DTCC

Securing Today. Shaping Tomorrow.®

JANUARY 2016

# EMBRACING DISRUPTION

## TAPPING THE POTENTIAL OF DISTRIBUTED LEDGERS TO IMPROVE THE POST-TRADE LANDSCAPE

A WHITE PAPER TO THE INDUSTRY

# TABLE OF CONTENTS

# INTRODUCTION

*DTCC is an industry-owned and governed financial market utility with more than 40 years of experience mitigating risk and driving operations and cost efficiencies for the financial industry. We believe that realizing the promise of distributed ledgers lies in aligning the technology with these core principles to leverage new opportunities and simplify or replace legacy systems.*

The emergence of the Bitcoin payment network[1] and its associated ecosystem of blockchains, sidechains and altchains have been described as a generational disruptive force in the financial services industry. While some of the concepts of distributed electronic currencies have existed since at least the 1990s[2], the implementation of Bitcoin and the white paper that described it were the watershed moment in use, adoption and popularization of a decentralized crypto-currency. While Bitcoin as a payment mechanism is being discussed and researched in many other forums, the Bitcoin technology platform, commonly referred to as the blockchain or distributed ledger, is considered in this paper for application to post-trade processing and other functions that are managed by financial market infrastructures.

The premise of the Bitcoin platform – a decentralized, trustless, replicated ledger of transactions – is the virtual opposite of the centralized, trusted, guarded, model of modern securities processing, which has long relied upon DTCC, among others, as a central authority. The trust model, along with the economies of scale of centralizing common back-office processes and the strict controls and regulatory oversight of DTCC, has ensured the safety and soundness of securities trade processing through periods of extreme volumes and systemic market shocks. It has also created the most cost efficient post-trade processing infrastructure in the world.

DTCC has a long history of driving innovation to strengthen the post-trade process. In this same spirit, DTCC embraces the potential application of distributed ledger technologies across a range of processing to further lower risk and costs for the industry. The purpose of this paper is to cut through the hype and provide DTCC's insights on opportunities for leveraging distributed ledger technologies to improve existing business models and legacy systems. As always, the core DTCC mission of protecting the markets infers that safety, soundness, integrity, resiliency and reliability, and the trust that DTCC has earned across more than 40 years of uninterrupted service to the global markets, will be a central element of those thoughts.

1 Bitcoin: A Peer to Peer Electronic Cash System https://bitcoin.org/bitcoin.pdf

2 E.g., ecash proposed by D. Chaum 1983, hashcash proposed by A. Back, E-Gold launched in 1996

# EXECUTIVE SUMMARY

Today's global financial markets are underpinned by a complex network of internal systems and service providers that support the processing of hundreds of millions of financial transactions each day. This amalgamation of internal and external systems may appear disorderly, but as a result of painstaking efforts over the years, they have been integrated to enable the seamless and efficient flow of assets, information and data across markets and regions. While the current system was not created through intentional architecture and design, it provides the necessary stability, reliability and certainty that ensure global markets are efficient, transparent and cost effective.

DTCC believes that distributed ledger technologies have the potential to address certain limitations of the current post-trade process by modernizing, streamlining and simplifying the siloed design of the financial industry infrastructure with a shared fabric of common information. There are several key features that make this technology a potentially attractive option to improve existing processes, including the fact that standard rules exist for securities transaction validation and replication; immutable linkage to transaction history and auditability.

While distributed ledger technology has captured the imagination of the industry, key challenges with the platform will need to be overcome before it can be widely adopted or considered enterprise-ready. In addition, the industry itself needs to determine whether using the platform is more cost effective than improving existing technology and whether it can overcome its inherent scale and performance challenges. Furthermore, there needs to be industry-wide discussion, including regulatory and policymaker engagement, and consensus on developing requirements and determining whether trusted third parties are best positioned to develop them.

The industry hype and research into this new platform has been unprecedented but also generally uncoordinated up to this point. As a result, the industry is at risk of repeating the past and creating countless new siloed solutions based on different standards and with significant reconciliation challenges – essentially a new system with the same challenges we face today. To avoid this, the industry should engage in a collaborative rearchitecture of core processes and practices to ensure standardization. DTCC believes it is best positioned to support and coordinate the evaluation and standardization of the distributed ledger platform, help address industry challenges and determine whether it is a better solution than existing technology. In addition, as an industry-owned and governed financial market utility with more than 40 years of experience mitigating risk and driving operations and cost efficiencies, DTCC is uniquely positioned to perform this role with absolute focus on the best interests of post-trade processing in a manner that serves the industry, regulators and the investing public.

In evaluating opportunities to leverage distributed ledgers to improve upon existing infrastructure, DTCC has identified several areas and processes for further review. Based on its research and analysis, DTCC recommends exploring distributed ledger initiatives in:

