A distributed ledger-based environment can serve as a mechanism for transacting and documenting controls and control results. Smart Contract logic can codify key controls, ensuring that all participants on the network apply the same control framework for their transaction records and processing.

Corda's ability to capture trade information and share transactional information on a "need to know" basis allows designated individuals in first and second lines of defense positions to review internal and external transactions. Approvals and attestations can be shared on the distributed ledger so individuals with oversight responsibilities have a clear audit trail of all participants, internal and external. This level of oversight would enable diligent controls over key processes including safekeeping and segregating customer securities, escrow account maintenance and gift and entertainment expenses.

We strongly recommend FINRA modernize existing regulations to accommodate DLT as a means of documenting, transacting and

storing transaction and lifecycle events across multiple asset classes. The non-rewriteable and timestamp capability of the distributed ledger could serve as an alternative to "optical disk technology" under FINRA Rule 4511. Additionally, the distributed ledger could also provide the same intent as WORM format required in FINRA Rule 17a-4.

Fees and Commission:

R3 agrees that any customer fees assessed in relation to DLT should comply with existing regulations. R3 believes customer fees can be significantly lowered due to automation of back office processes. Consistent with laws today, any fees associated with the DLT should be transparent with timely notification to the customer. Smart Contract logic enables consistent collection, application and recording of fees with a full audit trail.

Broker Capital:

R3 believes that DLT will assist banks in calculating capital requirements. Digital currency or digital receipts on a ledger would facilitate real-time position-keeping and exchange of allowable assets, including high quality liquid assets (HQLA) assets, across multiple product lines and trading desks.

Regulatory guidance on accepting digital currencies and digital receipts as allowable assets under capital requirements would be beneficial.

Customer Confirmation and Account Statements:

R3 does not think responsibilities for providing customer statements will change from the current process. For trades recorded on Corda, it will be easier for financial services firms and third parties to retrieve customer information to ensure customer statements are accurate. Given that the data sets upon which customer statements are based will have been independently affirmed by the counterparty as well as the receiving institution, regulators and customers can rely on the data

knowing that it has been attested by multiple parties, not just the reporting institution.

Conclusion

R3 appreciates the detailed information and guidance provided in FINRA's report and fundamentally believes that the concepts presented are a practical approach to the application of DLT in the securities industry.

As mentioned, R3 would welcome guidance as it relates to accepting digital currencies and digital receipts as allowable assets under capital requirements; as well as on legal and regulatory frameworks for the issuance of digital assets of off-ledger assets. In addition, consideration of a roadmap for central bank digital currency would be appreciated.

R3 strongly recommends FINRA modernize existing regulations to accommodate this technology's benefit through the means of documenting, transacting, and storing transaction and lifecycle events across multiple asset classes.

We would welcome the opportunity to continue our engagement with FINRA to guide the best application of this technology and to demonstrate the use of our distributed ledger platform, Corda.

Respectfully yours,

Charley Cooper

Managing Director, External Affairs