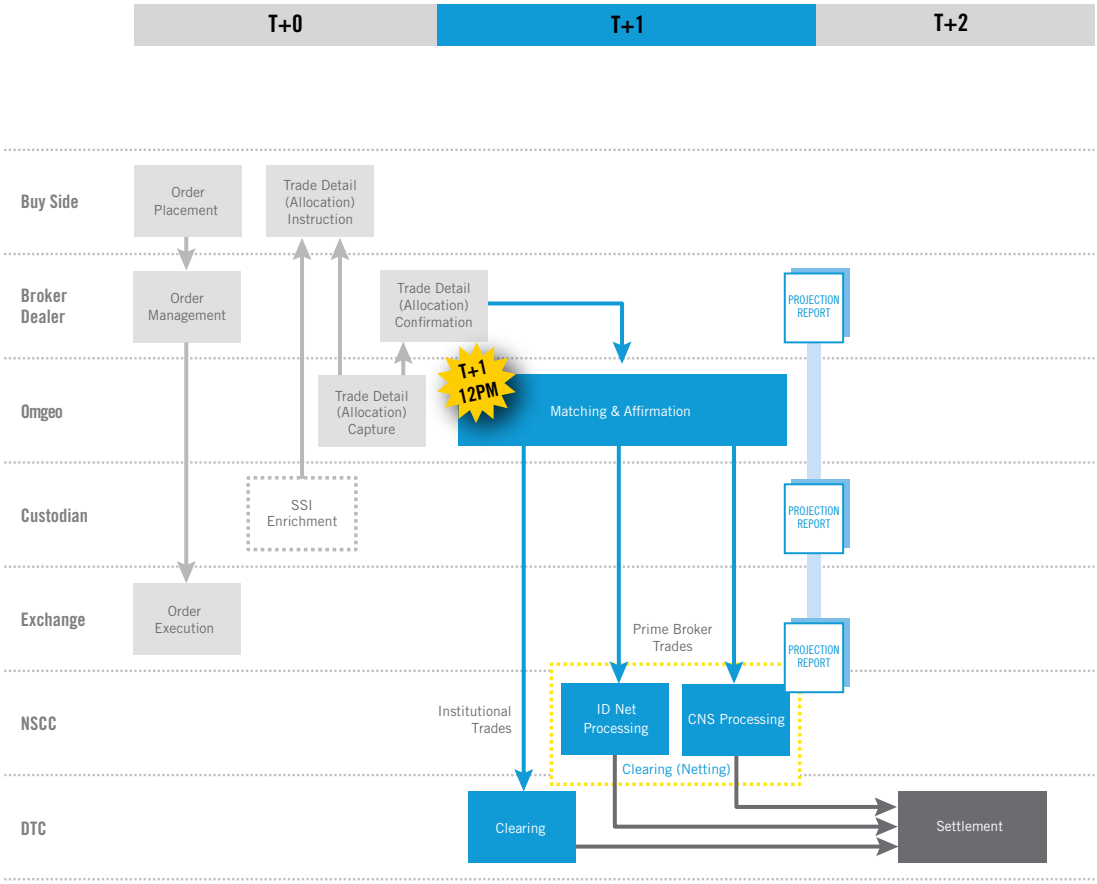
- Master data management
- Asset/securities issuance and servicing
- Confirmed asset trades
- Trade/contract validation, recording and matching for the more complex asset types that currently do not have strong, existent solutions
- Netting and clearing
- Collateral management
- Settlement

Importantly, while there has been a great deal of discussion around implementing real-time settlement using distributed ledger technology, the current U.S. equity market convention of T+3 is based on laws and market structures. Modernizing current practices and laws to enable real-time settlement are not dependent on the use of blockchain technologies.

DTCC strongly believes that the financial services industry has a once-in-a-generation opportunity to reimagine and modernize its infrastructure to address long-standing operational challenges. DTCC has the experience and capabilities to enable the integration of a financial industry distributed ledger ecosystem with the existing financial market infrastructures in a manner that is consistent with its mission and that further lowers risks and costs for all market participants.

# THE EVOLUTION OF TODAY'S FINANCIAL MARKETS

At its most basic level, trading is simple. An investor exchanges an asset of value and receives payment in return. Peer-to-peer. No intermediaries. And ideally, the exchange takes place at the same time. That is how trading occurred in the early days of the stock exchanges, with the trade agreement and settlement typically completed bilaterally. However, as exchanges matured and became more complex, and as more people accumulated assets and authorized trusted third parties to hold and manage those assets on their behalf, various service providers became trusted to manage the processing. Over time, periodic financial crises, oftentimes spawned from abuse of investor assets by those same trusted service providers, caused investor losses, prompting the addition of governance and utility infrastructures to oversee processing and to mitigate these and other risks. The result is the complex layers of interactions that exist today and is depicted in the image below, which illustrates the currently planned move to shorten the settlement cycle in the U.S. to two business days after a trade is executed, known as T+2.




This picture greatly simplifies the processing that occurs in each firm. In reality, buy-side and broker-dealer institutions have an amalgamation of systems that have been developed over the past 40 years through automation initiatives, regulatory mandates and the proliferation of marketplaces. Today, different internal systems and/or service providers address different aspects of trade order management, post-trade processing, asset account services and data management. Despite multiple layers of orchestrated interactions, reconciliations and workflows, modern global markets are highly efficiently, transparent and relatively low cost.

# LIMITATIONS OF THE CURRENT FINANCIAL MARKET INFRASTRUCTURES

Today's financial market infrastructures have a proven track record of providing stability, reliability and certainty – all key ingredients to ensuring the efficient operation of the markets, especially during periods of extreme volatility. The collapse of Lehman Brothers and MF Global, as well as the 2012 "electronic trading glitch" and 2010 flash crash incident, are just a few recent examples that reinforce the critical role of central counterparties and market infrastructure in protecting the integrity of the global financial system when a systemic shock occurs. However, the current system also has certain limitations that distributed ledger technology has the potential to address:

- **Multiple Versions of the Truth:** The layers of financial market systems are siloed and contain multiple versions of truth. There is minimal transparency into each system, and every bank maintains large, costly libraries of application code existing only to reconcile different versions of the truth.
- **Vulnerable to Technology Threats:** The legacy systems currently employed were not architected to protect against today's technological threats, including the potential for cyberattacks. As a result, the potential for data compromises due to system vulnerabilities exists.
- **Unnecessarily Complex:** Today's systems are very complex due to their evolution over the course of decades. Trading activities, along with clearing, settlement and collateral/capital/asset management systems, were built at different times and intended to serve different needs. Today, there are minimal widely used standards, systems are not well integrated and many manual processing steps still exist.
- **Not Equipped for 24/7/365 Processing:** Today's systems were mostly architected prior to the globalization of the industry and the resulting need for markets to operate 24 hours a day, 7 days a week, 365 days a year.

# KEY FEATURES OF BLOCKCHAIN AND DISTRIBUTED LEDGERS EXPLAINED

In assessing opportunities to leverage distributed ledgers to improve the current system for processing securities transactions, it is helpful to have an understanding of the Bitcoin payment network and the individual components that form its underlying technology platform.

The Bitcoin payment network was built as a peer-to-peer, distributed and decentralized platform to validate and track transactions without any central authority. Eight key capabilities that combined to create this innovative platform are described below:

- **The Asset Is Built-In:** The asset called Bitcoin (BTC) is produced and managed completely within the Bitcoin network. Therefore, the history and quantity of every movement of Bitcoins is mathematically verifiable by the recorded history in the distributed ledger of the Bitcoin network.
- **Party Identity Abstraction:** Security by obscurity is built in to the platform, meaning individual parties are never identified. Instead, security keys (public and private key pairs) are required to gain access to transaction output. Only the holder of the private key can send Bitcoins or get access to received Bitcoins. Only the private key owners know their total aggregated amount of Bitcoins.
- **Transaction Linkage:** Every transaction record (ledger entry) is linked to previous transactions and is standardized for every participating node. Every ledger entry is retraceable across its full history and can be reconstructed.
- **Transaction Scripts:** These are the standardized rules and conditions applied to a transaction. Every node applies the same rules. In the simple Bitcoin model, a Bitcoin is moved from one party to another according to rules. Newer versions of the blockchain have expanded the scope and capabilities of those rules, which form the basis of what is called "smart contracts."
- **Transaction Distribution:** There is a standard network protocol that allows every participating node to receive every transaction and apply the same validation rules.
- **Blockchain:** This is the single standard for how every node stores the transaction data (ledger data). Every node adheres to that standard and can have a full copy of the data. This is sometimes called the "distributed ledger." Records, or blocks of transactions, are added to the blockchain and include a link to the previously added block. This is the official point of immutable recording of a transaction.
- **Decentralized Consensus:** This consists of the standards and rules for how every node exchanges the block-chain information, the mathematical rules for all nodes to agree on the integrity of that data (sometimes called "proof of work") and the payment incentive to support the consensus model. A key point of the model and this entire platform is a method to ensure all transactions are validated and all valid transactions are added once and only once. No valid transactions can be omitted (sometimes referred to as censorship) and, in the case of the Bitcoin network, a Bitcoin cannot be double spent.
- **Trust vs. No Trust or Permissioned vs. Not Permissioned:** The "No trust" model refers to the public and open access of the Internet on which the Bitcoin network was built. Anyone can download the open-source software and join. The Bitcoin network was constructed to distrust any node based on a model that works as long as a

majority (>51%) of the nodes act as honest participants in the consensus activity described above. Trusted, or permissioned, implementations are significant modifications to that model, which requires permissioned servers to be approved and onboarded in order to participate.

In short, the blockchain is a network and a database; it has rules and built-in security; and it maintains internal integrity and its own history. These components create the value of the Bitcoin blockchain, but each of these concepts has the potential to be applied individually or in various combinations to improve existing processing of financial transactions.

The Bitcoin network provides near real-time settlement, which has been referred to as a unique innovation. As we will discuss in more depth later in this paper, real-time settlement is possible with existing technology and is already existing practice for some asset classes. The current general U.S. equity market convention of T+3 (settlement occurs three business days after the date of trade) as well as the industry plan to move to T+2 are not the result of technology limitations, but based on laws and market structures. Modernizing current practices and laws to enable real-time settlement are not dependent on the use of blockchain technologies.

# THE STATE OF DISTRIBUTED LEDGER TECHNOLOGY TODAY

It is only recently that some of the leading innovators and strategists in the financial markets have shifted their thinking from the specific use of distributed ledgers for crypto-currency transactions to employing the technology to support other financial and securities industry processing. While there are many experiments and use cases currently underway, at this time, there is no single distributed ledger application operating in production at large scale. This is due, in part, to fundamental technology challenges related to scale, latency, performance and security. In addition, the nonfunctional requirements, such as integration with operations and logging and monitoring tools, which are central to every enterprise production environment, have not yet been addressed. The state of distributed ledger technology today is that of development experiments, and there are few, if any, well-established and known technology vendors currently operating in this space. As a result, the product quality, enterprise support capabilities and actual long-term viability of the new vendors will need to mature in order to facilitate the evolution of this technology.

This reality has been skewed by the near daily announcements of new developments, new partnerships, new consortiums as well as a steady stream of news on improvements in the technology. For all that hype, these efforts are still at their very earliest stages. As of today, there are different implementations, different rules and different data and security models. Furthermore, there are no commonly accepted standards, and with multiple efforts being undertaken in the space, resolution will take time. While talk of the next big disruption suggests wide-scale adoption is imminent, the facts suggest otherwise. In reality, distributed ledgers are best considered an emerging technology in the processing of securities transactions.

## Limitations of Distributed Ledger Technology

In assessing the applicability of distributed ledgers to post-trade processing, it is important to understand that the distributed ledger platforms in use today are simply a ledger of transactions that is essentially replicated to all of the cooperating servers. The technology does not have built-in integration with existing systems and supporting infrastructure. It does not simply integrate with user identity management systems or have any master data about legal entities or securities. It does not include supporting workflows, exception processing or any of the extensive preprocessing logic that often accompanies complex matching, allocation and other processes that precede the point at which a transaction is considered complete.

A valuable feature of the distributed ledger platform is that all transactions are considered immutable and never to be modified, cancelled or revoked. The ability for clients to correct/cancel/adjust transactions that were inadvertently charged or credited to the wrong account is a common occurrence and well managed by today's financial institutions. Additionally, complex financial transactions often include the ability to reverse the transaction based on contractual stipulations as a desirable feature. The ability to cancel or reverse a transaction is not supported in today's distributed ledger platform, and it is not clear today how the platform could evolve to support that.

In addition, the technology is lacking in these other areas:

- It does not improve upon existing data retrieval, inquiry, reporting or analytic tools.
- It does not allow data searching in a manner that is even equivalent to modern databases.
- It does not provide high-speed access to data in the same manner as big data technology for purposes of data analytics.
- It does not integrate with modern data management tools.
- It does not address the nonfunctional requirements of most processing systems.

For distributed ledgers to reach their full potential, all of these functions, which exist in the current post-trade process and have been constructed over the years by experts and industry professionals, will need to be integrated into this new platform.

## Decentralized vs. Centralized Processing

Another important issue to consider in the widespread applicability of distributed ledgers is the trade-offs between decentralized processing and the more traditional computing model of centralized processing.

Decentralized processing is, by definition, a shared computing function among members of a community (trusted or not), which requires synchronization and coordination. Some implementations of distributed ledger, such as Bitcoin, use a consensus mechanism to manage coordination, while others use variations such as a lead node mechanism. Regardless, all such designs include steps that add latency to transaction processing. A decentralized design requires significant computing and storage resources because all nodes perform the computations and store the ledger data, which can also result in significantly increased network bandwidth requirements depending on the number of network nodes and the size of each transaction.

In contrast, the use of centralized processing provides a single view of information with a single judgment on a truth, typically on a single machine. The latency of this model is virtually zero. It is certainly possible to take some of the paradigms of the distributed ledger platform, such as improved security, standardized validation rules and verifiable transaction history, and implement them in a centralized system. But this model also requires complete trust in the integrity of the centralized system and in the organization that manages that system.

Global regulatory requirements for data privacy that are different based on geography raise additional challenges for decentralized systems that distribute every transaction to every node. In certain regulatory jurisdictions, the laws protecting an individual's data privacy restrict the ability to store certain data outside of the regulated region. Several vendors have recently proposed alternative "partitioned" ledgers to address these challenges, but given that all of the current work on distributed ledger technology has been done without regulatory oversight or endorsement, it is still unclear as to the level of regional data containment that will be required.

It is an open question for the financial industry as to whether the current use of central, responsible authorities, such as central repositories and custodians, is a desirable future state or whether distributed systems using mathematics and cryptography to guarantee integrity is a better alternative. The future state may evolve to require both forms of processing. DTCC's view is that the technology could be used to support either alternative and that the most logical and least risky way forward would be for the existing, regulated and trusted central authorities to introduce the standards, governance and technology to support distributed ledger implementations. The use of existing, regulated entities would naturally engage the regulatory community to support the potential policy changes that may be needed to allow this technology to succeed. In addition, we believe that the technology and ledger should be industry-owned so that there is strong alignment with industry-wide needs and that opportunities are focused on benefiting the industry in the broadest manner possible.

# BUILDING BLOCKS FOR LEVERAGING DISTRIBUTED LEDGERS IN FINANCIAL SERVICES

Despite the limitations noted in the previous chapter, DTCC believes that a secure distributed ledger, with complete, traceable, transaction history for a set of assets that is shared and accessible only between trusted parties, could provide a significant improvement in certain areas of today's infrastructure. It could support solutions to address current business challenges by ensuring:

- A common, shared, version of the truth – every trusted member has a copy of the same history of all transactions in an asset.
- All data is encrypted in a common manner according to modern standards and can only be decrypted and inspected by the owner of the required keys to the data.
- The shared ledger, used by every trusted party involved in trading a particular asset, establishes a network and data standard that can be integrated with tools, workflows and asset management systems in a simplified, consistent manner.
- The transaction distribution model defines a paradigm for always-on, active:active processing, which is more resilient to local database corruption than existing hardware replication models.

There are several key building blocks for leveraging distributed ledgers in financial services, including industry-wide acceptance and adoption of formally defined standards for financial instruments, legal entities and financial contracts that would be encoded within the distributed ledger of transactions. A critical core requirement is the governance and regulatory framework for the "trust boundaries" of the distributed ledger. The trust boundary is the place where the ledger integrates with anything that is not in the ledger, such as onboarding trusted entities as ledger members or entitling an entity to issue an asset into the ledger and validating that the rights to the specific asset are owned by that entity and that those assets are properly secured off the ledger. A distributed ledger can provide an immutable digital recording of an asset, and the transactional transfer of that asset for value, shared among the other parties in the ledger network. But if the asset itself is in physical form or not stored directly and completely on the ledger, then centralized trust remains with a custodian of the asset to ensure the asset exists, is protected, and is not entered into multiple, disconnected, shared ledgers.

The critical role of governing and managing the standards, rules and trust boundaries must be managed with indisputable integrity and accountability, independent of any commercial conflicts. This is the role that industry infrastructure organizations, such as DTCC, have provided to the financial markets for more than four decades.

**DTCC's Role in Leveraging Distributed Ledgers**

DTCC views itself as an enabler of a potential paradigm shift toward a new distributed platform with improved security, appropriate transparency and enhanced reliability that can reduce risk and simplify processing across the financial industry. As an industry-owned and governed infrastructure, DTCC could enable the integration of a financial industry distributed ledger ecosystem with the existing financial market infrastructures. DTCC sees this role as consistent with its mission and responsibility to drive innovation by introducing new platforms in the most considered, risk- and test-managed manner possible.

DTCC further believes that the capabilities provided by a secure distributed ledger have the potential to modernize, streamline and simplify the existing siloed design of the financial industry infrastructure with a shared fabric of common information. Achieving this goal will require a collaborative rearchitecture of core industry processes and

practices that were built over many decades, each somewhat differently and all requiring reconciliation with previous and subsequent systems. A collaborative industry modernization program that includes distributed ledger technology could reduce the process steps required for financial transactions and improve the security and resiliency of the remaining processing systems, thereby reducing costs and risks of transaction failure.

**Learning From the Past: Coordination and Standardization Essential**

Over the past year, many industry participants have begun to pursue individual experiments and have established islands of private partnership. As a result, it appears there is a disorganized and almost chaotic market-driven rush to productize different ledger opportunities. While it is the inherent nature of free markets to focus on short-term opportunities for gain, history could be repeating itself in that the existing state of complexity in financial market infrastructure arose through a similar series of uncoordinated implementations, market opportunities and regulatory responses.

The industry has been forced over the years to expend massive amounts of energy and resources trying to reconcile that approach because of a lack of coordination, collaboration and standardization. As financial institutions consider opportunities to move processing into distributed ledger infrastructure, there will be a need to connect and coexist with existing infrastructure for a considerable period of time. The integrity and soundness of those inter-connections will be critical to establishing trust in the new infrastructure. Creating an infinite number of different ledger silos will add cost, complexity and may actually increase risk to the system. The global reach and capability of this technology also creates challenges related to different global regulatory jurisdictions, but they may also prompt global policymakers to cooperate and create legal frameworks that enable new opportunities to nurture and flourish.

**Intellectual Property**

Intellectual property associated with this new technology also needs to be carefully considered – the open source and standards that were part of the premise of the original blockchain implementation must be balanced with the interests inherent in the commercial landscape of proprietary vendor solutions. A sustainable distributed ledger platform that is capable of serving markets broadly should require central industry coordination and governance, whether through industry associations, open consortia or industry utilities whose mission is to serve the industry.

**Enterprise Integration**

DTCC strongly believes that this is a generational opportunity to reimagine the financial industry infrastructure, and this can only be accomplished from a well-considered, collaborative, design approach. A likely first step would be defining the foundational building blocks to integrate a transaction ledger into an enterprise, such as integration with existing systems of financial entity information, user identity information and asset information.

# LEVERAGING DISTRIBUTED LEDGERS

This section provides DTCC's perspective on how distributed ledger technology may improve upon existing infrastructure. As a general framework for evaluation, the following advantages of a permissioned distributed ledger are evaluated for each business area opportunity.

| | |
|---|---|
| **STANDARDS:** | Does the use of distributed ledgers help enforce industry standardization of data formats and contractual rules? |
| **EFFICIENCIES:** | Can a distributed ledger eliminate manual interactions, data exchanges, data format conversions and reconciliations with other systems? |
| **FASTER PROCESSES:** | Does distributed ledger technology provide a platform to reduce time and risk to complete a transaction? |
| **TRANSPARENCY:** | Does the transparency provided by the distributed ledger benefit this business use of the technology? |
| **SECURITY:** | Does the inherent authorization and encryption of the distributed ledger improve the overall security of this business process and its data? |

DTCC considers these five features to be the most essential and significant improvements that a permissioned distributed ledger may offer compared to existing technologies. There are certainly other aspects of distributed ledger platforms that are being used or researched at this time, such as public transparency, incentivized mining and user anonymity, but for the regulated marketplaces, these five advantages most warrant evaluation.

As mentioned earlier, there are several very significant limitations to the technology today that preclude many financial transactions from being able to use this platform in any manner. These include limits on the size of individual transactions and the number of transactions that can be written simultaneously as well as the latency between writes to the ledger and final confirmation. But current research and experimentation is expected to improve those limitations to a point that would enable adoption. This paper is taking a forward view that those limits will be improved, so they will be ignored for the rest of this discussion.

A key question is whether the equivalent result – reducing risk and lowering costs – can be achieved with existing technology. This question can only be answered completely after experiments and trials validate the capabilities and limitations of distributed ledger technology. But the premise of this paper and this section is that the five features listed above, implemented in a distributed ledger solution, may provide a more effective solution for record keeping, trade processing and transfer of value transactions where more than two parties are involved.

This section reviews the different foundational building block categories of information sources that support transaction processing and considers whether a central, single source of trust is required or whether the advantages of the decentralized ledger approach could be leveraged. While ledger technologies do provide different capabilities as compared with existing data management platforms, they may not always be a better fit for purpose. Any discussion about reimagining the financial industry must include consideration of where existing technologies continue to provide a sufficient solution to the problem(s) they are solving.

# Record Keeping:

## Identity Management

Identity and access management systems are critical components of every financial industry organizations infrastructure. Within every financial firm, associating a user identity and their account of asset holdings (or Bitcoin wallet) requires a customer onboarding process. Providing identity information requires a secure source of trust, as some party will validate biometrics or other physical information and credentials. There are significant regulatory considerations, particularly around privacy protections for nonpublic, personal identity information. Identity and access management systems are often the one system within financial firms that have a single source of truth and are tightly integrated across their entire portfolio of front-, middle- and back-office applications. Identity and access management systems, with their nonpublic, personal information and keys to financial holdings, have also become the most appealing target for attack.

The current reality is that systems considered unbreakable and extremely secure are being compromised with relative ease. Given the nascent nature of distributed ledger technology, the data associated with identity would not be appropriate to have stored on a decentralized ledger until the technology has matured and proven its ability to survive an attack.

## Master Data Management

Master data, including entity information, asset information, business day and holiday information and other, usually nontransactional business information, is a foundational component of all securities transaction processing. This information will typically include master data that is local and intrinsic to an enterprise as well as master data that should be common across an entire industry. The current implementation of most master data systems is proprietary according to local enterprise requirements with few, if any, shared standards, much less actual data. This is a source of many reconciliation efforts across the entire financial industry, and without irony, is also the source of many reconciliation efforts across internal corporate silos.

DTCC's viewpoint is that basic industry master data is an ideal candidate for improvement using decentralized consensus, rule standardization and auditable change history. This information is used by the entire industry by definition, and the lack of consistency and quality is a recurrent industry problem. Further, this could be constructed in such a manner that multiple firms can be authorized as data submitters, there can be many data validators and the majority of users will be data consumers. However, it should be pointed out that some master data information that is specific to local laws written in nonprogrammatic legalese will be challenging to standardize in support of rules automation in the near future.

An additional point concerning master data management includes the requirement for supporting the secure access method of distributed ledger infrastructure, which is known as public key infrastructure. A trusted and commonly used mechanism to associate public keys with entity identities could be an essential, enabling component of a distributed ledger infrastructure. The distribution of public keys seems well suited to distributed ledger technology and has already been the subject of other work[3].

## Asset/Securities Issuance and Servicing

There are obvious benefits to the issuers of assets, and to the owners of those assets, of a consistent and widely known source of truth concerning the full ownership provenance of an asset. Use of the distributed ledger to manage security issuance and track current ownership could greatly simplify asset servicing in a manner that would be very difficult to achieve with legacy, centralized technology. A significant challenge will

3 Certcoin – A decentralized public key infrastructure https://eprint.iacr.org/2014/803.pdf

be the integration point of assets inserted into a distributed ledger, with assets that exist in legacy form away from ledger, such as those at custodians or with repositories like DTCC. Addressing this challenge in a manner that aligns with regulatory requirements focused on investor protection is an example of the trust boundary condition defined earlier. In this case, the trusted asset custodian is part of the central industry role DTCC has provided for more than 40 years and a role DTCC can leverage to build a bridge between the repository and the distributed ledger to enable secure access from this new platform to trusted assets in the repository.

## Securities Transaction Processes and Smart Contracts:

The following discussion reviews the various transactional processes that are part of the lifecycle of a securities transaction and considers whether the attributes of the decentralized ledger approach could be leveraged.

### Trade/contract validation, recording and matching

Financial asset sales or trades are, by definition, rules-based agreements between multiple parties. Therefore, if the rules of a platform can be utilized to fully express an agreement, then it can be managed through a decentralized platform. A sufficiently rich language defining contract terms can cover virtually any asset exchange. The potential benefits of distributed ledgers should be considered based on the different aspects of processing by asset type.

The scope of this category includes, as example, the wide variety of contract-based asset trades, basic cash equities and fixed income, repurchase agreements, swap transactions across all asset classes, account transfers, syndicated loans and variable annuities.

Confirmed asset trades are candidates for recording on distributed ledger technologies, with the best opportunities focused on the more complex asset types involving multiple parties that do not have strong existent solutions. Those complex contracts typically have multiple manual processing steps and rules that would benefit from standards and formal encoding. Today's processing requires data to be converted and sent to another system before validation is performed, and the resultant exception processing is often more complex than that which exists for accurate trades that conform to the contractual rules. The introduction of smart contract technology that could provide every firm with the same validation rules "in advance" would result in only quality, validated data entering the distributed ledger, which should simplify processing and reduce exception correction timeliness. Certainly it will require significant, cooperative, industry-wide work to define the standards for content, validations and agreement rules.

There are significant obstacles to utilizing distributed ledger technology for trade validation, recording and matching. For example, it is important to re-emphasize that distributed ledgers are only composed of a ledger and validation that the final, approved/agreed transaction is being written to the ledger – once and only once. There is no master data, no means of reaching across data domains, no inherent workflow and contract negotiation and no "matching" functionality that addresses common, real world mismatches and exception processing. The existing reference example of moving a Bitcoin – a single value currency – from party A to party B does not provide useful guidance for a multiparty asset transfer that involves up to a thousand optional fields with complex rules and cross dependencies. The value of the distributed ledger technology is that contracts are consistently validated and subsequently written to the distributed ledger as "immutable," meaning unchangeable, forever recording as the final contract. Modifications, cancellations and corrections are potentially addressed by "reverse" transactions. The many complex aspects of matching and exception management that are typical in financial transactions are not inherently solved by distributed ledger technology. The reality is that either point-to-point solutions or central matching may continue to have a required place for preledger processing.

An additional challenge comes from regional regulations for securities transactions, which are not globally uniform. Current distributed ledger technology copies all data to all ledgers without distinguishing transactions based on regional rules. A partitioned scheme that keeps certain transactions within certain locations may be required to satisfy local jurisdictional requirements.

Finally, and practically, asset classes that are currently well automated and that have high volumes may have achieved efficiencies of scale and minimization of risk. As a result, they may not have cost-justified support for a reimplementation on a distributed ledger. The disruption and expense of a distributed ledger conversion project may not bring any substantial benefit and may in fact increase costs and risk.

# Transfer of Value:

## Netting, Clearing

Netting is defined as an optimized settlement requirement between all parties involved in trading an asset. Clearing is using a central counterparty for each trade to simplify multiparty netting and reduce risk of settlement failure. The central counterparty (CCP) steps into every trade as the client's counterparty – the CCP becomes the seller to every buyer and the buyer to every seller. The CCP nets all trades for a specific settlement date to a single quantity due to, or due from, the client and can determine risk requirements if that client cannot meet its settlement obligations.

Netting and clearing could be implemented on a distributed ledger through appropriate rules to determine an optimized settlement. Those rules could implement central counterparty clearing or alternative netting schemes. In other words, from a conceptual technology view, the function of netting and clearing could be implemented on the distributed ledger technology.

Use of the distributed ledger platform for the netting, clearing and settlement of a trade is discussed below and crosses the threshold from distributed validation and information sharing purposes to the area that many proponents argue is the real value of the distributed ledger – asset for value transfer, in near real time, independent of a trusted third party. Crossing that threshold warrants a further look at the benefits of today's central counterparty-based processes and how the distributed ledger can be used to improve upon those.

## Central Counterparties

CCPs have become a hallmark of risk management in modern financial markets. They eliminate the risk of a trade party failing to execute on a trade contract. They perform a multilateral net for settlement, which greatly decreases the number of settlements that are needed, which reduces the risk profile of an individual counterparty, and as a result, lowers the risk of a settlement failure. They also support brokers and other agents by connecting buyers and sellers that do not have liquidity to settle trades themselves. Thus, CCPs play a critical role in creating stable, resilient and efficient markets and in reducing overall risk. Additional benefits of CCPs, including balance sheet netting and guaranteeing completion of trades that are future settling, such as Repo, all contribute to the smooth functioning of today's markets and help protect them during bankruptcies and credit crises, such as the financial crisis of 2008.

There are numerous examples of CCPs globally, but for the purposes of this paper, we use DTCC's U.S.-based equity and fixed income central counterparties as a standard for today's financial infrastructure.

Key features of DTCC's systems include:

- **Real-time processing of transactions**. DTCC receives virtually every trade from every market within seconds of trade execution. This includes connections to over 50 different exchanges and marketplaces. Trades are validated, matched, and confirms are returned to clients within seconds of submission. Same-day settling trade submissions ("as-of" trades in today's T+3 environment) move directly to the real-time settlement system.
- **Scale of processing.** DTCC's daily volume averages over 100 million individual trades. DTCC has tested its system performance to handle well over 800 million trades, which is just over twice its historical peak volume.

- **Cost efficiency of processing**. DTCC's equity clearance costs in the U.S. are just fractions of a penny per average trade, and regular improvements in technology have helped further lower that cost.
- **Interconnectedness.** The U.S. capital markets, consisting of 50+ exchanges and thousands of financial firms, have well-established interconnected systems that perform seamlessly every day.
- **Netting efficiencies:** Over 97% of daily equity trades are settled through netting, and the remaining 3% go through the full settlement mechanism. The cost and risk considerations of the ledger model of individual settlement of every submitted trade would need to be balanced against the existing efficiencies of the central netting model as well as the fact that not every trade party can settle.
- **Novation:** As a central counterparty, DTCC mitigates risk for the buyer and seller, guaranteeing trade completion even if one side defaults. Also, DTCC ensures soundness and solvency of trade partners by, among other things, maintaining rigorous standards for membership, requiring financial disclosure and conducting financial surveillance of its clients.
- **Balance sheet offset:** Central counterparty clearance provides risk mitigation benefits for any forward-settling exchange (e.g., loans) as well as financial accounting benefits, such as balance sheet offset for repurchase transactions, which can only exist with a trade central counterparty.

For most modern financial markets, these points present a high bar that distributed ledger technology must improve upon. Financial markets in developing regions may have a more greenfield opportunity, with lower volume requirements and a variety of risk tolerances, to use a different model for clearing that could involve a distributed ledger. But it is difficult to see the short-term opportunity to use this technology in modern markets. It is even more difficult to begin a long, expensive replacement process without a clear risk and cost reduction benefit.

DTCC is aware of and has been approached by a number of startups that are building issuance/trading/settlement/asset-servicing distributed ledgers. DTCC's position as an industry-owned market infrastructure is to provide fair and open access to all eligible clients and to enable connections to any client that brings capabilities that meet DTCC's financial, risk and regulatory requirements. But as noted above, DTCC is skeptical that moving assets from a centrally, risk-managed, regulated, governed repository to multiple vendors creating bifurcated markets with proprietary settlement and asset management mechanisms is a good thing.

## Settlement

There are a broad variety of settlement mechanisms for different financial transactions, ranging from the immediate real-time delivery versus payment settlement of Fedwire for money transfer and U.S. government securities transactions to weeks or even months for complex swaps and loans transactions. There are also many transactions that have multiple "lifecycle" events that require settlement, such as loans, which have a start settlement and an end settlement.

The success of the Bitcoin crypto-currency as a mechanism for transferring value with finality of execution on an immutable ledger demonstrates that for a simple case, the delivery vs. payment settlement can be programmable and managed in near real time by a decentralized, consensus network.

DTCC's equity and fixed income settlement process also occurs in real time throughout the day, so the distributed ledger by itself does not improve on that capability. Importantly, although DTCC's systems operate in real time, the markets themselves are currently structured to operate on a T+3 cycle (that is, settlement occurs three business days after the trade is executed) primarily to accommodate the needs of retail investors. So while DTCC receives new trades in real time and processes settlement of those trades three days later, the delay is entirely imposed by market practices, financial industry laws and regulatory requirements. As noted above, trades submitted on settlement date, marked "as of" three days prior, will go immediately from submission into the real-time settlement process for same day settlement.

Some of these issues were already a focus of improvement as noted in the industry's white paper on T+2 issued in 2015. The white paper also highlighted the cost, complexity and time needed to migrate to T-2. Distributed ledgers may be the catalyst to further shorten the settlement cycle to T-0 and create mechanisms and pricing to meet the needs of different players in the financial markets. As an example, a peer-to-peer trade that can settle immediately vs. payment could be priced differently than a brokered trade that requires central counterparty netting to net out the broker position and take on counterparty settlement risk. Achieving such will require significant changes to existing trading processes (e.g., block trade allocation), trade financing and a variety of other embedded market practices. At the same time, issues such as processing capacity, the adherence to the body of financial industry laws and regulations, and the complexity and cost transitioning from the current state to the future state must also be addressed.

A standard model of distributed ledger technologies for settlement can provide a secure, consistent source of truth of the current ownership and provenance of an asset to custodians, agents and the beneficial owners. That singular source of truth of ownership can simplify asset servicing, such as corporate action processing, dividend distribution and management of shareholder voting. While existing technology could incorporate all of this functionality, it would still require complex interactions and reconciliations that could potentially be simplified by the single but distributed version of truth in a distributed ledger. But the success of such a distributed ledger implementation would require that either all of that asset is on that specific ledger or a full integration with all of the off-chain assets, including all legacy custodians of those assets, as well as those assets that have been implemented on other chains/ledgers.

Asset types that do not currently have widely established and automated workflows for settlement, such as syndicated loans and other complex transactions that currently can take weeks to settle, could be solved with distributed ledger technology. Those trade contracts and settlements often involve multiple parties that all want to have a single consistent view of the transaction and its settlement, which is well matched by the inherent capabilities of ledger technology.

Settlement may be an ideal long-term target of opportunity for distributed ledger as the technology matures and scales. The issues that need consideration include revising laws, changing market practices and structures, incorporating the complex realities of asset servicing and working with regulators on issues such as investor protection. DTCC believes that this is an area of viable opportunity to leverage blockchain technology and also believes that as the custodian for the central securities repository for the U.S., it is uniquely positioned to help implement this technology and increase its adoption. DTCC expects to proceed by working with the industry and regulators to identify the strategic roadmap, governance processes and steps to proceed, with full requirements to exceed all of the safety and soundness that currently exists.

Moving settlement to a distributed ledger will require significant industry investment to modernize legacy systems and resources to maintain both environments for a period of time. But the benefits to the overall industry from reconciliation and simplification, as well as taking a fresh view of the T+2 initiative and common post-trade processing, should be evaluated holistically from the perspective of industry-wide efficiencies and risk mitigation.

## Collateral Management

DTCC support for settlement and asset servicing processing via distributed ledger extends to collateral management processing on the platform. The provenance of assets, the ability to track transaction movements and, with proper design, true ownership vs. temporary/borrowing is fundamental to the promise of distributed ledger technology. DTCC sees this functionality of blockchain technology as well suited to collateral management processing.

# CONCLUSION

The current financial industry infrastructure has proven highly resilient through many challenges across multiple decades. It is secure, stable, scalable, cost efficient and tightly connects the entire industry. It has continually innovated to adapt to new challenges, whether they come in the form of rising volumes, increased automation, globalization or regulatory mandate. It has been built on a foundation of financial market infrastructures, particularly those designated Systemically Important Financial Market Utilities (SIFMU) by the U.S. Financial Stability Oversight Council (FSOC), which must meet the highest standards of integrity, security, performance, scalability and resilience. They have endured for decades and operate seamlessly and efficiently to ensure the smooth operation of the world's financial markets. Any failure in the highly orchestrated processing of transactions that occurs seamlessly every day could literally grind the world's financial markets to a halt and disrupt economies globally. Significant change to this infrastructure must be carefully considered.

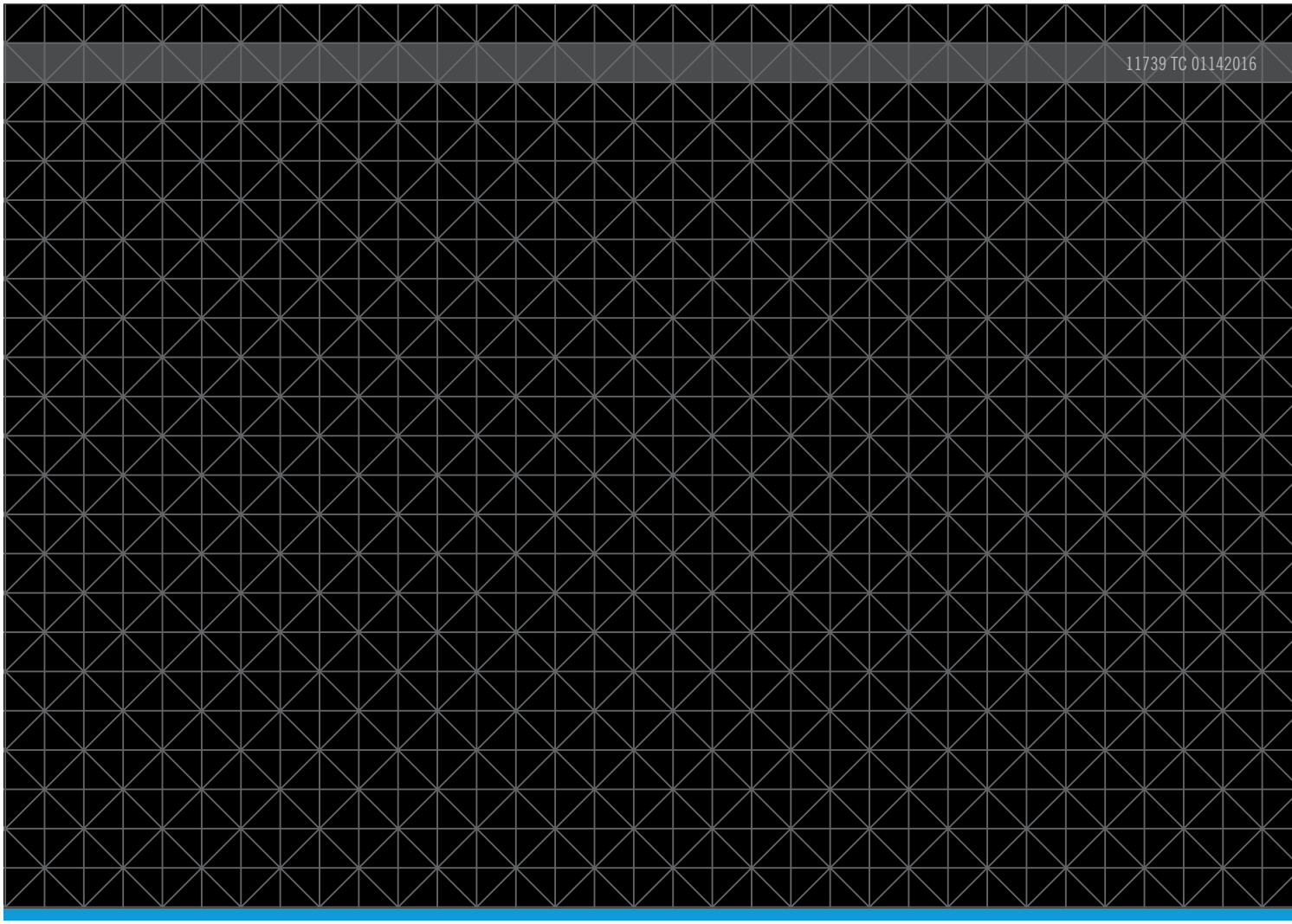
DTCC's conclusion is that a mature, supported, integrated distributed ledger technology has the potential to help improve a number of existing financial market infrastructure limitations. However, it may not be the solution to every problem because there may be alternative opportunities to lower the costs and risks of current infrastructure by standardizing industry workflows and expanding the use of cloud technologies.

The current state of distributed ledger technology today has its own challenges: it is immature, unproven, has inherent scale limitations in its current form and lacks underlying infrastructure to cleanly integrate it into the existing financial market environment. Improvements will come with time as they have with every new technology and as the industry learns from successes and failures of marketplace experiments.

DTCC's unique ownership and governance can enable industry use of this technology by providing focus on the best foundational building blocks and business use cases. Proofs of technology and small pilots targeting asset classes that are not fully automated provide a way to validate the viability of the technology to solve industry-wide challenges. These "white space" opportunities should be prioritized because they will provide the best conditions to learn the advantages and lessons of this alternative model without adding redundant costs to existing infrastructure. They will also minimize integration and co-existence challenges without trying to address problems that are already efficiently solved. This path will help establish the standards, the infrastructure and ecosystems needed to support an industry standard distributed ledger.

The current financial technology venture funding environment, along with the media frenzy over the next industry to be disrupted, has created a chaotic gold rush of new vendors, partnerships and existing firms all looking to leverage this technology. Many financial institutions are experimenting in private with a technology that uses consensus protocols to provide transparency. This mirrors the history of financial innovation beyond the few points in time where an industry mandate or regulation forced the industry to cooperate. The current path will result in a new jumbled, disconnected maze of distributed ledger silos.

The industry should seize the emergence of this technology as an opportunity to assess how to modernize and significantly lower risk and cost. DTCC understands this process because DTCC itself was the result of an industry-wide effort to modernize in the face of the technology conversion from paper to computer more than 40 years ago. DTCC is the result of that collaboration and uniquely provides an unbiased focus on risk reduction for the entire financial community. This is the opportunity to create an industry-wide initiative to develop the right architecture, prioritize the infrastructure building blocks and support focused and collaborative experiments to help the technology mature.


11739 TC 01142016